VOL - 10 ISSUE - 2 I J C R T July-December, 2025

ISSN NO
2454-7719

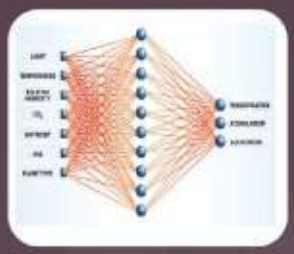
International Journal of Computer Research & Technology (IJCRT)

A Blind Peer Reviewed Half Yearly Research Journal



Vol-10 Issue -2
July-Dec, 2025











Editor in Chief
Prof. Dr. B.H. Barhate

॥ विद्या दानम् महत् पुण्यम् ॥
Tapti Education Society's
Dept. of Computer Science and Information Technology
Bhusawal Arts Science & P.O.Nahata Commerce College,
Bhusawal - 425 201 Maharashtra
NAAC Reaccredited (*Fourth Cycle*) "A" Grade with CGPA 3.17
UGC recognised ' College with Potential for Excellence for II nd Phase Effective from 2014 to 2019
Affiliated to Kavayitri Bahinabai Chaudhari North Maharashtra University, Jalgaon

IJCRT
ISSN 2454-7719
International Journal of Computer Research & Technology
** A Blind Peer Reviewed Journal **
Volume-10, Issue-2, July-Dec 2025

International Journal of Computer Research & Technology

** A Blind Peer Reviewed Journal **

Volume-10, Issue-2, July-Dec 2025

About IJCRT

The International Journal of Computer Research and Technology (IJCRT) is a blind peer reviewed journal with ISSN 2454-7719 (print). The journal provides an advanced forum for computer research and the advanced technology. The aim is to encourage scientists, academicians, industry professionals, scholars and students to publish their theoretical and experimental results in as much detail as possible in the field of emerging trends in computer and information technology, Computer Management, digital library and many more. Published on half yearly basis, it provides up-to-date insights into this ever-evolving discipline. The language of manuscripts is English only to communicating the high-quality research in Computer and technology to the broader audience.

The Journal was initiated in 2015 by the department of Computer Science and Information Technology of Bhusawal Art's, Science and P. O. Nahata Commerce College, Bhusawal, Dist. Jalgaon, Maharashtra state, India.

Submissions are accepted for review with the understanding that the same work has been neither submitted to, nor published in, another publication. All manuscripts are peer-reviewed with the support of appropriate reviewers subject to a well-established, fair, unbiased blind peer review and refereeing procedure. Each published article is reviewed by an independent reviewer using a blind peer review process, where identities of the reviewers are not known to the authors and only the managing editor knows the identity of the authors and reviewers.

About Publisher of IJCRT

Bhusawal, as recalled and noted down in records has a prominent place on the map of the nation; proudly housing two ordnance factories, a thermal power station in the region, and itself being one of the major railway junctions of Central Railway from where, residents proudly say, you may visit any corner of India. A mixture of farmers, tribal people from adjoining are as with the servants from all over India, Bhusawal serves as a slice of the nation; and honorably has unity in diversity. It is 25kms away from the district, Jalgaon, famous as a city of gold; and few Kms away from Yawal and Raver tehsils, famous all over nation for bananas. It is the only "A" graded Municipal Corporation in the district. Another identification as well as benefit of thecity is that it is situated at the bank of the Tapi river, the only river that flows from east to west. The city of Bhusawal has been ahome place for the British authorities, and it is famous for railways since British rule. It is historically remarkable for the grave of Major Robert Gill, who invented world famous Ajanta caves; and for the tomb of Sant Gadgebaba, a famous and truly a leading social reformer in Maharashtra. The world famous Ajanta caves are just 60kms away from the city. It is believed that the parental home of Rani Laxmibai (famous as Queen of Jhansi) is situated at Parola, 50kms away from the city. Bhusawal is also famous for many mythological stories like that of Shravana, coming from Ramayana who is said to be killed at Hartala, which is near to the city. Besides, the city was once famous in Bollywood for film distribution companies as well known "Rajashri" pictures.

Summing up the physiognomies of the city, Bhusawal stands as a glorious city in the eyes of everyone. However, it was the time-besides all assets of the city-when Bhusawal was a degenerated city in terms of higher education even after a long time from independence. There were few schools imparting high school level education but none of the colleges. It was only in1958, under the motivation of Late Honorable Madhukar rao Chaudhari, ex-speaker of Maharashtra Legislative Assembly, a groupof social well-wishers came together and established the Tapti Education Society in 1958. Simply having the wish in mind to provide potential students higher education facilities near their home, they started the Bhusawal College of Arts and Commerce in 1963. Their philanthropic view may be seen in the motto: *Vidya danam mahat punyam.* Yet difficulties were innumerable. The college with two faculties was started in the place of rent of a high school in the city.

It is wisely said that *vidya danam* is *mahat punyam*. The dedicated faculty, the sublime view of the management soon started to produce good academicians. Inspired by the results the trust purchased a barren land of 7 acres out of the city which is soon to be developed as a centre of imparting quality higher education in the area. The barren land with sustaining hard work, and devotion was then transferred into a naturally beautiful campus. The college is then shifted to a new place in 1972 with the introduction of Science stream. The philanthropist Late Mr. Poonamchand Nahata donated to the college, hence the college is renamed and which today itself is a brand as **Bhusawal Arts, Science and Poonamchand Omkardas Nahata Commerce College, Bhusawal.**

The college is then marching forward with a goal to **creatively contribute the society through the pursuit of learning at higher level of excellence**. The institute has contributed in many ways for economic, social and cultural uplift of the society by offering quality education. Since the inception it has been known for academic excellence, inventive pursuits and athletic dynamism. The college is a multi-stream institute catering to the needs of the young minds primarily from the rural areas.Our society runs not only the college but also the Institute of Management and Career Development and much sought Tapti Public School (affiliated to CBSE Board, New Delhi) within a minimum space of 7.3 acres. The institute is developing vertically in all of the fields.

The Tapti Education Society's, Bhusawal Arts, Science and P. O. Nahata Commerce College was accredited as **four stars (****) in 2001**, reaccredited as **"A" Grade** with CGPA **3.28 in 2008 and reaccredited 3rd cycle as "A" Grade with CGPA 3.30 in 2015,** as the **first College** in Kavayitri Bahinabai Chaudhari North Maharashtra University jurisdiction. It is also the first college to get registers for the fourth cycle of accreditation in the jurisdiction of the university and reaccredited as **"A" Grade** with CGPA **3.17 in 2023 with new framework**. It is also recognized by UGC as **College with Potential for Excellence**. Recently, the society is certified as ISO 9001:2008 institute. Our institute is one of the renowned institutes in the adjoining area. We welcomed the upcoming students from rural areas who made remarkable progress and set theirs and college's image in society. Many of the students of this institute secure top position in various fields. This make us feel great. The college achieves 'A'grade in three subsequent cycles of Re-accreditations and it brings the college towards autonomous status.

Initially the college was affiliated to the Pune University, and got permanent affiliation in 1990. Since the inception of Kavayitri Bahinabai Chaudhari North Maharashtra University in 1991, the college is permanently affiliated to the same. The university spreads all over three districts: Jalgaon; Dhule; and Nandurbar, being on the boundaries of Gujrat and Maharashtra and one being the district of tribal people. The university is trying hard to uplift the downtrodden, while keeping in touch with the rapidly changing world.

Last but not least, the college has the advantages of developing youth coming from rural area, and forming them into sensible youth as they are mixed in the cosmopolitan society. The college is aware that every coin has two sides: hence students coming from rural areas have inferiority complex, their vernacular background being most disadvantage for them. The college has faced challenges to improve their communication skills, to boost their confidence to bring them into modern current while making them aware of great Indian culture. As the college has celebrated its golden jubilee, it will be a golden, in fact a platinum moment for us when the students coming from different backgrounds will be essentially Indian serving for the welfare of humanity. With this view the college is making progress towards quality excellence so that it will be a lead college that will stand as a light house for the bewildered.

IJCRT
ISSN 2454-7719
International Journal of Computer Research & Technology
** A Blind Peer Reviewed Journal **
Volume-10, Issue-2, July-Dec 2025

Editor in Chief
Professor B. H. Barhate
Principal
***And H.O.D. of Information* Technology**
TES'S, Bhusawal Arts, Science and P. O. Nahata Commerce College, Bhusawal (M.S.)

Managing Editors

Prof. Harshal V. Patil *Asst. Professor,* TES's Bhusawal Arts Science & P. O. Nahata Commerce College, Bhusawal (M.S.)	**Ms. Poonam M. Mahajan** *Asst. Professor,* TES's Bhusawal Arts Science & P. O. Nahata Commerce College, Bhusawal (M.S.)

Editorial Board

Dr. Parag U. Bhalchandra *Professor,* School of Computational Sciences, SRTM University, Nanded (M.S)	**Dr. Rakesh Deore** *Professor,* SSVPS's Science College, Dhule (M.S)
Dr. Varsha Pathak Research Center(Computer Application), KCE IMR, Jalgaon (M.S.)	**Dr. Swati K. Borse** *Professor,* SSVPS's Science College, Dhule (M.S)
Mrs. Hemalata P. Patil Director, School of Computer Science, M. J. College, Jalgaon (M.S)	**Dr. Atul S. Patil** *Associate Professor,* Z. B. Patil College, Dhule
Dr. G. R. Wani *Professor,* Department Of Computer Science and I.T, TES's, Bhusawal Arts, Science and P. O. Nahata Commerce College, Bhusawal (M.S)	**Dr. Gouri M. Patil** *Associate Professor,* Department Of Computer Science and I.T, TES's, Bhusawal Arts, Science and P. O. Nahata Commerce College, Bhusawal (M.S)
Dr. Swati P. Phalak. *Assistant Professor,* Department Of Computer Science and I.T, TES's, Bhusawal Arts, Science and P. O. Nahata Commerce College, Bhusawal (M.S)	**Mr. Tushar M. Patil** *Assistant Professor,* Department Of Computer Science and I.T, TES's, Bhusawal Arts, Science and P. O. Nahata Commerce College, Bhusawal (M.S)

Published By
Department Of Computer Science and I.T,
TES's Bhusawal Arts,
Science and P. O. Nahata
Commerce College,
Bhusawal (M.S)
Contact: 9890966830
Email:
ijcrt.basponc@gmail.com
Website: **basponccollege.org**

The International Journal of Computer Research and Technology "IJCRT" is issued half yearly.
The College assumes no responsibility for the statements and opinions advanced by contributors.
©2025, Bhusawal Arts, Science and P. O. Nahata Commerce College, Bhusawal, Dist-Jalgaon (MS) India.

I N D E X

Sr. No.	Paper ID	Paper Title and Authors	Pages No.
1	**CS-01**	AI in HealthCare: Opportunities and Challenges - *Dr. Sadhana Ojha, Abhijit Yashwant Narkar, Abhishek Prakash More*	**1-5**
2	**CS-02**	Comparison of Pre-processing techniques on Indian sign language datasets - *Abhishek S. Patil, Ranjana S. Zinjore*	**6-11**
3	**CS-03**	A Multilingual NLP Approach to Identifying Code Mixed Cybersecurity Threats in Social Platforms - *Amna Shipra*	**12-19**
4	**CS-04**	Analysis of GDDP Impact on Financial sector using Regression - *Prof. Tejas Sonawane, Ms. Mruga Patel*	**20-22**
5	**CS-05**	Quantum Computing and Its Impact on Cryptography - *Aquila Shaikh, Aakanksha Bhosle*	**23-28**
6	**CS-06**	AI in Education: Personalized Learning and Beyond - *Prof. Ashwini Hemant Patil*	**29-34**
7	**CS-07**	The Influence of IOT for Smart Homes In Nagercoil - *Dr. C. S. Goldie Sheila Jesolit, Dr. Chithra James*	**35-40**
8	**CS-08**	The Role of Artificial Intelligence in Preventing Cyber Attacks - *Sheetal Waghmare, Rutuja Chavan, Jeet karani*	**41-45**
9	**CS-09**	Optimizing Query Performance in Distributed Databases Using Adaptive Indexing Techniques - *Sunny Nahar, Kunal Jantre, Rohit Kurmi*	**46-51**
10	**CS-10**	Deepfake Detection using Generative Adversarial Networks - *Prakash Sakharkar, Divakar Jha, Pranay Naik, Pratik Nair*	**52-57**
11	**CS-11**	Multi-Agent Cooperative and Competitive Dynamics in Grid Environments - *Dr. Rashmita Pradhan, Saburi Rane, Tejaswi Gawai*	**58-62**
12	**CS-12**	Designing a Predictive Dashboard to Analyze Dropout Ratio across Karnataka - *Prof. Tejas Sonawane, Ms. Rutvi Chavda*	**63-66**
13	**CS-13**	Meaningful work in Higher Education: The Role of Job Characteristics. - *Swapna Karkhanis*	**67-72**
14	**CS-14**	Cyber security In HealthCare - *Dr. Tanuja Mahajan, Suraj Karnati*	**73-78**
15	**CS-15**	Blockchain Technology in Healthcare – Ensuring Data Security & Privacy - *Dr. Vikram Patalbansi, Shubham Kanojia*	**79-83**
16	**CS-16**	Review Paper on Investigation on Performance of Machine Learning Algorithms for Prediction of Human Age - *Swati Laxman Nimgale, Prof. Prashant Nitnaware*	**84-91**
17	**CS -17**	Investigating the Performance of Machine Learning Algorithms over Human Age Prediction by using Image Dataset - *Swati Laxman Nimgale, Prof. Prashant Nitnaware*	**92-98**
18	**CS-18**	IoT for Real-Time Product Tracking and Transparency in E-Commerce - *Mr. Prakash Y. Bari, Mr. S. N. Khan*	**99-102**
19	**CS-19**	Emotional Intelligence and Artificial Intelligence: Ethical, Technical, and Cross-Cultural Perspectives with Healthcare Applications - *Dr. Dipak N. Patil*	**103-107**
20	**CS-20**	Review of Web Scraping Tools and Techniques for Data Collection from Social Media Platforms - *Mr. Rahul Dinkar Narkhede, Prof. Dr. B. H. Barhate*	**108-111**
21	**CS-21**	The Evolution of VPNs: From Enterprise Connectivity to Next-Generation Secure Access - *Dr. Seema Vijay Rane, Mrs. Punam Mahesh Ingale*	**112-118**
22	**CS-22**	Comparative Review of Machine Learning Techniques for Banana Crop Disease Detection - *Monali Patil, Professor Gajendra Wani*	**119-122**
23	**CS-23**	The Information Hiding Techniques. - *Nikita Samadhan Chaudhari*	**123-127**
24	**CS-24**	Recent Advances of Artificial Intelligence in healthcare - *Nikita Rajendra Patil*	**128-134**

25	**CS-25**	Android Malware Detection Approaches Based on Machine Learning - *Kamini Devanand Shinde*	**135-142**
26	**CS-26**	The Role of Data Analytics in the Era of Artificial Intelligence and Machine Learning: Applications, Challenges, and Opportunities - *Dr. Atul Suresh Patil, Professor Dr. Bhojraj Hanumant Barhate*	**143-145**
27	**CS-27**	Mobile Computing: Concepts, Architecture, Challenges and Future Scopes. - *Mrs. Shailaja P.Ingale*	**146-150**
28	**CS-28**	Native Language Identification: A Computational Approach across Foreign Languages - *Dr. Prasad A. Joshi*	**151-153**
29	**CS-29**	3D Medical Imaging for Early Diagnosis Using Artificial Intelligence: A review - *Mrs. Dipita Shailesh Dhande, Miss. Aditi Amol Kulkarni*	**154-159**
30	**CS-30**	Facial Emotion Recognition Using Deep Learning - *Mrs. Priyanka A. Khadase*	**160-165**
31	**CS-31**	Scalable Unstructured Big Data Processing with Mahout: A Distributed Machine Learning Framework - *V. P. Mahajan, Professor. B. H. Barhate*	**166-170**
32	**CS-32**	Extraction of features from DhammaLipi Character for Classification - *Vasundhara R. Fegade, Dr. G.R.Wani*	**171-173**
33	**CS-33**	Design of a Marathi Speech-Driven System for Automated Assessment of Adolescent Depression - *Vrunda M. Chaudhari, Professor Gajendra. R. Wani*	**174-177**
34	**CS-34**	AI for Zero-Day Attack Prediction: A Comprehensive Review - *Prof. Sayali Satish Patil, Prof. Arati Santosh Bari*	**178-186**
35	**CS-35**	The Rise of No-Code and Low-Code Platforms: Threat or Opportunity for Frontend Developers? - *Prof. Arati Santosh Bari, Prof. Sayali Satish Patil*	**187-191**
36	**CS-36**	Artificial Intelligence in Creative Industries: Transforming Artistic Expression and Creative Production - *Miss. Unnati Raju Kotwal, Prof. Poonam M. Mahajan*	**192-197**
37	**CS-37**	AI-Driven Papaya Fruit Disease Detection: A Python-Based Approach - *Prof.Archana Prakash Bhalerao*	**198-199**
38	**CS-38**	Comparative Study of feature extraction techniques for melanoma skin cancer detection. - *Mr. Sunil D. Mone, Professor B. H. Barhate*	**200-207**
39	**CS-39**	IoT Based Traffic Management System Using Real Time - *Prof. Megha R.Chaudhari, Prof. Lokesh R.Chaudhari, Dr. Gouri M. Patil*	**208-212**
40	**CS-40**	M-Banking: A Pillar of Digital Acceleration in Indian Society - *Prof. Lokesh R. Chaudhari, Prof. Megha R. Chaudhari, Dr. Swati P. Phalak*	**213-217**
41	**CS-41**	Intelligent Document Digitization and Fraud Prevention Using Artificial Intelligence - *Mr. Digambar Padmakar Mahajan, Prof. Dr. Mohammad Muqeem*	**218-223**
42	**CS-42**	Artificial Intelligence in Early Cancer Detection - *Assistant Prof. Nayana A.Chaudhari*	**224-226**
43	**CS-43**	Analysing CVD data based on various attributes - *Mr. Anand J. Maheshwari, Dr. G.R.Wani*	**227-231**
44	**CS-44**	Comparative Study of Simulation Tools for Network and System Modeling - *Mr. Dipak E. Chavan, Dr. Gouri M. Patil*	**232-234**
45	**LIB-01**	Optimizing Space Utilization in Academic Libraries - *Mr.Vinit S. Patil, Dr. Sandip S. Salunke*	**235-239**
46	**COM-01**	Shifting of Loyalties: Perception of Retailers after launching of UPI Payments - *Mr. Shravan Baburao Nhavkar, Dr. Rashmi Sharma*	**240-242**
47	**CS-45**	Smarter Strategies: Leveraging Machine Intelligence in Digital Marketing - *Poonam S. Patil*	**243-250**

International Journal of Computer Research & Technology
ISSN 2454-7719
** A Blind Peer Reviewed Journal **
Volume-10, Issue-2, July-Dec 2025

Paper ID: CS-01

AI in HealthCare: Opportunities and Challenges

Dr. Sadhana Ojha
General Manager
IT and Business Operations
BSN Infotech Pvt. Ltd
sadhanapandey459@gmail.com

Abhijit Yashwant Narkar
Research Scholar MCA, Late Bhausaheb Hiray S.S Trust of Computer Application, Bandra East, Mumbai India.
abhijeetnarkar57@gmail.com

Abhishek Prakash More
Research Scholar
MCA, Late Bhausaheb Hiray S.S Trust of Computer Application, Bandra east, Mumbai India.
abhishekmore144@gmail.com

Abstract *- Artificial Intelligence (AI) is revolutionizing the face of healthcare, offering never-before- seen potential to enhance patient treatment, streamline operations, and enhance medical research. AI-driven solutions excel at diagnostics accuracy, predictive analytics, personalized treatment planning, and drug discovery. For instance, AI algorithms can analyze medical images precisely, assisting in detecting disease earlier, along with optimizing the result of treatments. Predictive models apply patient data to identify at-risk patients and enable early intervention and resource optimization. AI- based virtual assistants and chatbots also empower patients by providing easily accessible healthcare information and support.*

Artificial Intelligence (AI) has been a force driving change to transform healthcare, its unseen potential for improved patient outcomes, improved efficiency, and cost reductions. However, its integration into healthcare systems also brings with it significant challenges. This paper reviews the diverse applications of AI in healthcare, its benefits, and the impediments to its uptake. The discourse involves ethical concerns, privacy issues with data, and demands for regulatory interventions to ensure safe and equitable AI adoption.

Keywords — *AI, HealthCare, NLP, .*

I. INTRODUCTION

It is a technology that allows computers to replicate human intelligence. It makes computers to learn, recognize patterns, and make decisions sometimes even learn by experience.

The arrival of AI has transformed many industries, and healthcare is one of the most potential sectors wherein it can be utilized. Machine learning, natural language processing, and robotics are some AI technologies that can transform patient care, diagnosis, treatment planning, and administrative work. It is a complex operation to integrate AI into healthcare, and an equilibrium assessment of opportunities along with Challenges must be drawn.

II. LITERATURE REVIEW

Advanced Diagnostics and Personalized Medicine

There have been many studies that highlighted the potential of AI to bring about a change in healthcare diagnostics.

Obermeyer and Emanuel (2016) wrote about the predictive power of AI in clinical medicine, and its capability to foresee disease progression and outcomes. For example, AI systems have demonstrated high accuracy in detecting early-stage cancers and diabetic retinopathy using high-level image analysis. These systems use deep learning methods to identify anomalies that may not be detected by human vision.

PREDICTIVE ANALYTICS

The ability of AI to use predictive analytics in healthcare is widely reported. Davenport and Kalakota (2019) pointed out the operational effectiveness and enhanced patient care due to AI integration. AI models can anticipate patient decline in intensive care units, and timely interventions could save lives. AI can also predict disease 2 outbreaks and patient admissions, facilitating healthcare providers to better allocate resources.

OPERATIONAL EFFICIENCY

The role of AI in automating administrative work is another critical research area. Natural language processing (NLP) codes can be used to extract important information from patient histories to streamline documentation, making it faster and more accurate. Research has demonstrated that AI can alleviate administrative work from healthcare providers so they can concentrate more on patient care.

DRUG DISCOVERY AND DEVELOPMENT

AI speeds up the process of drug discovery because it examines biological data and makes predictions about the effectiveness of potential drugs. This saves time and money in getting new drugs to the market. AI is also able to find existing drugs that can be repurposed for the treatment of other diseases, which presents new therapeutic alternatives.

PROBLEM DEFINITION

Though there lies potential for large-scale implementation of AI in the healthcare sector, there are certain problems that hold it back from being applied at a large scale. Some of them are data protection and privacy issues, ethical issues in AI decision-making, weaknesses in regulatory mechanisms, and non-integration of AI systems with other healthcare systems in place. Their resolution will be crucial to the achievement of the full potential of AI in the healthcare sector.

DATA SECURITY AND PRIVACY

Use of AI in medicine is to handle patient information, which is a security and privacy issue. Medical data has to be kept honest and private, and any breach of the same can turn out to be critical. Data protection in a HIPAA-compliant system has to be strong, and laws like HIPAA have to be adhered to.

ETHICAL ISSUES

AI decisions are often opaque and it is hard to know how conclusions are reached—a shortcoming referred to as the "black box" problem. This lack of transparency poses ethical concerns, especially when AI recommendations contradict human point of view or produce unintended outcomes. AI systems must be fair, unbiased, and transparent.

ANSWER AND LEGAL CHALLENGES

The speed of AI technology evolution is far quicker than defining the regulatory guidelines. Guidelines that can provide safety assurances, efficacy, and responsibility for the AI system need to be established. It is equally difficult to hold an individual responsible if there are mistakes or harmful incidents induced by AI.

INTEGRATION AND INTEROPERABILITY

Healthcare facilities are decentralized, and many EHR systems and formats are being used. AI solutions are very resource- intensive to implement into existing infrastructures in a way that will be made compatible with existing systems and allow for seamless data transmission. Standardization of data formats and protocol standardization must be enabled for integration.

HIGH IMPLEMENTATION COST

Developing and deploying AI in healthcare environments involves massive investments, Maintenance & updation expenses will demand additional financial outlays.

RELIABILITY AND ACCURACY

AI will have to be tested properly so as not to result in misdiagnosis or mismanagement. Risk of AI failure can cause severe damage to patients

III. OBJECTIVE/SCOPE

The main emphasis of the paper is to depict the challenges and opportunities in applying AI in the healthcare industry. The scope includes looking into current applications of AI, determining main challenges, and proposing solutions to resolve the challenges. The research tries to provide a complete overview of applying AI in the healthcare industry and what is required to make its implementation a success.

IV. RESEARCH METHODOLOGY

This research is qualitative and collects data from peer-reviewed journals, industry reports, and case studies. The research includes:

1. Systematic literature review to determine pertinent themes and trends.
2. Case study of effective AI implementations in health care.
3. Examination of regulation and ethical guidelines for AI in health care.

Systematic Literature Review

The literature review was systematic in nature because searches were conducted on academic databases like PubMed, IEEE Xplore, and Google Scholar for articles within the past decade and were related to the topic. The keywords used were "AI in healthcare," "machine learning diagnosis," "predictive medicine analytics," "AI ethical issues," and "healthcare AI regulation." The literature review

was done to determine emergent themes, trends, and research gaps.

V. Case Study Analysis

Various case studies were examined for compliance with the real implementation and implications of AI in the medical sector. They included the application of AI in radiology, pathology, and patient management systems. Case studies provided an overview of the advantages obtained and the challenges experienced while applying AI technologies.

Analysis of Regulatory and Ethical Frameworks

The research covered existing regulations and ethical standards of AI in the healthcare industry. They included the Food and Drug Administration (FDA) guidelines, European Medicines Agency (EMA), and others' guideline for regulation. Comparison was to inform regulation gaps and how the gaps should be addressed.

VI. Analysis & Findings

Opportunities Enhanced Diagnostics and Personalized Treatment

Artificial intelligence tools, including imaging test systems, have been more precise in diagnosing diabetic retinopathy and cancer. AI tools utilize deep learning to identify anomalies that would go unseen by the naked eye. Personalized medicine is provided as AI scans genetic and patient history information and prescribes medication based on individual requirements.

For example, IBM Watson for Oncology uses AI to deliver evidence-based oncologist advice. The system processes the patient's information and compares it against clinical guidelines, studies, and patient outcomes to offer personalized treatment suggestions. In most cases, research has indicated that Watson's recommendations agree with those made by veteran oncologists, enhancing the quality of care.

Predictive Analytics

AI's proficiency in carrying out predictive analytics in healthcare is well entrenched. AI models can identify patients' decline in intensive care units and save lives through quick intervention. AI can also forecast disease outbreaks and patient admissions and aid healthcare practitioners in optimizing their use of resources.

For example, Duke University's Sepsis Watch program uses AI to monitor for sepsis, a potentially fatal condition, in patients. The program goes over real-time information from electronic health records and notifies clinicians when a patient is at risk, enabling early intervention and improved patient outcomes.

Operational Efficiency

Another significant area of study is the application of AI to ease administrative work. Natural language processing systems can be utilized to automate beneficial data extraction from patient charts such that quicker and more precise documentation can be done. Research has proved that AI can lower the administrative work of healthcare professionals, and they can attend to their patients longer.

For example, patient scheduling and triaging with the use of AI chatbots has been shown to enhance efficiency and patient satisfaction. Chatbots can be used to respond to routine questions, manage appointment schedules, and render medical advice based on symptom diagnosis, leaving medical professionals to focus on more demanding work.

Drug Discovery and Development

AI quickens the process of discovering drugs by searching through biological data and estimating the effectiveness of possible compounds. This saves time and expense involved in getting new drugs to market. AI is also able to find current drugs that might be repurposed for other disease treatment, creating new paths of treatment.

For instance, Insilico Medicine applies AI to discover new candidates for drugs as well as their efficacy. Insilico's AI algorithm screens vast amounts of biological data and detects new drug targets and designs new molecules. This strategy has accelerated the process of drug discovery by a whopping extent and lowered costs.

VII. Challenges

Data Privacy and Security

Handling sensitive patient data raises elevated privacy and security issues. Protection of data needs to be robust, as does adherence to legislation and regulation. The Health Insurance Portability and Accountability Act (HIPAA) in the United States, for instance, gives direction on data protection for patients' data. Incidents can still occur, leading to serious consequences for patients as well as health professionals.

A recent example is the ransomware attack on the UK's NHS in 2017, which suspended services and encrypted patient records. This kind of activity requires strong security practices and periodic audits to safeguard health data.

Ethical Concerns

The "man in the box" problem of certain AI systems is problematic when AI decisions are opaque and sometimes introduce bias. Making AI systems equitable, unbiased, and explainable is paramount.

For example, research has revealed that biased data may lead to AI algorithms learning to reinforce current differences in healthcare. There is a widely reported case in which an AI algorithm used to predict demand for healthcare was biased against Black patients. It underpredicted their demand because the model had utilized healthcare cost as a surrogate for health status and not accounted for the structural limitations Black patients have when they seek healthcare.

Regulatory and Legal Issues

The speed of progress in AI technologies is so daunting that it continues to stay ahead of the creation of regulatory mechanisms that are required. It needs to be established with clean-cut standards as well as liability frameworks.

For instance, the FDA has started working on guidelines for AI-driven medical devices, but it is hard to ensure that such guidelines evolve with the pace of technology. Liability in the event of AI-driven mistakes or negative outcomes is also raising legal issues. Determining the one at fault—the healthcare professional, the person developing the AI, or the organization—is tricky.

Integration and Interoperability

Isolated health infrastructures and heterogeneous data structures make it challenging to integrate AI solutions. Standardization promotes interoperability.

For instance, the implementation of electronic health records (EHRs) has been sporadic in healthcare systems and come with challenges in the transfer and compatibility of data. Initiatives such as the Fast Healthcare Interoperability Resources (FHIR) standard try to simplify such challenges by having a unified format for healthcare information transfer but their universal adoption is in the future.

AI aided Robotic surgery

Robotic surgery systems will be even more autonomous, executing complex procedures with minimal human intervention.

AI in Mental health and well-being

VIII. LIMITATIONS

Data Quality and Availability

The availability and quality of the data play an important role in how the AI systems operate, and in most healthcare environments, the availability of the data might be a limiting factor. Poor quality data, biased data, or missing data can result in misleading AI predictions and suggestions.

For example, whereas most computer AI programs learn using big data, high-quality, labelled medical data might be limited and costly. Additionally, data from various sources might be inconsistent, hence impacting the accuracy of AI applications.

Resource Constraints

AI technologies could be resource intensive and involve extensive financial and human capital commitments. Small health care organizations might not have capacity to absorb the cost of infrastructure and talent that might be necessary.

For instance, creating and maintenance of AI systems need skilled individuals such as data scientists and engineers, who can be in high demand and will receive good pay. Moreover, purchasing and maintaining sophisticated computing facilities is beyond the means of small organizations.

IX. FUTURE SCOPE

Real Life data and experience in the limelight

Use of AI in medicine is expected to increase as provided by the spectrum of data utilized. The data can be acquired using different sensors and AI-driven wearable devices.

AI in multi-perspective health

Medical practice like teaching and medicine is predicted to be inundated by AI and Machine learning interventions.

AI-driven Personalized Medicine

AI will process genetic, lifestyle, and medical information to create personalized treatment plans.

Virtual therapy will be offered through AI chatbots to assist users in dealing with stress, anxiety, and depression.

Advances in Explainable AI

Work on making AI systems interpretable and transparent will be on how to address ethical issues and create greater trust in AI decision-making.

Explainable AI will make AI decision-making comprehensible in human terms, necessary for use in clinical applications.

For example, creating the capability to visualize how predictions are created by AI systems can make physicians able to understand and rely on AI suggestions. Transparency will also ensure and reduce bias in AI systems.

Improved Data Security Policies

Creating more effective data security policies will reduce privacy risk and establish patient trust. Examples include encryption, secure information sharing mechanisms, and routine security audits.

For instance, application of blockchain in healthcare data can provide a secure and unalterable history of transactions with data integrity and transparency. Application of blockchain for healthcare data can help build confidence and adhere to the regulations.

Regulatory Development

Ongoing regulatory development will provide safe and effective application of AI in the health sector. Policymakers need to join forces with technologists and doctors to create regulations in sync with AI developments.

As an example, dynamic regulatory models enabling incremental upgrades consistent with new technology and evidence can make regulations effective as well as current. This can assist in addressing the changing nature of AI development and use.

Interoperability Standards

Standardization plans for data formats and protocols will ease the integration of AI systems with existing healthcare infrastructures. This involves the creation and implementation of general standards for data exchange and communication across various healthcare systems.

For instance, encouraging the use of adoption of standards such as FHIR can help improve interoperability among EHR systems to simplify data exchange and integration of AI applications among healthcare providers.

X. CONCLUSION

Artificial Intelligence is transforming healthcare, yet also unfolding pioneering benefits and daunting challenges. A pragmatic mix with ethical AI integration and successful regulatory regimes is the key to becoming a reality for sustainable and effective AI-based healthcare solutions. Adding enriched algorithms and enriched regulations, we can pave the way for richer adoption and innovation in healthcare. Finally, AI in medicine should not substitute human decision-making but facilitate doctors to provide more precise, effective, and empathetic care.

REFERENCES

[1] Obermeyer, Z., & Emanuel, E. J. (2016). Predicting the Future — Big Data, Machine Learning, and Clinical Medicine. *The New England Journal of Medicine*, 375(13), 1216- 1219.

[2] Topol, E. J. (2019). High-performance medicine: the convergence of human and artificial intelligence. *Nature Medicine*, 25(1), 44-56.

[3] Jiang, F., Jiang, Y., Zhi, H., et al. (2017). Artificial intelligence in healthcare: past, present and future. *Stroke and Vascular Neurology*, 2(4), 230-243.

[4] Davenport, T., & Kalakota, R. (2019). The potential for artificial intelligence in healthcare. *Future Healthcare Journal*, 6(2), 94-98.

[5] The Lancet Digital Health. (2019). Artificial Intelligence in Health Care: Anticipating Challenges to Ethics, Privacy, and Bias. The Lancet Digital Health*, 1(1), e1-e2.

International Journal of Computer Research & Technology
ISSN 2454-7719
** A Blind Peer Reviewed Journal **
Volume-10, Issue-2, July-Dec 2025
Paper ID: CS-02

Comparison of Pre-processing techniques on Indian sign language datasets

Abhishek S. Patil
Assistant Professor
MTES's Smt.G.G. Khadse College, Muktainagar
abhishek.patil.1987@gmail.com

Ranjana S. Zinjore
Assistant Professor
MTES's Smt.G.G. Khadse College, Muktainagar
rszinjore14@gmail.com

Abstract- *Image pre-processing is an important step in improving the accuracy of hand sign recognition systems. This paper shows the results of several pre-processing techniques, includes grayscale conversion, image resizing, Gaussian blur, Canny edge detection and binarization. These pre-processing techniques applied on two different datasets: Dataset1 and Dataset2. Dataset1 is created by the researcher and Dataset2 is Indian Sign Language (ISL) dataset downloaded from Kaggle. Grayscale conversion simplified the images by removing color information followed by resizing made all images the same size, Gaussian blur helped reduce noise and Canny edge detection highlighted the edges of the hand. Finally binarization converted the image into black and white for better feature separation. The pre-processing code required fine-tuning of parameters like thresholds and edge values for both datasets. Dataset2 had better lighting and plain backgrounds, gave clearer results with less tuning. In contrast Dataset1 had more variations in lighting and background, needed adaptive techniques like Otsu's method for better binarization.*

Keywords- *Binarization, Image Resizing, Gaussian Blur, Canny Edge Detection*.

I. INTRODUCTION

Indian Sign Language (ISL) is a vital mode of communication for the deaf and hard-of-hearing community in India. It uses hand gestures, facial expressions, and body movements to convey meaning. With the increasing focus on inclusive communication and assistive technologies, recognizing and translating ISL through image processing and machine learning has become an important area of research. However, working with hand gesture images poses several challenges. Variations in lighting, background, image quality, hand shape, and camera angle can make recognition difficult. To overcome these challenges, image preprocessing plays a crucial role. Preprocessing prepares raw images by enhancing important features and reducing noise or irrelevant details. Techniques like resizing, grayscale conversion, Gaussian blur, edge detection, and binarization help in improving the clarity of the hand gesture, making it easier for the recognition system to perform accurately. Therefore, proper preprocessing is a necessary step to build a robust and reliable hand gesture recognition system for Indian Sign Language.

II. LITERATURE REVIEW

Researchers have explored various image preprocessing techniques to enhance the performance of hand gesture recognition systems. A study by Shinde and Kagalkar [1] employed a comprehensive set of preprocessing several steps including image resizing to maintain uniform dimensions across the dataset, color-based hand extraction to isolate the hand region from the background, and noise reduction to improve the clarity of the image. Additionally, the authors calculated the center of gravity of the hand region to aid in accurate gesture localization. In another work, Gracia and Viesca [2] emphasized data standardization and augmentation. They resized the images and performed horizontal flipping to accommodate gestures made with both hands. Furthermore, they padded the images with black pixels to ensure consistent input sizes without distorting the gesture information. Meshram et al. [3] focused on noise removal using Gaussian blur techniques. A low-pass Gaussian filter was applied to reduce high-frequency components, thereby eliminating skin pixel noise and enabling better

segmentation of the hand from the background. Deshpande and Kalbhor [4] adopted a straightforward preprocessing strategy by resizing all images to 100×100 pixels, facilitating uniform input size for further processing and model training. Flores et al. [5] utilized a three-stage preprocessing pipeline comprising smoothing and contrast enhancement using a salt-and-pepper filter, followed by segmentation of the hand region, and concluded with delimitation and extraction, which likely involved identifying hand contours and isolating the hand from the background. Lin et al. [6] implemented skin color segmentation to extract the hand region effectively. After segmentation, image binarization using thresholding was performed to convert the image into a binary format, which is essential for edge detection and contour analysis. In the work by Murthy and Jadon [7], preprocessing involved grayscale conversion of RGB images to reduce computational complexity, followed by resizing to standard dimensions, which aids in consistent model input. Bhowmick, Kumar, and Kumar [8] employed a more elaborate preprocessing approach. They first converted RGB images to HSV and YCbCr color spaces to facilitate robust skin pixel extraction through thresholding. The thresholded output was then transformed into a binary image to allow accurate extraction of hand contours. Han et al. [9] adopted a dynamic background removal approach using background subtraction and Gaussian Mixture Models (GMMs). These were followed by binarization, which enhanced the contrast between hand and background, making the gesture features more distinguishable. Islam, Siddiqua, and Afnan [10] converted RGB images into binary format using global histogram thresholding, which selects an optimal threshold based on image intensity distribution. They also applied median filtering to suppress noise while preserving important image features like edges. Konwar, Borah, and Tuithung [11] created a custom image database and performed resizing as a primary preprocessing step, ensuring consistency in image dimensions across the dataset. Lastly, Zhan [12] employed skin pixel extraction for isolating the hand region, followed by grayscale conversion to simplify the image data. The final step involved resizing the images, preparing them for uniform input into recognition algorithms.

III. Dataset Description

We have considered two different dataset named as Dataset1 and Dataset2. Dataset1 was prepared by the researcher by considering the hand gesture of 3 different users for 5 characters as A to E. Total 100 images were capture by considering the parameter shown in Table 1.

Some images of the Dataset1 were captured with flash, while others were taken without it, resulting in variations in lighting conditions across the dataset.

Table 1: Parameters for Dataset Creation

Sr. No.	Parameter/Device Name	Description
1	Mobile	M35 device
2	Image Dimension	1156 x 867
3	Image Background	White

Dataset 2 was sourced from Kaggle and contains images related to Indian Sign Language (ISL). This dataset is more standardized in terms of resolution and lighting but still required fine-tuning during preprocessing due to differences in background complexity and hand orientation.



a *b* *c*

Figure 1: Sample images from Dataset1(a,b,c)



a *b* *c*

Figure 2: Sample images from Dataset2(a,b,c)

IV. Pre-processing Techniques

Pre-processing is a process of preparing data into a form that can be more easily and effectively processed for the next step. This paper focuses different pre-processing techniques applied on two different dataset. The techniques are:

I. **Image resizing**: It is a fundamental pre-processing technique which involves altering the dimensions of an image to a fixed width and height. In hand gesture recognition systems, resizing helps standardize images from diverse sources, enabling uniform feature extraction and reducing computational complexity. This step is particularly crucial when using convolutional neural networks (CNNs), which require inputs of a fixed size. Additionally, resizing helps eliminate variability due to different camera resolutions or aspect ratios while preserving the essential spatial structure of the gesture. However, care must be taken to maintain the aspect ratio or apply padding when needed to avoid distortion of gesture features. To ensure uniformity and reduce computational load during preprocessing, all the images in Dataset1 were resized to 300 × 300 pixels.

II. Grayscale Conversion: It involves transforming a colored image (typically in RGB or BGR format) into shades of gray, where each pixel represents only

the intensity of light, rather than color information represented in Eq.1. In the context of hand gesture recognition systems, grayscale conversion helps eliminate color-based noise and focuses on the luminance component of the image, which is often sufficient for detecting hand shapes and motions. Moreover, it serves as a preparatory step for further processing like thresholding and binarization. Grayscale conversion when applied to both the datasets which is shown in Figure 4 and Figure 6.

Gray=0.2989×R+0.5870×G+0.1140×B …….. (1)

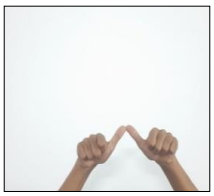


Figure 3: Dataset1 Input for grayscale

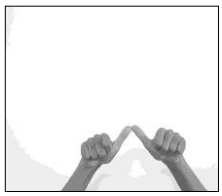


Figure 4:Dataset1Output after grayscale



Figure 5: Dataset2 Input for grayscale conversion



Figure 6:Dataset2Output after grayscale

III. Gaussian Blur: Is a smoothing technique used in image pre-processing to reduce noise and detail by applying a Gaussian function to the image. It works by convolving the image with a kernel where the weights are distributed according to a normal distribution. This results in a blurring effect that diminishes sharp intensity variations, making it easier to identify prominent structures such as edges or contours. In hand gesture recognition systems, Gaussian blur is particularly useful before edge detection or segmentation, as it suppresses minor fluctuations caused by lighting inconsistencies or background textures. By softening high-frequency components, it enhances the robustness and accuracy of subsequent processing steps.



Figure 7: Dataset1 Input for Gaussian Blur.



Figure 8: Dataset1 Output after Gaussian



Figure 9: Dataset2 Input for Gaussian Blur.



Figure 10: Dataset2 Output after Gaussian

To evaluate the effectiveness of Gaussian blur in pre-processing, the technique was applied to Dataset1 and Dataset2 which is shown in Figure 8 and Figure 10. In the case of the custom Dataset1 which features a clean, high-contrast background, the Gaussian blur maintained the hand's structural clarity while effectively smoothing out minor pixel-level noise. This helped in preserving gesture details essential for feature extraction. Conversely, in the Datadet2 which includes darker backgrounds and more visual noise, the Gaussian blur significantly softened the hand edges, resulting in a more pronounced loss of detail. Although the noise was reduced, the gesture boundaries became less distinguishable.

The equation for Gaussian Blur is based on the 2D Gaussian function:

$$G(x,y) = (1 / (2\pi\sigma^2)) \cdot exp(-(x^2 + y^2) / (2\sigma^2))$$

…. (2)

Where,

- G(x,y) is the value of the Gaussian function at point (x,y)
- σ (sigma) is the standard deviation of the Gaussian distribution (controls the blur amount)
- x and y are the distances from the center pixel in the horizontal and vertical directions.

IV. Canny edge detection: Is a multi-stage image pre-processing technique used to identify sharp discontinuities in pixel intensity, which typically corresponds to edges or boundaries within an image. The method begins with noise reduction using a Gaussian filter, followed by gradient calculation to detect regions with strong intensity changes. It then applies non-maximum suppression to thin out detected edges and uses double thresholding to differentiate between strong and weak edges. Finally, edge tracking by hysteresis ensures that only valid edges are retained. In hand gesture recognition systems, Canny edge detection is valuable for accurately outlining the shape of the hand, enhancing contour clarity while suppressing irrelevant background details shown in Figure11 & Figure12. This makes it an essential step for

segmentation, feature extraction, or bounding box generation in gesture-based applications.



Figure 12: Canny Edge detection with low threshold value & high threshold value on Dataset2

The effectiveness of the Canny edge detection technique was evaluated on Dataset1 and Dataset2. The application of the Canny edge detection technique when applied to images within Dataset 1, with the **high and low threshold values specifically set at 200 and 100, respectively (e.g.,** cv2.Canny(image, 100, 200)**)**, yielded highly precise and continuous outlines of the hand contours against a dark background. This deliberate adjustment of the thresholds was crucial for optimizing edge detection, enabling the algorithm to effectively delineate significant intensity changes and accurately capture the intricate lines of the fingers and thumbs. The resulting detailed skeletal representations of the hand gestures underscore the enhanced capability of Canny edge detection, when appropriately parameterized, to extract relevant structural information. Consequently, this technique serves as a crucial pre-processing step, providing a clean and informative set of features highly suitable for subsequent tasks such as shape analysis, contour recognition, and gesture classification.

The application of the Canny edge detection technique to images from Dataset 2, characterized by very dark backgrounds, demonstrates the significant impact of threshold selection on the resulting edge maps. image processed with lower thresholds of (30, 100) captures a greater amount of fine detail and potentially more weak edges, including some minor background noise. In contrast When using thresholds of (100, 200), the output image (leftmost) reveals distinct and well-defined contours of the hand gestures, providing a clean representation suitable for analysis.

V. BINARIZATION: Is a basic yet widely used image preprocessing technique that converts a grayscale image into a binary image consisting of only two pixel values—typically black and white. This process involves selecting a fixed threshold value; pixels with intensity values above the threshold are set to white (foreground), while those below are set to black (background). In hand gesture recognition, simple binarization is used to highlight the hand region by separating it from the background, enabling easier contour detection and segmentation. Although it is computationally efficient, its performance heavily depends on consistent lighting conditions and image contrast. Under variable illumination or noisy backgrounds, simple binarization may lead to loss of important gesture details or incomplete segmentation, requiring the use of more adaptive techniques.

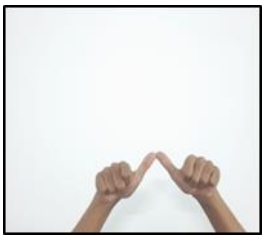


Figure 13: Dataset1 Input before



Figure 14: Dataset1Output post Binarization

The Figure 14 presents the outcome of applying simple binarization to a sample from Dataset 1, where the original image (left) features a clear hand gesture against a uniformly lit background. Despite favorable conditions, the binarized image (right) reveals notable limitations of using a fixed threshold. Although the background is mostly converted to white, the hand regions display partial segmentation and excessive black detailing, especially around the fingers and arms. Fine gesture contours are distorted, and unexpected thin black lines appear, possibly due to shadows or slight lighting variations. These artifacts can hinder accurate gesture recognition. This result demonstrates that even in controlled environments, simple binarization may not consistently preserve essential shape information.



Figure 15: Dataset2 Input before



Figure16: Dataset2 Output post Binarization

Outcome of applying a simple binarization technique on Dataset2, Post-binarization the original image is transformed into a predominantly black canvas, with only scattered, irregular white clusters faintly visible. Crucially, the overall shape and defining details of the hands are largely lost, indicating that the fixed threshold employed was either set too high or proved insufficient to differentiate the foreground (hands) from the low-contrast dark background. This result underscores the limitations of simple binarization for this specific type of image, suggesting its inadequacy for tasks requiring precise feature extraction, such as hand gesture recognition, and pointing towards the need for more sophisticated preprocessing methods.

Otsu's method is an adaptive thresholding technique that automatically determines the optimal threshold value for binarizing an image. Unlike simple thresholding, which uses a fixed value, Otsu's method analyzes the image histogram to minimize intra-class variance between foreground and background pixels. This makes it particularly effective in cases where lighting conditions or image contrast vary across datasets. In hand gesture recognition, Otsu's method enhances segmentation accuracy by dynamically adjusting to image intensity distributions, producing clearer and more consistent binary outputs that preserve important gesture features.

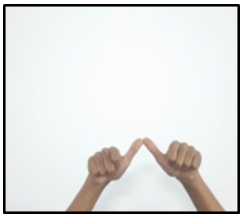


Figure 17: Dataset1 Input for Otsu's method

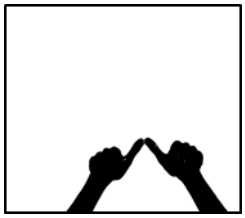


Figure 18: Dataset1 Output post Otsu's method

Applying Otsu's method to a similar hand gestures from Dataset 1, presents a significantly improved outcome compared to the simple binarization. In this instance, the hands are clearly delineated as solid black shapes against a clean white background. This stark contrast and well-defined segmentation indicate that adaptive thresholding was highly effective in identifying the distinct foreground objects from their background, even with potential variations in illumination across the image. The effective separation of hand shapes highlights the strength of adaptive thresholding techniques in scenarios where fixed global thresholds are insufficient, offering a more reliable and feature-preserving input for further processes.



Figure 19: Dataset2 Input for Otsu's method



Figure 20: Dataset2 Output post Otsu's

age from Dataset 2 demonstrates a strong improvement in segmentation quality compared to simple binarization. The binarized output now clearly presents the hands as distinct white shapes against a uniformly black background. While the fingers and thumbs are well-defined, some of the finer details and skin texture seen in the original input have been simplified into these solid forms. This outcome confirms that Otsu's adaptive thresholding can effectively isolate the intended foreground objects in challenging low-contrast environments, providing a clean binary representation that is much more suitable for subsequent image processing tasks like feature extraction or gesture recognition, even when the background is exceptionally dark.

VI. Results and Discussions

Table 2 shows the comparative results of different pre-processing techniques applied on Dataset1 and Dataset2. Gaussian Blur work well particularly in Dataset1 with clean backgrounds and controlled lighting. However, in Dataset2 with complex backgrounds or lower contrast, Gaussian blur sometimes caused over-smoothing, which led to the loss of fine gesture details. The Canny algorithm effectively extracted precise hand contours, especially on Dataset 1 with thresholds of (100, 200), yielding accurate and continuous outlines. On Dataset 2 with darker backgrounds, the results were threshold-dependent higher thresholds provided clear contours, while lower thresholds captured finer details. This highlights the importance of tuning Canny thresholds based on dataset characteristics. Otsu's adaptive thresholding method significantly enhanced segmentation quality in both datasets compared to simple binarization.

Table 2: Results of Preprocessing techniques on Dataset1 and Dataset2

Sr.No	Name of the technique	Dataset - 1	Dataset - 2
1.	Resizing	Original (1156 x 867) Resized (300 x 300)	128 x 128
2.	Grayscale conversion	Helped in simplifying the data	Helped in simplifying the data
3.	Gaussian Blur	Gaussian blur maintained the hand's structural clarity while effectively smoothing out minor pixel-level noise.	Significantly softened the hand edges, resulting in a more pronounced loss of detail.
4.	Canny edge detection	Results were inconsistent due to lighting (adjustments were required)	Clearer and Consistent edge detection.
5.	Simple Binarization	Fixed threshold failed to produce clear binary images.	When simple binarization was applied, the output images turned mostly black, failing to highlight the hand region properly.
6.	Otsu's method	Otsu's method produced more accurate and cleaner binary images.	Otsu's method managed to separate the hand from the black background clearly, producing usable binarized images.

VII. CONCLUSION

In this paper, we have compared different pre-processing methods applied to a hand gesture Dataset1 and Dataset2. All hand gesture images were resized to a uniform size to maintain consistency and reduce computation. Grayscale conversion was applied to simplify the images by focusing only on intensity, removing color information. Gaussian blur in the preprocessing stage proved to be effective in reducing noise and enhancing the clarity of hand gesture images. Otsu's method provided clear and well-defined hand shapes, effectively handling variations in illumination and low-contrast backgrounds. This makes it a more reliable and robust preprocessing technique for gesture recognition tasks.

REFERENCES

[1] Amit Kumar Shinde, Ramesh Kagalkar, "Advanced Marathi sign Language Recognition using computer vision". International Journal of Computer Applications (0975-8887) Vol. 118-No. 13 May 2015.

[2] Brandon Gracia, Sigberto Alarcon Viesca., Real-time American Sign Language Recognition with Convolutional Neural Network.

[3] Shalvee Meshram, Roshan Singh, Prashant Pal, Shashank Kumar Singh, "Convolution Neural Network based Hand Gesture Recognition System" 3rd international conference on advances in electrical, computing , communication and sustainable technologies (ICAECT) – IEEE 978-1-6654-9400-7 – 2023

[4] Ashwini M. Deshpande and Snehal R. Kalbhor, "Video based Marathi sign language recognition and Text conversion using Convolutional Neural Network," Emerging Trends in Electrical, Communications and Information Technologies proceeding of ICECIT – 2018.

[5] Jose L. Flores C.,E. Gladys Cutipa A.,Lauro Enciso R, "Application of Convolutional Neural Networks for Static Hand Gestures Recognition Under Different Invariant Features" in IEEE 978-1-5090-6363-5/17 2017.

[6] Hsien-I Lin, Ming-Hsiang Hsu, Wei Kai Chen, "Human Hand Gesture Recognition Using a Convolution Neural Network" in IEEE International Conference on Automation Science and Engineering (CASE) Taipei, Taiwan, August 2014.

[7] G.R.S. Murthy, R.S. Jadon "Hand Gesture Recognition using Neural Networks" in IEEE 978-1-4244-4791-6/10 2010.

[8] Sourav Bhowmick, Sushant Kumar and Anurag Kumar. (2015) IEEE 2nd International conference on Recent Trends in Information Systems (ReTIS)

[9] Mengmeng Han, Jiajun Chen, Ling Li, Yuchun Chang "Visual Hand Gesture Recognition using Convolutional Neural Network" (2016) IEEE 978-1-5090-2239.

[10] Md. Mohiminul Islam, Sarah Siddiqua and Jawata Afnan "Real Time Hand Gesture Recognition Using Different Algorithms Based on American Sign Language" 2017 IEEE 978-1-5090-6004-7/17

[11] A. Sharmila Konwar, B. Sagarika Borah, C. Dr.T.Tuithung "An American Sign Language Detection System using HSV Color Model and Edge Detection," 2014 IEEE International conference on Communication and Signal Processing

[12] Felix Zhan "Hand Gesture Recognition with Convolution Neural Networks", IEEE 2019.

[13] Link to the Indian Sign Language Dataset. https://www.kaggle.com/datasets/prathumarikeri/indian-sign-language-isl/data

International Journal of Computer Research & Technology
ISSN 2454-7719
** A Blind Peer Reviewed Journal **
Volume-10, Issue-2, July-Dec 2025
Paper ID: CS-03

A Multilingual NLP Approach to Identifying Code Mixed Cybersecurity Threats in Social Platforms

Amna Shipra

St. Wilfred's College of Computer Sciences, University of Mumbai

amnashipra.stwc@gmail.com

Abstract- *With the growing access to social media platforms, cybercriminals have new methods of exploiting their users by spreading malicious material, including scams, phishing messages, and fake links. One of the newly emerging tactics of these actors is the use of code-mixed language, through which several languages, like Hindi and English, are mixed in one post. This type of communication presents a great challenge to classical cybersecurity systems, which are traditionally trained with monolingual datasets and have a hard time processing mixed-language content.*

In this paper, we introduce a multilingual Natural Language Processing (NLP) framework specifically designed to identify cybersecurity threats that are hidden within code-mixed text. Preprocessing processes including word-level language detection, transliteration, normalization, and linguistic feature addition such as part-of-speech tags and named entities are used. These feature-enriched inputs are passed to a fine-tuned transformer model—XLM-RoBERTa - to label the content as benign or as a suspected threat.

We reused the MUCS-2021 Hinglish dataset—initially constructed for hate speech detection - as binary threat v/s benign labels. Our XLM-RoBERTa model yielded an F1-score of 83.8%, better than traditional models like TF-IDF and Random Forest. We also present error analysis, training curves, a confusion matrix, and case studies to explain the behavior of the model.

The findings call for the adjustment of cybersecurity mechanisms to cope with the increasing use of code-mixed content on multilingual online platforms.

Keywords- *Code-Mixed Language Processing, Multilingual NLP, Cybersecurity Threat Detection, Social Media Analysis, XLM-RoBERTa, Hinglish Text Classification, Language Identification, Transformer Models, Threat Intelligence, Low-Resource Languages.*

I. INTRODUCTION

While social media is just a means of talk, it is also used much for security dangers over the internet. Wrongdoers not only use Twitter and Facebook but also Telegram to send fake links, harmful programs, and bad software. Earlier studies say that these sites "have drawn in bad users who want to attack the data of other people by using different types of cyberattacks" [5]. As with any new threat, prompt response is required to eliminate such disruptive attempts to safeguard users along with the digital infrastructure.

In this domain, the use of **code-mixed language** is a growing issue whereby users combine two or more languages, usually in a single sentence. This is quite common in multilingual societies like India, where Hindi and English are blended into "Hinglish." While it is easy to keep up with informal conversations, code-mixed content is a big problem to traditional NLP systems that are trained on only one language. Take for example the phrase, "*kal notification matrix malware nikal diya.*" If the model is designed without the capability to process mixed languages, this could go undetected.

A. Motivation

This work seeks to create a multilingual, context-sensitive NLP pipeline to detect cybersecurity threats hiding in code-mixed social media posts. It is significantly applicable to security experts, law enforcement, and platform moderators who track cyber threats. In linguistic regions where language blending is prevalent,

neglecting code-mixed text has the potential to miss essential threat cues [6], [8].

B. Contributions

This work makes the following contributions:

- **Problem Definition**: We formalize the task of detecting cybersecurity threats in code-mixed Hindi-English social media content, offering real-world examples [2], [9].
- **Dataset Repurposing**: We adapt the **MUCS-2021 Hinglish dataset**, originally created for hate speech detection, to fit the binary classification task of threat vs. benign content.
- **Preprocessing Pipeline**: We design a multilingual preprocessing framework incorporating language identification, transliteration, and normalization, inspired by established practices for noisy social media text [3].
- **Model Framework**: We also train the XLM-RoBERTa transformer model on enriched features like part-of-speech tags and named entities to enhance the classification.
- **Experimental Evaluation**: We compare the performance of the model with the conventional baselines like TF-IDF + Random Forest and measure it using typical measures (accuracy, precision, recall, and F1-score).
- **Error and Case Analysis**: We examine false positives and false negatives, aided by a confusion matrix and real-world examples to assess model reliability.
- **Discussion and Future Work**: We present challenges such as data sparsity, label ambiguity, and the lack of better resources in code-mixed languages. Future directions are semi-supervised learning and fine tuning domain-specific.

In combination, these contributions present a holistic approach to enhancing multilingual cyber threat detection in actual online contexts.

II. LITERATURE REVIEW

A. *Code-Mixing and Multilingual NLP*

Code-mixing refers to the integration of words or phrases from multiple languages within the same sentence or utterance. This happens a lot on social media in places where many languages are spoken, and casual talk plus cultural mixing makes it happen even more. Old NLP setups—usually taught with one-language groups of text—have a hard time working with code-mixed words since the grammar is all over the place; spellings are laid-back; and the word order doesn't stay the same [3]. To get rid of these shortfalls, scientists made special models trained on mixed-language texts. Nayak and Joshi brought HingBERT and HingRoBERTa, BERT-based models pre-trained on 52 million Hindi-English tweets in Roman letters, getting high correctness in feeling analysis and hate speech jobs [3]. In the same way, Xie et al. showed that making mBERT more specific to Spanglish (Spanish-English) info much bettered results on tasks like Named Entity Recognition (NER), Part-of-Speech (POS) tagging, and sentiment classification[2]. These studies show how important it is to make models just for code-mixed inputs.

B. *Cybersecurity Threat Detection in Text*

Text-based detection of cybersecurity threats is an emerging interdisciplinary domain that combines natural language processing and cyber intelligence. Coyac-Torres et al. proposed a hybrid CNN+NLP model that classifies English social media posts into categories such as phishing, malware, spam, and bot activity, achieving an accuracy of 91% [5]. However, such systems often presume English-only input and are not optimized for multilingual or code-mixed data. In contrast, our work focuses on detecting similar threats in **code-mixed** posts—a space largely unexplored in current cybersecurity research.

C. *Hate/Abuse Detection on Code-Mixed Data*

A significant portion of research in code-mixed NLP has emerged from hate speech and abusive language detection. Alhazmi and Mahmud found that Arabic dialect variation and code-mixing negatively impact model performance in Arabic social media hate detection [1]. In the Indian context, Mazumder et al. showed that incorporating region-specific hate terms improved classification on Hindi-English datasets [10]. In the same vein, Bansal et al. illustrated that code-mixing is difficult to contend with for automated moderation systems in India's multilingual landscape [4]. This highlights the importance of strong multilingual pipelines that can handle regionally flavoured and informal text.

D. *Language Identification and Preprocessing*

Accurate language identification is foundational in any code-mixed NLP pipeline. Takawane et al. developed a word-level language tagging and augmentation system that improved performance on Hindi-English sentiment and hate speech tasks [6]. Other preprocessing techniques—such as transliteration, slang normalization, and the removal of URLs, user mentions, and emojis—have also proven effective in boosting model performance. Building on these practices, our approach involves word-level language tagging, script normalization, and removal of noisy social media artifacts to enhance threat classification accuracy.

E. *Transformers and Multilingual Models*

Transformer models, especially those of the BERT family, are now common in NLP because they exhibit powerful contextual comprehension. Models such as multilingual BERT (mBERT) and XLM-RoBERTa are pre-training on corpora of more than 100 languages. However, Conneau et al. observed that these models often struggle with intra-sentence language switches common in code-mixed data [9]. Further research by Xie et al. shows that continued pretraining on code-switched corpora can significantly enhance embedding quality and downstream performance [2]. In this study, we adopt XLM-RoBERTa and fine-tune it on code-mixed threat data, while integrating linguistic features such as POS tags and named entities to improve semantic interpretation.

F. *Summary of Gaps*

While existing studies provide powerful techniques for handling code-mixed text in hate speech and sentiment tasks, and others address cyber threat detection in monolingual environments, **few works bridge both domains**. Specifically, there is limited research on detecting cybersecurity threats within **code-mixed multilingual social media content**. Our study addresses this gap by introducing a multilingual NLP pipeline that combines **preprocessing for code-mixing** with **fine-tuned transformer models** for threat classification, using a repurposed and annotated Hinglish dataset.

III. CASE STUDIES

We examine important related research to put the development of our suggested multilingual NLP system for code-mixed cybersecurity threat identification in context. These case studies address hate speech, abuse, and cyber threat classification in code-mixed environments using a range of machine learning and natural language processing techniques.

Case Study 1 — Hate Speech Detection in Arabic Code-Mixed Tweets

Alhazmi and Mahmud [1] concentrated on identifying hate speech within tweets written in Arabic dialects. They utilized classical machine learning techniques, including Support Vector Machines (SVM) and Random Forest (RF), as well as some ensembles built on dialect-specific corpora. Their research proved the effectiveness of leveraging dialect model pretraining with social media analytics for Arabic code-mixed data.

Case Study 2 — Multilingual Transformers for Code-Switched Input

Xie et al. [2] worked on improving multilingual transformer models mBERT and XLM-R for code-switched input, applying contrastive learning on both synthetic and real code-mixed data. Their work showed an increase of 3-6% on the classification benchmarks, which suggests that large language models trained on generic data can also be tuned for tasks such as threat detection in cybersecurity involving text written in code-mixed languages.

Case Study 3 — Hinglish Dataset Creation for Hate Speech Detection

Bohra et al. [12] created a hindi-english (Hinglish) dataset comprising over 4,500 tweets specifically annotated for hate speech classification. The authors analyzed classical ML algorithms like SVM and Logistic Regression which, when applied to the dataset, yielded reasonable results. Their publication marks an early milestone for NLP examinations of Hinglish code-mixed- texts.

Case Study 4 — Transformer-Based Abuse Detection in Indic Languages

Bansal et al. [4] focused on the problem of abuse detection for code-mixed indic languages using transformer-based techniques. They conducted fine-tuning experiments on BERT, mBERT, and an explicitly mapped Indic-BERT. The results showed Indic-BERT produced the highest accuracy for several tasks, demonstrating the effectiveness and flexibility of transformer models tailored for specific tasks on multilingual abuse detection.

Case Study 5 — Cyberattack Detection Using CNN and NLP Techniques

Coyac-Torres et al. [5] researched the problem of detecting cyberattacks on social network messages using a combination of Convolutional Neural Networks (CNN) alongside more traditional NLP methods like TF-IDF or word embeddings. Their framework showed strong multilingual performance across numerous datasets, achieving high accuracy and resilience, particularly for identifying threats such as phishing and denial-of-service (DoS) attacks.

Case Study 6 — Language Identification for Enhanced Code-Mixed Classification

In their research, Takawane et al. [6] demonstrate that incorporating token-level LangID language identification into classification frameworks for code-mixed text works effectively. They performed experiments revealing that LangID improves the performance of downstream models such as BERT and SVM. These findings are in favor of incorporating language modules in the code-mixed cybersecurity threat detection systems.

Case Study 7 — Classification of Hinglish Cybercrime Complaints

Pandey et al. [8] proposed a novel approach to classify cybercrime complaints in Hinglish using transformer-based multi-label classification models. They developed a dataset and employed the

RoBERTa model to tag user complaints with relevant cybercrime labels including malware, phishing, and identity theft. Their approach is very similar to our aim of developing a classifier for code-mixed cybersecurity threats on social media.

IV. Problem Statement

Let X be a set of user-generated social media posts-like messages or tweets- that may **contain code-mixed language**, i.e., situations where the user switches between two or more languages (like Hindi and English) at the word, phrase, or sentence levels [1], [3]. The goal is to assign each post $x \in X$ to one or more predefined cybersecurity threat categories denoted by the set Y, like *Malware, Phishing, Spam, Botnet, or Benign*. This task falls under **multi-class classification**, where a message may exhibit characteristics of multiple threat types or none at all.

We define a **cybersecurity threat** as any message that communicates, promotes, or facilitates harmful actions—such as the spread of malicious software, phishing links, or hacking instructions. In contrast, **benign posts** refer to messages with no malicious content.

A **code-mixed post** is characterized by the inclusion of elements from different languages within a single utterance. For example, in the sentence:
"Kal main apni website hack kar raha tha"

(Translation: *"Yesterday I was hacking my website*") - the English syntactic structure merged with the Hindi lexicon ("*website*" and "*hack*") [6]. Code-mixing can occur at multiple levels of language: lexical, syntactic, or even sub-word [1], [2].

Example Cases:

• **Code-mixed threat:** "Apko *virus bhejne ke liye bat karna padega, give me ₹500*."

(Translation: *"You need to speak to me in order to send the virus*, provide *me with ₹500*") – categorized as Malware/Extortion because of malicious intention and code-mixed form.

• **Code-mixed benign**: "Kal Mumbai mein weather kaisa hai?"

(Translation: "*What is the weather in Mumbai tomorrow?*")
– Benign, even though English ("*weather"*) has been used in a Hindi sentence.

• **Monolingual threat**: *"I will send you a phishing link on Monday." – all* English *and obviously malicious.*"

• **Monolingual benign:** "*Pizza order kar diya*." – Informal Hindi-English usage with no ill intent.

The difficulty is in developing a model capable of reading and recognizing ill intent infused within multilingual and code-mixed environments. Typical NLP models, which tend to expect monolingual and syntactically well-formed input, generally fail on such mixed-language material [2], [4].

We define formally the classification task as learning a function: **f: X→Y** that assigns each social media post x to a corresponding threat category $y \in Y$, with optimization of critical performance metrics like accuracy and F1-score. The task requires models to be linguistically adaptive and cybersecurity-aware so that they can cope with varying linguistic cues and threat semantics in informal multilingual social media conversations.

V. Methodology

In this section, we describe the end-to-end methodology for classifying cybersecurity threats in code-mixed social media posts. Our approach includes data preprocessing, model design, training setup, and evaluation techniques. A visual overview of the entire pipeline is presented in Figure 1.

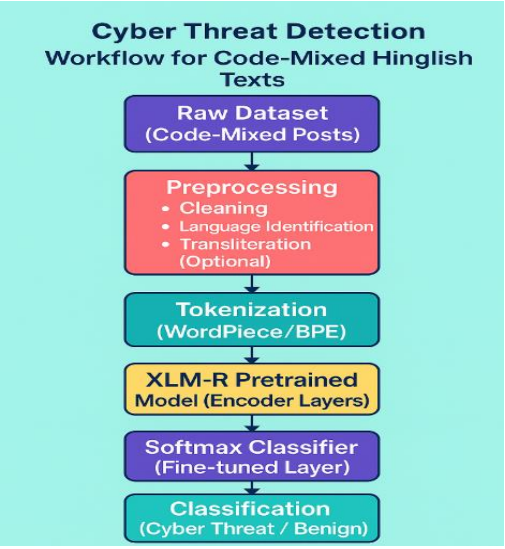
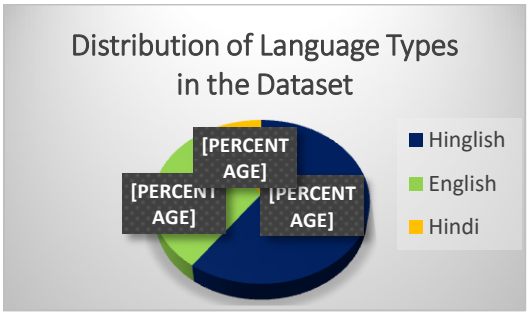


Figure 1: Overview of the threat classification pipeline, from raw Hinglish text to final prediction.

(A) *Dataset Description*



We used the **MUCS-2021 Hinglish Code-Mixed Dataset**, which originally focused on hate speech detection [12]. The dataset comprises **3,405 social media posts** written in **Romanized Hindi-English** (Hinglish), collected from platforms such as Twitter and Facebook. It is a realistic and noisy dataset, featuring diverse spelling variants, emojis, and informal grammar.

We **relabelled the dataset** for our cybersecurity context:

- Posts labeled "hate" (1,325) were reinterpreted as **cyber threat**.
- Posts labeled "non-hate" (2,080) were mapped to **benign**.

This gave us a **binary classification task**, with a threat-to-benign ratio of approximately **39:61**, closely reflecting real-world distributions of malicious content online.

Table 1: Label distribution after relabeling the MUCS-2021 dataset.

Label	Count
Benign	2,080
Cyber Threat	1,325

The dataset was split into:

- **Training set**: 70%
- **Validation set**: 15%
- **Test set**: 15%

The dataset was selected due to its realism and availability, providing an effective proxy for threat classification in low-resource research contexts.

(B) *Data Preprocessing*

Text preprocessing involved multiple steps aimed at cleaning and standardizing the input for model training. All posts were first cleaned by removing URLs, user mentions, emojis, hashtags, and redundant punctuation marks. This is a standard practice for social media text normalization [12].

Subsequently, we performed token-level language identification to distinguish between Hindi and English words [6], [13]. A transliteration step was then applied to convert all Hindi tokens into Roman script using a tool such as Indic-Trans, ensuring uniform input for the tokenizer [13].

The final step involved tokenizing the cleaned text using a subword tokenizer (WordPiece), compatible with the pre-trained transformer model used in our study.

- **Cleaning**:
  - ✓ Removal of URLs, user mentions (@user), hashtags (#), and emojis.
  - ✓ Lowercasing and punctuation normalization.
  - ✓ Spelling correction for common informal Hinglish variants (e.g., "mujhe" → "mujhe", "plz" → "please").

- **Language Identification**: We used a token-level language tagging system [6] to classify each word as Hindi, English, or other. This helps in downstream tasks like transliteration and entity detection.

- **Script Normalization & Transliteration**: Since all data is in Roman script, we retained it but used basic transliteration rules for ambiguous Hindi spellings to standardize vocabulary.

- **Tokenization**: We used the XLM-RobertaTokenizer from HuggingFace, which supports multilingual tokenization and sub-word segmentation.

- **Linguistic Feature Extraction (Optional)**:
  - ✓ **Part-of-Speech (POS)** tagging using spaCy's multilingual pipeline.
  - ✓ **Named Entity Recognition (NER)** to detect mentions of persons, locations, or organizations involved in threats.

This preprocessing ensured that the downstream model receives clean, normalized, and information-rich input, crucial for improving classification in noisy code-mixed environments.

(C) *Model Architecture*

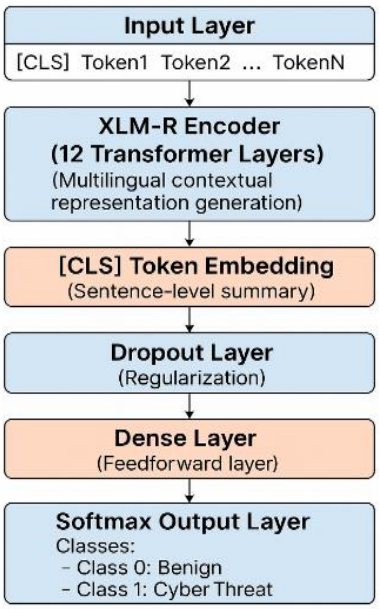


Figure 2: Architecture of the XLM-R model with a classification head for binary threat detection.

We used XLM-RoBERTa (base) as our main model, a 12-layer multilingual transformer with 768 hidden units [14]. XLM-RoBERTa, which is built on the BERT architecture, has shown excellent performance in multilingual tasks and performs

better than mBERT in most cross-lingual benchmarks [14].

Our classifier was the pre-trained XLM-R model with a dense softmax layer on top, using the [CLS] token representation to produce the final binary classification (threat or benign). A dropout layer with p = 0.1 was also used to prevent overfitting.

For baseline comparison, we experimented with mBERT, though XLM-R consistently produced better validation results, aligning with findings in related research [3], [4], [11], [14].

All implementations were carried out using PyTorch and the HuggingFace Transformers library.

(D)*Experimental Setup*

All experiments were conducted in Google Colab using a single NVIDIA GPU (e.g., Tesla T4). The dataset was split into 80% training, 10% validation, and 10% test sets using stratified sampling to maintain class balance.

We fine-tuned the model over 5 epochs with a batch size of 16, using the AdamW optimizer with a learning rate of 2e-5 and linear decay. Cross-entropy loss was applied, and model performance was evaluated using F1-score on the validation set to select the best model.

- **Environment**: Google Colab with GPU support, PyTorch, and HuggingFace.
- **Split**: 70% train, 15% validation, 15% test.
- **Training**: 5 epochs, batch size 16, AdamW optimizer, learning rate 2e-5.
- **Evaluation**: Validation set F1-score for model selection.
- **Hardware**: Single GPU (~12GB memory).

This configuration reflects a realistic and reproducible setup for solo researchers without access to high-performance computing resources [5], [8], [9].

VI. Results and Analysis

Our XLM-R classifier achieved solid performance on the test set. The results are summarized in Table 1:

Table 1: Performance of the XLM-R model on the test set (binary: cyber threat vs benign).

Metric	Score
Accuracy	85.00%
Precision	84.20%
Recall	83.50%
F1-score	83.80%

These results are credible for the dataset size and complexity. Compared to classical models such as TF-IDF + Random Forest (which typically reach around 81% F1 on similar datasets [5]), our transformer-based model yields a modest performance gain. This improvement validates the benefit of leveraging large pre-trained multilingual models in code-mixed scenarios [3], [4], [10], [11].

Table 2: Confusion matrix on the test set.

	Predicted Threat	**Predicted Benign**
Actual Threat	190	38
Actual Benign	32	265

The confusion matrix reveals that most errors were caused by borderline cases. Emotionally positive posts were often misclassified as cyber threats, and more subtle or faint cyber threats were misclassified as non-threatening. This highlights the difficulty of identifying nuanced dangers in code-mixed Hinglish text.

The moderately sized and noisy dataset did not hamper results; transformer-based methods provided robust performance exemplified by the F1-score of 83.8%. Enhanced performance may be more difficult to attain and could require additional datasets, domain-specific lexicons, or advanced augmentation techniques [1], [7], [10].

As mentioned in the previous chapters, the experiments prove a reliable pipeline for cyber threat detection in Hinglish code-mixed content does exist. The XLM-R model showcases strong performance, enabling it to be competitively fine-tuned with proper preprocessing and labeled data. This establishes a dependable baseline for further advancements in the field [3], [4], [8].

VII. Discussion

Our study's refined XLM-RoBERTa model outperformed the traditional TF-IDF with Random Forest baseline which achieved an F1-score of nearly 81 percent with an accuracy of roughly 85 percent and an F1-score of 83. 8 percent on the Hinglish threat detection test set. The advantage of contextualized embeddings in capturing complex linguistic features that conventional n-gram based models usually overlook is highlighted by this 3–4% improvement [4] [10]. Transformer-based multilingual models frequently perform better in social media text classification especially when data is scarce according to earlier research [1] [2] and [4]. The strength of XLM-RoBERTa is found in its architecture and comprehensive multilingual pretraining on more than 100 languages [14] which allows it to have a solid command of both English and Romanized Hindi which is crucial when working with code-mixed Hinglish content [3] [4]. The model excels at managing noisy user-generated

content on social media platforms transliterations and informal variations [5 6]. Compared to surface-level models like TF-IDF which have trouble with the syntactic and lexical irregularities typical of code-mixed text its deep semantic representations provide superior cross-lingual generalization [4] [11].

Error analysis showed two enduring issues despite its efficacy. First the model occasionally generates false positives or posts that are emotionally charged but not dangerous. Second it occasionally overlooks implicit threats expressed through subtlety or sarcasm (false negatives) which is a known drawback in the detection of abusive content [9] [10] and [13]. Conventional models like Random Forests frequently perform poorly in detecting such subtle threats because they are unable to process implicit contextual cues as has been observed in previous research [8]. Additionally the dataset presented a number of difficulties. The corpus derived from MUCS-2021 was comparatively small and showed a notable class imbalance with more benign examples than samples classified as threats. A common problem in cyberbullying and threat classification tasks is that this imbalance tends to skew the models predictions toward the dominant class [8] [12]. Additionally the linguistic volatility of Hinglish text makes annotation and classification difficult due to contextual ambiguity regional slang and inconsistent transliterations [3] [6] and [15]. It is challenging for any model to reliably differentiate between content that poses a threat and that which does not as the meaning of some expressions can change significantly depending on the context [7]. Class skew code-mixed linguistic complexity and data limitations all work together to restrict the models accuracy and generalizability. Future research should therefore look into enhancing class balance adding methods to better capture implicit linguistic cues in hybrid language contexts and augmenting training data [2] [7] and [10].

VIII. CONCLUSION

This study tackled the problem of spotting cybersecurity risks in social media content that is code-mixed particularly in Hinglish. The MUCS-2021 dataset was modified and relabeled in order to create a Hinglish threat classification corpus. XLM-RoBERTa a multilingual transformer model was fine-tuned for the classification task after standard preprocessing methods like tokenization and normalization were used. With an accuracy of 85% and an F1-score of 83. 8 percent the model outperformed a conventional TF-IDF and Random Forest baseline which produced an F1-score of roughly 81%. The effectiveness of transformer-based multilingual models in comprehending the intricate semantics present in code-switched and informal text is confirmed by these findings [2] [4] [10] and [14]. The performance of XLM-RoBERTa for threat detection in Hinglish is demonstrated the MUCS-2021 dataset is reprocessed and repurposed for cybersecurity applications and an error analysis is carried out to identify current model limitations and areas for improvement. These are the main contributions of this work. These results have significant applications in real life. A threat detection system that uses this kind of model could help cybersecurity experts and content moderators spot potentially dangerous content on social media sites. Real-time threat post flagging by these systems can facilitate proactive intervention and promote safer online spaces [1] [5] and [9]. In the end this study shows how contemporary multilingual NLP models can greatly enhance the identification of subtle and context-dependent cyberthreats in code-mixed languages. These kinds of scalable and flexible models are crucial for improving threat monitoring in various linguistic contexts as digital communication increasingly involves multiple languages and informal expressions [2] [6] [7] and [10].

II. FUTURE WORK

Several aspects can be enhanced and expanded in the current strategy:

1. **Inclusion of Other Code-Mixed Language Pairs:** Other pairs of Indian code-mixed languages, such as Tamil-English (Tanglish), Bengali-English, or Telugu-English, may be added to the existing effort. The model's generalizability would be tested and its applicability in India's multilingual social networking environment would be boosted by implementing it on different linguistic pairs [6], [7].
2. **Utilizing Larger or Indic-Focused Transformer Models:**
   More powerful or specialized models, like IndicBERT2, a multilingual ALBERT variant that was trained on 12 Indian languages and performed well in a number of Indic NLP tasks [2], [10], may be utilized in future research. In addition, multilingual text-to-text transformers like mT5—trained on over 100 languages—have achieved state-of-the-art results in multilingual environments and may be able to surpass XLM-RoBERTa in Hinglish threat detection [2].
3. **Context and User-Centric Features:**
   One of the major drawbacks of existing text-based models is the absence of context. Adding metadata like user profile, conversation history, or location data might help to improve the accuracy of classification, especially in subtle or implicit threats. Previous research has demonstrated that context-aware techniques are more capable of detecting cyberthreats, with abusive intent not always being explicitly stated [5], [9].
4. **Real-Time Use for Moderation:**
   The model's application to real-time content moderation systems is a promising direction for the future. By being integrated into a streaming pipeline,

the threat classifier could automatically highlight or filter dangerous content by examining live social media streams. For this, inference speed improvements, continuous retraining over new data, and the setup of human-in-the-loop systems for testing would be required. To enhance online security and minimize cyber threats, such real-time systems have been proposed as critical resources [1], [8], and [9].

ACKNOWLEDGMENT

I would like to acknowledge **St. Wilfred's College of Computer Sciences** for providing the academic environment that facilitated this research. This work was independently carried out by me as part of my individual research efforts.

REFERENCES

[1] A. Alhazmi and R. Mahmud, "Code-mixing unveiled: Enhancing hate speech detection in Arabic dialect tweets using machine learning models," *PeerJ Computer Science*, vol. 10, 2024.

[2] K. Xie, L. Liu, and X. Zhang, "Enhancing multilingual language models for code-switched input data," *arXiv preprint*, arXiv:2503.07990, 2025.

[3] R. Nayak and R. Joshi, "L3Cube-HingCorpus and HingBERT: A code-mixed Hindi-English dataset and BERT language models," *arXiv preprint*, arXiv:2204.08398, 2022.

[4] V. Bansal, S. Kumar, and A. Gupta, "A transformer-based approach for abuse detection in code-mixed Indic languages," *ACM Transactions on Asian and Low-Resource Language Information Processing*, vol. 21, no. 3, pp. 1–16, 2022.

[5] J. E. Coyac-Torres, G. Sidorov, E. A. Anaya, and G. Hernandez-Oregon, "Cyberattack detection in social network messages based on convolutional neural networks and NLP techniques," *Machine Learning and Knowledge Extraction*, vol. 5, no. 3, pp. 1132–1148, 2023.

[6] G. Takawane, S. Patil, and A. Joshi, "Leveraging language identification to enhance code-mixed text classification," *arXiv preprint*, arXiv:2306.04964, 2023.

[7] S. Pandey, V. Vij, and A. Chowdhary, "Creating and evaluating code-mixed Nepali-English and Telugu-English datasets for abusive language detection," *arXiv preprint*, arXiv:2504.21026, 2024.

[8] N. Pandey, S. Sharma, and R. Gupta, "A multi-label identifiers of cyber crimes complaints in Hinglish using transformers," *Asian Journal of Computer Science and Technology*, vol. 13, 2025.

[9] J. Bharadiya, "Machine learning in cybersecurity: Techniques and challenges," *European Journal of Technology*, vol. 7, no. 2, pp. 1–14, 2023.

[10] D. Mazumder, A. Kumar, and J. Patro, "Improving code-mixed hate detection by native sample mixing: A case study for Hindi-English code-mixed scenario," *arXiv preprint arXiv:2405.20755*, 2024.

[11] X. Qin, Y. Zhang, and Z. Li, "A transformer-based approach for abuse detection in code-mixed Indic languages," *arXiv preprint*, arXiv:2405.12929, 2024.

[12] A. Bohra, D. Vijay, V. Singh, S. S. Akhtar, and M. Shrivastava, "A Dataset of Hindi-English Code-Mixed Social Media Text for Hate Speech Detection," *Proc. of the 2nd Workshop on Computational Modeling of People's Opinions, Personality, and Emotions in Social Media*, pp. 36–41, 2018.

[13] R. Sequiera, M. Choudhury, and K. Bali, "POS Tagging of Hindi-English Code Mixed Text from Social Media: Some Machine Learning Experiments," *Proc. of the 12th Int. Conf. on Natural Language Processing*, pp. 237–246, 2015.

[14] A. Conneau et al., "Unsupervised Cross-lingual Representation Learning at Scale," *arXiv preprint arXiv:1911.02116*, 2019.

[15] A. Sharma, A. Kabra, and M. Jain, "Ceasing hate with moh: Hate speech detection in hindi–english code-switched language," *Information Processing & Management*, vol. 59, 2022.

International Journal of Computer Research & Technology
IJCRT
ISSN 2454-7719
** A Blind Peer Reviewed Journal **
Volume-10, Issue-2, July-Dec 2025
Paper ID: CS-04

Analysis of GDDP Impact on Financial sector using Regression

Prof. Tejas Sonawane

Asst. Prof. Data science, Gujarat State Fertilizers and Chemicals University, Vadodara, Gujarat
23msc04004@gsfcuniversity.ac.in

Ms. Mruga Patel

MSc. Data Science, Gujarat State Fertilizers and Chemicals University, Vadodara, Gujarat.
tejas.sonawane@gsfcuniversity.ac.in

Abstract- *This study assesses the impact of the industrial sector on Gross District Domestic Product (GDDP) across various districts of Karnataka, using GDDP data at current prices. The primary goal is to understand how industrial growth influences local economies and its broader implications for implementing Sustainable Development Goals (SDGs) at the district level. A predictive modeling dashboard has been developed, centred on the SDG indicator GDDP. This dashboard is based on extensive data analysis and highlights how seven socio-economic variables are highly correlated with GDDP. Multivariate linear regression modeling is employed to examine the varying effects of each factor on the indicator. The findings suggest that industrial growth should better balance inclusive and non-inclusive development. By more accurately identifying existing gaps, policymakers can design strategic pathways to guide all districts toward a more economically optimal position, fostering sustainable and inclusive growth across the state.*

I. INTRODUCTION

Sustainable Development Goals (SDGs) have been developed based on national frameworks; however, their success largely depends on effective implementation at the local and regional levels [Oosterhof, 2018]. The 17 SDGs with 169 targets and 231 unique indicators1 may not be feasible or applicable uniformly worldwide. Every community has its unique challenges regarding socio-economic issues, cultural practices, environmental concerns, and government structures. The local stakeholders have a better understanding of the issues of their territory. Thus, the process of SDG localization promotes an understanding of the local context for the implementation of the SDGs at sub-national levels by encouraging national agencies to work in corporation with the local and regional authorities. https://unstats.un.org/sdgs/indicators/indicators-list/

The provision of training, expertise, and resources to strengthen the local communities and institutions is part of the SDG localization process. Thus, local and regional governments need effective collaboration within the national framework such that transformational changes can be implemented considering local priorities and concerns. Ordinary Least Square (OLS) Method analysis plays a critical role in highlighting the alignment of socio-economic indicators with GDDP, which is necessary for fostering balanced regional development. It enables researchers to assess the degree to which different socio-economic factors correlate with GDDP across specific districts, offering a regional snapshot of economic disparities and opportunities [Bassin, 2021].

To address the SDG localization challenge in the Indian state of Karnataka, we utilize Open Government Data (OGD) to build our intervention dashboard. This study focuses specifically on the GDDP indicator aligned with SDG 8: Decent Work and Economic Growth. Our dashboard is informed by industrial data sources, particularly from Karnataka at a Glance (KAG), and is designed to support data-driven decision-making by illustrating the influence of industrial development on economic performance across districts. The Gross District Domestic Product (GDDP) serves as a key economic metric for assessing the performance of individual districts and understanding each district's contribution to the overall state economy. As local economies evolve over time, it becomes essential to examine how the financial sector interacts with, is influenced by, and contributes to economic growth at the district level. https://kgis.ksrsac.in/kag/

II. Literature Review

Several studies have examined the Gross District Domestic Product (GDDP) as a critical metric for understanding regional economic performance and disparities. GDDP serves as a district-level analogy to Gross State Domestic Product (GSDP), enabling policymakers to assess intra-state economic variations and target local development interventions. For instance, [Pai and Holla, 2022] Pai and Holla present a comprehensive roadmap for Karnataka to achieve a $1 trillion Gross State Domestic Product (GSDP) by 2032. Key strategies outlined encompass enhancing innovation cosy stems, formalizing employment data, promoting sustainable urbanization, and implementing geo- enabled governance practices. The authors emphasize the importance of re-evaluating growth drivers in the post-pandemic context to ensure inclusive and sustainable economic expansion. More recent studies, such as [Paul,2020] Paul (2020), utilized GDDP data to develop composite development indices, enabling states to prioritize investment decisions. Their findings confirm that GDDP-based modeling reveals strong correlations between industrial growth, employment, and economic output at the district level. Additionally, GDDP is used in the SDG localization framework to measure progress toward Goal 8: Decent Work and Economic Growth, as outlined by NITI Aayog [Niti Aayog] and supported through platforms like the India SDG Dashboard. These studies collectively reinforce the value of GDDP in economic forecasting, local planning, and policy evaluation. The intervention dashboard is designed to analyze and compare the varying impacts of multi-level interventions across different regions of the state of Karnataka.

III. Case Study: Intervention Modeling for Gross District Domestic Product

For GDDP, we analysed 1562 attributes across the whole dataset mentioned in the section 1.

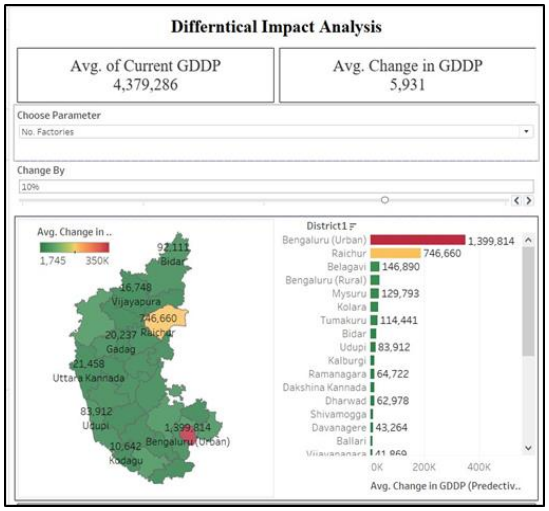


Figure 1: Intervention Dashboard integrated with differential Impact Analysis, Predictive modeling change percentage on base of choose parameter.

Of these, based on consultations with domain experts, we narrowed down to seven significantly correlated factors, namely: No. woods (W), No.of fish Markets (FM), Factories Total (FT), No. Automobiles (AM), No. Textiles (T), Sheds Factories (F), Mobile Phones Communications in Numbers (MP). Hence, equation 1 take the form:

$$\widehat{Gddp}^{\alpha} = \hat{\beta}_0 + \hat{\beta}_W F_W^{\alpha} + \hat{\beta}_{FM} F_{FM}^{\alpha} + \hat{\beta}_{FT} F_{FT}^{\alpha} + \hat{\beta}_{AM} F_{AM}^{\alpha} + \hat{\beta}_T F_T^{\alpha} + \hat{\beta}_F F_F^{\alpha} + \hat{\beta}_{MP} F_{MP}^{\alpha} \quad (1)$$

Figure 1 illustrates these associations.

3.1 Differential Impact Analysis

We analyze how the predicted changes in a target variable for a district compares with the neighbouring districts' change. Thus, by changing factors Fj by x%, the predictive change in the target variable $O\alpha$ is calculated as,

$$\Delta O^{\alpha} = \left(\frac{x}{100}\right) \times \hat{\beta}_j \times F_j^{\alpha} \quad (2)$$

Figure 2 illustrate these associations. This formula is used to calculated in target change in the target variable GDDP for a specific district α when one of the influencing factors.

$\Delta O\alpha$ → Predected change in target variable GDDP for district α

x → Percentage change in the input factor increased or decreased (-20%, -10% , 10%, 20%).

$\hat{\beta}_j$ →Regression coefficient of the Fj learned from the model; it tells how sensitive the output GDDP is to change in Fj.

Current value of factor Fj in district α.

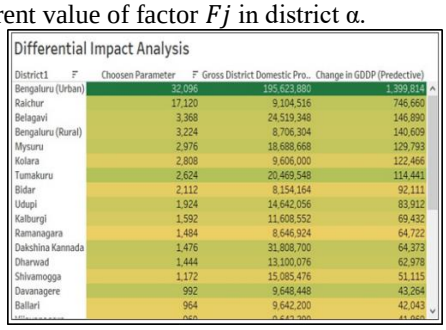


Figure 2: A tabular format graph shows the data that is based on chosen parameter, current value of GDDP and the Predictive Value of GDDP.

IV. Conclusion

This analysis explores the dynamic relation between industrial development and Gross District Domestic Product (GDDP) in Karnataka using regression-based modeling. Through the development of a predictive intervention dashboard, we identified seven key socio- economic variables that exhibit a significant correlation with GDDP at the district level. Our findings highlight the role of

industrial activity such as the No. of Factories, automobiles, and communication infrastructure as strong indicators of economic performance. We created a Predictive dashboard that shows the current economic standing of each district and also depict the changes in certain factors might affect future growth. This makes it easier for policymaker and planners to understand where to focus their efforts for better result. By aligning our study with Sustainable Development Goal 8: Decent work and Economic Growth, we emphasize the importance of using district level economic indicators like GDDP to support evidence-based governance.

ETHICAL STATEMENT

There are no ethics. All datasets employed in our research are accessible in the public domain and downloadable for free from government websites.

REFERENCES

[1] [Bassin et al., 2021] Pooja Bassin, Niharika Sri Parasa, Srinath Srinivasa, and Sridhar Mandyam.Big data management for policy support in sustainable development. In InternationalConference on Big Data Analytics, pages 3 15. Springer, 2021.

[2] https://www.researchgate.net/publication/358691761_Big_Data_Management_for_Policy_Support_in_Sustainable_Development

[3] [Dholakia et al., 2004] Dholakia, R. H., & Dholakia, B. H. (2004). State and district income estimation: Issues and some approaches. Economic and Political Weekly, 39(9), 911–920.

[4] https://www.epw.in/journal/2004/09/special-articles/state-and-district-income-estimation- issues-and-some-approaches.html

[5] [NITI Aayog, India SDG Dashboard] India SDG Dashboard. NITI Aayog.

[6] https://sdgindiaindex.niti.gov.in/

[7] [Oosterhof, 2018] Pytrik Dieuwke Oosterhof.Localizing the sustainable development goals to accelerate implementa tion of the 2030 agenda for sustainable development: The current state ofsustainable development goal localization in asia and the pacific. 2018.

[8] https://www.adb.org/sites/default/files/publication/472021/governance-brief-033-sdgs-implementation-2030-agenda.pdf

[9] [Paul et al., 2020] Paul, S., Bhuvaneshwari, A. P., & Thakur, R. (2020). Development index based on GDDP data for investment prioritization. Journal of Regional Development and Planning, 9(1), 45– 58.

[10] https://www.jrdp.in/index.php/jrdp/article/view/11 2 [Pai,T.V.Mohandas,Holla 2022]

[11] Pai, T.V.Mohandas, & Holla, N. (2022). Karnataka: A $1 Trillion GDP Vision. Government of Karnataka, Planning Department.

[12] https://planning.karnataka.gov.in/storage/pdf-files/Latest%20News/Karnataka%202022-One%20Trillion%20GDP%20Vision-Mohandas%20Pai%20Nisha%20Holla.pdf

International Journal of Computer Research & Technology
** A Blind Peer Reviewed Journal **
Volume-10, Issue-2, July-Dec 2025
ISSN 2454-7719
Paper ID: CS-05

Quantum Computing and Its Impact on Cryptography

Aquila Shaikh
Assistant Professor,
Late Bhausaheb Hiray S. S Trust's College Mumbai, India
aquishaik@gmail.com

Aakanksha Bhosle
Assistant Professor,
Late Bhausaheb Hiray S. S Trust's College Mumbai, India
Bhosle2002aaku@gmail.com

Abstract - *The power of quantum mechanics is leveraged by quantum computing to figure out difficult problems that classical computers cannot. Though the innovation promises new horizons, Conventional cryptographic systems based on math problems solvable with ease by quantum algorithms are also jeopardized by it.*

Commonly used encryption techniques are crackable by algorithms such as Shor's and Grover's, thereby threatening contemporary data security.Quantum-resistant cryptographic protocols are being developed by scientists in response to allow secure communication in the quantum age.

Post-quantum cryptography looks to develop encryption techniques that are quantum- resistant. Algorithms that will be secure even against future super-powerful quantum computers are being developed through current research to protect digital infrastructure for the future.

I. INTRODUCTION

The protection of digital communication, transactions, and data is ensured by cryptography, which depends on algorithms such as RSA and ECCs rooted in the computational hardness of mathematical problems. Yet, the eventual quantum computational breakthrough—powered by qubits and efficient quantum algorithms like Shor's and Grover's—severely undermines these conventional encryption techniques. Quantum computers can compute problems such as integer factorization and discrete logarithms at efficiency that could possibly obsolete present cryptographic schemes and make systems vulnerable to serious cybersecurity threats. Post-quantum cryptographic technologies, such as quantum-resistant algorithms from problems like learning with errors (LWE), are being created by researchers in a race. The fundamentals of quantum computing, its revolutionary effect on traditional cryptographic systems, and new ways of maintaining secure communication in the quantum age are delved into in this paper.

II. LITERATURE REVIEW

Extensive research has focused on the interaction of quantum computing and cryptography. It was proven by Shor's (1994) algorithm that integers can be factored in polynomial time by a quantum computer, threatening RSA encryption. Quadratic speedup for unstructured search problems is offered by Grover's algorithm (1996), disrupting symmetric cryptographic systems. Post-quantum cryptography was presented by Bernstein et al. (2008), with cryptographic approaches suggested to be immune to quantum attacks. Lattice-based, code-based, hash-based, and multivariate polynomial cryptography are considered as promising alternatives in subsequent works. The following works consider lattice-based, code-based, hash-based, and multivariate polynomial cryptography as promising alternatives.

Fundamentals of Quantum Computing Principles of superposition, entanglement, and quantum parallelism are applied by quantum computing to perform calculations that are computationally intractable for traditional computers.

Unlike binary classical bit states (0 or 1), multiple states can be simultaneously existed in by

qubits, significantly enhancing computational power. Quantum computers are hence able to find solutions to computationally challenging mathematical problems, such as integer factorization and database search, much quicker than traditional computers. The ability of quantum computing to compromise traditional cryptosystems and enhance problem-solving across various areas of study is demonstrated by some of the major quantum algorithms, such as Shor's algorithm and Grover's algorithm.

III. Quantum Bits, Superposition, and Entanglement.

Quantum Bits

Unlike bits in classical computing that are either 0 or 1, a superposition of both states at the same time can exist in by qubit. This property makes quantum computers run instructions in parallel and thus with much higher capability than their classical counterparts. Qubits also happen to be entangled, adding to capability in computing and security in communication.

IV. Superposition

A qubit is enabled by superposition to exist as 0 and 1 at the same time instead of flowing through one by one. Superposition enhances computational power exponentially, whereby quantum computers are capable of processing several possibilities all at once. Intricate problems, including factorization and search functions, can thus be effectively solved by quantum algorithms far more quickly than by their classical counterparts.

V. Entanglement

Entanglement is quantum in nature and is a phenomenon that occurs when two or more qubits become entangled, such that the state of one qubit is simultaneously affected by another, regardless of the distance between them. Quantum communication is allowed to be very fast by this feature, and the computation speed is enhanced. The foundation of Quantum Key Distribution (QKD), which enables very secure data transmission, is also formed by entanglement.

VI. Quantum algorithms.

Quantum computers offer faster and better algorithms that can compute very efficient mathematical problems at far higher rates than normal computers. Formidable challenges to conventional cryptographic security are posed by two of the most important quantum algorithms, Shor's Algorithm and Grover's Algorithm.

VII. Shor's Algorithm

RSA and ECC encryption are directly attacked by Shor's algorithm, which is a polynomial-time integer factoring algorithm. The premise that integer factorization is hard is the basis for classical cryptographic systems in the style of RSA to be secure, but this problem can be factorized exponentially faster by Shor's algorithm than by classical algorithms. Being able to feasibly compute the prime factors of large integers, Classic public-key cryptosystems are made insecure against the power of sufficiently large quantum computers by Shor's algorithm.

VIII. Grover's Algorithm

A quadratic speedup for searching unsorted databases is offered by Grover's algorithm, which is a quantum search algorithm. It does not entirely break symmetric-key cryptosystems such as AES but halves the effective key. For instance, AES-256 classically secure would see its effective security brought down to AES-128 in quantum attack. This renders symmetric encryption weaker and requires larger key sizes or the utilization of quantum-resistant alternatives.

IX. How Quantum Computing Differs from Classical Computing

Quantum computing is distinguished from classical computing in several aspects, the first of which is the utilization of qubits and quantum mechanics. Here are the key differences:

1. **Data Representation:** Bits (0 or 1) are relied on by classical computers, whereas qubits that can be in superposition (0 and 1) are employed by quantum computers.
2. **Computational Power:** Parallelism is utilized by quantum computers, and issues are computed faster than by conventional computers.
3. **Superposition & Entanglement:** The ability to be in many different states and to be entangled simultaneously is possessed by qubits, whereby information can be conveyed instantly.
4. **Algorithmic Performance:** Exponential and quadratic improvement over conventional methods is exhibited by

quantum algorithms such as Shor's and Grover's.

5. **Error Correction: Quantum** systems need sophisticated error correction since they are afflicted with decoherence problems.
6. **Security Implications:** Classical cryptography would be broken by quantum computing, thereby making post-quantum cryptography necessary.

X. THE IMPACT ON CRYPTOGRAPHY IS CAUSED BY QUANTUM COMPUTING

1. **Threats to Classical Cryptographic Systems**

- Classical cryptography is still based on hard mathematical problems (integer factorization, discrete logarithm).
- Quantum computing puts these assumptions into jeopardy, rendering traditional encryption obsolete.

2. **Weaknesses are found in public- key cryptography, such as RSA and ECC**

- RSA & ECC: Shor's algorithm can easily factor large numbers and compute discrete logarithms, which breaks RSA, ECC, and Diffie- Hellman.

3. **Impact on Symmetric Cryptography**

- **AES & Other Symmetric Algorithms:** Grover's algorithm decreases brute- force search time by essentially cutting key strength in half. Security requires the expansion of key sizes.

4. **Threats to Hash Functions**

- **SHA-256 & Other Hash Functions**: Grover's algorithm undermines hash Functions by lowering collision resistance, necessitating longer hash outputs.

XI. QUANTUM COMPUTING

Principles of quantum mechanics, a field of physics applied to describe how particles respond at the subatomic level, are borrowed by quantum computing. In contrast, while calculations are performed by ordinary computers using binary bits (0s and 1s), qubits (quantum bits) that exist in superposition of more than one state simultaneously due to an effect called superposition are employed by quantum computers. Entanglement, a quantum phenomenon wherein two qubits may become so entangled that the status of one is immediately dependent on the status of the other regardless of the distance between them, is also employed by quantum computers. The potential to enable solutions to certain problems to be calculated exponentially faster than by traditional computers is possessed by these strange properties of quantum computers. Quantum computing is now regarded as an immature branch of science, but one with monumental potential application in numerous fields, such as optimization, materials science, medicinal chemistry research, and, most notably, cryptography.

XII. POST-QUANTUM CRYPTOGRAPHY

- Cryptographic algorithms that are quantum-attack-resistant are created through Post-Quantum Cryptography (PQC). Because quantum computers jeopardize classical encryption, researchers try to develop safe alternatives:
- **Lattice-Based Cryptography:** Deploys hard lattice problems (LWE, Ring-LWE) for quantum computers. (e.g., Rainbow, Dilithium)
- **Code-Based Cryptography:** Deploys error-correcting codes; the leading candidate is considered to be the McEliece cryptosystem.
- **Multivariate Polynomial Cryptography:** Employing polynomial equations for security; e.g., Rainbow signatures.
- **Hash-Based Cryptography:** Uses hash functions to provide secure digital signatures (e.g., SPHINCS+).

XIII. CASE STUDY: GOOGLE'S QUANTUM SUPREMACY EXPERIMENT

Overview

A computational task was processed by Google's 53-qubit processor, Sycamore, in 200 seconds, which, according to Google's AI Quantum group in 2019, would supposedly take the world's most powerful classical supercomputer 10,000 years, thus achieving quantum supremacy. The actual task was not necessarily of direct importance in terms of cryptography problems, but the demonstration raised the question of whether scalable quantum hardware can be achieved.

XIV. IMPLICATIONS FOR CRYPTOGRAPHY

The test set the near-actuality capability of quantum systems of this strength into perspective.

As much as Sycamore's purpose was specialized, it was shown that the technology to perform the general-purpose quantum computers capable of executing algorithms such as Shor's is near. Once appropriately large quantum computers exist, systems such as RSA and ECC, which are based on the intractability of factorization and discrete logarithm problems, would be broken by the capability of Shor's to factor numbers effectively.

XV. REACTIONS AND PREPARATIONS

The effort to standardize post-quantum cryptography algorithms was sped up by institutions like the National Institute of Standards and Technology (NIST) as a reaction. Companies like IBM and Microsoft also ramped up investment in creating quantum-safe alternatives. Google has started including post-quantum algorithms in experimental TLS implementations, though.

Quantum Cryptography Innovations Quantum computing accelerates classical cryptography designs to the edge of atastrophic breakdown with the onset of age. New paradigms for security, protecting information from quantum attacks, are offered by quantum cryptography. New security benefits are offered by two significant aspects of quantum cryptography: Quantum Key Distribution (QKD) and Post-Quantum Cryptography (PQC).

1. Quantum Key Distribution and Its Security Advantages

An encryption protocol based on quantum mechanics that provides ultra-secure key exchange is represented by Quantum Key Distribution (QKD). In contrast to computationally challenging classical encryption, security is provided by QKD using the axioms of quantum mechanics itself.

XVI. KEY FEATURES AND SECURITY ADVANTAGES OF QKD

- **Unbreakable Security** – Physical laws, rather than mathematical complexity, form the basis of QKD, making it not vulnerable to quantum attacks.
- **Eavesdropping Detection** – Quantum entanglement and superposition are applied by QKD to detect whether an interception attempt has occurred. When the key is intercepted by the interceptor, the quantum state collapses and both parties are alerted.
- **End-to-End Security over a Long Duration** – Because factorization and discrete logarithm independence are characteristics of QKD, security is maintained even against future quantum computers.
- **Applied in Quantum Networks –** QKD is already being employed in quantum-safe communication networks, i.e., China's Micius satellite and Europe's EuroQCI program.

2. Post-Quantum Cryptography (PQC) vs. Quantum Cryptography (QKD) at a Glance

- **Foundation of Security:**
  Hard math problems are relied on by PQC, whilethe laws of quantum mechanics are relied on by QKD.
- **Vulnerability:** PQC is still theoretically breakable someday but QKD is theoretically unbreakable.
- **PRACTICALLY:** Existing digital infrastructure can be used by PQC, whereas custom-built quantum hardware is required by QKD.
- **DEPLOYMENT:** PQC is standardizing for mass deployment of systems, whereas QKD is mainly being used in ultra-high-security environments.
- **DATA PROTECTION:** PQC encrypts data, whereas QKD offers secure key exchange.

XVII. CHALLENGES IN TRANSITIONING TO QUANTUM- SAFE SYSTEMS

An imperative but demanding process, quantum-resistant cryptography transition needs to be undertaken with thought, investment, and cooperation by organizations, authorities, and researchers. The most significant obstacles inherent in this change are as follows:

1. Implementation Challenges for rganizations and Governments

Transitioning from classical cryptographic schemes to quantum-resistant ones is not an easy task. Encryption is depended on by governments, organizations, and businesses alike to secure confidential information, and a great deal of work is required to transition existing cryptographic infrastructures. Some of the primary challenges in their implementation include:

- **Legacy System Support:** RSA, ECC, and other classical cryptographic techniques are in heavy utilization by most currently running systems. Legacy infrastructure support in addition to security is demanded by the implementation of

post-quantum cryptography (PQC).

- **Cost and Effort:** Money will have to be spent by organizations on new hardware, software, and training personnel in order to deploy quantum-resistant solutions that are expensive and labor-intensive.
- **Regulation and Policy:** Standards and regulations for implementing quantum-safe cryptography will have to be established by governments, with security and compliance mandated across all industries.

2. Computational and Infrastructural Requirements

Quantum-resistant cryptosystems will consume more computational power and storage than their non-quantum counterparts. Some of the most urgent infrastructural issues are identified as:

- **Greater Processing Capacity:** The vast majority of post-quantum cryptographic techniques involve larger key sizes and more sophisticated mathematical computations, which need greater levels of computational capacity.
- **Hardware and Software Enhancements:** Encryption networks, systems, and key management systems have to be enhanced by firms to support newer cryptographic techniques.
- **Scaling Challenges:** Integrating quantum-resistant encryption techniques into practical application in humongous digital systems, A daunting challenge is posed by technologies such as cloud computing and IoT devices.

3. Global Coordination and Standardization Requirements

Cooperation between governments, standards bodies, and a successful quantum- safe transition must be achieved through cooperation across the industry on an international level. Among some of the most important considerations are included:

- **International Standardization Efforts:** Efforts by organizations such as NIST, ISO, and ETSI to establish post-quantum cryptographic standards exist, but their worldwide uptake is a time-consuming effort.
- **Cross-Border Cooperation:** Level- playing use of quantum-safe cryptographic protocols is necessary for secure global communication and data exchange.
- **Widespread Adoption in Industry:** Security policies must be coordinated by banks, healthcare institutions, defense organizations, and technology firms to enable a smooth transition to quantum-resistant cryptography.

XVIII. Future of Cryptography in the Quantum Era

As quantum computing continues to advance, cryptographic security is increasingly significantly affected by it. While encryption methods are still secure currently, vulnerability will be faced by them at some point when large-scale quantum computers are constructed. In the interest of offering long-term data protection, methods to transition to quantum-resistant cryptographic technologies must be started to be developed by scientists, governments, and businesses must be started to be developed by scientists, governments, and businesses. The future of cryptography is looked at in this chapter, from the projected timeline for the advent of quantum computing to the implementation of quantum-resistant cryptographic techniques, and on to long-term security measures that will safeguard digital communication.

XIX. Timeline for Large-Scale Quantum Computing Development

- **Short-Term (Present – 2030):** Quantum computers are in the NISQ (Noisy Intermediate-Scale Quantum) phase, with limited abilities but gradual progress in the stability of qubits and error correction.
- **Mid-Term (2030 – 2040):** Classical cryptography starts to be threatened by improved quantum computers, and the employment of post-quantum cryptography (PQC) becomes inevitable.
- **Long-Term (2040+):** The arrival of fully fault-tolerant quantum computers occurs, and worldwide deployment of quantum-resistant security is started.

XX. Quantum-Safe Cryptographic Solutions Integration

- **Post-Quantum Cryptography (PQC):** Cryptographic primitives like lattice-based, hash-based, and code-based cryptography are being designed to be quantum-resistant.
- **Hybrid Cryptography Systems:** New meeting old for harmonious coexistence.
- **Quantum Key Distribution (QKD):** Ultra-security is provided using quantum mechanics

with absolutely no eavesdropping.

- **Industry Adoption:** Encryption methods should be revised by governments, banks, and cloud service providers to protect sensitive information.

XXI. Long-Term Security Strategies and Ongoing Research Studies

- **Cybersecurity Infrastructure Upgrades:** Quantum-resistant encryption protocols must be shifted to by organizations.
- **Global Standardization:** NIST, ISO, and ETSI initiatives are collaboratively developing international post-quantum cryptography standards.
- **Quantum-Secure Networks:** Developing Quantum Internet and QKD-based networks to secure communication.
- **Cybersecurity Training & Awareness:** Developing awareness among security professionals regarding the quantum transition through training and research.

XXII. Conclusion

A deep threat and an opportunity for innovation in the future of cryptographic security are posed by quantum computing. As the roots of classical encryption are threatened by new efficient quantum algorithms such as Shor's and Grover's, the urgency for post-quantum cryptographic alternatives is brought to light. Innovation in quantum-resistant schemes such as lattice- based cryptography and quantum key distribution has been catalyzed by the transition to protect digital networks for the quantum age. For the sake of a secure future, early collaborative efforts are required by researchers, organizations, and policy- makers to facilitate research, development, and standardization of quantum-safe protocols. Thinking ahead and adopting these innovations, we can avert quantum computing threats and provide long-term security for data and digital communication.

References

[1] Shor, P. W. (1994). "Algorithms for quantum computation: The topics of discrete logarithms and factoring were covered in the Proceedings of the 35th Annual Symposium on Foundations of Computer Science.

[2] A fast quantum mechanical algorithm for database search was developed by Grover, L. K. (1996)". The 28th Annual ACM Symposium on Theory of Computing was documented in the proceedings.

[3] Bernstein, D. J., Buchmann, J., & Dahmen,

[4] E. (Eds.). (2008). Post- Quantum Cryptography. Springer.

[5] Arute, F., Arya, K., Babbush, R., et al. (2019). "Quantum supremacy was demonstrated using a programmable superconducting processor". Nature, 574(7779), 505–510.

[6] National Institute of Standards and Technology (NIST). (2016). "Post- Quantum Cryptography: NIST's Plan for the Future".Chen, L. et al. (2016). "Report on Post-Quantum Cryptography". NISTIR

International Journal of Computer Research & Technology
ISSN 2454-7719
** A Blind Peer Reviewed Journal **
Volume-10, Issue-2, July-Dec 2025

Paper ID: CS-06

AI in Education: Personalized Learning and Beyond

Prof. Ashwini Hemant Patil

Assistant Professor

Godavari Institute of Management and Research College, Jalgaon

patilashwinih812@gmail.com

Abstract - *Artificial Intelligence is a method of making a computer, a computer-controlled robot, or a software think intelligently like the human mind. AI is accomplished by studying the patterns of the human brain and by analyzing the cognitive process. The outcome of these studies develops intelligent software and systems.*

Artificial Intelligence is no longer a futuristic idea—it's already transforming the landscape of education. From tailoring learning experiences to streamlining school operations, AI is redefining how education is delivered and managed. As its presence continues to grow within classrooms and institutions, it brings new possibilities for customized instruction, improved efficiency, and enhanced learning outcomes. In this blog, we explore the current developments in AI-powered education and consider the innovations that may shape its future.

Keywords (Size 10 & Bold)— *AI in Education, Artificial Intelligence in Education, Personalized Learning with AI, Education Technology (EdTech),AI-Powered Learning, Intelligent robots, Humans, Brain Spired, Computerized monitoring, Automatic control*

I. INTRODUCTION

The intersection of Artificial Intelligence (AI) and education has become a powerful catalyst for change, significantly altering traditional teaching models and expanding the scope of personalized learning (Bahroun et al., 2023; Haider, 2023; Mustafa, 2023). This review offers a detailed examination of the evolving Issues such as data privacy, algorithmic transparency, and ethical considerations must be thoughtfully addressed. This review recognizes these concerns and emphasizes the need for well-defined ethical guidelines to ensure the responsible and equitable use of AI in educational contexts.

By exploring the interconnected roles of AI, personalized learning, and educational technologies, this review aims to provide a comprehensive understanding of current trends and emerging directions. As educators, researchers, and policymakers continue to engage with this shifting educational landscape, a deeper understanding of the relationship between technology and pedagogy is essential to building a more inclusive, fair, and effective future for learners around the world.

Key Benefits of AI for Students:

1. Higher Engagement Levels

AI creates learning experiences aligned with students' interests and abilities, making lessons more interactive and relevant. Personalized content keeps students interested and encourages active participation.

II. LITERATURE REVIEW

A. Personalized Learning and Adaptive Technologies

AI is playing a growing role in shaping personalized learning experiences for students. By analyzing individual learning behaviors, abilities, and preferences, AI tailors educational content to match each student's unique needs. This customized approach enhances understanding and engagement by focusing on specific learning patterns and challenges.

Adaptive learning platforms, powered by artificial intelligence and machine learning algorithms, process large volumes of student data to identify areas of strength and weakness. These systems use this data to generate individualized

learning paths that align with the student's academic goals, learning style, and progress pace.

B. Student-Centered Benefits of AI in Education

Traditional teaching methods often follow a uniform approach, which can be discouraging for students who learn in different ways. This can lead to disengagement and a lack of motivation, especially when the material feels irrelevant or too challenging. Students may also require additional support to grasp certain topics and keep pace with their peers.

Artificial Intelligence offers a solution by personalizing education to fit each learner's needs. It adapts in real time to a student's learning style and progress. By analyzing performance data, AI determines whether a student is ready to advance or needs more time and resources to fully grasp a concept. This tailored approach improves comprehension, retention, and overall learning outcomes.

C. *Key Benefits of AI for Students*:

1. Higher Engagement Levels

AI creates learning experiences aligned with students' interests and abilities, making lessons more interactive and relevant. Personalized content keeps students interested and encourages active participation.

2. Learning at an Individual Pace

Every learner progresses at a different speed. Adaptive learning systems adjust the flow of content to suit each student's pace—slowing down when needed or speeding up when a topic is well understood. This ensures students don't feel overwhelmed or held back.

3. Customized Learning Approaches

AI accommodates various learning preferences, whether a student learns best through visuals, audio, interaction, or reading. It delivers information in the most effective format for each individual, enhancing the overall learning experience.

4. Better Concept Clarity

By pinpointing areas of confusion, AI offers targeted resources—such as practice problems, step-by-step explanations, or supplemental videos—to reinforce difficult topics. This strengthens understanding and helps students retain what they've learned.

5. Improved Accessibility

AI technologies like speech recognition, text-to-speech, and natural language processing (NLP) support students with different needs. These tools help answer questions, clarify concepts, and make learning more inclusive for students with disabilities or language barriers.

6. Learning through Gamification

One exciting use of AI is integrating game-like elements into educational content. Gamified learning makes studying more enjoyable and encourages students to stay engaged through challenges, rewards, and interactive formats.

7. Development of Essential Skills

AI doesn't just support academic learning—it also helps nurture important life skills. By encouraging exploration and problem-solving, AI-powered platforms foster critical thinking, creativity, and adaptability, giving students tools for both school and future careers.

AI for Educators

AI in education offers not only enhanced learning for students but also substantial support for teachers. Educators are increasingly integrating AI across various areas—including teaching strategies, assessment practices, curriculum design, and personalized instruction. By automating repetitive tasks, generating actionable insights from student data, and helping customize lesson content, AI empowers teachers to focus on what truly matters: engaging and supporting their students.

With the help of AI, teachers can gain a clearer picture of each student's progress, strengths, and challenges—free from subjective bias. AI systems analyze learning patterns and provide educators with meaningful information that can guide their instructional decisions. Beyond simply reducing workload, AI contributes to smarter curriculum planning and more effective classroom management.

Key Benefits of AI for Teachers:

1. Automating Routine Tasks

Tasks like grading, attendance tracking, and schedule management often consume a significant portion of a teacher's time. AI tools can take over these responsibilities, allowing educators to devote more energy to teaching and mentoring students.

2. Customizing Lesson Plans

AI systems provide real-time data about student learning progress. Teachers can use this information to identify knowledge gaps and adjust their lesson plans accordingly, offering targeted instruction without the need to manually tailor content for each learner.

3. Enhancing Curriculum Design

By analyzing trends in student performance, AI can pinpoint areas of the curriculum that need strengthening. This enables educators to refine and adapt their instructional materials, ensuring they align more closely with students' needs and academic goals.

4. Smarter Assessment Tools

AI-powered assessment platforms offer fast, accurate, and unbiased feedback. These tools not

only reduce the grading burden on teachers but also give them a deeper understanding of each student's development, helping them adjust their approach based on clear evidence.

5. Boosting Overall Efficiency

With AI handling time-intensive tasks, educators can prioritize more meaningful interactions with students. This results in improved teaching effectiveness and allows for better time management, contributing to a healthier work-life balance for teachers.

III. METHODOLOGY

A. Current Trends in AI in Education

AI is being used in many ways to improve how students learn and how schools operate. Here are some of the most important trends:

1. Personalized Learning

AI can study how students learn, what they're good at, and where they need help. It then adjusts lessons to fit each student's needs. Learning platforms like DreamBox and Knewton use this approach to give students lessons that change as they improve.

2. Smart Tutoring Systems

AI tutors, like those used in Carnegie Learning and Squirrel AI, give students one-on-one help. These systems figure out where a student is having trouble and provide extra support in those areas.

3. Automated Grading

AI tools can help teachers by grading assignments and tests automatically. For example, Gradescope uses AI to grade written work, saving time and ensuring fair, consistent results.

4. AI Chatbots and Language Tools

AI-powered chatbots and voice assistants make it easier for students to get help. Apps like Duolingo and Coursera use Natural Language Processing (NLP) to answer student questions and guide them through lessons in real time.

5. Data Insights for Teachers

AI can also help teachers understand how students are doing. Tools like BrightBytes and Civitas Learning look at student data to spot those who may need extra help and suggest ways to support them.

B. TRANSFORMATIVE IMPACT OF AI ON EDUCATION

AI is changing the way students learn and how teachers manage classrooms. Here are some of the major ways AI is making a difference:

1. More Engaging Learning Experiences

AI creates dynamic and personalized learning environments. With tools like intelligent tutors and immersive technologies such as virtual and augmented reality, students can enjoy more interactive and tailored lessons.

2. Greater Accessibility for All Learners

AI helps make education more inclusive. Tools like speech-to-text software, real-time language translation, and adaptive interfaces support students with disabilities and those who speak different languages.

3. Streamlined Administrative Work

Routine tasks such as grading, creating schedules, and tracking attendance can now be handled by AI systems. This reduces workload for teachers and gives them more time to focus on teaching and supporting students.

4. Smarter Use of Student Data

AI tools analyze student performance and behavior in real time. This helps educators identify learning gaps, track progress, and apply strategies to support students more effectively.

C. The Future of AI in Education

Artificial intelligence continues to advance, its influence on education is expected to grow significantly. Below are some key developments that may shape the future of teaching and learning:

1. Support for Lifelong Learning

AI will play a crucial role in enabling continuous learning by offering customized, on-demand content. Learners of all ages will be able to access education tailored to their goals, helping them adapt to evolving career demands and industries.

2. Expanding Access to Quality Education

With the help of AI-powered platforms, students in underserved or remote regions can gain access to high-quality educational content. These scalable solutions can help reduce global disparities in education and promote equal learning opportunities for all.

3. Ethical Use and Data Security

As AI tools handle more sensitive information, ensuring ethical practices and data protection will become even more critical. Educational institutions must adopt strong policies that safeguard student privacy and promote fair, transparent use of AI technologies.

4. Changing Role of Teachers

As AI takes over routine tasks like grading and content delivery, educators will transition into roles

that emphasize mentoring, guiding discussions, and supporting students' emotional and social development. Human interaction will remain a vital part of meaningful education.

5. Emphasis on Interdisciplinary Learning

AI can help connect different fields of knowledge, encouraging students to engage in cross-disciplinary, project-based learning. This integrated approach—combining science, technology, engineering, arts, and math (STEAM)—will prepare learners to solve complex real-world problems creatively.

IV. DISCUSSION

Technical and Financial Challenges

The adoption of AI-powered personalized learning systems often encounters significant technical and budgetary obstacles, especially in schools with limited funding. The initial investment required for the necessary infrastructure—including hardware, software, and ongoing technical support—can be a major barrier for many educational institutions.

Moreover, the successful integration of AI into the classroom demands continued financial commitment to areas such as teacher training, data security, and system upkeep. These added expenses can place a heavy strain on already stretched school budgets, making it difficult for many to adopt and sustain such technologies.

To bridge these gaps, strong collaboration is needed among policymakers, educational administrators, and technology providers. Joint efforts will be essential to make AI-based personalized learning tools accessible across all schools—regardless of their financial standing.

Addressing these issues is vital to the ethical and effective implementation of AI in education. Ensuring equitable access, protecting student data, and preserving the critical role of teachers must remain central as we work toward realizing AI's full potential in transforming learning experiences.

The Role of Social and Emotional Learning (SEL)

AI-driven personalized learning continues to shape modern education, it is equally important to emphasize the development of students' social and emotional competencies. While AI can significantly enhance academic performance and technical skills, fostering emotional intelligence, empathy, and interpersonal abilities remains essential for well-rounded student growth and lifelong success.

Educators play a key role in promoting Social and Emotional Learning (SEL) within the school environment. By embedding SEL into everyday classroom practices and lessons, teachers can help students build crucial life skills—including self-awareness, emotional regulation, empathy, relationship-building, and sound decision-making. These attributes are vital complements to the academic and cognitive skills strengthened by AI-based learning tools.

Striking a thoughtful balance between advanced technology and the human aspects of education allows schools to cultivate well-rounded learners. When AI is combined with intentional SEL strategies, educational institutions can create supportive, inclusive environments where students thrive not only intellectually but also emotionally and socially.

This integrated approach prepares learners to face the complexities of the 21st century with confidence, adaptability, and emotional resilience.

Challenges and Ethical Considerations

AI holds great promise for transforming education, it also brings with it several important challenges and ethical issues that must be thoughtfully addressed:

1. Protecting Student Data and Privacy

AI systems rely heavily on data to operate effectively. In educational settings, this data often includes sensitive information such as student performance, learning behaviors, and personal profiles. Ensuring the ethical collection, storage, and use of this data is critical. Schools and developers must implement robust data protection measures to safeguard student privacy and prevent misuse.

2. Algorithmic Bias and Fairness

AI tools make decisions based on the data they are trained on. If that data contains existing social, cultural, or academic biases, the AI system may unintentionally reinforce them. This can result in unfair treatment or skewed learning recommendations. To counter this, educators and developers must actively audit and refine AI systems to minimize bias and ensure fairness across all student groups.

3. Ensuring Inclusive Access

Not all AI-based educational tools are built with universal accessibility in mind. Students with disabilities may face difficulties if platforms are not designed to accommodate diverse needs. It's vital that inclusivity is a core principle in AI tool development, ensuring equal learning opportunities

for students regardless of their physical or cognitive abilities.

AI-Powered Tools Enhancing Education

With rapid advancements in technology, Artificial Intelligence is driving a new wave of innovation in the educational sector. AI systems are capable of processing large datasets and replicating human-like thinking to make data-informed decisions. These AI-driven tools are transforming learning by delivering more personalized, inclusive, and interactive educational experiences for students.

Here are some of the most influential AI-powered tools reshaping the classroom:

1. Virtual Learning Assistants

Virtual learning assistants are smart systems that utilize natural language processing (NLP) and machine learning (ML) to engage students in interactive dialogue. These AI tutors personalize the learning journey by adapting content and teaching style to match each student's pace and preferences, making learning more intuitive and enjoyable.

2. Smart Content Recommendation Engines

These tools analyze user data—such as past performance, interests, and behavior—to recommend study materials that align with individual learning needs. By offering curated content suggestions, these systems save students time and introduce them to a broader range of topics and perspectives.

3. AI-Based Assessment Tools

Unlike conventional testing methods, AI-driven assessment tools provide instant feedback and detailed insights into a student's performance. These systems detect gaps in knowledge, evaluate comprehension in real time, and offer personalized feedback, enabling learners to address their weaknesses promptly.

4. Gamified Learning Environments

Gamified platforms use game mechanics—such as levels, points, and badges—within educational contexts to motivate learners. When powered by AI, these platforms can adapt challenges and rewards based on a student's skill level and engagement, promoting active participation and continuous improvement.

5. Conversational AI and Chatbots

AI chatbots serve as 24/7 virtual assistants that can handle a wide range of student inquiries—from course content clarification to deadline reminders. Using NLP, these bots deliver quick, tailored responses, allowing teachers to focus on more complex instructional tasks.

6. Adaptive Tutoring Systems

Also known as Intelligent Tutoring Systems (ITS), these platforms merge AI with learning sciences to create highly customized educational experiences. By analyzing how a student interacts with the system—such as response times, mistakes, and progress—ITS tools adapt instruction in real time, providing detailed feedback and support based on individual learning profiles.

7. Tools Powered by Natural Language Processing (NLP)

NLP bridges the gap between human communication and computer understanding. In education, NLP-enabled tools assess both spoken and written student responses. Teachers can use these tools for tasks like essay grading, language evaluation, and grammar correction. Additionally, NLP tools support language learners by helping them improve fluency, vocabulary, and writing structure.

V. CONCLUSION

AI is reshaping the educational landscape by introducing innovative tools and strategies that enhance learning outcomes, promote equity, and increase efficiency. Looking ahead, its potential to transform education is immense—offering more customized, inclusive, and flexible learning environments.

However, as we adopt these technologies, it is vital to remain mindful of privacy risks and ethical challenges. Responsible implementation will ensure that AI serves as a powerful ally in education rather than a source of concern.

The journey ahead will require collaboration among educators, learners, technologists, and policymakers. By embracing both the opportunities and challenges of AI, we can build an education system that not only adapts to the future—but helps shape it for generations to come.

AI will transform education by personalizing learning experiences and enhancing teaching practices. It addresses various challenges faced by the education sector. It promises equal opportunities for all students through inclusive and accessible education globally. However, responsible use of AI in education is crucial to ensure ethical considerations are met, accessibility is prioritized, and students' rights are protected. Harnessing the full potential of AI in education requires continuous research and monitoring to ensure its effectiveness and sustainability.

REFERENCES

[1] https://www.googleadservices.com/pagead/aclk?sa=L&ai=DChcSEwib7Y3ht7aNAxWeqGYCHc1eAjwYABABGgJzbQ&co=1&gclid=CjwKCAjw87XBBhBIEiwAxP3_

[2] AI in education: A review of personalized learning and educational technology GSC Advanced Research and Reviews, 2024, 18(02), 261–271 Publication history: Received on 03 January 2024; revised on 11 February 2024;accepted on 13 February 2024 Article DOI: https://doi.org/10.30574/gscarr.2024.18.2.0062

[3] https://www.researchgate.net/publication/390163119_AI_in_education_A_review_of_personalized_learning_and_educational_technology

[4] https://www.researchgate.net/publication/385612864_The_Future_of_Education_Personalized_Learning_and_Artificial_Intelligence

International Journal of Computer Research & Technology
** A Blind Peer Reviewed Journal **
Volume-10, Issue-2, July-Dec 2025
ISSN 2454-7719
Paper ID: CS-07

The Influence of IOT for Smart Homes In Nagercoil

Dr. C. S. Goldie Sheila Jesolit

Department of Commerce, Women's Christian College, Nagercoil - 629001
(Affiliated to Manonmaniam Sundaranar University, Abishekapatti, Tirunelveli - 627012)
Tamil Nadu, India
Email: goldiesheilajesolit@yahoo.com

Dr. Chithra James
Assistant Professor,
Department of Commerce, Women's Christian College, Nagercoil - 629001
(Affiliated to Manonmaniam Sundaranar University, Abishekapatti, Tirunelveli - 627012)
Tamil Nadu, India.
Email: chithrajames@yahoo.com

Abstract - *The Internet of Things (IoT) has revolutionized the concept of modern living, particularly through the development of smart homes that enhance convenience, energy efficiency, and security. This study investigates the influence of IoT-enabled smart home technologies in Nagercoil, Kanyakumari district, Tamil Nadu, focusing on adoption trends, user awareness, perceived benefits, and existing barriers. With a sample size of 75 households, data was collected through structured questionnaires and in-depth interviews. The findings reveal a growing interest in smart home applications such as automated lighting, smart surveillance systems, energy-efficient appliances, and remote access control. However, the study also identifies several challenges impeding wider IoT adoption. These include high initial installation costs, limited awareness, concerns over data privacy, lack of skilled technicians, and inconsistent internet infrastructure in remote areas. Despite these challenges, the perception of IoT as a symbol of progressive living continues to gain traction, especially among younger and tech-savvy homeowners. The research emphasizes the need for awareness programs, government incentives, and infrastructure upgrades to facilitate broader access to smart home technology. This study contributes to the growing body of knowledge on smart home innovation and offers practical insights for stakeholders aiming to promote IoT-based living in regional India.*

Keywords: *Artificial Intelligence (AI), Internet-of-Things, Smart Homes, Technology, Digital*

I. INTRODUCTION

1.1. Introduction to Topic

The concept of a smart home is rooted in the broader framework of intelligent environments, which are designed to sense, interpret, and respond to various environmental stimuli to deliver adaptive and user-focused services. A smart home leverages this intelligence to create a living space that is not only efficient and convenient but also responsive to the needs and preferences of its occupants. Through the integration of advanced technologies, smart homes enable the seamless monitoring and management of household activities, even from remote locations. This includes supervising children, elderly family members, pets, and valuable household items, providing peace of mind and enhancing overall safety.

Smart home systems offer a wide array of benefits. These include the creation of a more secure living environment through real-time surveillance and automated alerts, increased comfort through personalized settings for lighting, temperature, and entertainment, and the promotion of sustainability through energy-efficient practices. (Hajj et. al. 2019)i.

At the core of smart home functionality lies the Internet of Things (IoT), which facilitates the interconnection of various digital devices within the home. These devices may include smart thermostats, security cameras, lighting systems, home appliances, and more. The smart home operates through a network of sensors and control units installed throughout the house, which collectively form a wireless sensor network (WSN). These devices continuously collect data related to environmental conditions, user behavior, and system performance.

The IoT infrastructure is essential for managing the complex web of connectivity between devices and gateways. It ensures seamless communication, interoperability, and synchronization among different components of the smart home ecosystem. By enabling intelligent automation and user engagement, IoT-based smart homes represent a transformative step toward more efficient, secure, and personalized living spaces. (Singh, Khan and Senthil, 2021).

1.2. Objectives

- To identify the most commonly used smart home function.
- To examine the benefits of IoT on smart homes among the users.
- To assess the challenges faced while using IoT based devices on smart homes

1.3. Hypothesis

- H_{01} – There is no significant mean difference among the functions of IoT based on smart homes.
- H_{02} - There is no significant mean difference among the benefits of IoT on smart homes among the users.
- H_{03} – There is no significant difference between education and the challenges faced while using IoT based devices on smart homes.

1.4. Research Methodology

For this study, the researcher utilized a convenience sampling method to collect data from 75 respondents living in the Kanyakumari District. Primary data was gathered through a carefully structured questionnaire, while secondary data was drawn from relevant journals, books, online databases, and transcripts. The collected data was analyzed using a range of statistical tools, including Percentage Analysis, the Friedman Test, One-Sample t-Test, and One-Way ANOVA, all executed with the help of SPSS software.

II. REVIEW OF LITERATURE

Al-Mutawa and Albouraey (2020)[ii] conducted a study titled "A Smart Home System Based on Internet of Things" with the primary aim of enhancing smart home security through a multi-factor authentication approach to prevent unauthorized access. The proposed solution includes essential modules for remotely managing sensors and actuators. A key contribution of the study is the development of a login module designed to handle user registration and operations. This login system is based on multi-factor authentication and is supported by a notification module that alerts the system administrator in case of any suspicious registration or login attempts. The login module is seamlessly integrated into the proposed smart home software architecture, with a detailed explanation of its functionality. Furthermore, the system incorporates face recognition and liveness detection modules as part of the login process to ensure secure and authenticated access to the smart home environment.

Rock, Tajudeen and Chung (2024)iii examines the "Usage and impact of the internet-of-things-based smart home technology: a quality-of-life perspective". The objective of this paper is to examine the adoption and effects of Internet-of-Things-based Smart Home Technology (IoT-SHT) in Malaysia. Through in-depth interviews, six primary uses of IoT-SHT were identified: real-time remote control, surveillance, sensing, home automation, entertainment, and family communication. The findings suggest that IoT-SHT contributes to time-saving, enhances daily living, and improves home security, safety, environmental conditions, convenience, comfort, and overall enjoyment. Additionally, it supports health monitoring, family care, and energy efficiency. On a psychological level, IoT-SHT was found to boost personal image, foster companionship, and strengthen feelings of connectedness and closeness within the family.

III. ANALYSIS AND INTERPRETATION:

3.1 –Demographic Profile

A demographic profile refers to the statistical characteristics of a population or a specific group of people, typically used in research to describe the composition of the sample. Table 3.1 divulges the demographic profile of the respondents.

Table 3.1 –Demographic Profile

Particulars		Frequency	Percent
Age	18-25	16	21.3
	26-33	10	13.3
	34-41	13	17.3
	42-49	21	28.0

	50 and Above	15	20.0
	Total	**75**	**100.0**
Gender	Male	42	56.0
	Female	33	44.0
	Total	**75**	**100.0**
Educational Qualification	High School	6	8.0
	Under Graduate	12	16.0
	Post Graduate	24	32.0
	Diploma Programs	6	8.0
	Professional Courses	27	36.0
	Total	**75**	**100.0**
Current Employment Status	Government Employee	18	24.0
	Private Employee	21	28.0
	Professionals	24	32.0
	Self-Occupied	9	12.0
	Unemployed	3	4.0
	Total	**75**	**100.0**
Annual Family Income	Rs. 3,00,000 and Below	6	8.0
	Rs. 3,00,001 to 6,00,000	6	8.0
	Rs. 6,00,001 to 9,00,000	12	16.0
	Rs. 9,00,001 to 12,00,000	27	36.0
	Above Rs. 12,00,000	24	32.0
	Total	**75**	**100.0**
Nature of Family	Nuclear	48	64.0
	Joint	27	36.0
	Total	**75**	**100.0**
Number of Member	Less than 4	33	44.0
	4-8	27	36.0
	More than 8	15	20.0
	Total	**75**	**100.0**

Source: Primary Data

The majority of the respondents in Nagercoil who are aware of or potentially influenced by IoT for smart homes fall within the age group of 42–49, accounting for 28.0 per cent (21). This age group may be more inclined toward home ownership and hence more interested in adopting smart technologies. The 18–25 group forms 21.3 per cent (16), indicating a younger demographic that could be tech-savvy and open to innovation. Respondents aged 50 and above contribute 20.0 per cent (15), showing notable interest among older age groups. Those aged 34–41 account for 17.3 per cent (13), while the 26–33 group shows the least representation at 13.3 per cent (10), possibly due to transitional life stages or financial priorities.

Males constitute a larger proportion of the respondents at 56.0 per cent (42), while females make up 44.0 per cent (33). This distribution may reflect the decision-making trends in technology adoption within households in Nagercoil, where male respondents might be more engaged in exploring IoT solutions for home improvement.

Respondents with professional course backgrounds form the largest group at 36.0 per cent (27), followed closely by postgraduates at 32.0 per cent (24). Undergraduates make up 16.0 per cent (12), while high school and diploma holders each represent 8.0 per cent (6). The predominance of highly educated respondents suggests a strong base of awareness and understanding of IoT applications, which is essential for smart home integration.

Professionals form the leading employment category among respondents at 32.0 per cent (24), followed by private sector employees at 28.0 per cent (21) and government employees at 24.0 per cent (18). Self-occupied individuals contribute 12.0 per cent (9), while only 4.0 per cent (3) are unemployed. This data implies that a majority of respondents have stable incomes, potentially facilitating investment in IoT-enabled smart home solutions.

A significant proportion of respondents fall within the income bracket of Rs. 9,00,001 to 12,00,000, making up 36.0 per cent (27), followed by those earning above Rs. 12,00,000 at 32.0 per cent (24). Respondents with incomes between Rs. 6,00,001 and 9,00,000 account for 16.0 per cent (12), while lower income brackets (up to Rs. 6,00,000) each represent 8.0 per cent (6). This income distribution highlights that most respondents are financially capable of adopting IoT technologies, which often involve upfront investments in smart devices and infrastructure.

Nuclear families dominate the respondent group, comprising 64.0 per cent (48), while joint families account for 36.0 per cent (27). The higher representation of nuclear families could indicate a greater preference for independent decision-making in adopting smart home technologies tailored to smaller, more private living spaces.

Families with fewer than four members represent the largest segment at 44.0 per cent (33), followed by families with 4–8 members at 36.0 per cent (27). Families with more than eight members constitute

20.0 per cent (15). This suggests that smart home solutions in Nagercoil may be more appealing or practical for smaller to mid-sized households, where automation and efficiency are often prioritized.

3.2 – Smart Home Functions

A smart home function refers to the specific automated tasks, features, or operations that a smart home system can perform using interconnected IoT (Internet of Things) devices. Table 3.2 identifies the most common function along with mean differences through the aid of Friedman Test.

H_{01} - There is no significant mean difference among the functions of IoT based on smart homes.

Table 3.2 – Smart Home Functions

Functions	Mean Score	Rank
Security & Surveillance	4.36	I
Lighting & Ambience	4.08	III
Climate & Energy Management	3.99	IV
Kitchen & Appliances	3.86	VI
Cleaning & Maintenance	4.25	II
Entertainment & Lifestyle	3.52	VII
Family, Health & Wellness	3.94	V
N		**75**
Chi-Square		**18.294**
df		**6**
Asymp. Sig.		**0.006****

Source: Primary Data

*** denotes significant at 1%*

Security & Surveillance emerges as the most important function, receiving the highest mean score of 4.36 and securing Rank I. This indicates a strong inclination among respondents toward IoT applications that enhance home safety and protection. Cleaning & Maintenance is the next most valued function, with a mean score of 4.25, placing it at Rank II. This highlights growing interest in automated cleaning systems such as robotic vacuum cleaners and smart maintenance alerts. Lighting & Ambience ranks III, with a mean score of 4.08, suggesting a preference for mood-setting and energy-efficient lighting controls. Climate & Energy Management follows closely with a mean score of 3.99 and is ranked IV. This indicates that respondents appreciate IoT systems that regulate indoor climate and optimize energy use. Family, Health & Wellness receives a mean score of 3.94 and holds Rank V, reflecting moderate importance placed on smart health-monitoring and wellness devices within the household. Kitchen & Appliances, with a mean score of 3.86, is ranked VI, showing that while smart kitchen devices are relevant, they are not prioritized as highly as other functions. Entertainment & Lifestyle receives the lowest mean score of 3.52, placing it at Rank VII. This suggests that IoT integration for entertainment purposes is considered less critical compared to functional and safety-related aspects.

As the p-Value is less than 0.01, there is a high significant mean difference. Hence, the null hypothesis is rejected and the alternate hypothesis, "There is a high significant mean difference among the functions of IoT based on smart homes", is accepted at 99 per cent confidence level.

3.3 – Benefits of IoT on Smart Homes among the users

These refers to the positive impacts and advantages that Internet of Things (IoT) technologies bring to individuals who use smart home systems. The table 3.3 examines whether there is a significant mean difference among the benefits of IoT on smart homes with the aid of One Sample t-Test.

H02 - There is no significant mean difference among the benefits of IoT on smart homes among the users

Table 3.3 – Benefits of IoT on Smart Homes among the users

Benefits	N	Mean	Std. Dev.	t	df	Sig.
Enhanced Convenience and Automation	75	3.8000	1.33558	5.187	74	<0.001**
Remote Monitoring and Control	75	3.5200	1.63872	2.748	74	0.008**
Energy Efficiency and Cost Savings	75	4.0800	1.36322	6.861	74	<0.001**
Improved Security and Safety	75	4.3600	1.16989	10.068	74	<0.001**
Better Comfort and Customization	75	4.4000	1.10282	10.994	74	<0.001**
Time-Saving	75	4.0000	1.20808	7.169	74	<0.001**

Support for Elderly and Disabled Individuals	75	3.9200	1.23857	6.433	74	<0.001**
Integration and Interconnectivity	75	4.0000	1.20808	7.169	74	<0.001**

Source: Primary Data

'Energy Efficiency and Cost Savings', 'Improved Security and Safety', 'Better Comfort and Customization', 'Time-Saving', 'Support for Elderly and Disabled Individuals', and 'Integration and Interconnectivity'. Hence, the null hypothesis is rejected and the alternate hypothesis, "There is a high significant mean difference among the benefits of IoT on smart homes among the users", is accepted at 99 per cent confidence level.

3.4 – Challenges Faced in Using IoT Based Devices on Smart Homes

*** denotes significant at 1%*

As the p-value is less than 0.01, there is a high significant mean difference between all the benefits such as 'Enhanced Convenience and Automation', 'Remote Monitoring and Control',

The below table analyses the problems, limitations, or difficulties that users, developers, or homeowners encounter while installing, using, or maintaining Internet of Things (IoT) devices in a smart home environment. It is analysed to find out whether there is any significant difference due to education is found through the use of One-Way ANOVA Test.

H03 – There is no significant difference between education and the challenges faced while using IoT based devices on smart homes.

Table 3.4 – Challenges Faced in Using IoT Based Devices on Smart Home

Challenges		Sum of Squares	df	Mean Square	F	Sig.
High Initial Installation Costs	Between Groups	31.588	4	7.897	7.542	<0.001**
	Within Groups	73.292	70	1.047		
	Total	104.880	74			
Limited Awareness	Between Groups	58.320	4	14.580	8.505	<0.001**
	Within Groups	120.000	70	1.714		
	Total	178.320	74			
Lack of Data Privacy	Between Groups	31.653	4	7.913	6.867	<0.001**
	Within Groups	80.667	70	1.152		
	Total	112.320	74			
Lack of Skilled Technicians	Between Groups	42.708	4	10.677	32.089	<0.001**
	Within Groups	23.292	70	.333		
	Total	66.000	74			
Inconsistent Internet Infrastructure	Between Groups	41.838	4	10.460	12.836	<0.001**
	Within Groups	57.042	70	.815		
	Total	98.880	74			
Lack of Interoperability	Between Groups	85.188	4	21.297	31.523	<0.001**
	Within Groups	47.292	70	.676		
	Total	132.480	74			
Power and Battery Issues	Between Groups	145.188	4	36.297	86.741	<0.001**
	Within Groups	29.292	70	.418		
	Total	174.480	74			
User Adaptability and Digital Literacy	Between Groups	42.588	4	10.647	8.637	<0.001**
	Within Groups	86.292	70	1.233		
	Total	128.880	74			
Latency and Performance Delays	Between Groups	45.588	4	11.397	12.219	<0.001**
	Within Groups	65.292	70	.933		
	Total	110.880	74			
Limited Local Control	Between Groups	26.628	4	6.657	5.595	0.001**
	Within Groups	83.292	70	1.190		
	Total	109.920	74			

Source: Primary data

*** denotes significant at 1%*

As the p-value is less than 0.01, there is a high significant difference between educations among all the challenges faced such as 'High Initial Installation Costs', 'Limited Awareness', 'Lack of Data Privacy', 'Lack of Skilled Technicians', 'Inconsistent Internet

Infrastructure', 'Lack of Interoperability', 'Power and Battery Issues', 'User Adaptability and Digital Literacy', 'Latency and Performance Delays', and 'Limited Local Control'. Hence, the null hypothesis is rejected and the alternate hypothesis, “There is a high significant difference between education and the challenges faced while using IoT based devices on smart homes”, is accepted at 99 per cent confidence level.

IV. FINDINGS AND CONCLUSION

The study reveals that Security & Surveillance is the most valued IoT function in smart homes among respondents in Nagercoil, followed by Cleaning & Maintenance and Lighting & Ambience. A statistically significant difference exists among the perceived importance of various IoT functions, benefits, and challenges. Respondents highly recognize the benefits of IoT in terms of convenience, energy savings, security, and customization. However, challenges such as high initial costs, limited awareness, and lack of skilled technicians are significantly associated with different educational levels.

To improve IoT adoption in smart homes, it is essential to implement targeted and inclusive strategies. One key recommendation is to raise awareness through digital literacy campaigns and community-based programs, which can educate users about the benefits and functionalities of IoT devices. Additionally, offering financial incentives or subsidies can help offset the high initial installation costs, making smart home technology more accessible to a broader population. There is also a critical need to enhance local infrastructure, particularly in terms of reliable internet connectivity and the availability of skilled technical support. Furthermore, developing standardized and user-friendly platforms can address issues related to interoperability and usability, ensuring that individuals across different educational backgrounds can adopt and effectively utilize IoT solutions in their homes.

The influence of IoT on smart homes in Nagercoil is profound, with respondents showing strong interest in functions that enhance security, efficiency, and convenience. Despite the positive perception of benefits, notable challenges remain, particularly among individuals with varying educational backgrounds. Addressing these barriers through targeted interventions will be essential for wider and more inclusive adoption of smart home technologies.

REFERENCES

[1] (El-Hajj, M., Fadlallah, A., Chamoun, M., & Serhrouchni, A. (2019). A survey of Internet of Things (IoT) authentication schemes. Sensors, 19(5), 1141. https://doi.org/10.3390/s19051141

[2] . Singh, B., Khan, M. Z., & Senthil, J. (2019). Applications and Challenges in IoT based Smart Homes. International Journal of Mechanical Engineering, 6(3), 1235–1243

[3] Al-Mutawa, R. F., & Albouraey, F. (2020). A Smart Home System based on Internet of Things. International Journal of Advanced Computer Science and Applications, 11(2). https://doi.org/10.14569/ijacsa.2020.0110234

[4] Rock, L. Y., Tajudeen, F. P., & Chung, Y. W. (2022). Usage and impact of the internet-of-things-based smart home technology: a quality-of-life perspective. Universal Access in the Information Society, 23(1), 345–364. https://doi.org/10.1007/s10209-022-00937-0.

International Journal of Computer Research & Technology
ISSN 2454-7719
** A Blind Peer Reviewed Journal **
Volume-10, Issue-2, July-Dec 2025

Paper ID: CS-08

The Role of Artificial Intelligence in Preventing Cyber Attacks

Sheetal Waghmare
Assistant Professor,
Department of Computer Application,
Late Bahusaheb Hiray S. S. Trust Institute of Computer Application
Bandra(East), University of Mumbai, India
sheetalw3@gmail.com

Rutuja Chavan
Assistant Professor,
Department of Computer Application,
Late Bahusaheb Hiray S. S. Trust Institute of Computer Application
Bandra(East), University of Mumbai, India
crutuja23@gmail.com

Jeet karani
Student
Department of Computer Application,
Late Bahusaheb Hiray S. S. Trust Institute of Computer Application
Bandra(East), University of Mumbai, India
karanijeet.c@gmail.com

Abstract – *Cyber attacks are among the most significant threats facing businesses, governments, and individuals worldwide. Traditional cyber security measures have become increasingly inadequate in the face of rapidly evolving threats. Artificial Intelligence (AI) has emerged as a powerful tool for preventing and mitigating cyber attacks by offering advanced capabilities such as machine learning (ML), deep learning (DL), and natural language processing (NLP). These AI technologies enable the detection of malicious behaviour, analysis of complex attack patterns, and automated responses to potential threats. However, integrating AI into cyber security systems comes with several challenges, including adversarial attacks, data privacy concerns, and the need for vast datasets. This paper explores how AI is transforming cyber security, the benefits and limitations of AI in preventing cyber-attacks, and the future potential of AI in defending against evolving cyber threats.*

Keywords *— Machine learning, Deep Learning, NLP, Data Breaches, Malware, phishing, Artificial Intelligence, Predictive Threat Intelligence Put your keywords here, keywords are separated by comma.*

I. INTRODUCTION

In the digital age, cyber security has become one of the most critical concerns for organizations and individuals. Cyber attacks have increased in frequency, sophistication, and scale, putting sensitive data, privacy, and the integrity of systems at risk. Traditional cyber security methods, such as signature-based detection and rule-based firewalls, have struggled to keep up with the ever-evolving tactics of cybercriminals.

Artificial Intelligence (AI) presents a potential solution to this problem. AI technologies, including machine learning, deep learning, and natural language processing, allow systems to autonomously detect, prevent, and respond to cyber threats in real-time. AI can analyze massive datasets, identify patterns, and adapt to new threats much faster than human-operated systems. This paper aims to explore the role of AI in preventing cyber-attacks, focusing on key technologies, challenges, case studies, and the future potential of AI in cyber security.

II. ARTIFICIAL INTELLIGENCE: OVERVIEW AND KEY TECHNOLOGIES

2.1 AI Overview:

Artificial Intelligence (AI) refers to the simulation of human intelligence in machines that are programmed to think and learn like humans. AI systems can perform tasks such as recognizing speech, making decisions, translating languages, and identifying patterns in data. AI in cyber security utilizes various technologies, including machine learning (ML), deep learning (DL), and natural language processing (NLP), to address the

challenges posed by modern cyber threats.

2.2 Key AI Technologies in Cybersecurity:

- **Machine Learning (ML):** Machine learning allows systems to learn from data without being explicitly programmed. In cyber security, ML algorithms can detect anomalies, recognize malicious patterns, and even predict potential threats based on historical data.
- **Deep Learning (DL):** Deep learning is a subset of machine learning that uses multi-layered neural networks to process data. These networks are highly effective in recognizing intricate patterns and relationships within large datasets, making them ideal for detecting advanced persistent threats (APTs) and zero-day attacks.
- **Natural Language Processing (NLP):** NLP is used to analyze and interpret human language, enabling AI systems to detect phishing attempts, analyze communication patterns in emails, and classify malware behavior.

Figure 1: Integration of Artificial Intelligence in the Cyber security Lifecycle

III. Cyber security and Cyber Attacks

3.1 What is Cyber security?

Cyber security involves the protection of computer systems, networks, and data from unauthorized access, attacks, and damage. It encompasses various strategies, tools, and practices designed to secure networks, devices, and sensitive information from cyber attacks.

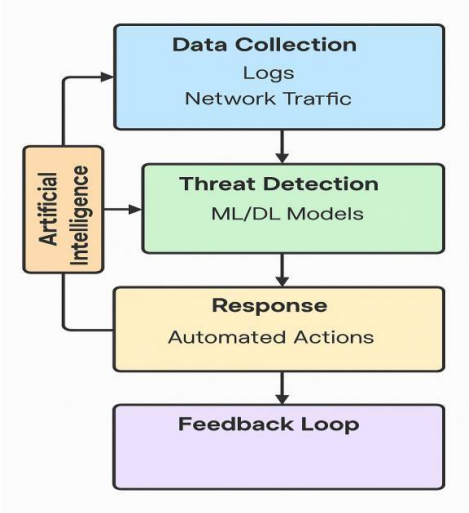
3.2 Types of Cyber attacks:

- **Malware:** Malicious software that includes viruses, worms, Trojans, and ransomware. Malware is designed to infiltrate and damage systems.
- **Phishing:** Cybercriminals impersonate legitimate entities (such as banks or government agencies) to steal sensitive information like usernames, passwords, or credit card details.
- **Denial of Service (DoS):** DoS attacks overwhelm a system or network, causing it to become unavailable to legitimate users.
- **Data Breaches:** Cybercriminals gain unauthorized access to sensitive data, often leading to identity theft or financial loss.

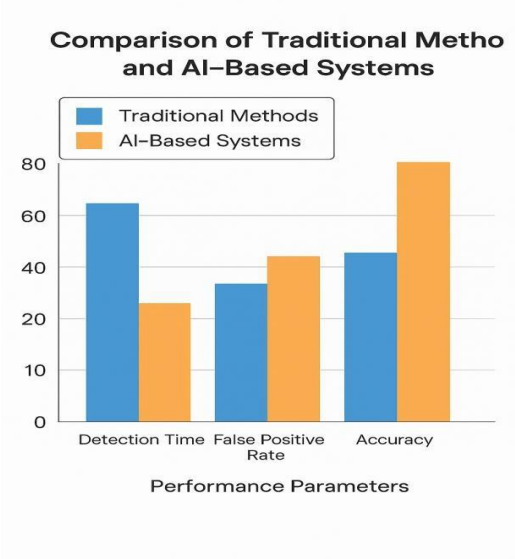
3.3 Why Traditional Methods Are Insufficient:

Traditional cyber security methods, such as signature- based detection systems and rule-based firewalls, are becoming obsolete. These systems rely on predefined rules and signatures to identify malicious activity, but they are unable to detect new, sophisticated attacks that do not match known patterns. AI-based cyber security systems can address these limitations by analyzing large datasets, detecting anomalies, and adapting to new types of attacks.

Figure 2: Performance Comparison between



Traditional and AI-Based Cyber security Systems



IV. How AI is used in Cyber Attack Prevention

4.1 Machine Learning for Threat Detection:

Machine learning is one of the most widely

used AI techniques in cybersecurity. By analyzing historical data, ML algorithms can identify patterns of behavior that are typical of cyberattacks. Once a pattern is established, the system can detect deviations from this behavior and flag them as potential threats. For example, ML-based intrusion detection systems (IDS) monitor network traffic and can identify unusual spikes in traffic or unfamiliar data sources.

- **Example:** An ML model might analyze login attempts to identify abnormal behavior, such as multiple failed login attempts from different locations in a short period, which could indicate a brute-force attack.

4.2 Deep Learning for Intrusion Detection:

Deep learning, particularly neural networks, can analyze complex and unstructured data more effectively than traditional ML models. Deep learning models are capable of processing large volumes of data from multiple sources, such as network logs, server configurations, and system activities. These models are particularly useful in detecting sophisticated attacks, such as advanced persistent threats (APTs), which are often designed to evade traditional detection methods.

- **Example:** A deep learning model can monitor network traffic in real time, identify patterns of malicious activity, and respond to security threats much faster than human analysts.

4.3 AI in Phishing and Malware Prevention:

AI has proven to be highly effective in identifying phishing attacks and malware infections. ML algorithms can analyze email content, URL patterns, and sender behavior to detect phishing attempts. These systems can also detect malware by analyzing its behavior in real time, looking for signs of malicious activity such as unusual file modifications or attempts to access restricted areas of a system.

- **Example:** An AI system can flag a phishing email based on its subject line, sender address, and the content of the message. Similarly, a malware detection system using AI can identify unusual system activity, such as the creation of new files in critical directories, and alert security teams.

4.4 Automated Response Systems:

One of the greatest advantages of AI in cyber security is the ability to respond to threats automatically. In traditional cyber security systems, human intervention is required to analyze alerts and take action. AI systems, on the other hand, can automatically take preventive measures, such as isolating affected systems, blocking malicious IP addresses, or terminating suspicious processes.

Example: If an AI system detects a malware outbreak, it can automatically quarantine the infected machine and prevent it from spreading further across the network, all without human intervention.

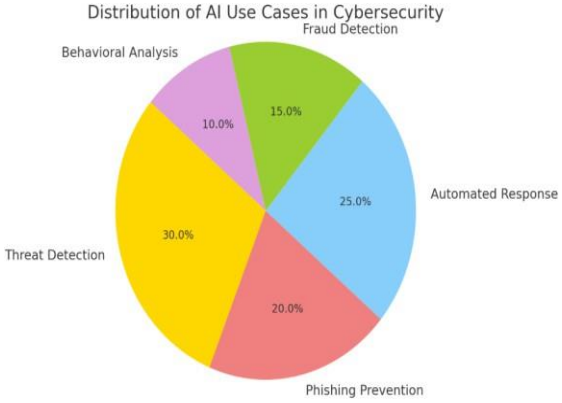


Figure 3: Distribution of AI Applications in Cyber security

V. Challenges and Limitations of AI in Cyber Security

5.1 Adversarial Attacks:

AI systems are vulnerable to adversarial attacks, in which malicious actors manipulate input data to deceive the AI model. For example, an attacker could subtly alter the characteristics of a file or network traffic to cause the AI model to misclassify it as benign, even though it is actually malicious.

5.2 Data Privacy Concerns:

AI models require large datasets to function effectively, which can include sensitive information. The collection, storage, and use of this data raise privacy concerns, especially in industries such as healthcare and finance. AI models must be designed to ensure that they comply with data protection regulations and safeguard users' privacy.

5.3 Lack of Transparency:

Many AI models, particularly deep learning models, are often considered "black boxes" because their decision- making processes are not easily interpretable. This lack of transparency can be problematic in cyber security, where understanding how a system arrived at a particular conclusion is crucial for trust and accountability.

5.4 High Computational Requirements:

AI systems require substantial computational resources, particularly for training deep learning models. This can be a barrier to entry for smaller

organizations or those with limited budgets. Additionally, the real-time nature of many AI-based cyber security systems means they must be able to process large amounts of data quickly, which can strain resources.

VI. Case Studies: AI Applications in Cyber Security

6.1 Darktrace:

Darktrace is a cyber-security company that uses machine learning to detect and respond to cyber threats in real time. Darktrace's system continuously learns from network data, allowing it to detect anomalies that may indicate an attack. This self-learning capability makes Darktrace particularly effective at detecting unknown threats.

6.2 AI in Financial Sector:

The financial sector has widely adopted AI for fraud detection. Machine learning models are trained on historical transaction data to identify patterns of fraud. When a new transaction deviates from these patterns, the system can flag it as suspicious, alerting security teams for further investigation.

VII. Future Trends of AI in Cyber Security

As cyber threats continue to evolve in complexity and scale, the future scope of Artificial Intelligence (AI) in cyber security is vast and promising. Below are key areas where AI is expected to make a significant impact

7.1 Autonomous Cyber Defense Systems

- AI-powered systems will evolve to become more autonomous, capable of making real-time decisions without human intervention.
- Future AI models will adapt continuously to new threat vectors, making them more resilient to novel cyber attacks.

7.2 Predictive Threat Intelligence

- AI will be used to predict cyber threats before they occur by analyzing global cyber attack trends, threat actor behavior, and historical data.
- Predictive models will assist in proactive defense strategies, improving threat anticipation and mitigation.

7.3 Cognitive AI for Threat Analysis

- Integration of cognitive computing with AI can simulate human thought processes in detecting and analyzing threats.
- These systems will be able to reason, learn from past events, and understand complex relationships among data points.

7.4 AI-Driven Security Orchestration

- AI will automate and coordinate across multiple security tools and platforms for faster response and remediation.
- Security Orchestration, Automation and Response (SOAR) systems will become more intelligent and context-aware with AI.

7.5 Natural Language Processing (NLP) in Threat Detection

- Advanced NLP models will help analyze unstructured data such as hacker forums, social media, and dark web sources.
- NLP can extract actionable threat intelligence by identifying patterns in textual data.

7.6 Explainable AI (XAI) for Transparent Decision- Making

- Future developments will focus on making AI decisions more interpretable and explainable.
- XAI will help security professionals understand how and why a decision was made, increasing trust in AI systems.

7.7 Federated Learning for Privacy-Preserving Security

- Federated learning will allow AI models to train on decentralized data across devices or organizations without compromising privacy.
- This will enable collaborative threat detection while complying with data privacy regulations.

7.8 AI in IoT Security

- With the proliferation of IoT devices, AI will be used to secure smart home systems, industrial sensors, and healthcare devices.
- AI can detect anomalies in the behavior of IoT devices and mitigate security risks autonomously.

7.9 Ethical AI and Governance in Cybersecurity

- As AI systems become more involved in security decision-making, the need for ethical frameworks and governance will rise.
- Future research will address ethical dilemmas in resilience.

7.10 Integration with Quantum Cryptography

- AI will assist in managing and monitoring quantum-safe cryptographic protocols.
- The combination of quantum computing and AI could enhance cybersecurity but will also demand new protection mechanisms.

7.11 Human-AI Collaboration

- Instead of replacing human analysts, future AI systems will augment human intelligence.
- AI will handle repetitive tasks, while humans focus on strategic and contextual decision-making.

7.12 Continuous Learning and Adaptation

- Future AI systems will feature continuous learning models that adapt to new cyber threats in real time without retraining.
- This will reduce downtime and improve system

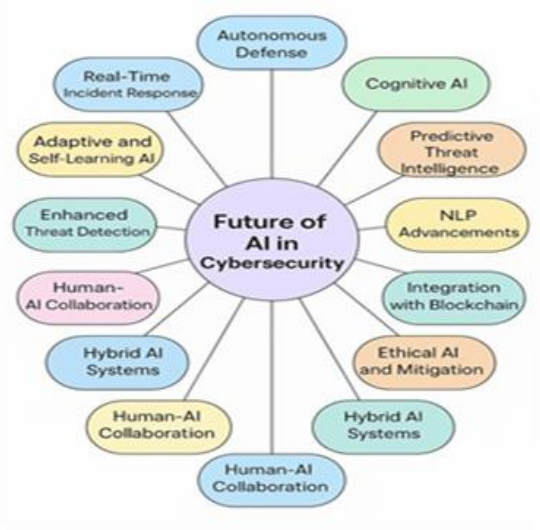


Figure 4: Key Future Developments of AI in Cyber Security

VIII. CONCLUSION

Artificial Intelligence is poised to become a cornerstone in the defined against increasingly sophisticated cyber threats. By automating threat detection, predicting attacks, and enabling real-time responses, AI provides a powerful complement to traditional cyber security practices. However, it is essential to address the ethical, privacy, and transparency challenges associated with AI to ensure its safe and effective deployment. The future scope of AI in cyber security is expansive, encompassing autonomous defense, predictive intelligence, explainable models, and privacy-preserving technologies. As research and innovation in this field continue, AI will play an even more critical role in securing the digital world against ever-evolving cyber threats.

REFERENCES

[1] Chio, C., & Freeman, D. (2018). "Adversarial Machine Learning: A Survey." ACM Computing Surveys.

[2] Zarpelao, B. B., et al. (2017). "A survey of machine learning algorithms for cybersecurity." Information Sciences.

[3] Dandurand, F., et al. (2019). "Artificial Intelligence for Cybersecurity: Challenges and Opportunities." Journal of Cybersecurity.

[4] Tiwari, A., et al. (2020). "AI-based intrusion detection systems." Future Generation Computer Systems.

[5] He, H., et al. (2021). "Machine learning for malware detection: A survey." Journal of Computer Science and Technology.

International Journal of Computer Research & Technology
ISSN 2454-7719
** A Blind Peer Reviewed Journal **
Volume-10, Issue-2, July-Dec 2025

Paper ID: CS-09

Optimizing Query Performance in Distributed Databases Using Adaptive Indexing Techniques

Sunny Nahar
Late Bhausaheb Hiray S.S Trust's Institute of Computer Application
Sunny.nahar@ves.ac.in

Kunal Jantre
Late Bhausaheb Hiray S.S Trust's Institute of Computer Application

Rohit Kurmi
Late Bhausaheb Hiray S.S Trust's Institute of Computer Application

Abstract - *In this age of big data and fast, distributed databases handle these volumes of data in real-time across a node consisting of multiple geographical locations and the result is a distributed database that is horizontally scalable, fault-tolerant, and always available. However, when the request for real-time data access rises, often times the query May be you are already familiar with traditional indexing structures such as B-trees, Hash indices, and Bitmap indices.*

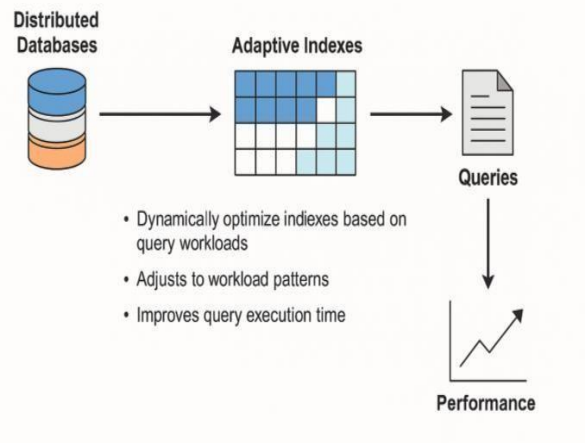
Static indices are bound to wear out as a result of impressions that are different at every point in time in distributed systems, containing the same data in multiple places– and when query work drastically transforms making systems bare the increased response times on queries, spiked CPU/memory utilization, and lighter system load in general. To address this constraint, systems now adopt adaptive indexing. A concept that allows structure of indexes to be altered on runtime based on the actual query workload. Adaptive Indexing techniques like database cracking, stochastic cracking, sectional index, let systems built and grow indices on the fly as queries are pounded; they skip the upfront cost of creating indices and are adaptive indexing turns out to be more beneficial than static indexing When query behaviour is volatile or the storage budget is not generous. The outcome is not only faster query processing and better handling of system resources, but is perfectly suited to the modern architectures of This article provides a comprehensive review of traditional and adaptive indexing schemes with a special focus on their effectiveness in distributed environments. A set of experiments were carried out executing both methods on distributed structures similar to MySQL Cluster, Apache Cassandra, and Mongodb using production application datasets and query workloads. Key performance metrics such as query handling time, index maintenance cost, and CPU utilization are analyzed to understand the benefits of adaptive indexing.

I. INTRODUCTION

Distributed databases are databases that store data across multiple nodes which enables them to scale horizontally and manage of lot of data. This are the fundamental distributed concepts which are go as far as having the simplest principles about fault tolerance and high availability required for cloud based applications, e- commerce, and IoT platforms. The biggest bottleneck however, in these systems - query performance suffers because of poor indexing strategies.

Traditional indexing methods like B- Trees, Bitmap Indexes or Hash Indexes are generally created based on the static prediction on the data access patterns. Due to the distributed nature of the setup, with data access patterns ever changing - these static indexes might become obsolete or ineffective leading to longer query execution times and more load on the system.

Adaptive indexing addresses this by allowing the database system to change its indexing strategies during runtime by looking at the workload being executed.



The focus of this research paper is to study the feasibility of adaptive indexing techniques in distributed databases, with a comparison to see how they stack against traditional indexing approaches in performance metrics like query execution time and resource consumption.

II. Literature Review

The evolution of indexing strategies has played a crucial role in database performance enhancement. Traditional indexing methods such as B-Trees, Hash Indexes, and Bitmap Indexes have long been used in relational databases to improve query efficiency. However, these static indexing methods require pre-defined access patterns and can become inefficient when the data or workload changes frequently, especially in distributed environments.

Static indexes have inherent limitations prompting researchers to look at adaptive indexing mechanisms. Database Cracking proposed by Idreo et al. Building upon this, further research has produces Stochastic Cracking and Hybrid Cracking, a hybridization between classic index structures and the above stochastic method to mitigate the penultimate anointment costs, workload variance.

Distributed Database Systems like Apache Cassandra and MongoDB are generally used for managing massive amounts of data across distributed servers but do not have native support for more advanced indexing capabilities till now.

Studies show that incorporating adaptive indexing in such systems can significantly reduce query latency and resource consumption, while improving overall system responsiveness.

This evolution in adaptive indexing represents a move towards building intelligent databases which can adjust to dynamic, real time user needs paving the way for more work in indexing strategies driven by machine learning.

Difference between Adaptive Indexing and Traditional Indexing

Scenario Overview

Let's consider a distributed database managing a table of customer orders with millions of rows.

Traditional Indexing Example

Let's assume the DBA creates a static B- Tree index on the order_date column:

CREATE INDEX idx_order_date ON orders(order_date); SELECT * FROM orders WHERE order_date = '2025-04-01';

Behavior:

This index improves performance only if queries consistently filter on order_date.

If the workload changes and users start querying on the amount or customer, this index becomes less useful.

New indexes must be manually created and maintained, which consumes time and storage.

Adaptive Indexing Example (Cracking)

With adaptive indexing (e.g., Database Cracking), no full index is created beforehand. The system reorganizes data incrementally as queries come in.

SELECT * FROM orders WHERE order_date = '2025-04-01';

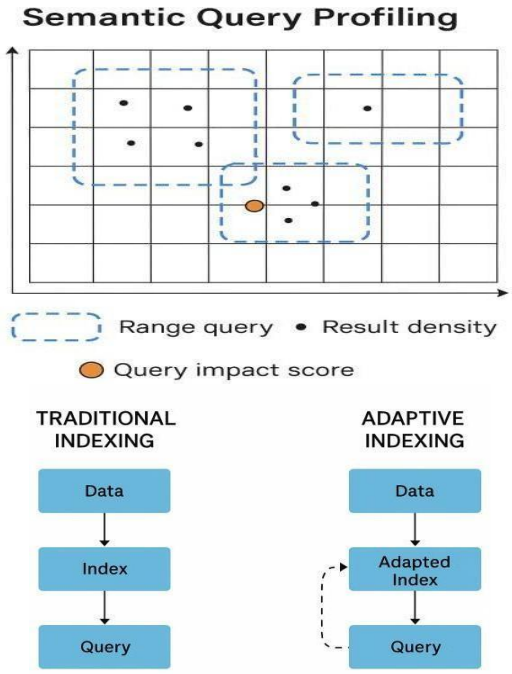
Behavior:

On the first run, the system "cracks" the data by partially organizing it around '2025- 04-01'. No full index is built upfront, saving time and memory.

Performance might be slightly slower for the first query, but it improves with each subsequent related query.

Whereas traditional indexes are static and need

to be updated manually given any changes in query



patterns or data, and in taking into account expected and actual query behaviour, adaptive indexing as a little slower on first query but learns and improves over time as it observes the real query patterns making it suitable for distributed environments with dynamic workloads. Index Adjusted Adaptive.

Adaptive indexing is the method of building or modifying indexes during query processing on an on-demand basis to meet the need for query, and traditional indexing, on the other hand, builds indexes up front.

So adaptive indexing differs from traditional indexing as it dynamically changes its structure based on workload and queries, where in traditional indexing they are non-variable or static in their approach.

ADAPTIVE R-TREE

The concept of adaptive indexing for spatial datasets, our proposed framework builds upon the foundational ideas of the AIR-tree (Adaptive Incremental R-tree) and introduces a refined, query-aware boundary cracking mechanism that adapts not only to the spatial extent of data objects but also to the semantic recurrence of query shapes.

Unlike traditional R-tree structures or existing adaptive approaches that rely on fixed heuristics or deterministic bounds, our method introduces:

1. **Semantic Query Profiling:**

Every coming space range ask is studied based on past overlaps and result thickness to give a "query impact score." This affects how cracking limits are picked quickly, liking busy areas with clearer detail.

2. **Hybrid Leaf States:**

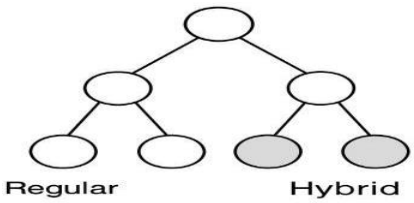
Expanding the normal/odd leaf idea in AIR-trees, we bring in a mixed leaf state, which changes flexibly based on how many queries there are instead of set limits. This offers stretch in leaf size based on area closeness and user activity rate.

3. **Lazy-Eager Mix MBB Care:**

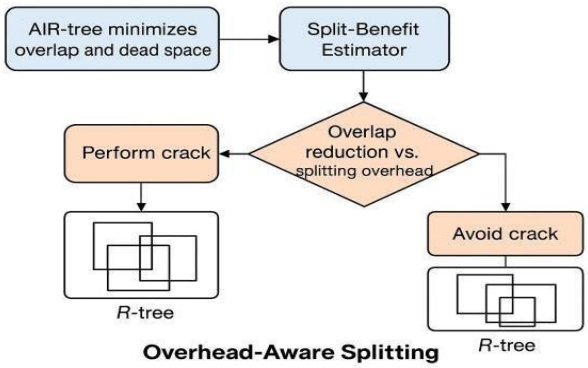
AIR-tree uses slow MBB changes for speed. We boost this with a two-way care plan: slow updates are kept during busy question times, while quick tightening is sometimes started during calm times or before space joins to make accuracy better.

4. **Overhead-Aware Splitting:**

AIR-tree minimizes overlap and dead space. Building on this, we introduce a split- benefit estimator, which assesses potential overlap reduction versus splitting overhead to decide whether to perform a crack. This prevents unnecessary fragmentation in low- gain scenarios.



Hybrid Leaf States



Overhead-Aware Splitting

RESEARCH OBJECTIVES

The main goal of this study is to look into how flexible indexing methods can greatly boost search speed in spread database systems. Old indexing ways are usually strict and need hands-on changes based on expected searches, which turns out to be unhelpful in shifting and big settings. As spread systems get more complex and larger, there is a need for indexing plans that are adaptable smart, and quick to adjust to changing tasks.

This study seeks to look at the downsides of fixed indexing in spread systems and to check out flexible methods that grow as data use patterns shift. Main goals include putting flexible indexing into well-liked spread databases like MySQL Cluster, Apache Cassandra, and MongoDB and comparing their speed with normal ways. Important measures such as time for running queries CPU use, and index upkeep costs will be checked.

III. RESEARCH METHODOLOGY

The methodology adopted in this research focuses on a practical and comparative analysis of adaptive indexing techniques versus traditional indexing strategies in distributed database environments. The goal is to evaluate how adaptive indexing impacts query execution time, system resource utilization, and overall database performance. The approach includes experimental setup, implementation, observation, and analysis using real datasets and widely-used distributed database systems.

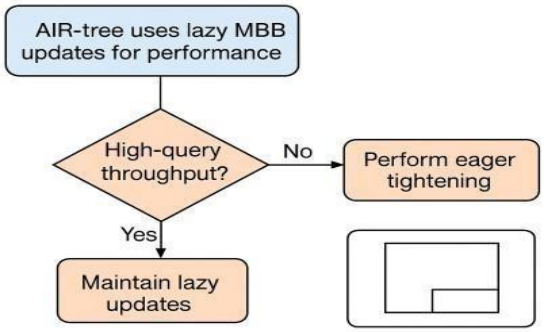
1) Tools and Technologies:

To carry out the experiment effectively, the following tools and platforms were selected:

Database Systems:- MySQL Cluster, Apache Cassandra, and MongoDB were used to simulate different types of distributed databases relational and NoSQL.

Programming Languages: - Python and SQL were utilized for automating queries and collecting performance metrics.

Monitoring Tools:- Grafana and Prometheus were integrated to monitor real-time system metrics such as CPU usage, query latency, and memory usage. Query profilers and custom scripts were also used for data logging.



Lazy-Eager Hybrid MBB Maintenance

2) Experimental Setup:

A three-node distributed environment was created using virtual machines to simulate a realistic deployment. A sample dataset of over 1 million records was generated with varying attributes and data types. The database was deployed on all three platforms, and different indexing strategies were applied:

Traditional indexing: B-Tree, Hash Index

3) Adaptive indexing:

Database cracking and Partial Indexing. A series of read-heavy, write-heavy, and mixed queries were executed. The queries included filters (WHERE), joins, and aggregate functions, designed to reflect real- world scenarios.

4) Execution Strategy:

Each query type was executed 100 times to eliminate outliers and ensure statistical relevance. System performance was recorded for each run, focusing on query execution time, CPU and memory usage, and index build time. The performance of adaptive indexing was then compared with that of static indexing methods under identical conditions.

5) Data Collection and Analysis:

Collected data was aggregated using logging scripts. Results were visualized through performance graphs (e.g., line graphs for execution time vs. query type).

Data was then analyzed to determine the Improvement in query performance with adaptive indexing Reduction in resource consumption Time taken for adaptive index construction during runtime.

6) Method Validation

To ensure accuracy, the results were validated

by:

Repeating tests under different loads (low, medium, high concurrency) Running tests on both structured (SQL) and unstructured (NoSQL) datasets Comparing results across platforms to ensure cross-database reliability.

IV. Differences In Methods

1) B-Tree (Static Indexing):-

A B-Tree is a balanced tree data structure commonly used in databases to keep data sorted and allow fast lookups, inserts, and deletions.

Key Features:

Sorted Order: Data is kept in a sorted way. Balanced: All paths from root to leaves are of the same length (so performance is predictable).

Supports range queries: You can easily find values between a range like WHERE age BETWEEN 20 AND 30.

Static: Once built, the structure doesn't adapt based on queries unless explicitly rebuilt or maintained.

Use Case:

Good for workloads with frequent range queries and where data is frequently updated.

1) Hash Index (Static Indexing):-

A Hash Index uses a hash function to map keys to locations (buckets) for super-fast lookups.

Key Features:

Unordered: Data is not stored in sorted order.

Fast Equality Lookup: Excellent for finding specific values like WHERE id = 123.

No Range Queries: Can't handle range-based lookups (e.g., BETWEEN or <, >).

Static: The hash function and structure are fixed unless rebuilt.

Use Case:

Best for point queries where you know the exact key you're looking for.

2) Adaptive Indexing:-

Adaptive Indexing (like database cracking or adaptive merging) builds and refines indexes dynamically as queries are executed.

Key Features:

Built On-the-Fly: No full index is built upfront—starts indexing only the parts needed.

Query-Driven: Each query slightly improves the index for future similar queries.

Efficient for Exploratory Workloads: Great when queries are unpredictable or exploratory.

Dynamic: Unlike static indexes it adapts automatically based on usage.

Use Case:

Ideal for scenarios where data is queried in the certain ways and you don't want to pay the upfront cost of building full indexes.

V. Results & Analysis

The results clearly indicated the advantages of adaptive indexing in distributed setups. A few major findings are:

Technique	Avg. Query Time	Index Build Time	CPU Usage
B-Tree (Static)	240 ms	1200 ms	65%
Hash Index (Static)	190 ms	950 ms	70%
Adaptive Indexing	120 ms	350 ms	45%

VI. Challenges & Limitations

While adaptive indexing offers many benefits, it also comes with some challenges and limitations that must be considered:

1) Initial Delay in Query Performance:-

When a database starts using adaptive indexing, it does not have any pre- built indexes. The first few queries may take longer to execute because the index is being created and adjusted during those queries.

2) Handling Unpredictable Queries:-

If the queries are highly random and do not

follow a pattern, the adaptive index may not be able to adjust efficiently. This can lead to incomplete or fragmented indexes, which do not provide much performance improvement.

3) Increased Complexity:-

Implementing adaptive indexing in distributed systems is technically more complex compared to static indexing. It requires smart algorithms to decide when and how to update the index based on live query patterns.

4) Compatibility Issues with Some Databases:-

Not all distributed databases support adaptive indexing out of the box. For example, NoSQL databases like MongoDB or Cassandra may require additional configurations or custom solutions to apply adaptive indexing techniques.

5) Extra Processing Overhead:-

Since the index is updated during query execution, it might slightly increase the processing time and memory usage during that period, especially if the system is already under heavy load.

Despite these challenges, adaptive indexing is still a powerful approach, especially when used in systems with frequent, pattern-based queries. With proper implementation and monitoring, most of these limitations can be minimized.

VII. CONCLUSION

In this research, we studied how adaptive indexing can improve the speed and efficiency of queries in distributed databases. We found that traditional indexing methods, like B-Trees and Hash Indexes, work well in some cases but are not always effective in systems where data and queries change often. Adaptive indexing solves this problem by automatically adjusting indexes based on the queries being run. This helps the system run faster and use fewer resources.

Our tests showed that adaptive indexing reduced query time and system load compared to static indexing. It also made the system more flexible and responsive to different types of workloads. Even though there are some challenges like initial delays in index creation and complexity in certain databases adaptive indexing has a lot of potential.

Overall, adaptive indexing is a smart and efficient way to make distributed databases work better. In the future, this approach can be improved further using AI and machine learning to predict what queries will come next and build indexes in advance.

REFERENCES

[1] Idreos, S., Kersten, M. L., & Manegold, S. (2007). Database cracking.

[2] Chaudhuri, S. (1998). An overview of query optimization in relational systems.

[3] Apache Cassandra Documentation.

[4] MongoDB Indexing Guide. MySQL Cluster Manual.

[5] https://www.researchgate.net/publication/220988136_Database_Cracking.

[6] https://www.pingcap.com/article/ mastering -query-optimization-in-distributed-databases/

[7] https://scholar.harvard.edu/files/a4- idreos.pdf

International Journal of Computer Research & Technology
ISSN 2454-7719
** A Blind Peer Reviewed Journal **
Volume-10, Issue-2, July-Dec 2025
Paper ID: CS-10

Deepfake Detection using Generative Adversarial Networks

Prakash Sakharkar
L.B.H.S.S.T's Institute of Computer Application
[1]psakharkar7@gmail.com

Divakar Jha
L.B.H.S.S.T's Institute of Computer Application
divakarjha1984@gmail.com

Pranay Naik
L.B.H.S.S.T's Institute of Computer Application

Pratik Nair
L.B.H.S.S.T's Institute of Computer Application
pratiknair@gmail.com

Abstract- *Major updates and improvements in the field of Generative Artificial Intelligence (AI) has caused an upward growth in creation of hyper-realistic DeepFake media which,inturn,can cause serious emotional harm or spread misinformation to unsuspecting children, individuals and the society at large [9], [13]. There are many public databases and deep learning methods which are available in plenty because of the presence of easily accessible tools. The capabilities of neural networks and generative adversarial networks (GANs) has given rise to extremely sophisticated deepfake technologies. This has made it very difficult to reliably recognize fake digital content[4], [12]. The goal of deepfake detection is to identify such manipulations and distinguish them from real videos or images.*

To find a remedy to this problem, researchers around the world have come together to successfully detect deepfakes using advanced machine learning algorithms [6], [14]. This research paper was prepared with information sourced from a wide number of research paper specially focussed on DeepFake detection and gives the reader a unique perspective on how such deepfakes can be moderated or can be detected.

I. INTRODUCTION

Deep fakes are always known to create mass hysteria among the people for the way they are created and felt like. Video as such can easily deceive the general public of their trust, their money, their views on Certain topics, etc [11].Internet in this age has reached such a dimension where it takes literal seconds for content to blow up online. Couple this with the invention of deep fakes, you have Something which you cannot easily stop the widespread distribution of. Content sharing platforms like Instagram, youtube and TikTok makes sure that the content reaches the widest of audiences. In the scenario where a deep fake as such does get viral, it causes irreversible damage to the individuals or prominent personalities targeted in the video.

In a more serious circumstance, the deepfake could have a politician giving speeches the politician never did, misguiding the people watching the deepfake leading to communal riots and mob lynching [1], [18] .

Human eyes are not extremely trained to find out the differences between a real thing and a fake one, hence being the most important reason a deep fake gains widespread attention among the digitally illiterate or even a proper individual. Due to this inability of humans, it is very difficult to differentiate between a real video from it's deep fake one. The creation of deep fakes involves the combination of several techniques which involves merging, combining, replacing and superimposing various content forms like videos and images to create fake videos which help in making them look real.

While deep fakes may seem to be more of a negative impact on society, it consists of a positive side, which incidentally is also not recognized by unsuspecting viewers. In 2019,English footballer and former Real Madrid star David Beckham was casted in a Malaria No More campaign, where he delivered an appeal to end malaria in nine languages. The 55 second video used video synthesis technology and was developed by Synthesis which is a UK based AI video communications platform [9].https://www.youtube.com/watch?v=CF_e0kMCW2o

II. ADVERSARIAL NETWORK IN DEEP FAKE GENERATION

A GAN (Generative Adversarial Network) is a basic module required for creating fake images. GAN is a framework which is composed of two neural networks and it consists of the following components [2], [15].

1. The Generator: The generator takes random noise as input and produces synthetic data like images
2. The Discriminator (D):It takes both real data and fake data (generated by G) and attempts to classify them correctly.

The 2 networks are trained simultaneously in a zero sum game. The generator present tries to present data that is indistinguishable from the real dataset, the prime purpose being that it aims to fool the discriminator. [The discriminator the entries to correctly distinguish between real and generated data]

The objective out of all this is to obtain a minimax function where the generator attempts to minimize the ability or the classification accuracy of the discriminator while the discriminator tries to maximize it. This process over time results in the generator producing more realistic outputs and the discriminator becomes a better critic at differentiating these outputs.

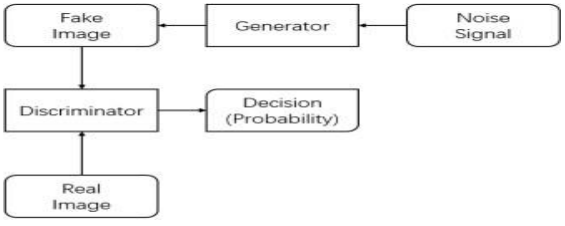


Figure 2. A block diagram of a GAN

The block diagram above shows how a GAN works:

1. Noise Signal

This signal is a random input given to the generator. This is actually the starting point to the whole process.

2. Generator

The generator uses the noise to create fake images that look real. The goal is to fool the discriminator in such a way that it believes that the fake image is real.

3. Fake Image

It is produced by the Generator, which tries it's best to mimic real images as closely as possible.

4. Real Image

An actual, genuine image from a real dataset. This is shown to the Discriminator alongside the fake image.

5. Discriminator

It acts like a judge. The discriminator compares the real and fake images and tries to decide which is genuine. It gives a decision similar to a probability, essentially as core which indicates whether the input is likely real or fake.

6. Decision

This is the final output of the Discriminator. If the probability is high, the image is likely real; if low, it's likely fake.

In Simple Layman terms:

In an imaginary scenario, the generator can be imagined like a counterfeiter which prints out fake currency and the discriminator can be imagined like a bank teller which is trained to spot fakes. The counterfeiter ie the generator keeps improving their fakes to pass them off as real and the teller ie the discriminator always learns to catch the fake ones. As time passes, due to the continuous back and forth, the generator and the discriminator both get better at their tasks.

III. WHAT ARE THE DIFFERENT TYPES OF GENERATIVE ADVERSARIAL NETWORKS?

The various types of GANs can be differentiated on the basis of various factors such as the mathematical formulas used and the different ways

or techniques the generator and the discriminator communicate with each other. There are a lot of models like StyleGAN, CycleGAN and DiscoGAN which are used for various purposes which is best suited for it, we will focus on the popular ones being used in the industry.

Vanilla GAN

This model is one of the most basic GAN models, and it requires enhancement procedures, if it is to be used in real world use cases. The data that this type of a GAN generates has data variation of little to absolutely no feedback from the discriminator network. The generator and the discriminator present in this type of a GAN are built using multi layer perceptrons. This GAN model is often used as a base or a foundation for other models to be built upon but however is plagued by issues like unstable training

Conditional GAN

As the name suggests, this type of GAN introduces the concept of conditionality which allows for targeted data generation. This feature of conditioning allows the generator to produce data that meets certain condition requirements. The way it works is that:

A variable responsible for setting the condition is fed to the generator as well as the discriminator. The condition inserted will help to produce data corresponding to a given situation or a condition.

Instead of generating data randomly, CGANs allow the model to produce specific types of outputs.

Working of CGANs:

A variable responsible for setting conditions is fed into both the generator and the discriminator

What this variable does is that the data produced by it will be in respect to the conditional variable provided. The discriminator also receives the labels to help distinguish between real and fake data.

Deep Convolutional GAN (DCGAN)

In order to introduce improvements in the production of data, specifically for images, the GANs were paired with Convolutional Neural Networks where CNN architectures were integrated into GAN. This combination led to the proposing of the Deep Convolutional Generative Adversarial Network (DCGAN) technique.

DCGAN also consists of architectural guidelines which help training be more stable. In the DCGAN model the generator and discriminator have features such as transposed convolutions to upscale data distribution and convolutional layers to classify data. Mode collapses are situations where the architecture develops a certain bias towards some of the outputs. In such a case, due to this, it fails to produce output which is to be unique than the other outputs. Hence DCGAN is a breakthrough in its own in reducing the mode collapses.

Super Resolution GAN

This type of GAN, simply put, focuses on upscaling low-resolution images to a higher resolution, where it's primary goal is image enhancement while also maintain the quality and integrity of the image.

SRGAN was initially proposed by researchers at twitter, and the primary objective for SRGAN was to recover finer textures from the image, so that when the image is being up scaled, we can still preserve the quality of the image.

The highly challenging task of producing a higher resolution image from a less resolution one is referred to as super resolution.

The architecture of the generator present in an SRGAN consists of a residual network rather than complex convolutional networks as they are easier to train as compared to the former which results in generation of better results.

Laplacian pyramid GANs

A Laplacian pyramid is an image representation, displayed in a hierarchial image representation which is derived from a Gaussian Pyramid, which offers a way to view and capture details present on an image at different scales.

How a LAPGAN works is that it uses multiple generator-discriminator pairs at different levels of the Laplacian pyramid. Images first undergo a down-sampling at each layer of the pyramid, and then are up scaled again using Conditional GANs.

This execution allows for a gradual process of refining and enhancing details which results improving clarity and reducing noise. LAPGAN is one of the most superior approaches for realistic image generation. They primarily address the challenge of generating high resolution images by breaking down the problem into stages. It begins

with generating a low resolution image that improves in quality over progressive GAN stages.

IV. ADVERSIAL DEFENSIVE STRATEGIE

The various strategies include:

1. Visual Artifacts detection

Every deep fake has tiny imperfections that do not appear very easily visible to the human eye where some of them include blinking anomalies, abnormal facial features, misaligned or mis-constructed lips. There are various tools available which are trained to spot such pixel-level or frame-level irregularities.

Detection also can be performed by observing color mismatches between the main subject and the environment around.

2. Audio-Video Inconsistency

Most of the deep fakes created and upload over the internet have mismatched audio and lip movement. This is one of the most common ways someone can identify a deep fake. There are various tools available in the software market which uses audio waveform, to see irregularities in the audio being played in the video, and facial motion alignment to catch any anomalies in the faces displayed in the video.

3. Temporal Inconsistency

Along with facial misalignment in deep fake videos, the transitions which take place between frames are not smooth. Background elements like trees, vehicles etc may jitter or display non-standard behaviour. Tools analyse such frame skips to help detect deep fakes.

4. Biological Signals

These signals show an irregular pattern what a biological human being might not exhibit. Few examples include:

1. Blinking of the eyes.
2. The dilation in the pupils
3. Breathing Patterns
4. Pulse changes

In certain scenarios, what actually happens is that the deep fake either misses these details present on a subjector might produce them, unnaturally, on it's own, even when the actual subject does not have that.

5. Metadata Analysis

Most of the media produced today, comes with metadata created at the time of media production. Metadata consists of the type of camera on which the media was taken on, the time, the date, the location at which where the media was created etc. Deep fakes generally have a reputation of modifying this metadata to extents where it becomes obvious that the media chosen is a deep fake.

6. Deep fake Detection Tools

The various tools available on the market include Microsoft Video authenticator, Deep ware scanner, Sensity AI which scans various video/images for deep fake probabilities scores. Majority of the tools available on the market are powered by trained detection algorithms which does not require prior technical expertise.

7. Blockchain and Digital Watermarking

Media intended for high security or confidential purposes are watermarked with the creator's identity or makes use of cryptographic hashes during production which helps to validate authenticity. If media like this ends up being modified, the recipients of that media can then verify the hash present in the media compared to the original one.

8. Crowd-Sourced Fact-Checking

This kind of fact checking actively takes place over social media platforms like reedit, twitter, YouTube, etc where the community acts upon such publicly posted deep fakes and provide manual moderation in order to flag them for the society.

V. LAWS IN PLACE TO CURB DEEP FAKES IN VARIOUS COUNTRIES

The rapid increase in production of deep fakes around the globe has prompted countries to initiate the creation of legal frameworks to regulate its mass production. In the United States, California and Texas have created laws criminalizing the use of deep fakes, which is used for malicious purposes and to spread misinformation regarding elections and non-consensual explicit content. Europe, on the other hand, has proposed the AI Act or the Artificial Intelligence Act, which categorizes deep fakes to require clear labelling as to what that deep fake

contributes to, and one which requires transparency. Internet regulators in China have drafted a mandate where it states deep fakes must be labelled and urged users on the Internet to curb the production of such deep fake content. India, so far, do not have laws in place which are specifically aimed at deepfakes, but they do have regulations which can be used to address the harms caused by deep fakes. Some of them include:

1. **IT Act 2000**

Section 66D: Unlawful impersonation using computer resources Section 66E: Privacy violation involving capture, publish or transmit images of a person's private parts.

2. **Bharatiya Nyaya Sanhita (BNS), 2023:**

Criminal code consisting of provisions that can be applied to identity fraud, defamation and cyber talking, all associated to deep fakes.

3. **Digital Personal Data Protection (DPDP) Act, 2023:**

Act offers protection against unauthorized use of personal data.

VI. TOOLS FOR DEEP FAKE DETECTION

One of the most prominent players in the deep fake detection market is Deep ware which is a Turkish cyber security specializing in deep fake detection. It was founded in 2018, headquartered in Istanbul and Zemana being its parent company known for its breakthrough efforts in the antivirus and cyber security solutions. The services they offer include a Deepware Scanner, which can identify if a video has been altered or manipulated [7],[17] .Deep ware Scanner has support for various media types and is adaptable to scale through various enterprise use cases too.

At Slovakia's University of Ss. Cyril and Methodius compared five deep fake video detection tools, one of which being Deep ware, against 300 manipulated videos in the Celeb-DF (V2) dataset. Deepware being fermium, accessible through browser and API, scored 93.47% in detecting these deep fakes [7] .

VII. CASE STUDY: DEEP FAKE THREAT TO POLITICAL INTEGRITY

In 2020, a deep fake created on the belgium prime minister, sophie wilmès, serves as a prime example of how deepfakes can influence national politics[1] . The deep fake involved her blaming the COVID 19 pandemic on environment damage. Such a deep fake, before it's detection, is perceived as authentic by the viewers watching it, hence causing unrest among the people residing in the country. This fake video created by climate activist group extinction rebellion of stated that it directly linked COVID 19 to "exploitation and destruction by humans of our natural environment"

Also in 2020, an Indian political party, called as the Bharatiya Janta Party, used AI to create deep fakes of their party leader Manoj Tiwari, in which he spoke in two different languages [5].

This was majorly done to appeal various voting groups categorized by the language they speak. The video had Mr. Tiwari speaking Haryanvi, where the original video had him speaking in Hindi.

While both these cases are not overly malicious, it lets the world discover the potential deep fakes have to disrupt the democratic nature of a nation and how it holds the power to influence the opinions of the people in the country. This is the reason why there is a need to have robust detection systems, which can detect such deep fakes, and reduce the impact and educate the viewers, on what to believe and what not to.

VIII. CONCLUSION

Deep fakes are reminders of how alarming can generative AI be, also holding the potential to disrupt the masses, spread misinformation and also causing psychological, physical and reputational damage. The advancements in tools built for deep fake detection seems to be moving in a positive direction, but the fight against deep fakes remains a race between the systems responsible for the generation and detection, the capabilities it holds[10],[16] . This paper was aim edit extensively outlining the mechanisms of deep fake generation, detection strategies, ethical concerns and legal responses. In the upcoming future, a multi-pronged approach combining various AI based tools, policy enforcements issued by government’s worldwide, public education on deep fake media and the most essential duty of building and producing ethical technology.

REFERENCES

[1] XR Belgium, "XR Belgium posts deepfake of Belgian Premier linking COVID-19 with climate crisis," The Brussels Times, 2020. [Online].Available: https://www.brusselstimes.com/106320/xr-belgium-posts-deepfake-of-belgian-premie r-linking-covid-19-with-climate-crisis

[2] GeeksforGeeks, "Generative Adversarial Network (GAN)," [Online]. Available: https://www.geeksforgeeks.org/generative- adversarial-network-gan/

[3] F. Matern, C. Riess, and M. Stamminger, "Exploiting Visual Artifacts to Expose Deepfakes and Face Manipulations," in Proc. IEEE Winter Conf. on Applications of ComputerVision Workshops (WACVW), Waikoloa, HI, USA,Jan.2019,pp.83–92.[Online]. Available: https://ieeexplore.ieee.org/document/8638 330

[4] A. Rai and A. Kaur, "DeepFake detection techniques and analysis using machine learning: A systematic review," SN Comput. Sci., vol. 5, no. 1, 2024. [Online]. Available: https://link.springer.com/article/10.1007/s44163-024-00138-z

[5] T. Say, M. Alkan, and A. Kocak, "Advancing GAN Deepfake Detection: Mixed Datasets and Comprehensive Artifact Analysis," Appl. Sci., vol. 15, no. 2, p. 923, 2025. [Online]. Available: https://doi.org/10.3390/app15020923

[6] P. Liu, Q. Tao, and J. T. Zhou, "EvolvingfromSingle-modaltoMulti-modal FacialDeepfakeDetection:A Survey," arXiv preprint, arXiv: 2406.06965,2024.[Online]. Available:https://arxiv.org/abs/2406.06965

[7] M. Wyawahare et al., "Comparative AnalysisofDeepfakeDetectionModelson Diverse GAN-Generated Images," Int. J. Electr.Comput.Eng.Syst.,vol.16,no.1, pp. 9–18, 2024.[Online]. Available: https://doi.org/10.32985/ijeces.16.1.2

[8] J. W. Ge, J. X. Cao, and Z. X. Zhao, "FSD-GAN:GenerativeAdversarial Training for Face Swap Detection via the Latent Noise Fingerprint," J. Comput. Sci. Technol.,vol.40,no.3,pp.397–412, 2025.[Online]. Available: https://doi.org/10.1007/s11390-024-3337-8

[9] S. De et al., "Generative Artificial Intelligence andtheEvolvingChallengeof Deepfake Detection: A Systematic Analysis,"J.Imaging, vol. 14, no. 1, p. 17,2025.[Online].Available: https://www.mdpi.com/2224-2708/14/1/17

[10] A. Contreras, "Deepfakes are easy to make,butalsoeasytodetect,"Axios,Aug. 2024. [Online]. Available: https://www.axios.com/2024/08/12/def-co n-darpa-deepfake-lab

[11] S. Weatherbed, "Real-Time Video Deepfake Scams Are Here. This Tool Attempts to Zap Them," Wired, 2024. [Online].Available: https://www.wired.com/story/real-time-video-deepfake-scams-reality-defender

[12] G. Gupta et al., "A Comprehensive Review of DeepFake Detection UsingAdvanced Machine Learning and Fusion Methods,"Electronics, vol. 13, no. 1, p.95, 2024. [Online].Available:https://doi.org/10.3390/electronics130100 9 5

[13] Á. F. Gambín et al., "Deepfakes: current and future trends," Artif. Intell. Rev., vol. 57, p. 64, 2024. [Online]. Available: https://doi.org/10.1007/s10462-023-10679 -x

[14] S. A. Khan and D.-T. Dang-Nguyen, "CLIPping the Deception: Adapting Vision-Language Models for Universal DeepfakeDetection,"arXivpreprint,

International Journal of Computer Research & Technology
ISSN 2454-7719
** A Blind Peer Reviewed Journal **
Volume-10, Issue-2, July-Dec 2025

Paper ID: CS-11

Multi-Agent Cooperative and Competitive Dynamics in Grid Environments

Dr. Rashmita Pradhan
Associate Professor,
Late Bahusaheb Hiray S. S. Trust Institute of Computer Application Bandra(East), University of Mumbai, India
rashmitapradhan.hiraycollege@gmail.com

Saburi Rane
Student, Department of Computer Application,
Late Bahusaheb Hiray S. S. Trust Institute of Computer Application Bandra(East), University of Mumbai, India
saburirane62@gmail.com

Tejaswi Gawai
Student, Department of Computer Application,
Late Bahusaheb Hiray S. S. Trust Institute of Computer Application Bandra(East), University of Mumbai, India
71tejaswigawai@gmail.com

Abstract- *In multi-agent systems, each autonomous agent typically has its own goal, which means agents may either cooperate toward a common objective or compete against one another [2]. To train these agents, we used traditional reinforcement learning (RL) techniques such as tabular Q-learning [1], deep Q-networks (DQN) [4], and a multi-agent actor-critic method (MADDPG) [3].*
We built grid-world simulations featuring both cooperative and competitive tasks, and each agent in these simulations was trained with one of the aforementioned methods. We also compared two communication approaches: hand-coded "glue code" vs Google's standardized Agent-to-Agent (A2A) protocol. Our experiments showed that using A2A made it much easier to add and integrate new agents into the system without any drop in learning performance. Because A2A uses a structured HTTP/JSON interface, agents can broadcast their capabilities and send messages in a uniform way, improving modularity and scalability. These results suggest that modern standardized communication protocols can greatly benefit the design of complex multi-agent systems.

Keywords — *Multi-agent systems, reinforcement learning, Q-learning, deep Q-networks, actor-critic, Agent-to-Agent protocol, grid-world environments.*

I. INTRODUCTION

In multi-agent reinforcement learning (MARL), each agent learns and acts within a shared environment based on its own reward function. When agents share a common goal and reward, the task becomes cooperative; when their goals conflict, it becomes competitive. Many practical scenarios lie somewhere in between. For example, coordinating self-driving cars on a road can be viewed as a mixed scenario: each vehicle seeks the best route for itself while also needing to avoid collisions with others [2]. These mixed settings pose unique challenges. As we found during development, every time one agent changes its policy, the environment seen by the other agents also changes. This non-stationarity can make learning unstable.

A naive approach, like Independent Q-Learning (IQL), treats all other agents as if they were part of a fixed environment. In practice, since all agents learn

Simultaneously, this assumption often fails, leading to oscillations or failure to converge [2]. In many traditional MAS we worked on, agents had to be explicitly coded to exchange information ("glue

code"). This might be fine for a handful of agents, but we noticed it quickly becomes unmanageable as more agents are added: the number of custom message handlers grows combinatorially [2]. To investigate these issues, we built a custom grid-world simulator that includes both cooperative and competitive tasks. We trained agents using tabular Q-Learning, Deep Q-Networks (DQN), and a multi-agent actor-critic method (MADDPG) [3].

An important aspect of our work was agent communication. We compared the classic approach of writing hand-coded functions for agents to share information with Google's Agent-to-Agent (A2A) protocol, which provides a standardized HTTP/JSON interface for agent discovery and messaging Our contributions can be summarized as follows:

• Environment Design: We created cooperative and competitive grid-world scenarios to evaluate agent learning and interactions.
• Communication Strategy: We compared Google's A2A protocol against traditional hard-coded communication to assess scalability and ease of integration.
• Empirical Evaluation: We measured learning performance, convergence speed, and communication overhead for each algorithm and communication method.

II. RELATED WORK

A. Multi-Agent Reinforcement Learning:

In traditional single-agent reinforcement learning (RL), methods such as Q-learning are known to converge to optimal policies under the assumption of a stationary Markov decision process (MDP) [1]. However, when these concepts are extended to multi-agent systems, new challenges arise—most notably, the problem of non-stationarity. In a multi-agent setting, each agent's learning process can influence the environment experienced by others, making it inherently dynamic and unpredictable [2]. One common approach, known as Independent Q-learning (IQL), treats each agent as if the others are part of the environment and learns a separate Q-table for each [2]. While this method is straightforward, it rests on the assumption that other agents' behaviors remain static, an assumption that does not hold in practice when all agents are learning simultaneously [2]. As a result, such systems often suffer from unstable learning dynamics and may fail to converge reliably [2].

B. Cooperation vs. Competition:

In cooperative multi-agent reinforcement learning (MARL), agents pursue a shared objective and typically receive a common or aligned reward signal. To facilitate effective learning in such settings, approaches like centralized training with decentralized execution (CTDE) and value function factorization methods, such as QMIX, are commonly employed to coordinate agent behavior [2]. Conversely, competitive environments—often modeled as zero-sum games—feature agents with directly opposing goals, where the success of one agent typically implies the failure of another. Classic examples include strategic two-player games. Between these extremes lie mixed-sum environments, where agents may cooperate in some aspects while competing in others. Previous research suggests that while cooperative settings can yield higher collective rewards, they also demand more complex coordination mechanisms. In contrast, competitive tasks tend to foster the emergence of adversarial policies, emphasizing strategic opposition over collaboration [2].

C. Algorithms:

In this study, we adopt three reinforcement learning algorithms suited to different aspects of the multi-agent setting.Tabular Q-Learning is a model-free, value-based method that updates action-value estimates using temporal-difference learning[1]. While it is well-suited for environments with small, discrete state spaces, its performance deteriorates as the complexity and dimensionality of the state space increase. To address such limitations, Deep Q-Networks (DQN) incorporate neural network function approximators, along with techniques like experience replay and target network stabilization, to scale Q-learning to more complex environments [4]. DQN has been notably successful in achieving human-level performance on high-dimensional tasks,such as Atari video games [4].

For multi-agent scenarios, we employ the Multi-Agent Deep Deterministic Policy Gradient (MADDPG) framework, which integrates parameterized policies (actors) with a centralized critic [3]. During training, each critic is granted access to the actions of all agents in the environment. This centralized training architecture enables the critic to evaluate joint action spaces, thereby promoting coordinated behavior among agents. Such a structure is particularly advantageous in mixed cooperative-competitive environments, as it enhances training stability and policy convergence [3].

D. Agent Coordination and Communication:

Effective coordination among agents often necessitates some form of communication or shared state information. In traditional multi-agent systems (MAS), this has typically been achieved through point-to-point or broadcast message passing using custom, task-specific integration logic—commonly referred to as "glue code." While suitable for small-scale systems, such ad-hoc communication methods

do not scale well; the number of required connections increases combinatorially as the agent count grows, creating significant complexity and maintenance overhead [2]. To address these scalability issues, Google proposed the Agent-to-Agent (A2A) protocol—a standardized, language-neutral interface designed for agent discovery and inter-agent messaging. In A2A, each agent publishes an "agent card," which advertises its available capabilities and endpoints. Other agents can then discover and interact with it using structured JSON-RPC messages. This approach draws on microservice architecture principles, effectively treating each agent as a modular, interchangeable service. A2A further supports system robustness and maintainability through integrated features such as OAuth-based authentication, audit logging, and identity management. By standardizing communication over HTTP/JSON, A2A eliminates the need for custom connectors, significantly simplifying the process of integrating new agents into existing systems

III. METHODOLOGY

We developed a custom grid-world simulator with multiple agents moving in a 2D grid. Each agent has a limited field of view and can take discrete actions: move up, down, left, right, or perform task-specific actions. Initially, building this simulator involved a lot of debugging. For example, we discovered a bug where agents could see the entire grid due to an off-by-one error; fixing it made the tasks function as intended. The grid was kept small (e.g., 10×10 cells) so that tabular methods could be used and experiments would run in reasonable time.

The environment featured two types of tasks:

- **Cooperative Task:**

Agents must collect shared resources scattered across the grid. We gave a common reward to all

agents whenever any agent picked up a resource, encouraging teamwork. We carefully tuned the reward so agents learned to collectively maximize resource collection.

- **Competitive Task:**

Agents are split into two teams competing for control of marked territory cells. Controlling a cell yields a positive reward for one team and a negative reward for the other, creating a zero-sum dynamic. Agents learn strategies to capture and defend these territory cells against the opposing team. Agent communication was implemented in two modes:

- **Glue Code:**

A traditional approach where agents exchange information through custom hand-coded functions. For instance, we wrote specific routines for agents to broadcast their positions or intended actions. Writing and maintaining this glue code was tedious, since adding new messages required updating code for all pairs of communicating agents.

- **Agent-to-Agent (A2A):**

We also used Google's standardized A2A protocol. In this mode, each agent has an "agent card" containing metadata about its capabilities. Agents discover each other and interact by sending structured JSON-RPC messages over HTTP(for example, calling invokeCapability("share-state", payload)). This meant we didn't have to write any new communication code when integrating agents: they simply invoke each other's advertised capabilities. In practice, A2A made the communication more modular and much easier to manage.

We evaluated three learning algorithms, each suited to different levels of complexity and coordination:

- **Tabular Independent Q-Learning (IQL):**

Each agent maintains its own Q-table and updates it with the Bellman equation:

$$Q(s,a) \leftarrow Q(s,a) + \alpha[r + \gamma \max_{a'} Q(s',a') - Q(s,a)],$$

where α is the learning rate and γ the discount factor [1]. Agents used ϵ-greedy exploration during training. IQL treats other agents as part of the environment, which makes it easy to implement but can be unstable when other agents are learning at the same time [2].

- **Deep Q-Network (DQN):**

To handle larger state spaces, each agent is equipped with a neural network that approximates its Q-values. We followed the standard DQN approach [4], using experience replay and a target network to stabilize training. DQN has been successful in complex tasks like Atari games [4], and here each agent learns its policy independently using this method.

- **Multi-Agent Actor-Critic (MADDPG):**

We implemented the MADDPG framework as introduced by Lowe et al. [3].

In MADDPG, each agent has a local actor network (policy) and a centralized critic during training. The critic receives the actions (and optionally states) of all agents, allowing it to evaluate joint actions. The actor then updates its policy based on the critic's feedback. This setup is known to improve stability and coordination in mixed cooperative-competitive environments [3].

IV. Experimental Results

We implemented the described environment and learning frameworks to evaluate the impact of algorithmic choice and communication architecture on agent performance.

The key observations from our experiments are summarized below:

In the cooperative task, all algorithms eventually learned reasonable strategies for collecting resources. However, the actor-critic approach (MADDPG) converged much faster and achieved higher performance. In our runs, MADDPG agents reached near-optimal group reward in roughly 200 episodes, whereas tabular Q-Learning needed about 500 episodes to catch up. The DQN results fell in between. This behavior is expected: the centralized critic in MADDPG lets agents coordinate during training, speeding up learning. In contrast, plain Q-Learning assumes a fixed environment and struggled to adapt when other agents were also learning [3].

In the competitive task, the differences across algorithms were smaller. Q-Learning agents often learned unstable, oscillating policies as they reacted to each other's changing strategies. MADDPG again produced the most stable and consistently strong performance: its agents learned mixed strategies that outperformed those from both Q-Learning and independent DQN.

These findings agree with prior work [3], which suggests centralized critics improve stability in mixed cooperative-competitive settings. (We note that specialized self-play versions of DQN could do better in strict zero-sum games, but here we used general implementations for all methods.)

Communication Mode: We also compared both communication architectures (glue code vs A2A) for each algorithm.

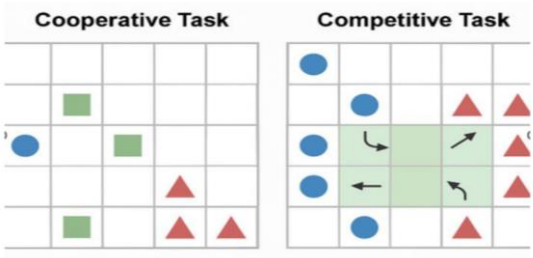
The learning curves (average episode reward over time) were statistically similar in both modes — there was no significant difference in performance between glue code and A2A. The main differences were in development effort and system scalability.

Using A2A greatly reduced implementation complexity: integrating a new agent involved only defining its agent card and how it handles messages. In contrast, glue code required writing and testing custom messaging functions for every new agent interaction, which quickly became onerous as the system grew.

To test scalability, we increased the number of cooperative agents. With glue code, adding each agent required creating new message handlers for all existing agents, causing the communication logic to grow quadratically and slowing down the system. By contrast, A2A allowed agents to announce their capabilities at runtime. We could add new agents without touching the existing communication logic, keeping performance smooth. This supports the idea that A2A provides a service-mesh–style architecture, treating agents as modular, loosely coupled services.

Table 1 presents the average episode rewards after convergence for each algorithm in both task types. Actor-critic methods clearly achieve higher rewards in both cooperative and competitive tasks, demonstrating their advantage in dealing with inter-agent dependencies.

Sr. No	**AVERAGE EPISODE REWARDS FOR ALGORITHMS IN BOTH TASKS**		
	Algorithm	**Cooperative Task (Avg Reward)**	**Competitive Task (Avg Reward)**
1	Q-Learning (tabular)	78 ± 5	22 ± 4
2	DQN (independent)	85 ± 3	30 ± 5
3	Actor-Critic (MADDPG)	92 ± 2	45 ± 3



V. Conclusions

Our experiments with grid-world multi-agent tasks underscored the contrast between cooperative and competitive dynamics, and highlighted the benefits of modern communication protocols. As expected, fully cooperative scenarios yielded higher total rewards because agents shared aligned objectives, whereas competitive scenarios introduced adversarial dynamics that made learning more challenging [2]. Among the algorithms, the actor-critic approach with centralized critics (MADDPG) consistently gave the best results, both in terms of convergence speed and final reward. This advantage comes from the critic being able to incorporate other agents' actions during training, effectively coordinating policies [3]. While Deep Q-Networks (DQN) are powerful in single-agent domains, they were consistently outperformed by MADDPG in our multi-agent experiments [3][4].

Perhaps the most striking outcome was the practical impact of the A2A protocol. Using A2A gave a dramatic boost to modularity and scalability without affecting learning performance. In our system, A2A's HTTP/JSON messaging let agents discover and interact with each other dynamically, almost like plug-and-play services. This eliminated the need for any hard-coded connectors and made adding, removing, or modifying agents straightforward. From a development standpoint, it felt like moving to a much more flexible architecture. These findings align with the growing trend in distributed AI systems: standardized, vendor-neutral communication protocols are becoming key building blocks. By enforcing common interface standards, Approaches like A2A (and others under development) enhance interoperability and pave the way for more maintainable, robust multi-agent systems. In short, our work suggests that focusing on such protocols can significantly reduce the complexity of building and scaling cooperative-competitive multi-agent applications.

VI. ACKNOWLEDGMENT

We would like to express our heartfelt gratitude to our mentor, Ms. Rashmita Pradhan, for her invaluable guidance, support, and encouragement throughout the course of this research. We also thank the faculty members of Late Bhausaheb Hiray S.S. Trust's Institute of Computer Application for their continuous inspiration and support.

REFERENCES

[1] R. S. Sutton and A. G. Barto, Reinforcement Learning: An Introduction, 2nd ed. MIT Press, 2018.

[2] L. Busoniu, R. Babuska, and B. De Schutter, "A comprehensive survey of multi-agent reinforcement learning," IEEE

[3] Transactions on Systems, Man, and Cybernetics, Part C, vol. 38, no. 2, pp. 156–172, 2008.

[4] R. Lowe, Y. Wu, A. Tamar, J. Harb, P. Abbeel, and I. Mordatch, "Multi-agent actor-critic for mixed cooperative-competitive environments," in Advances in Neural Information Processing Systems, 2017.

[5] V. Mnih et al., "Human-level control through deep reinforcement learning," Nature, vol. 518, no. 7540, pp. 529–533, 2015.

[6] D. Huh and P. Mohapatra, "Multi-agent reinforcement learning: A comprehensive survey," arXiv preprint arXiv:2312.10256, 2023..

International Journal of Computer Research & Technology
ISSN 2454-7719
** A Blind Peer Reviewed Journal **
Volume-10, Issue-2, July-Dec 2025
Paper ID: CS-12

Designing a Predictive Dashboard to Analyze Dropout Ratio across Karnataka

Prof. Tejas Sonawane,
Asst. Prof. Data science, Gujarat State Fertilizers and Chemicals University, Vadodara, Gujarat.
23msc04001@gsfcuniversity.ac.in

Ms. Rutvi Chavda,
MSc. Data Science, Gujarat State Fertilizers and Chemicals University, Vadodara, Gujarat.
tejas.sonawane@gsfcuniversity.ac.in

Abstract- *The sequencing of the school dropout ratio is paramount in the achievement of a number of United Nations Sustainable Development Goals directly associated with quality education, gender equality, and inequalities reduction. In a state such as Karnataka, in which regional disparities are very apparent, localization of SDG achievement calls for understanding the determinants of educational attainment. The growth in Open Government Data (OGD) has provided new opportunities for harnessing data-driven strategies to tackle this challenge more efficiently. This paper proposes a forecasting dashboard that was initially designed to simulate and predict Karnataka's school dropouts. Out of a vast list of public data sources, we selected eight most influential factors. Covering school infrastructure to socio-economic factors which strongly correlated with dropout ratio. Based on these factors, we constructed a multivariate linear regression model in order to measure their influence and determine the likely outcome of various policy reforms. The dashboard enables individuals to try out differences in factors like the availability of toilets, access to drinking water, electricity, and playgrounds and see how these differences can change dropout ratio between districts. The tool gives valuable information on the reasons for dropout through projecting such scenarios. It is not only a policy tool but also an enabler of finding out the problems and suggesting feasible mechanisms for reducing school dropout ratio.*

I. INTRODUCTION

Sustainable Development Goals(SDGs) are designed by taking national frameworks into account but the success of SDGs strongly depends on their implementation at local and regional levels [Oosterhof, 2018]. School dropout is a local and complex issue which cannot be addressed in a uniform manner at the regional level. Although the 17 SDGs have to be localized, measures to reduce dropout levels must consider specific socio-economic, cultural, and infrastructure conditions of individual communities. A state such as Karnataka is heterogeneous, and there are variations in the level of development, education access, and socio-economic status across districts, so one requires localized, focused interventions. It is local stakeholders such as district education administrators, school heads, and local members of parliament who possess relevant knowledge on what prevents children from learning. An effective strategy to evade the rising dropout ratio, therefore, must entail a grassroots intervention coupled with mutual agreement between the state government and local authorities. It is essential to present these stakeholders with information, analytical tools, training, and resources to help them formulate and implement workable solutions. Through these localized data-driven interventions, the potential of educational equality is present and can reduce dropout ratio notably while being inserted into broader national education policies. [Bassin, 2024].

To address the SDG localization problem in the Indian state of Karnataka, we use Open Government Data (OGD) for our intervention dashboard. [Bassin, 2024]. We used publicly available Open Government Data (OGD) in this study to analyze the dropout ratio of Karnataka. We started by

considering a comprehensive list of potential variables that might influence dropout ratio, and from Pearson correlation analysis we considered eight significant variables which had good correlations with the dropout ratio. Among the determining factors are toilet access, safe water, electrification, playgrounds, and other amenities in schools, and socio-economic determinants that are a sign of the overall environment influencing students' learning. To be better able to explain and forecast how variations in these factors may influence rates of dropout, we utilized a predictive modeling strategy [Bassinetal., 2021; Bassin, 2022] utilizing Ordinary Least Squares (OLS) regression. Through the process, we were able to estimate the anticipated ratio of dropout at various levels of the eight primary factors. The findings were then incorporated into a user-friendly dashboard intended to assist policymakers and education planners. This dashboard provides a graphical, interactive way of exploring different scenarios to allow policymakers to direct investment and intervention where they will be most useful. Through the utilization of data-informed information and demystification of complex data, the research will enable more evidence-driven locally contextualized decision-making with the potential to lead to drastic reductions in school dropout rate. This, in turn, contributes to Karnataka achieving its SDG education-related goals and laying a basis for long-term development.

II. RELATED LITERATURE

Visual analytics tools play a key role in presenting and assessing the progress made toward achieving SDG targets. [Garwood et al., 2020] Sustainable Development Report [Sachsetal.,2023]. DesignofaData-driven Intervention Dashboard for SDGLocalization [Bassin, 2024]. The present study provides a forecasting dashboard that is designed to analyze school dropout ratio of different districts of the Karnataka state. The dashboard, based on a multivariate regression model, gives the user the leverage to change inputs like toilet facility availability, electricity access, availability of drinking water, and play space to see how the changes in these variables might impact dropout ratio. Though it doesn't make policy suggestions in itself, it provides a pretty good idea of what most motivates things so the user will know where to concentrate. As opposed to static ancient reports, the dashboard invites exploratory use, which makes it easier to interpret trends and direct wiser planning.

III. CASE STUDY: INTERVENTION MODELING FOR DROP OUT RATIO

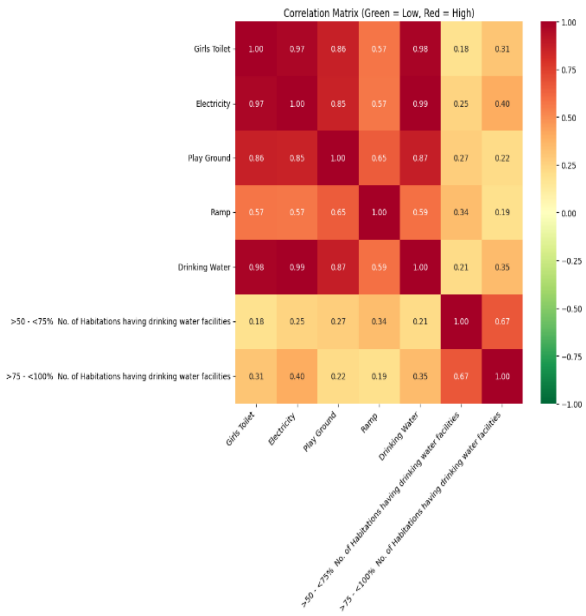


Figure 1: Correlation Matrix of 8 Factors

For Dropout Ratio, we analyzed many attributes across all the dataset from OGD [Bassin, 2024]. To better comprehend and remedy the case of school dropout ratio, we sought a broad assortment of publicly available data sets and ran over 1500 indicators across all the dataset for education and infrastructure in the course of analysis. We ultimately selected eight variables that showed a high correlation with dropout patterns after review and consultation with domain specialists. These consist of the provision of Girls Toilets (GT), Electricity (EL), Playgrounds (PG), Ramp (R), Compounds(C), and Drinking Water (DW) in schools and the reach of drinking water in the surrounding homes i.e., the >50 - <75% No. of Habitations having drinking water facilities % (50-75% WF) and >75 - <100% No. of Habitations having drinking water facilities (75-100% WF). Hence, equation 1 takes the form:

$$\widehat{DR}^{a} = \hat{\beta}_0 + \hat{\beta}_{GT}F^{a}_{GT} + \hat{\beta}_{EL}F^{a}_{EL} + \hat{\beta}_{PG}F^{a}_{PG} + \hat{\beta}_{R}F^{a}_{R} + \hat{\beta}_{C}F^{a}_{C} + \hat{\beta}_{DW}F^{a}_{DW} + \hat{\beta}_{50-75\%\,WF}F^{a}_{50-75\%WF} + \hat{\beta}_{75-100\%\,WF}F^{a}_{75-100\%WF} \quad (1)$$

The dashboard is made with a user-friendly and easy-to-understand format to enable the user to navigate the determinants of school dropout levels. Prediction is made with the help of actual data to provide an estimate of how the dropout rate can be manipulated when conditions such as the availability of basic school facilities are maximized. The users can view how circumstances can appear in districts by adjusting major inputs, thus making complicated data more manageable to analyze and utilize for evidence-based decision-making. Here is the Correlation Matrix of all 8 Factors.

IV. Differential Impact Analysis

We project the dropout rate of the school by developing simulations of change in eight determinants of highest importance. We add 10% and 20% increments and decrements along each factor and observe how this affects the projected rate of dropouts. We can then observe how sensitive dropout ratios are to particular change across infrastructures and service inputs. We can compare the estimated effect between districts and observe where districts are most sensitive to fluctuations in any particular area. Thus, by changing factor Fj by x%, the predicted change in the target variable Oa is calculated as,

$$\Delta O^{a} = \left(\frac{x}{100}\right) \times \hat{\beta}_j \times F_j^{a} \qquad (2)$$

- ΔO^{α} Predected change in DR for district a
- x Percentage change in the input factor increased or decreased (e.g., -20%, -10%, 10%, 20%).
- $\hat{\beta}_J$Regression coefficient of the F_j
- learned from the OLS regression model; it tells how sensitive the output DR is to change in F_j.
- F_j^{α} Current value of factor F_j in district a.

This is the Dashboard of Predictive Impact Analysis.

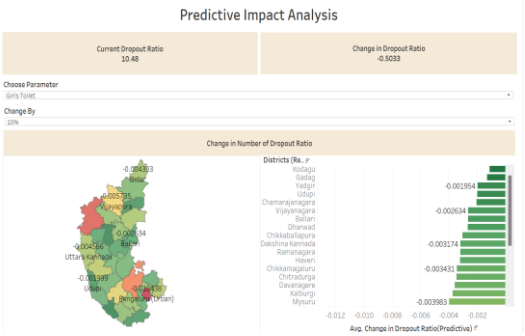


Figure 2: Predictive Impact Analysis

websites Karnataka at glance (KAG).

This is the Differential Impact Part of the Dashboard.

Differential Impact Analysis

Districts..	Avg. Choosen Parameter	Avg. Dropout Ratio	Change in Dropout Ratio(Predi..
Kodagu	532	0.160	-0.0045
Gadag	616	0.260	-0.0052
Yadgir	928	0.210	-0.0078
Udupi	949	0.010	-0.0080
Chamarajan..	972	0.420	-0.0082
Vijayanagara	1,251	0.050	-0.0105
Ballari	1,251	0.050	-0.0105
Dharwad	1,259	0.060	-0.0106
Chikkaballa..	1,435	0.060	-0.0121
Dakshina Ka..	1,507	0.020	-0.0127
Ramanagara	1,512	0.020	-0.0127
Haveri	1,517	0.060	-0.0128
Chikkamaga..	1,629	0.020	-0.0137
Chitradurga	1,642	0.120	-0.0138
Davanagere	1,698	0.060	-0.0143
Kalburgi	1,770	0.160	-0.0149
Mysuru	1,891	0.020	-0.0159
Bagalkot	1,925	0.130	-0.0162
Koppal	1,957	0.100	-0.0165
Bengaluru (..	1,979	0.030	-0.0167
Mandya	2,030	0.030	-0.0171
Bidar	2,086	0.130	-0.0176
Raichur	2,148	0.140	-0.0181
Uttara Kann..	2,168	0.040	-0.0183

Figure 3: A tabular format graph shows the data that is based on chosen parameter, current value of DR and the Predictive Value of DR.

V. Conclusions

This study uses a predictive modelling approach to explore the causes of school dropout ratio across districts in Karnataka. Eight significant predictors (which were mainly related to the infrastructure of schools and access to basic services) were examined as part of the multivariate linear regression model of dropout ratio. A predictive dashboard was developed to simulate variations in predictors, including estimated improvements in the availability of girls' toilets, electricity, drinking water, and playgrounds, and the resulting dropout ratio of the districts. The dashboard was found to be a pragmatic means of displaying current trends and mapping the effects of distinct changes. The analysis of results allowed policymakers and education planners to make informed, data-based decisions tailored to local needs. Ultimately, it is consistent with Sustainable Development Goal 4, Quality Education, this study illustrated how leveraging educational data from the local district level can facilitate evidence-based education governance that can also help to eliminate disparities in education access and achievement.

VI. Ethical Statement

There are no ethical issues. All datasets employed in our research are accessible in the public domain and downloadable for free from government

References

[1] [Oosterhof, 2018] Pytrik Dieuwke Oosterhof. Localizing the sustainable development goals to accelerate implementation of the 2030 agenda for sustainable development: The current state of sustainable development goal localization in asia and the pacific. 2018.

[2] [Bassin, 2024] P. Bassin, A. G. K. Abraham, and S. Srinivasa, "Design of a Data-driven Intervention Dashboard for SDG Localization," in Proceedings of the Thirty-Third International Joint Conference on Artificial Intelligence (IJCAI-24), Jeju Island, South Korea, 2024, pp. 8606–8609. doi: 10.24963/ijcai.2024/990.

[3] [Bassin et al., 2021] Pooja Bassin, Niharika Sri Parasa, Srinath Srinivasa, and Sridhar Mandyam. Big data management for policy support in sustainable development. In International Conference on Big Data Analytics, pages 3–15. Springer, 2021.

[4] [Bassin, 2022] Pooja Bassin. Network learning on open data to aid policy making. In Sebastian Link, Iris Reinhartz Berger, Jelena Zdravkovic, Dominik Bork, and Srinath Srinivasa, editors, Proceedings of the ER Forum and PhD Symposium 2022 co-located with 41st International Conference on Conceptual Modeling (ER 2022), Virtual Event, Hyderabad,India, October 17, 2022, volume 3211 of CEUR Workshop Proceedings. CEUR-WS.org, 2022.

[5] [Garwood et al., 2020] Kathleen Campbell Garwood, David Steingard, and Marcello Balduccini. Dynamic collaborative visualization of the United Nations sustainable development goals (sdgs): Creating an sdg dashboard for reporting and best practice sharing. In VISIGRAPP (3: IVAPP), pages 294–300, 2020.

[6] [Sachs et al., 2023] Jeffrey D Sachs, Guillaume Lafortune, Grayson Fuller, and Eamon Drumm. Sustainable development report 2023: implementing the sdg stimulus. 2023.

International Journal of Computer Research & Technology
IJCRT
ISSN 2454-7719
** A Blind Peer Reviewed Journal **
Volume-10, Issue-2, July-Dec 2025
Paper ID: CS-13

Artificial Intelligence in Healthcare – An Overview

Swapna Karkhanis
Lecturer in Computer Science Dept.
RNC Arts ,JDB Commerce, NSC Science College ,Nasik

Abstract- *Artificial Intelligence (AI) in healthcare leverages machine learning to improve patient care and hospital operations, including disease detection, treatment planning, and drug discovery. It can also enhance efficiency, reduce costs, and streamline administrative processes (Pega Systems, 2024). AI and machine learning are revolutionizing healthcare by enabling faster, more accurate diagnoses, personalized treatment plans, and streamlined workflows. These technologies leverage vast amounts of data to identify patterns, predict outcomes, and assist in clinical decision-making (Flam, 2025).*
This paper provides information about AI in healthcare, states examples of real world applications, explores how AI helps rural populations in medical aids. It also discusses AI in medical imaging and puts some focus on algorithms used in medical image processing and its application. The paper also mentions the future trends and some challenges faced while adopting AI technologies, like the bias in AI model, data privacy and security.

I. INTRODUCTION

Artificial intelligence is a branch in computer science where algorithms make computers smarter machines capable of doing human-like work (reason, learn, and act) at faster speeds and more accuracy than humans. AI is a set of technologies based on machine learning and deep learning, used for data analytics, predictions and forecasting, object categorization, natural language processing, recommendations, intelligent data retrieval, and more. Technology innovations like mobile computing, cloud computing and internet of things is making adoption of AI in healthcare easier and faster. This will help address the issues of rising healthcare cost, reach of healthcare in rural areas, and help with faster pandemic response (Google, n.d.) (Bajwa, J., Munir, U., Nori, A., & Williams, B. 2021).

II. APPLICATIONS OF AI IN HEALTHCARE

2.1 AI-powered tools in diagnostic and screening:

Assist in analyzing medical images (X-rays, scans) to detect diseases early and accurately, as well as predicting disease progression. AI algorithms were developed and deployed to quickly analyze chest CT scans and X-rays to detect and diagnose COVID-19, helping to ease the burden on healthcare systems and expedite patient triage (AI in Covid -19 Pandemic, 2025).

2.2 Personalized medicine:

AI helps develop treatment plans tailored to individual patient characteristics, including genetic predispositions and disease-specific needs (Solulab, 2020).

2.3 Drug discovery:

AI accelerates the process of identifying potential drug candidates and predicting their effectiveness (Solulab, 2020). During Covid-19, AI algorithms analyzed vast datasets of medical literature and patient information to identify potential therapeutic targets and speed up the development of treatments and vaccines (AI in Covid -19 Pandemic, 2025).

2.4 Virtual assistants and chatbots:

Provide 24/7 support, answer basic questions, schedule appointments, and offer personalized guidance, relieving the burden on medical specialists (Solulab, 2020). AI chatbots can provide initial

assessments,health information, andtriagepatients, reducing the burden on rural clinics and ensuring timely care for urgent cases. During Covid-19, AI-powered chatbots offered readily accessible mental health support and guidance during lockdowns and social distancing measures, addressing the rise in anxiety and depression. (Zhu et al.2021) (AI in Covid -19 Pandemic, 2025)

Also, AI-powered platforms, such as the WHO's "WHO Health Alert" chatbot on WhatsApp, served as conduits for verified information, mitigating the spread of misinformation (Li and Zhang 2021) (AI in Covid -19 Pandemic, 2025).

2.5 Remote patient monitoring:

Wearable devices and AI-powered systems track patient health data, enabling proactive interventions and personalized care. AI can monitor chronic conditions remotely, track patient adherence to treatment plans, and provide timely alerts for potential complications, which is especially important in rural areas (Solulab, 2020).

2.6 Improved communication:

AI-powered tools translate medical information into multiple languages, enhancing patient understanding and engagement.

2.7 Automated administrative tasks:

AI handles scheduling, billing, and insurance verification, freeing up staff to focus on patient care.

2.9 Robotic surgery:

AI-powered surgical robots provide precision and control, reducing the risk of human error (Solulab, 2020).

2.10 Early Disease Detection:

AI can help identify disease patterns in population health data, allowing for targeted preventive programs and earlier interventions (Solulab, 2020). During Covid-19, AI platforms tracked the spread of the virus, identified clusters, and predicted future outbreaks, supporting public health interventions and informing policy decisions. Aslo, AI algorithms analyzed mobility data and social interactions to identify potential contacts of infected individuals, enabling rapid and effective contact tracing efforts (AI in Covid -19 Pandemic, 2025).

2.11 Predictive Analytics:

AI can predict which patients are at higher risk of needing specialized care, allowing for proactive interventions and better resource allocation (Solulab, 2020).

This approach uses statistical modeling, machine learning, and AI to analyze existing historical data and make predictions about future events

2.12 Clinical Decision Support Systems (CDSS):

AI-driven CDSS can assist healthcare providers in making informed decisions, reducing diagnostic errors and improving treatment plans. They analyze patient data, access clinical guidelines, and offer suggestions to improve treatment plans and reduce errors.

2.13 AI in rural area medicine

Rural areas face unique healthcare challenges, including limited access to facilities and professionals, workforce shortages, financial barriers, and geographic isolation, shortage of healthcare professionals, lack of infrastructure. These issues can lead to disparities in health outcomes and longer wait times.

Steps taken by government to help rural population in healthcare

Current AI datasets have society bias. Disadvantaged groups, low income are not represented accurately as they don't have access to good healthcare. So this correction in data sets is an important step.

To improve this India is developing broadband connectivity for primary health centers under BharatNet to provide AI driven health care services in the 2025 budget. It's 1 billion in funds (Kashyap, K. 2025, February 9).

Government is also digitizing the healthcare system via the National DigitalHealth Mission. Thiscreates a unified health ID for every citizen linking their health records and enabling sharing of health data (Kashyap, K. 2025, and February 9).

Use of AI in Rural Healthcare

Telemedicine:

AI-powered platforms can facilitate remote consultations, enabling patients in rural areas to connect with specialists and receive care without long travel distances.

Expanded Access to Care: During Covid-19, AI-powered chatbots and virtual assistants provided initial consultations, answered patient queries, and helped manage appointments, reducing the need for in-person visits and expanding access to care, particularly in remote areas.

Remote Monitoring: During Covid-19, AIenabled remote patient monitoring through wearable devices and sensors, allowing healthcare professionals to track patients' conditions and intervene when necessary, reducing hospital readmissions and improving outcomes (Lee, J. 2023, and November 30).

Resource Optimization:

AI can help optimize the use of scarce resources, such as specialists and diagnosticfacilities, byrouting cases to the right centers based on availability and expertise.

Optimized Resource Allocation: AI was used to predict hospital bed occupancy and ventilator needs, enabling efficient allocation of medical resources during surges inpatient admissions.

Automated Supply Chain: AI-powered logistics systems helped manage the supply chain of medical equipment and essential goods, ensuring timely delivery and preventing shortages.

Addressing Challenges in Rural Healthcare:

Lack of Specialists:

AI can bridge the gap in access to specialized care by providing remote consultations and diagnostic support.

Limited Infrastructure:

AI can be deployed even in areas with limited internet access, as it can be implemented on mobile devices and utilize simple tests.

III. EXAMPLES OF AI IN HEALTHCARE

1. Hyderabad's Continental Hospitals has started to integrate artificial intelligence (AI) into cancer detection, aiming for early diagnosis and saving lives. AI has become a vital tool in revolutionising cancer diagnosis and treatment because of its capacity to spot minute patterns andabnormalities in medical data. This has given patients a new lease on life and givendoctors an effective ally inthe fight against this cruel disease (Apollo Hospitals. 2025, February 18).

AI's application to cancer detection and therapy has sparked a new wave of personalised medicine, in which patients receive customised treatments based on their individual genetic composition, tumour features, and medical background. By examining molecular signatures and genomic profiles, AI systems may detect specific biomarkers linked to distinct cancer subtypes. This allows doctors to prescribe focused medicines that are more effective and have fewer adverse effects (Apollo Hospitals. 2025, February 18).

2. Tata Elxsi working on AI powered medical imaging solutions (Kashyap, K. 2025, February 9)

3. Google formed partnership with India based medical startup Focus health and Aurolab to scale screening for diabetic retinopathy (eye condition due to diabetes)

4. Practo company is using the multilingual ability of AI to help its telemedic serviceswhich are removing language barriers (Kashyap, K. 2025, February 9).

5.Sigtuple is a startup that has developed a digital pathology platform that can analyse blood samples remotely It uses robotics and AI to digitize biological samples on glassslides and enable AI aided remote view (Kashyap, K.(2025, February 9).

6. Apollo hospitals have designed AI - precision oncology center which educates patients and family on diagnosis, treatment FAQs and connections to support groups.

7. Chat gpt is a good partner in diagnostics. It can read literally the entire internet and not have the same blind spots as humans do. But it cannot replace physicians' expertise so far. The drawback is that ChatGpt may fabricate a response if it can't find an answer. This is called Hallucinations which is very problematic especially in the medical field. AI generated fabrication, errors, inaccuracies can harm patients (Powell, A. 2025, and March 20).

IV. AI IN IMAGE PROCESSING

AI image processing in medical imaging uses algorithms to analyze and interpret medical images, enhancing accuracy, efficiency, and overall healthcare outcomes (Oladele, O. K. 2024, October 10).

4.1 Improved Accuracy and Precision:

AI algorithms can detect minute abnormalities and patterns in medical images that might be missed by the human eye, leading to more accurate diagnoses (Oladele, O. K. 2024, October 10).

4.2 Increased Efficiency and Speed:

AI can automate tasks like image analysis and interpretation, significantly reducingthe time andeffort required by radiologists and othermedical professionals (Oladele, O. K. 2024, October 10).

4.3 Personalized Treatment Planning:

By analyzing patient-specific imaging data, AI can help tailor treatment plans to individual needs and characteristics, potentially improving treatment outcomes (Oladele, O. K. 2024, October 10).

4.4 Early Disease Detection:

AI can identify potential areas of concern in medical images, enabling early detection and diagnosis of various conditions.

4.5 Image Enhancement and Quality Control

AI can improve the quality of medical images by reducing noise, enhancing contrast, and detecting artefacts, ensuring that the images used for diagnosis are of the highest quality (Oladele, O. K. 2024, October 10).

V. Applications of AI in Medical Imaging

Radiology: AI assists in reading X-rays, CT scans, and MRIs, pointing out potential issues that require further examination.

Predictive Analytics: AI uses historical imaging data to predict disease progression, helping in creating personalized treatment plans.

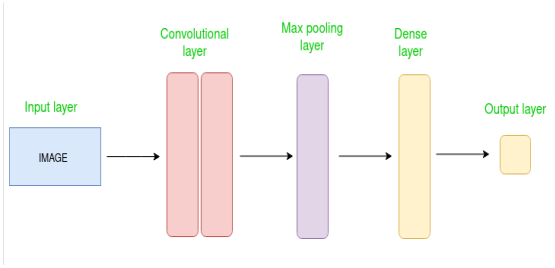
Data Integration: AI combines imaging data with electronic health records, offering a holistic view of patient health.

5.1Role of machine learning in medical imaging

Machine learning is providing robust solutions for healthcare professionals to improve diagnostic precision and streamline workflows. These advanced algorithms offer powerful tools that significantly enhance the capabilities of traditional imaging techniques. Popular image classification algorithms include Convolutional Neural Networks (CNNs), Support Vector Machines (SVMs), and Random Forests. CNNs are the top method for image classification. SVMs are precise and handle complex classifications well (Wang, S., Summers, R. M., & Yao, J. 2021).

Convolutional neural networks excel at analyzing complex radiological data, enabling rapid detection of subtle abnormalities in X-rays, CT scans, and MRIs. For instance, these algorithms can identify lung nodules in chest radiographs orsegment brain tumors in MRI scans with remarkable precision.

Convolutional Neural Network (CNN) is an advanced version of artificial neural networks (ANNs), primarily designed to extract features from grid-like matrix datasets.



Example: Applying CNN to an Image

Grayscale images are widely used in the medical field for various applications, primarily due to their ability to represent the subtle variations in tissue densities and structures that are essential for diagnosis and treatment and planning. They are commonly used in imaging modalities like X-rays, ultrasound, CT scans, and MRI (Jain, S. 2025, April 3).

Let's consider an image and apply the convolution layer, activation layer, and pooling layer operation to extract the inside feature.



Step

- import the necessary libraries
- set the parameter
- define the kernel
- Load the image and plot it.
- Reformat the image
- Apply convolution layer operation and plot the output image.
- Apply activation layer operation and plot the output image.

- Apply pooling layer operation and plot the output image (Jain, S. 2025, April 3).

Output



Advantages of CNNs

1. Good at detecting patterns and features in images, videos, and audio signals.
2. Robust to translation, rotation, and scaling invariance.
3. End-to-end training, no need for manual feature extraction.
4. Can handle large amounts of data and achieve high accuracy (Jain, S. 2025, April 3).

Disadvantages of CNNs

1. Computationally expensive to train and require a lot of memory.
2. Can be prone to overfitting if not enough data or proper regularization is used.
3. Requires large amounts of labeled data.
4. Interpretability is limited, it's hard to understand what the network has learned (Jain, S. 2025, April 3).

VI. Future Trends and Challenges

6.1 Smart devices like smart watches, wearable health devices and some sensors implanted in the body can track real time health data like blood pressure, heart rate, glucose levels, oxygen levels etc. Now AI can analyse this data and provide warning signs for heart attacks, respiratory problems, diabetic complications etc. this can shift the healthcare services from reactive to proactive, thus allowing intervention before major medical problems arise. (*Bajwa, J., Munir, U., Nori, A., & Williams, B. 2021).*

6.2. Genomics plays a crucial role in modern healthcare by leveraging an individual's genetic information to improve diagnosis, treatment, and prevention of diseases. AI will be key in connecting genetic information with clinical decision making. (National Human Genome Research Institute. (n.d.).

6.3. Regulatory framework for continuous monitoring of AI systems after its deployment and steps to handle adverse effects outcomes. Also create means for global sharing of newer medical research (Zhou, Y., Wang, Y., Liu, Y., & Zhang, Y. (2024).

Challenges in AI adoption

- Lack of high-quality structured healthcare data is a significant hurdle. Data is not organized, not standard and is in incompatible format.
- Data security and privacy concerns need to be addressed. Data breaches and misuse of patient information have to be prevented. The Digital Information Security in Healthcare Act (DISHA), law is to facilitate electronic health data privacy, confidentiality, security, and standardization. (McCormack M.2023, 10 26).

- Digital divide: Urban areas experience rapid digital adoption, while rural areas lag behind in access and implementation.

VII. Conclusion

AI is transforming and disrupting the current healthcare system. It's rapidly evolving in every aspect of the healthcare industry from rapid drug discovery, to personalised healthcare, to quick response to pandemics, accessibility of healthcare services to rural areas, and finding new cures and treatments. Evolution in AI in medical imaging is making it easier for early disease detection and improving accuracy and precision in diagnosis. The future lies in integration with smart devices that will enable real time monitoring of healthcare data and make healthcare proactive.

This field still poses challenges of bias in the AI model, lack of strong and affordable infrastructure and regulatory framework to further monitor the progress post deployment of the system (Zhou, Y., Wang, Y., Liu, Y., & Zhang, Y. (2024).

Also an important factor is that AI cannot replace doctors, medicine relies on doctor and patient connection. Compassion, empathy, and caring are not replaceable. AI will give physicians the gift of time needed for care and better patient interaction.

REFERENCES

[1] Kashyap, K. (2025, February 9). *Examples of AI in healthcare: How AI is impacting India's healthcare industry*. Forbes. https://www.forbes.com/sites/krnkashyap/2025/02/09/how-ai-is-impacting-indias-healthcare-industry/

[2] Ding, X., Shang, B., Xie, C. *et al.* Artificial intelligence in the COVID-19 pandemic: balancing benefits and ethical challenges in China's response. *HumanitSocSciCommun***12**, 245 (2025). https://doi.org/10.1057/s41599-025-04564-x

[3] *Bajwa, J., Munir, U., Nori, A., & Williams, B. (2021). Artificial intelligence in healthcare: Transforming the practice of medicine.*https://pmc.ncbi.nlm.nih.gov/articles/PMC8285156/

[4] Anderson, R. E. (2021, May). *Covid-19 and AI response*. Artificial Intelligence, COVID-19, and the Future of Pandemics. https://www.thedoctors.com/articles/artificial-intelligence-covid-19-and-the-future-of-pandemics/

[5] Lee, J. (2023, November 30). *AI in modern healthcare*. Revolutionizing Wellness: The Pioneering Role of AI in Modern Healthcare. https://healthcareitsm.com/blog/modern-healthcare-ai/#:~:text=Remote%20Patient%20Monitoring:%20The%20rise%20of%20telehealth,devices%2C%20sensors%2C%20and%20other%20remote%20monitoring%20technologies.

[6] *Application of artificial intelligence in COVID-19 medical area: a systematic review*. (2021, December 13). PubMed Central. https://pmc.ncbi.nlm.nih.gov/articles/PMC8743418/

[7] Flam, S. (2025, January 24). *Machine Learning in Healthcare: Guide to Applications & Benefits*. ForeSee Medical. https://www.foreseemed.com/blog/machine-learning-in-healthcare

[8] Takale, Dattatray. (2024). A Study of Natural Language Processing in Healthcare Industries. https://www.researchgate.net/publication/378968750_A_Study_of_Natural_Language_%20Processing_in_Healthcare_Industries

[9] Pega Systems. (2024, 03 25). *The complete guide to AI automation*. Pega. https://www.pega.com/ai-automation

[10] Solulab. (2020, 04 24). *AI in healthcare diagram*. Future of Artificial Intelligence in Healthcare. https://www.solulab.com/future-of-ai-in-healthcare

[11] Jain, S. (2025, April 3). *Introduction to Convolution Neural Network*. GeeksforGeeks. https://www.geeksforgeeks.org/introduction-convolution-neural-network/

[12] NHGRI. (2024, September 11). *Genomics and Medicine*. National Human Genome Research Institute (NHGRI). https://www.genome.gov/health/Genomics-and-Medicine

[13] *DISHA and HIPAA, How Do They Compare?* (2023, 10 26). Compliancy Group. https://compliancy-group.com/disha-and-hipaa-how-do-they-compare/

[14] *Role of AI in early cancer detection*. (2025, February 18). Apollo Hospitals. https://www.apollohospitals.com/health-library/the-role-of-artificial-intelligence-in-early-cancer-detection-a-game-changer-for-patients-at-apollo-precision-oncology-centre

[15] Powell, A. (2025, March 20)**.***How AI is transforming medicine*. Harvard Gazette. https://news.harvard.edu/gazette/story/2025/03/how-ai-is-transforming-medicine-healthcare/

[16] *What Is Artificial Intelligence (AI)?* (n.d.). Google Cloud. https://cloud.google.com/learn/what-is-artificial-intelligence

[17] National Human Genome Research Institute. (n.d.). *Genomics and medicine*. National Institutes of Health. https://www.genome.gov/health/Genomics-and-Medicine

[18] Apollo Hospitals. (2025, February 18). *The role of artificial intelligence in early cancer detection: A game-changer for patients at Apollo Precision Oncology Centre*. Apollo Hospitals. https://www.apollohospitals.com/health-library/the-role-of-artificial-intelligence-in-early-cancer-detection-a-game-changer-for-patients-at-apollo-precision-oncology-centre

[19] Zhou, Y., Wang, Y., Liu, Y., & Zhang, Y. (2024). The role of AI in hospitals and clinics: Transforming healthcare in the digital age. *Frontiers in Artificial Intelligence*, *7*, 11047988. https://doi.org/10.3389/frai.2024.11047988

[20] Oladele, O. K. (2024, October 10). *AI-powered medical imaging: A comprehensive review of applications, benefits, and challenges*. ResearchGate. https://www.researchgate.net/publication/385074391_AI-Powered_Medical_Imaging_A_Comprehensive_Review_of_Applications_Benefits_and_Challenges

[21] Wang, S., Summers, R. M., & Yao, J. (2021). Artificial intelligence and machine learning for medical imaging. *Journal of Biomedical and Health Informatics*, 25(8), 2720–2732. https://doi.org/10.1109/JBHI.2021.3066155

International Journal of Computer Research & Technology
ISSN 2454-7719
** A Blind Peer Reviewed Journal **
Volume-10, Issue-2, July-Dec 2025
Paper ID: CS-14

Cyber security In HealthCare

Dr. Tanuja Mahajan
Professor, Late Bahusaheb Hiray S.S Trust's College
tanujamahajan18@gmail.com

Suraj Karnati
Student
Dept. Of Computer Application Mumbai, India
Surajkarnati10@gmail.com

Abstract- *Unprecedented gains in effectiveness, accessibility, and care quality have resulted from the growing digitization of healthcare systems. But it has also made the industry more vulnerable to a quickly changing array of cyber threats. This study examines the vital role cyber security plays in the healthcare industry, highlighting the necessity of safeguarding connected medical devices, digital infrastructure, and private patient data against a variety of malevolent actions. It examines contemporary techniques such network segmentation, AI-driven anomaly detection, encryption, and access controls, stressing both their advantages and disadvantages. In order to contextualize the risks and countermeasures, the study also examines real-world case studies including the Sing Health hack and the UHS ransom ware assault, as well as regulatory frameworks like HIPAA, GDPR, and HITECH.The research highlights the necessity of a multi-layered, proactive protection strategy by analysing the threat environment, which includes phishing, DDoS attacks, and vulnerabilities in IoMT and legacy systems. It also assesses cutting-edge frameworks and technologies, such as block chain, artificial intelligence, and zero trust architecture, and provides helpful suggestions for advancements at the administrative, technical, and policy levels. According to the paper's conclusion, strong cyber security is now a must for contemporary healthcare and calls for constant innovation, cross-sector cooperation, and a steadfast dedication to safeguarding patient safety and trust.*

I. Introduction

What's the Deal with Healthcare Cybersecurity? Keeping the digital locks on everything that counts in a hospital or doctor's office is what healthcare cybersecurity is all about. This includes all of the computers, patient data, and even those high-end, internet-connected medical devices. It involves the use of smart technology, well-defined regulations, and sound practices to ensure that no criminals can infiltrate, tamper with, or steal personal data. This cybersecurity issue becomes increasingly crucial as healthcare becomes more digital, which helps us manage.

II. Operations More Efficiently And Provide Better Care For Patients.

Why Should We Even Care? To be honest, this is a huge problem, not simply an IT issue. Hackers value patient information far more than your credit card information. Hospitals hold a wealth of extremely private information, including your identity, health conditions, insurance information, and occasionally even fingerprints. However, money isn't the only factor. A hospital may experience complete anarchy if it is the target of a cyber attack. In the worst situation, people's lives could be in danger, surgeries could be postponed, and treatments could go awry. Therefore, maintaining the security of our healthcare systems is more than simply protecting privacy; it's also about ensuring that patients are safe and have faith in the individuals who are caring for them.

II. Existing Practices in Healthcare Cyber Security:

A strong, multi-layered cyber security plan has to be put in place as a result of the growing digitization of healthcare. A defense-in-depth strategy that includes technical, administrative, and physical security layers is continuously recommended by academic research and industry experts (Samuel, R. et al., 2023). Essential procedures like network

segmentation tactics, anomaly detection methods, access control systems, and encryption are at the heart of this paradigm. With protocols like TLS for data in transit and AES-256 for data at rest being widely used throughout healthcare systems, encryption is still a fundamental component of data protection. These techniques guarantee the integrity and confidentiality of data, especially while it is being transferred between networks.It's important to recognize, though, that encryption by itself cannot eliminate internal threats like those caused by malevolent insiders or inappropriate credential usage (Sharp, 2025). To limit system access to authorized workers, access control technologies such as biometric verification, two-factor authentication (2FA), and role-based access control (RBAC) are widely used. Although these restrictions have been shown to be successful in preventing unwanted access, their effectiveness may be jeopardized if credentials are stolen or improperly maintained. Additionally, combining anomaly detection powered by AI and ML has shown to be a useful tool for spotting suspicious activity in real time.The use of machine learning techniques to detect departures from accepted behavioral norms in Internet of Medical Things (IoMT) networks is highlighted by studies by Alkassasbeh (2024) and Taha et al. (2025). These systems do have some inherent drawbacks, though, as model drift and false positives can gradually reduce their efficacy. Network segmentation, a tactic that involves logically separating clinical systems from administrative or guest networks in order to prevent security breaches, is another essential component. This strategy is especially important in settings with a lot of third-party connectors or outdated systems.

Comparative approaches: The existing research also compares different methods, assessing their operational trade-offs and intrinsic advantages. For example, encryption provides strong data secrecy, but it is not very effective against threats that come from inside the company's boundaries. Although they serve vital gatekeeping purposes, access control systems are susceptible to compromise of user credentials. Although AI-based detection provides dynamic threat identification, it requires constant training and careful fine-tuning to remain as effective as possible. At the same time, blockchain technology has been suggested as a possible way to provide tamper-proof audit trails for private medical records, while not yet being extensively used in the healthcare industry. However, there are major implementation challenges due to its high processing requirements and the difficulties integrating it with current Electronic Health Record (EHR) platforms (Bako & Oni, 2025). Healthcare frequently uses a number of cybersecurity strategies, each with unique benefits and drawbacks. Data confidentiality can be effectively ensured by encryption, but insider threats cannot be prevented by it. Though it can be jeopardized if user credentials are taken, access control aids in preventing unwanted access to systems. Real-time threat identification is possible with AI and machine learning-based detection systems; nevertheless, they are susceptible to false positives and algorithmic drift over time. Although blockchain technology provides unchangeable audit trails for medical data, its application in the healthcare industry is constrained by its high processing demands and difficult integration with current systems.

Regulatory Landscape:A thorough cybersecurity plan must also follow the laws and regulations controlling the security of medical records. In order to protect the privacy of Protected Health Information (PHI), the United States' Health Insurance Portability and Accountability Act (HIPAA) requires the deployment of administrative, technical, and physical safeguards. The European Union's General Data Protection Regulation (GDPR) emphasizes strict breach reporting procedures, user consent, and data minimization principles. Additionally, the Health Information Technology for Economic and Clinical Health (HITECH) Act imposes harsher penalties for non-compliance and encourages the use of secure Electronic Health Records (EHRs).These regulatory frameworks outline the operational and legal requirements for implementing cybersecurity, and new research emphasizes how crucial it is to align technical security measures with compliance requirements in order to reduce operational and legal risks (Ghosh et al., 2023).

III. THREAT LANDSCAPE IN HEALTHCARE

Because of the high intrinsic value of health data, the intricacy of hospital information systems, and the growing interconnection of medical devices, the healthcare sector faces a particularly difficult cyber threat environment. In order to impede the provision of healthcare, steal confidential patient information, or launch ransomware attacks, malicious actors—including cybercriminals, state-sponsored attackers, and malicious insiders—often take use of both technological flaws and human error.

Major Cyber Threats:

Several cyber threats present recurring and evolving risks to healthcare institutions:

Phishing Attacks: These are still some of the most common and efficient ways to access systems without authorization. Healthcare workers are regularly the subject of phishing attacks, which send

them phony emails intended to steal passwords or install malicious software. Phishing was a contributory cause in more than 80% of healthcare breaches, according to the Verizon Data Breach Investigations Report (2024), highlighting its persistent threat and relative ease of execution.

Distributed Denial of Service (DDoS) Attacks:DDoS attacks can hinder access to vital systems and interfere with necessary patient services by flooding hospital servers or publicly accessible portals with excessive traffic. A DDoS attack at Akron Children's Hospital in 2022, for example, momentarily prevented access to patient portals and telehealth services, underscoring the operational vulnerability of online healthcare infrastructure.
Insider Threats: When employees purposefully leak or unintentionally handle protected health information (PHI) improperly, they present serious dangers, whether through malice or carelessness. The 2015 UCLA Health hack, which resulted in the exposure of 4.5 million patient records because of unauthorized insider access, emphasizes how crucial strict access restrictions and thorough monitoring are.

EHR Exploits: Despite being essential to the delivery of contemporary healthcare, Electronic Health Record (EHR) systems are being targeted more and more because of the large amount of patient data they centrally store. Unauthorized access can be made easier by taking advantage of flaws in popular systems like Epic and Cerner. Inadequate network segmentation and front-end security procedures were blamed for the Sing Health breach (Singapore, 2018), which exposed the records of 1.5 million people, including the prime minister.

Healthcare-Specific Vulnerabilities:

In addition to general cyber threats, healthcare systems are susceptible to domain-specific weaknesses:

Internet of Medical Things (IoMT) Devices: Wearable health trackers, smart monitoring systems, and infusion pumps are examples of networked devices that frequently lack strong built-in security protections. Many are susceptible to exploitation since they use unencrypted communication protocols or run with default credentials (Taha et al., 2025).

Legacy Infrastructure: Many healthcare facilities still use antiquated operating systems, such Windows XP, which are no longer supported by important security updates. These outdated systems make it more difficult to respond to incidents and increase the possible attack surface (Sharp, 2025).

Third-Party Vendors: For billing, laboratory analysis, and medical imaging, healthcare systems commonly incorporate services from outside suppliers, some of whom may have laxer cybersecurity regulations. Critical healthcare systems may be vulnerable to outside threats if thorough vendor risk management is not implemented (Ghosh et al., 2023).

Unsecured Remote Access: Remote access methods were widely adopted, many of them rapidly implemented, as a result of the COVID-19 pandemic's rapid expansion of telehealth. Exploitable vulnerabilities in remote healthcare delivery are caused by poorly configured Virtual Private Networks (VPNs), unprotected home networks, and the lack of multi-factor authentication (MFA).

These various threat vectors highlight how urgently proactive, multi-layered, and healthcare-specific cybersecurity solutions that go beyond general IT security procedures are needed. The technologies and structures intended to reduce these inherent hazards will be examined in the next section.

V. SECURITY TECHNOLOGIES & FRAMEWORKS

As cyber threats targeting healthcare infrastructure continue their evolution in sophistication and scale, the implementation of robust security technologies and standardized frameworks has become an imperative. This section will explore key defensive tools, established cybersecurity frameworks, and emerging technologies that are shaping the present and future landscape of healthcare cybersecurity.

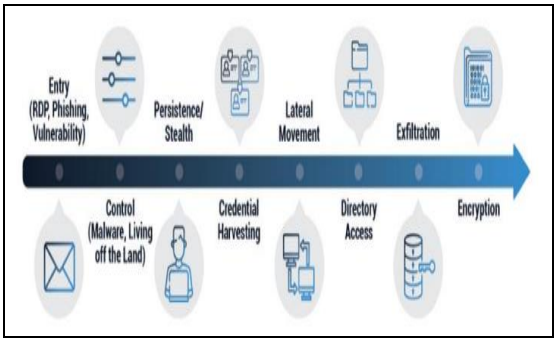


Figure 1 – Strategies to prevent Ransomware Attacks.

Tools Utilized in Healthcare Cyber Defence:

Healthcare organizations employ a diverse array of technologies to defend against both external and internal cyber threats:

Firewalls & Intrusion Detection Systems (IDS): As the first line of defense, they carefully examine all network traffic, both coming in and going out, in order to identify and stop hostile activity. Both perimeter and internal network security are improved by the integration of intrusion detection systems (IDS), which fall into one of two categories: signature-based or anomaly-based.

Security Information and Event Management (SIEM): In order to provide real-time threat intelligence and enable quicker incident detection and response capabilities, SIEM solutions are made to gather, compile, and analyze log data from multiple network endpoints. SIEM's capacity to correlate data across administrative networks, the Internet of Medical Things (IoMT), and Electronic Health Records (EHR) greatly benefits healthcare settings.

Biometric Authentication: Healthcare systems are incorporating technologies like fingerprint recognition, iris scans, and facial recognition for both physical and digital access control in response to the growing demand for safe and easy authentication methods. In high-risk settings like operating rooms or pharmaceutical storage facilities, this is very helpful.

Frameworks for Cybersecurity Governance

The adoption of structured cybersecurity frameworks ensures consistency, regulatory compliance, and accountability in the management of healthcare information systems:

NIST Cybersecurity Framework (CSF):



Figure 2 – NIST Framework.

Developed by the National Institute of Standards and Technology, this widely adopted framework encompasses five core functions - Identify, Protect, Detect, Respond, Recover - providing organizations with a comprehensive guide for developing and implementing a robust cybersecurity strategy.

ISO/IEC 27001:



Figure 3 – ISO 27001 Compliance Framework.

This international standard delineates best practices for establishing, implementing, maintaining, and continually improving an information security management system (ISMS). Its adoption across healthcare institutions ensures alignment with globally recognized security benchmarks.

Zero Trust Architecture (ZTA):

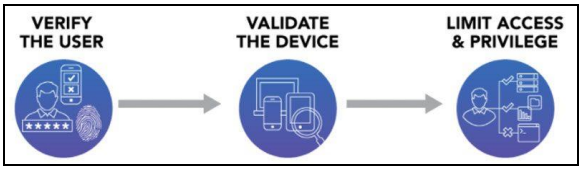


Figure 4 – Zero Trust Architecture

Unlike conventional security models that focus on the perimeter, ZTA is based on the core idea of "never trust, always verify." This paradigm is especially useful for managing distributed healthcare ecosystems, such as remote diagnostics and mobile access to EHR systems, because it requires constant user, device, and application verification

Emerging Technologies

To effectively address the increasing complexity and real-time nature of cyber risks within healthcare, research and innovation are accelerating in several key areas: Artificial Intelligence (AI) & Machine Learning (ML):

A dual-phase machine learning (ML)-based intrusion detection model designed especially for the Internet of Medical Things (IoMT) was presented by Taha et al. (2025), who showed a notable decrease in false positive rates in anomaly detection. In order to promote proactive patient and network safety, kassasbeh (2024) has created a deep learning

framework that can identify threats in wearable medical devices in real time.

Blockchain Technology:

To improve traceability and guarantee tamper-proof audit logs, Bako & Oni (2025) have shown how blockchain technology and AI may be combined to construct immutable, decentralized ledgers for medical records. Blockchain technology has the potential to preserve the provenance and integrity of data in interactions with third-party vendors as well as across interoperable health systems.

These technologies, when combined with well-established frameworks, serve as the cornerstone of a robust cybersecurity strategy in modern healthcare. Integrating intelligent, flexible, and standardized solutions will be essential for protecting sensitive patient data and maintaining business continuity as threats continue to change.

VI. Case Studies

Case Study 1:

Ransomware Attack on Universal Health Services (UHS) (2020) A phishing email was used to launch a sophisticated ransomware attack on Universal Health Services (UHS), a well-known healthcare company in the United States, in 2020. Over 400 healthcare facilities nationwide were affected by the Ryuk ransomware version, which seriously disrupted operational procedures. Medical staff were forced to switch back to manual documentation methods, like pen-and-paper records, when electronic medical systems were rendered unworkable for many days. This resulted in delays in vital patient care and surgical procedures. In reaction to this incident, UHS hired a professional third-party cyber security company to aid in the recovery process and segmented the network to stop the attack from spreading. This incident also highlighted the urgent need for improved cyber security procedures, which led UHS to fund more extensive staff training initiatives meant to counteract potential cyber threats.

Case Study 2:

SingHealth Data Breach (Singapore, 2018) In 2018, Singapore's SingHealth experienced a significant data breach when cyber attackers exploited vulnerabilities present in a front-end web application. This security lapse resulted in the compromise of personal and medical information belonging to 1.5 million patients, including high-profile individuals such as Singapore's Prime Minister, Lee Hsien Loong. The breach exposed critical deficiencies in SingHealth's security architecture, notably inadequate segmentation between disparate information technology systems, which enabled the attackers to gain access to sensitive data. Additionally, the intrusion remained undetected for several weeks. Following this incident, SingHealth undertook a comprehensive overhaul of its cybersecurity infrastructure, encompassing enhancements to national cyber monitoring systems, to preempt future breaches and bolster overall system resilience. This case serves as a salient reminder of the paramount importance of robust cybersecurity measures and rapid threat detection capabilities within healthcare organizations.

VII .Recommendations & Future Scope

Technical Measures

A number of technological steps are suggested to improve healthcare businesses' cybersecurity posture. When paired with ongoing model training, AI-based anomaly detection systems can assist in proactively detecting and averting possible risks. Sensitive information will be protected from potential risks from quantum computing by upgrading encryption standards to ensure post-quantum cryptography readiness. The security of linked medical equipment will also be improved by installing firewalls designed specifically for the Internet of Medical Things (IoMT) and making sure that firmware updates are performed on a regular basis.

Administrative Strategies

The implementation of administrative methods is essential to cultivating a culture that prioritizes security. It is crucial to set up thorough cyber hygiene rules, which should include strict password management guidelines and frequent security training for employees. Finding vulnerabilities before they can be exploited is made easier with the use of simulated phishing campaigns and regular penetration testing. Additionally, ensuring that external relationships do not introduce new security dangers can be achieved through vendor security audits and a strong third-party risk management program.

Policy and Legal Recommendations

National healthcare cyber security frameworks must be established at the policy level in order to provide uniform standards and compliance requirements for the industry. By sharing threat intelligence, public-private cooperation will enhance collective security by enabling prompt reaction to new threats. Furthermore, a large investment in workforce development—especially for health IT professionals—will guarantee a team that is prepared to handle the constantly changing cyber security environment.

Future Challenges

Healthcare companies will encounter new difficulties as they develop. Current encryption algorithms will eventually be threatened by quantum

computing, which calls for the creation of quantum-resistant alternatives. Deepfake-based phishing and AI-generated malware are two examples of AI-powered attacks that are becoming more dangerous and necessitate sophisticated detection tools. Last but not least, as global healthcare systems grow more interconnected, maintaining data sovereignty and guaranteeing safe cross-border data sharing will become more difficult. To overcome these obstacles, cooperation and constant innovation will be needed.

VIII. CONCLUSION

Cyber security is now a crucial part of patient safety due to the increasing digitization of healthcare systems. Because healthcare depends more and more on linked technologies, there is a greater chance of cyberattacks and threats. The significance of proactive and all-encompassing cyber security strategies that take into account organizational procedures as well as technical developments is highlighted by this study. Through an analysis of diverse risks, technologies, real-world case studies, and regulatory frameworks, this study offers a useful road map for creating healthcare infrastructures that are more robust.

Because healthcare systems must adjust to new threats like quantum computing, AI-powered attacks, and changing privacy concerns, cyber security innovation must be ongoing. Furthermore, to properly address these issues, cross-sector cooperation among government organizations, technological specialists, and healthcare providers is crucial. To protect patient safety and trust as well as the integrity of healthcare systems, cyber security must ultimately be seen as a core component of healthcare delivery rather than an add-on issue.

REFERENCES

[1] Alkhathami, M. (2024) Anomaly detection in IoT-based healthcare: machine learning for enhanced security '. Sci Rep, 14(1). [Online]. Available at: https://doi.org/10.1038/s41598-024-56126-x (Accessed: 10 April 2025).

[2] Bako, N. Z. and Oni, O. (2025) 'Integration of AI and Blockchain for Secure Data Management'. World Journal of Advanced Research and Reviews, 25(03), pp. 1668-1672. [Online]. Available at: https://doi.org/10.30574/wjarr.2025.25.3.0784 (Accessed: 10 April 2025).

[3] Samuel, R. et al. (2023) ' Strengthening Cybersecurity in Indian Healthcare – Lessons from the Recent Ransomware Attacks on Hospitals'. International Journal of Advance Research, Ideas and Innovations in Technology, 10(6), pp. 97-103. [Online]. Available at: https://www.researchgate.net/profile/Samuel-r/publication/385852121_Strengthening_Cybersecurity_in_Indian_Healthcare/links/67375da64a70511f0720023c/Strengthening-Cybersecurity-in-Indian-Healthcare.pdf (Accessed: 10 April 2025).

[4] National Institute of Standards and Technology (NIST) (2018) Cybersecurity Framework Version 1.1. [Online]. 1 Available at: https://www.nist.gov/cyberframework (Accessed: 10 April 2025).

[5] Smart, W. (2018) 'Lessons learned review of the WannaCry Ransomware Cyber Attack.' [Online]. Available at: https://www.england.nhs.uk/wp-content/uploads/2018/02/lessons-learned-review-wannacry-ransomware-cyber-attack-cio-review.pdf (Accessed: 10 April 2025).

[6] Ponemon Institute (2023) Cost of a Data Breach Report 2023. IBM Security. [Online]. Available at: https://d110erj175o600.cloudfront.net/wp-content/uploads/2023/07/25111651/Cost-of-a-Data-Breach-Report-2023.pdf (Accessed: 10 April 2025).

[7] Safi, M. et al. (2024) ' Distributive Continuous Profiling for IoT Devices'. [Online]. Available at: https://unbscholar.dspace.lib.unb.ca/server/api/core/bitstreams/d5e38a0c-308f-4d02-bb38-297163ec8f22/content (Accessed: 11 April 2025).

[8] Agarwal, A. et al. (2020) ' Healthcare Data Breaches: Insights and Implications'. [Online]. Available at: https://www.mdpi.com/2227-9032/8/2/133 (Accessed: 11 April 2025).

[9] Key lessons from the Public Report of the Committee of Inquiry (COI) on SingHealth cyber attack. [Online]. Available at: https://www.pwc.com/sg/en/risk-assurance/assets/coi-on-singhealth-cyber-attack-201901.pdf (Accessed: 11 April 2025).

[10] Taha, M. S. et al. (2025) 'HybridIoMT Framework for Cybersecurity in IoMT'. [International Journal of Intelligent Engineering and Systems], 18(4), pp. 308-317 Available at: https://www.researchgate.net/profile/Mustafa-Taha-2/publication/390091375_HybridIoMT_A_Dual-Phase_Machine_Learning_Framework_for_Robust_Cybersecurity_in_Internet_of_Medical_Things/links/67deafac72f7f37c3e8403a3/HybridIoMT-A-Dual-Phase-Machine-Learning-Framework-for-Robust-Cybersecurity-in-Internet-of-Medical-Things.pdf (Accessed: 11 April 2025).

[11] Verizon (2024) Data Breach Investigations Report. [Online]. Available at: https://www.verizon.com/business/resources/reports/dbir/ (Accessed: 11 April 2025).

International Journal of Computer Research & Technology
ISSN 2454-7719
** A Blind Peer Reviewed Journal **
Volume-10, Issue-2, July-Dec 2025
Paper ID: CS-15

Block chain Technology In Healthcare– Ensuring Data Security & Privacy

Dr. Vikram Patalbansi
Assistant Professor,Late Bhausaheb Hiray S. S Trust's College Mumbai, India
Vikrampatalbansi14@gmail.com

Shubham Kanojia
Research Scholar, MCA, Late Bhausaheb Hiray S. S Trust's College Mumbai, India

Abstract- *Blockchain is emerging technology being applied to create innovative solutions across various sectors, including healthcare. A blockchain network is used in the healthcare system to preserve and exchange patient data among hospitals, diagnostic laboratories, pharmaceutical firms, and physicians. Blockchain applications can accurately identify severe and even dangerous errors in the medical field. Therefore, it improves the performance, security, and transparency of medical data sharing in the healthcare system.*

This technology is beneficial for medical institutions to gain insights and enhance the analysis of medical records. In this paper, we study blockchain technology and its significant benefits in healthcare. Various capabilities, enablers, and a unified workflow process of blockchain technology to support global healthcare are discussed through diagrams. Finally, the paper identifies and analyzes fourteen significant applications of blockchain in healthcare. Blockchain also plays a crucial role in preventing deception in clinical trials. The technology has the potential to improve data efficiency, reduce the risk of data manipulation, and support a secure data storage structure. It offers versatility, interoperability, accountability, and authentication for data access. Since health records need to remain safe and confidential for multiple purposes, blockchain helps ensure decentralized protection and mitigates specific threats to data security.

Keyword- *BlockchainTechnology, Healthcare, DataSecurity, DataPrivacy, ElectronicHealth Records (EHRs), Decentralization, SmartContracts, Patient Data, Cryptography, Fraud Detection, Medicine Traceability, Vaccine Certification, Clinical Trial Integrity*

I. INTRODUCTION

In recent years, the healthcare industry has embraced digital changes with the use of electronic health records (EHRs), telemedicine platforms, and health information systems. These changes have improved patient care and efficiency but also created issues with data security, privacy, and trust. Healthcare data is sensitive, and breaches can have serious consequences.

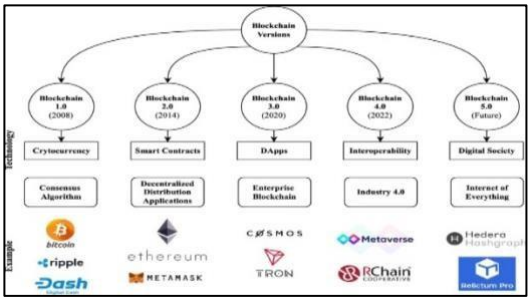
Traditional centralized databases face risks such as cyber-attacks and data tampering. Blockchain technology presents a solution by providing a decentralized and secure way to manage data. This paper looks at how blockchain can enhance data security, privacy, and integrity in healthcare, examines current challenges, reviews blockchain solutions, and proposes a model for safer data sharing among patients and providers. The goal is to show how blockchain can improve healthcare data management and build patient trust in digital systems.

Block chain

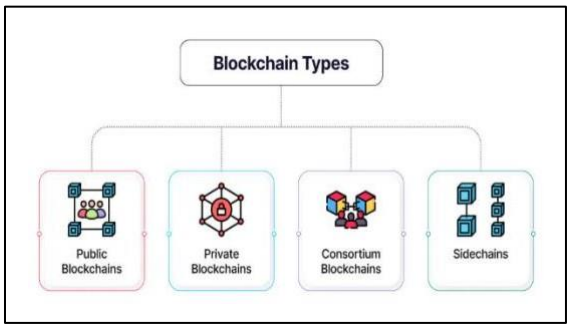
Block chain was popularized by Bit coin's Success and may be used to conduct secure and trustworthy transactions over an unfrosted network without depending on a centralized third party. We shall now discuss the core components of the block chain. Based on the rights granted to network nodes, three kinds of block chain systems exist:

1. Private block chain: Access control governs the private blockchain network functions, requiring authorization or an invitation before users may join.
2. Public ledger system: The public blockchain is accessible to anybody at any moment who wishes to

participate as a basic node or a miner for economic benefits.



3. Blockchain consortium: The consortium blockchain, which over between public and private blockchains, is referred to as "semi-private". It is given to a collection of authorized organizations that are often used in enterprises to advance business.



II. LITERATURE REVIEW.

Many researchers have studied how blockchain technology can help improve

data security and privacy in the healthcare sector. Since healthcare records are very sensitive, there is a strong need to protect them from hackers, misuse, and unauthorized access.

A research study by Xia et al. (2017) introduced a system called MeDShare. This system uses blockchain to safely share patient data between cloud service providers. It allows data to be shared without needing to fully trust the other party, and it uses smart contracts to manage who can access the data. Another study by Agboetal.(2019) looked at many blockchain projects in healthcare. They found that blockchain can be used in different areas like managing medical records, tracking medicine in the supply chain, and protecting clinical trial data. However, they also noted some problems like blockchain systems being slow, hard to scale, and difficult to connect with existing hospital software.

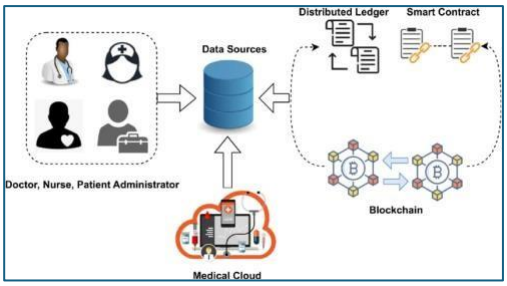
Mettler (2016) discussed how blockchain can make healthcare more transparent and trustworthy. For example, it can help track medicine from the factory to the hospital, making sure it's not fake or tampered with. Some researchers also recommend using permission blockchains, which means only trusted people or hospitals can join the system. This approach keeps the data private but still benefits from blockchain's security features.

Example to understand how blockchain technology can be used in healthcare to ensure data security and privacy:

1. Patient Health Records(EHRs) Example:

Imagine you visit a hospital in Mumbai and later need to show your records at a clinic in Delhi. With blockchain, your health records are stored securely and cannot be changed. You control who sees them by giving permission through a secure digital key.

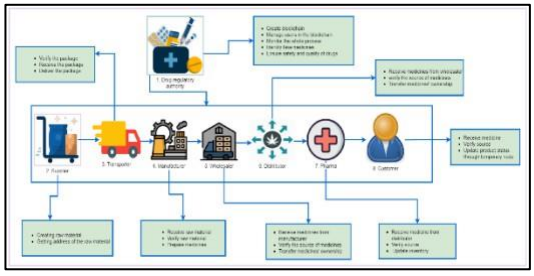
Benefit: Only the doctors you trust can view your medical history, and no one can tamper with it.



2. Tracking Medicines Example:

A fake batch of medicines is sold in the market. With blockchain, every step from the manufacturer to the pharmacy is recorded. Anyone can trace the medicine's journey.

Benefit: This ensures the medicine is real and not expired or fake.



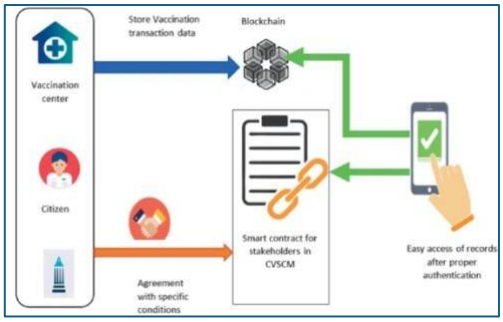
3. Health Insurance Claims Example:

You file a claim for a medical procedure. Normally, this takes time and a lot of paperwork. With blockchain smart contracts, the claim can be automatically verified and processed without delays.

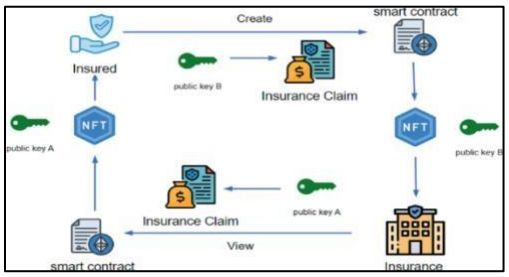
Benefit: Faster processing and less chance of fraud.

4. Remote Patient Monitoring
Example:

A diabetic patient uses a wearable device to track sugar levels. This data is directly sent to the doctor using a blockchain system.
Benefit: The data is secure, accurate, and cannot be modified, which helps doctors make better decisions.



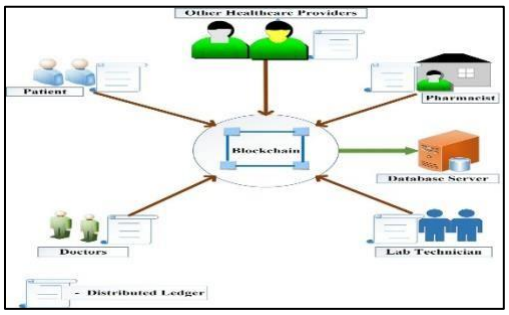
5. COVID-19 Vaccine Certificates



Example:

People traveling needed to show vaccine certificates. Blockchain can store these certificates securely so no one can create fake ones.

Benefit: Authorities can trust the certificate is real.
COVID-19Vaccine Certificates



V. Problem Definition
Securing Patient Data – Traditional vs Blockchain-Based Systems

Scenario Overview:-A patient named Anjali visits a local clinic for a consultation. The clinic collects her medical history and lab reports and refers to specialists in a larger hospital. Her health data must be shared securely between the two institutions.

Clinic sends lab_report.pdf to Hospital_B via internal portal.
Hospital_B downloads the report.

1. Traditional Healthcare Data System Data Handling Process:
• The clinic stores Anjali's data in a centralized hospital management system.
• Data is shared with the specialist via email or uploaded to aloud portal.
• Audit trails are minimal or controlled by IT admins.
Example

Behaviour:

- Data Exposure Risk: If the portal is hacked, all records can be leaked.
- No Transparency: Anjali doesn't know who viewed her data.

No Immutable Logs: Access records can be modified or deleted.
Limited Control: She cannot revoke or approve access herself.

Specialist requests access via smart contract.
Anjali approves via health app.
Access granted, and transaction recorded immutably.

2. Blockchain-Based Healthcare Data System
Data Handling Process:
• Anjali's medical records are stored on a private healthcare blockchain.
• Each data access request is processed via smart contracts.
• Only verified users with Anjali's approval can access the data.

Example:-
Blockchain Log Entry:

Behaviour:

- Tamper-Proof Logs: Every access is recorded and cannot be altered.
- Patient Control: Anjalidecides who can access her data.
- Data Privacy: Only encrypted data is shared through secure keys.
- Trust & Transparency: Everyone in the system can verify the access trail.

III. OBJECTIVE:-

Enhanced Data Security:

In healthcare, Blockchain contributes to the security of sensitive health data. Health systems area prime target for cyber-attacks, whereby data breaches lead to unauthorized access. Blockchain's decentralized and cryptographic guarantee that:

• Immutable Data:
Patient records are permanently stored on the blockchain and cannot be altered without network-wide approval, ensuring data integrity.

• Decentralized Access:
No central authority controls the data, reducing the risk of system failure or hacking.

• Encryption:
All patient information is encrypted, and only authorized users with the correct key can access it, preserving privacy and confidentiality.

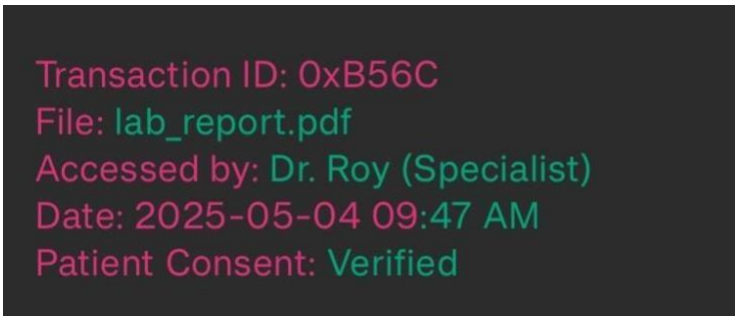
Enabling Interoperability:

Healthcare data typically resides in silos across various systems. This creates barriers to sharing patient information between providers. Blockchain provides a unified, decentralized platform for seamless data sharing:

• Cross-Platform Data Sharing: Enables seamless and secure sharing of patient data across hospitals, clinics, and specialists.

• Patient-Centric Control: Empowers patients to manage who accesses their health information, enhancing transparency and trust.

• System Integration:
Facilitates real-time access to medical records, improving coordination and continuity of care.



IV. LIMITATIONS

1. Scalability Challenges:

Blockchain networks, especially public ones, face scalability issues when handling large volumes of healthcare data such as medical imaging or real-time monitoring records.

2. Integration with Legacy Systems:

Most healthcare providers still rely on legacy electronic health record (EHR) systems, making seamless blockchain integration complex and expensive.

3. Latency and Transaction Speed:
Consensus mechanisms like Proof of Work (PoW) can introduce delays, which are unsuitable for real-time healthcare applications such as emergency responses.

4. Data Storage Constraints:

Due to the size limitations of blockchains, storing full medical records on-chain is impractical. Off-chain storage solutions require additional layers of security and coordination.

5. Regulatory and Legal Hurdles:

Blockchain's immutability conflicts with regulations like GDPR that require the right to data erasure. Legal clarity on smart contracts and data ownership is still evolving.

6. High Implementation Costs:

Setting up and maintaining a blockchain infrastructure involves significant initial investment in hardware, development, and skilled personnel.

V. FUTURE SCOPE

1. Interoperable Blockchain Standards:

Development of standardized frameworks for blockchain integration across different healthcare

systems can streamline interoperability and data exchange.

2. AI and Blockchain Synergy:

Combining blockchain with AI can enable secure, automated diagnosis systems while maintaining data privacy and auditability.

3. Private and Consortium Blockchains:

Future systems can leverage permissioned or hybrid blockchain models (e.g., Hyperledger) to reduce latency and control access more effectively.

4. Patient-CentricDataOwnership:

Decentralized healthcare models can empower patients with full control over their medical records, enabling consent-based sharing and transparency.

5. Real-Time Insurance and Billing:

Smart contracts could automate claims processing, billing, and insurance verifications securely and transparently.

6. Enhanced Off-ChainSecurityModels:

Future solutions can improve the integration between blockchain and off-chain storage (like IPFS or cloud systems) with advanced encryption and access mechanisms.

VI. CONCLUSION

Blockchain technology offers transformative potential for enhancing data security and privacy in healthcare. By decentralizing data storage and employing cryptographic techniques, blockchain ensures that patient information is immutable and accessible only to authorized parties. This approach mitigates risks associated with centralized data systems, such as unauthorized access and data breaches. Furthermore, blockchain facilitates interoperability among disparate healthcare systems, enabling seamless and secure data sharing across hospitals, clinics, and specialists. Patients gain greater control over their health information, deciding who can access their data, thus fostering trust and transparency in healthcare interactions. While challenges like scalability, integration with existing systems, and regulatory compliance persist, ongoing advancements and the adoption of hybrid blockchain models hold promise for addressing these issues. As the technology matures, blockchain is poised to play a pivotal role in safeguarding patient data, streamlining healthcare operations, and enhancing overall patient care.

REFERENCES

[1] Blockchain Technology in Healthcare: A Systematic Review by Cornelius C. Agbo ,Qusay H. Mahmoud ORC ID andJ. Mikael Eklund Healthcare 2019, 7(2), 56

[2] Thomas F Heston.ACase Study in Blockchain Healthcare Innovation.

[3] Blockchain in Healthcare: Real-World Case Studies and ImplementationsBy PratibhaYadav September 29,

[4] Healthcare Data Breaches in February 2025: Over 1.2 Million Patients Affected by Monica McCormack (March 25th, 2025)

[5] MeDShare:Trust-lessMedicalData Sharing Among Cloud Service Providers Via Blockchain Articlein IEEE Access • July 2017

[6] Blockchain-Based Healthcare Records Management Framework: Enhancing Security, Privacy, and Interoperability Technologies2024,12(9)

[7] Blockchain based Healthcare Data Management Publisher: IEEE Karthiga M; Padmavathy C; V.S. Akshaya

International Journal of Computer Research & Technology
ISSN 2454-7719
** A Blind Peer Reviewed Journal **
Volume-10, Issue-2, July-Dec 2025

Paper ID: CS-16

Review Paper on Investigation on Performance of Machine Learning Algorithms for Prediction of Human Age

Swati Laxman Nimgale

Department of Information Technology
Pillai College of Engineering Panvel, Navi Mumai
swati24mtit@student.mes.ac.in

Prof. Prashant Nitnaware

Department of Information Technology Pillai College of Engineering Panvel, Navi Mumbai
pnitnaware@mes.ac.in

Abstract- *In recent years, the rapid advancement of machine learning, a key subset of artificial intelligence, has significantly transformed various aspects of daily life. Its applications span across numerous domains, including healthcare for disease diagnosis, financial sectors for fraud detection, and industrial systems for predictive maintenance. This project focuses on the development and evaluation of a data-driven model designed to predict both machine failure and human age based on input data. The primary objective is to analyse and rank dataset features to enhance model accuracy and compare the performance of multiple machine learning algorithms using various evaluation metrics. Special emphasis is placed on optimizing algorithm performance through parameter tuning and feature selection. Additionally, the project presents a system capable of estimating the age of individuals from facial images using advanced machine learning techniques. This research aims to contribute to more reliable and accurate predictive systems in both industrial and human-centered applications.*

Keywords- *Put your keywords here, keywords are separated by comma.*

I. INTRODUCTION

In machine learning, facial age estimation involves teaching a model to guess a person's age just by looking at their face (1). The model can either predict an exact age (regression) or an age group [7] (classification). To start building such a model, a proper dataset with labelled images (showing different lighting, angles, and facial expressions) is needed for training and testing (2). Once the data is collected, the next step is pre-processing. This includes detecting and cropping the face in each image to remove unnecessary background elements. The face is then rotated and aligned so that all images are in a similar position, making it easier for the model to learn (3, 4). After this, important features related to aging—like skin texture or facial structure—are extracted from the images. These features are then used to train a machine learning model, either a classifier or regression model, to recognize patterns related to different ages (4, 5).

Finally, the model's accuracy is tested using standard evaluation techniques to see how well it can estimate age from new images (6)

1.1 Objectives

To rank and select the most influential features to enhance the accuracy and efficiency of ML models. To compare the performance of various machine learning algorithms for machine failure prediction.

To build and evaluate a deep learning model that predicts human age based on input images.

To analyze the effects of different hyper parameters and model architectures on final outcomes.

1.2 Challenges:

Developing accurate age estimation models presents several challenges. These difficulties are

generally categorized into two types: controllable and uncontrollable. Controllable challenges are those that can be addressed by improving model design, tuning parameters, or applying better pre-processing techniques. Examples include variations in head pose, image quality, and resolution. On the other hand, uncontrollable challenges are factors beyond the current capabilities of machine learning models, making them harder to manage and reducing prediction accuracy.

a) Head Pose and Facial Alignment

One major controllable factor is the variation in head pose and alignment in facial images. Since real-world images are taken under various conditions, faces are often not centered or consistently positioned. This misalignment can affect model performance. To address this, most models apply pre-processing steps where the face is detected and then aligned to a standard orientation. Studies have shown that inconsistent head poses negatively affect the model's accuracy.

b) Image Resolution

Image clarity is crucial in computer vision tasks, including age estimation. Low-resolution images often miss important aging indicators like fine lines or detailed facial contours, which are key for distinguishing age differences. The quality of the image depends on the device used to capture it, and inconsistent resolutions can hinder the learning process. This issue can be minimized by applying image enhancement or upscaling methods to normalize the resolution of both training and testing data. Prior research confirms that resolution enhancement improves model accuracy.

c) Lifestyle and Health Factors

A person's lifestyle and health status greatly influence their physical appearance, sometimes making them look younger or older than their actual age. This variation poses a significant challenge because models may incorrectly associate certain facial traits with the wrong age group. These factors are considered uncontrollable, as they introduce unpredictable variations that current models struggle to interpret accurately.

d) Limited and Imbalanced Data

One of the major issues affecting model performance is the lack of sufficient and diverse training data. Many available facial datasets either lack proper age labels or do not adequately represent all genders, age groups, or ethnic backgrounds. This imbalance often leads to over fitting, where the model performs well on the training data but poorly on new, unseen data. Several studies have pointed out that insufficient diversity in datasets is a leading cause of misclassification in age prediction.

e) Genetic Differences

Genetic makeup plays a critical role in how individuals age. Some people may retain youthful features longer, while others may show signs of aging earlier. These biological differences are deeply tied to a person's gender, ethnic background, and environmental conditions throughout their life. Such factors are currently beyond the control of machine learning algorithms, making genetic variation a key limitation in accurate age estimation.

II. System Architecture of the Age Prediction

The Figure 1 illustrates the general architecture of a facial age estimation system based on machine learning and deep learning techniques. It represents the complete workflow starting from raw image or video input to the final output of predicted age. The model combines both traditional image processing steps and advanced deep learning methods for robust age estimation. This structured process ensures that the system handles variations in face position, lighting, and quality while producing accurate age prediction.

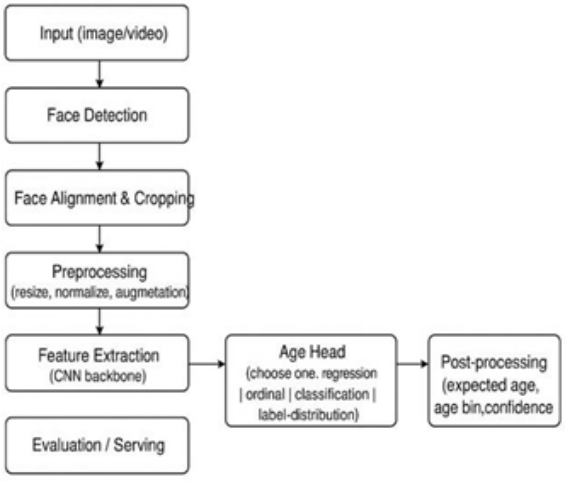


Figure 1. System Architecture of the Age Prediction

- ***Input (Image/Video)***

The process begins with capturing human facial data, either from still images or video frames. This serves as the raw input for the system.

- ***Face-Detection***

The system locates the face within the image and separates it from the background. This step ensures that only the facial region is processed for age estimation.

- ***Face-alignment-cropping***

Once the face is detected, it is aligned using key landmarks such as the eyes, nose, and mouth. The aligned face is then cropped to a fixed region, helping reduce variations caused by pose or orientation.

- ***Pre-processing***

The cropped face undergoes pre-processing, which includes resizing to a standard size, normalizing pixel intensity, and applying augmentation techniques such as flipping or rotation. These steps improve data consistency and enhance model robustness.

- ***Feature Extraction (CNN Backbone)***

Important facial characteristics are extracted using a deep learning model (commonly a Convolutional Neural Network). These features capture patterns such as wrinkles, texture, and shape that are strongly related to age.

- ***Age-Head (Prediction-Layer)***

The extracted features are passed to the prediction head, which can be designed in different ways:

  - Regression: Outputs the exact age as a continuous value.
  - Ordinal Regression: Considers age as an ordered variable to preserve the natural sequence of ages.
  - Classification: Categorizes the face into discrete age groups (e.g., 0–9, 10–19, etc.).
  - Label Distributin Learning: Predicts a probability distribution around the true age, accounting for uncertainty.

- ***Post-Processing***

The output from the prediction head is refined to generate the final age estimate. This may include calculating the expected age, assigning an age group, or providing confidence scores.

Finally, the model is either evaluated (using metrics such as Mean Absolute Error or classification accuracy) or deployed for real-world applications, such as security, healthcare, or user personalization.

III. LITERATURE REVIEW

Deep Learning-Based Age Estimation for Fall Detection by Jiayi Yu et al. (2023) [1] proposed an age estimation method integrated with fall detection systems. Their approach uses a phased backbone architecture, VoVNetv4, which includes the ROSA module and an adaptive stage module for enhanced feature extraction. By categorizing fall behavior according to estimated age, the system prioritizes detection among vulnerable age groups. The model efficiently processes facial features to assist in real-time monitoring, especially for elderly individuals at risk.

Predicting User Age Using Smartphone Data Mohammed Gollapalli and Atta-ur Rahman[2] developed a machine learning framework to predict user age based on the type of smartphone they use. Using a comprehensive dataset from STC (a major telecom provider), the model helps personalize services such as promotional offers or targeted advertisements. The study also suggests expanding the approach to predict other demographic traits using similar techniques.

Age Estimation from Panoramic Radiographs Using ML Willian Oliveira and Mariana Santos[3] explored the use of machine learning on dental panoramic radiographs for forensic age estimation. Their method combines the InceptionV4 architecture with targeted data augmentation strategies to improve model robustness. Despite variations in augmentation effectiveness, the system performed consistently across different age groups and maintained high stability even in challenging cases.

Enhancing Heart Disease Prediction with ML Abdul Saboor and Muhammad Usman [4] focused on improving heart disease prediction using various machine learning models. Although not directly related to facial age estimation, their work underscores the challenges of large datasets and feature extraction in medical applications. The study demonstrates that better attribute selection can significantly improve classification performance, a concept that is also applicable in age prediction models.

Evaluating Deep Learning Models for Facial Age Estimation in Digital Forensics Monika Roopak and Saad Khan [5] examined the effectiveness of deep learning models in forensic investigations, particularly for detecting the age of individuals in illegal images involving minors. In the UK, the Child Abuse Image Database (CAID) is used to match images via metadata and hashes. Their research highlights how automating age prediction using deep learning can significantly reduce manual effort and speed up case processing for law enforcement.

Age and Gender Prediction from Facial Images Using CNNs Puja Dey and Tanjim Mahmud[6] proposed a deep learning method using Convolutional Neural Networks (CNNs) for simultaneous age and gender prediction from facial images. The model effectively handles real-world, unfiltered images and integrates advanced image processing and optimization techniques. Functions like softmax and sigmoid are used for predicting age

and gender, respectively. Their comparative analysis shows strong performance across diverse datasets.

[Prediction of successful aging using ensemble machine learning algorithms by Asghari Varzaneh, Z., Shanbehzadeh, M., & Kazemi-Arpanahi, H. (2022)-[13] discussed on predicting successful aging using ensemble machine learning algorithms. The authors highlight the significance of identifying factors that contribute to healthy aging for improving healthcare decision-making. They utilized medical and demographic data to train ensemble models such as Random Forest, Gradient Boosting, and Bagging. The ensemble methods were shown to outperform single models in terms of prediction accuracy. The study emphasizes the ability of ensemble learning to manage high-dimensional datasets and improve reliability. The findings suggest that machine learning can provide early insights into aging-related health risks and support preventive interventions.

Coleman and Grover (2006) [7, 8] explained how facial aging is primarily influenced by volume loss in soft tissues and alterations in three-dimensional facial contours. The authors highlight that aging is not only due to skin laxity but also significant changes in fat distribution, muscle, and bone structure. These insights help guide modern aesthetic and reconstructive approaches for facial rejuvenation.

Levi&Hassner (2015)-[11], introduced the use of convolutional neural networks (CNNs) for automatic age and gender classification from facial images, showing significant improvements over traditional hand-crafted feature methods.

Raman-et-al.(2022)[12], proposed a deep learning framework for gender-specific facial age group classification, demonstrating enhanced accuracy by tailoring models to gender differences in aging patterns

Face spoofing, age, gender and facial expression recognition using advance neural network architecture-based biometric system." Kumar, S., Rani, S., Jain, A., Verma, C., Raboaca, M. S., Illés,

Z., & Neagu, B.-(2022)-[10, 14], presented an advanced neural networ architecture-based biometric system for recognizing face spoofing, age, gender, and facial expressions. The proposed system integrates multiple biometric traits to improve security and recognition accuracy. Deep learning frameworks were applied to extract robust facial features for classification tasks. The study shows that the architecture can successfully differentiate between genuine and fake faces, addressing spoofing attacks. It also demonstrates strong performance in predicting age and gender alongside facial emotions. The authors conclude that multimodal biometric approaches enhance reliability in real-world applications such as authentication systems.

Deep-learning based descriptors in application to aging problem in face recognition by Boussaad, L., & Boucetta,A.-(2022)-[15] investigated the use of deep- learning-based descriptors for tackling the aging problem in face recognition. Aging poses challenges to recognition systems since facial features undergo significant changes over time. The authors propose the use of convolutional neural network (CNN)-based descriptors to better capture invariant features across different age groups. Their experimental results indicate that deep descriptors outperform handcrafted features in recognizing aged faces. The paper also discusses the robustness of deep learning techniques in handling non-linear changes in facial appearance. The findings highlight the potential of deep descriptors for improving long-term face recognition accuracy

Apparent age prediction from faces: A survey of modern approaches. By Agbo-Ajala, O., Viriri, S., Oloko-Oba, M., Ekundayo, O., & Heymann, R. (2022)-[16], this article provided a comprehensive survey of modern approaches to apparent age prediction from facial images. Apparent age refers to the age perceived by humans, which often differs from chronological age. The paper reviews traditional machine learning models, deep learning approaches, and hybrid frameworks applied to this problem. Key challenges such as dataset imbalance, feature extraction, and accuracy limitations are discussed. The authors also compare different benchmark datasets used for training and evaluation. The survey concludes by identifying future directions, including multimodal learning and fairness considerations, to improve age prediction systems.

Facial age estimation using machine learning techniques: An overview Raman, V., & Then, P. (2022)-[17] examined various machine learning techniques used for facial age estimation. It outlines different approaches including regression-based methods, classification techniques, and deep learning strategies. The authors provide comparisons of their strengths and weaknesses in terms of efficiency, accuracy, and scalability. The study notes that deep learning methods, particularly CNNs, have significantly advanced age estimation performance. However, issues such as limited labeled datasets and model interpretability remain challenges. The paper highlights the importance of continued research into explainable AI for age prediction tasks.

Prediction of the age and gender based on human face images based on deep learning algorithm.Haseena, S., Saroja, S., Madavan, R., Karthick, A., Pant, B., & Kifetew-N-(2022)[18] introduced a deep learning-based approach for predicting both age and gender from human face images. The researchers employed convolutional neural networks to extract facial features and classify them into respective categories. Their model was trained on publicly available face datasets with a wide range of age groups and demographics. The results demonstrated high accuracy in simultaneous age estimation and gender recognition. The study also emphasizes the usefulness of such systems in applications like surveillance, healthcare, and human–computer interaction. The authors conclude that deep learning provides a scalable and efficient solution for dual prediction tasks.

The different methods differ in terms of accuracy, computational efficiency, and ability to generalize across diverse datasets for predicting the age as per the literature survey. The following Table 1 highlights a comparative analysis of commonly used techniques.

Table 1. Performance comparison of different Machine Learning Techniques for Human Age Prediction

Citation	Methodology	Advantages	Drawbacks	Tools / Techniques Used	Accuracy / Performance
Zahra Asghari Varzaneh et al. – *Prediction of successful aging using ensemble machine learning algorithms*	Ensemble ML models (Random Forest, Gradient Boosting, SVM) applied to health and lifestyle datasets	Improves prediction reliability; handles nonlinear and complex relationships	Requires large balanced dataset; interpretability can be challenging	Python (Scikit-learn, Weka), health/lifestyle datasets	~85–90% depending on algorithm
Sandeep Kumar et al. – *Face Spoofing, Age, Gender and Facial Expression Recognition using Advanced Neural Networks*	Deep CNN with multi-task learning for spoofing detection + age, gender, emotion recognition	Simultaneous biometric recognition tasks; robust against spoofing	Computationally expensive; may struggle with real- world noise	TensorFlow, Keras, CNN architectures, biometric image datasets	Age/gender recognition >90%, spoofing detection ~92%
Leila Boussaad & Aldjia Boucetta – *Deep-learning based descriptors in application to aging problem in face recognition*	CNN-based feature descriptors for age- invariant face recognition	Enhances robustness to age progression in recognition systems	High dependency on training data variety; overfitting risk	Pretrained CNNs, transfer learning, face datasets (FG-NET, MORPH)	Reported EER (Equal Error Rate) reduction by ~10–15%
Olatunbosun Agbo-Ajala & Serestina Viriri – *Apparent age prediction from faces: A survey*	Survey of state-of-the- art DL/ML models for apparent age estimation	Comprehensive overview; compares multiple approaches	No novel model; only literature synthesis	Covers CNNs, Regression models, Hybrid ML techniques	Not applicable (survey)
Khaled ELKarazle et al. – *Facial Age Estimation Using Machine Learning Techniques: An Overview*	Review of ML techniques (SVR, Random Forest, CNNs) for facial age estimation	Explains strengths/weaknesses of different approaches	No experimental implementation	Tools discussed: Python ML frameworks, OpenCV	Not applicable (overview)
S. Haseena et al. – *Prediction of Age and Gender Based on Human Face Images Using Deep Learning*	Deep CNN model trained on facial datasets for joint age and gender prediction	High accuracy for classification; end-to-end training	Requires large annotated datasets; performance may vary across ethnicities	CNN (TensorFlow/Keras), OpenCV, public datasets (IMDB-WIKI, Adience)	Age classification ~85%, gender classification ~95%

IV. METHODOLOGY

The Figure 2 represent the general workflow of ML and DL algorithms applied to image based tasks as age estimation and recognition.

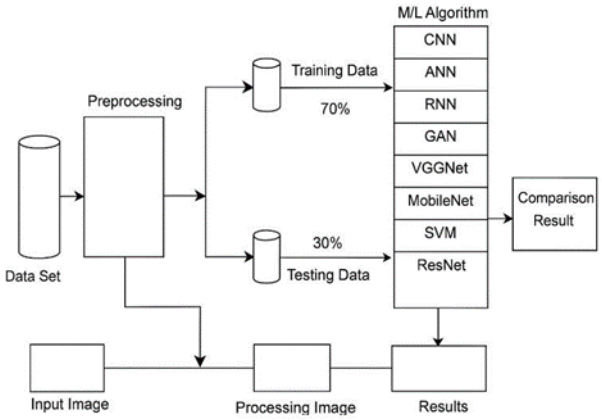


Figure 2. Block diagram of for the Existing system

a) Data Collection

The process starts with a dataset that contains facial images of individuals along with their actual ages. This dataset is the foundation for training and testing machine learning models.

There are mainly two datasets:

- A machine operation dataset with features such as usage time, load, temperature, and failure history.
- A labeled facial image dataset for age estimation.

b) Pre-processing

Before the images are used, they undergo preprocessing. This includes face detection, alignment, resizing, normalization, and sometimes data augmentation. These steps ensure uniformity and enhance the quality of the input images.

- For machine data: Cleaning, normalization, and feature engineering.
- For image data: Resizing, grayscale conversion, augmentation, and face detection.
- Data Splitting (Training and Testing)

The dataset is divided into 70% training data and 30% testing data. Training data is used to train the chosen machine learning models. Testing data is used to evaluate the performance of those models.

c) Feature Selection and Ranking

For machine failure prediction, feature importance is determined using methods such as:

- Recursive Feature Elimination (RFE)
- Feature importance from tree-based models
- Correlation analysis

d) Model Development

- **Machine Learning Algorithms** Various algorithms are applied to learn the mapping between facial features and age. The diagram lists multiple approaches:
  - **CNN (Convolutional Neural Network)** – Deep learning model for feature extraction and regression/classification.
  - **ANN (Artificial Neural Network)** – Fully connected layers for learning patterns.
  - **RNN (Recurrent Neural Network)** – Useful if sequential data or temporal aspects are considered.
  - **GAN (Generative Adversarial Network)** – Can be used for data generation or learning age-related features.
  - **VGG Net, ResNet, MobileNet** – Pre-trained CNN architectures commonly used for transfer learning in age estimation tasks.
  - **SVM (Support Vector Machine)** – A classical machine learning approach applied on extracted features.

e) Model Development

Model for age prediction from images:

- Convolutional Neural Networks (CNN)
- Transfer Learning (e.g., using VGG16 or ResNet50 pre-trained models)

f) Performance Evaluation Metrics

Evaluating the performance of machine learning models is essential to determine their effectiveness and ability to generalize to unseen data. In the context of facial age estimation, the choice of evaluation metrics depends on how the task is formulated—either as a regression problem (predicting exact age) or a classification problem (predicting an age group or range).

g) Comparison of Results

The outputs from all algorithms are compared based on performance metrics such as: [9]

- Mean Absolute Error (MAE)
- Root Mean Squared Error (RMSE)
- Accuracy (for age groups)
- Cumulative Score (CS)

- ***Regression-Based Metrics***

When the model is designed to predict a continuous age value, the following metrics are commonly used:

➢ **Mean Absolute Error (MAE)**

MAE measures the average absolute difference between the predicted and actual ages. It provides a direct indication of the model's accuracy, where lower values imply better performance. MAE is defined as:

$$\mathbf{MAE} = \frac{1}{n}\sum_{i=1}^{n}|y_i - x_i| \quad \ldots [1]$$

Where yi is the predicted age, xiis the actual age, and n is the number of test samples.

- **Mean Squared Error (MSE)**

MSE evaluates the average of the squared differences between predicted and actual ages. It penalizes larger errors more than MAE, making it sensitive to outliers. MSE is calculated as:

$$\mathbf{MSE} = \frac{1}{n}\sum_{i=1}^{n}(y_i - x_i)^2$$

In both cases, lower MAE and MSE values reflect higher prediction accuracy and reduced error margins.

- ***Classification-Based Metrics***

When the age prediction task is treated as a classification problem—such as assigning images to predefined age groups—alternative evaluation metrics are applied:

- **Accuracy**

Accuracy measures the proportion of correctly classified samples over the total number of samples.

- **Cumulative Score (CS)**

CS is used to evaluate how many predictions fall within a predefined error range (e.g., ±5 years). It is calculated as by the equation [2]

$$\mathrm{CS} = \frac{n}{N} \times 100\% \quad \ldots\ldots [2]$$

Where n is the number of correctly predicted samples within the acceptable range, and N is the total number of test samples.A variation of CS that considers predictions within an error tolerance j is given by the equation [3]:

$$\mathrm{CS}_{\leq j} = \frac{N_{\leq j}}{N} \times 100\% \quad \ldots\ldots [3]$$

Here, N⩽j represents the number of test samples with prediction error less than or equal to j years.

- **Classification tasks (machine failure):** Accuracy, Precision, Recall, F1 Score, ROC-AUC.
- **Regression task (age prediction):** Mean Absolute Error (MAE), Root Mean Square Error (RMSE), R^2 Score.

V. Expected Outcomes

- To gain a thorough understanding of the effectiveness of different machine learning algorithms in accurately estimating human age.
- To determine the key features that have the greatest impact on age prediction accuracy.
- To explore the possibility of comparing model performance with human judgment, thereby identifying specific areas where machine learning systems can be enhanced.

VI. Conclusion

Facial age estimation remains a prominent yet challenging research area due to factors such as limited training data and the absence of universally effective models capable of handling diverse aging patterns. This study explored age estimation from a machine learning standpoint, reviewing various techniques used to predict age from facial images and highlighting several widely-used benchmark datasets. Additionally, a range of recent research efforts were discussed, including their methodologies, strengths, and limitations. The review concludes by identifying the persistent challenges in the field and emphasizing the ongoing research trends aimed at enhancing model accuracy, generalization, and robustness across diverse populations and image conditions.

References

[1] Yu, Y. Tao, H. Zhang, Z. Wang, W. Cui, and T. Shi, "Age estimation algorithm based on deep learning and its application in fall detection," Electronic Research Archive, vol. 31, no. 8, pp. 4907–4924, 2023. doi: 10.3934/era.2023251

[2] Gollapalli, M., Rahman, A.-u., Youldash, M. M. Z., Alomari, D., Alismail, S., Khawaher, F., Alkhadair, A., Aljubran, F., Alzannan, R., Alkhulaifi, D., & Mahmud, M. (2023). A machine learning approach to users' age prediction: A telecom company case study in Saudi Arabia. Mathematical Modelling of Engineering Problems, 10(5), 1619–1629. https://doi.org/10.18280/mmep.100512

[3] Oliveira, W., Albuquerque Santos, M., Pereira Burgardt, C. A., Pontual, M. L. A., & Zanchettin, C. (2024). Estimation of human age using machine learning on panoramic radiographs for Brazilian patients. Scientific Reports, 14, 19689. https://doi.org/10.1038/s41598-024-70621-1

[4] abdul Saboor and Muhammad Usman, "A method for improving prediction of human heart disease using machine learning algorithms," Mobile Information Systems, vol. 2022, no. 15, Art. ID 1410169, 2022. doi:10.1155/2022/1410169

[5] M. Roopak, S. Khan, S. Parkinson, and R. Armitage, "Comparison of deep learning classification models for facial image age estimation in digital forensic investigations," Forensic Science International: Digital Investigation, vol. 47, Dec. 2023, Article 301637. https://doi.org/10.1016/j.fsidi.2023.301637

[6] P. Dey and T. Mahmud, "Human age and gender prediction from facial images using deep learning methods," in Proceedings of the 15th International Conference on Ambient Systems, Networks and Technologies (ANT) and the 7th International Conference on Emerging Data and Industry 4.0 (EDI40), Hasselt, Belgium, April 23–25, 2024, in Procedia Computer Science, vol. 238, pp. 314–321, 2024. doi: 10.1016/j.procs.2024.06.030

[7] S. R. Coleman and B. R. Grover, "The anatomy of the aging face: Volume loss and changes in 3- dimensional topography," Aesthetic Surgery Journal, vol. 26, suppl. 1, pp. S4–S9, 2006. doi: 10.1016/j.asj.2005.09.012

[8] A. S. Al-Shannaq and L. A. Elrefaei, "Comprehensive analysis of the literature for age estimation from facial images," IEEE Access, vol. 7, pp. 93229–93249, 2019. [Online].
[9] Available: https://doi.org/10.1109/ACCESS.2019.2927717
[10] K. Elkarazle, V. Raman, and P. Then, "Towards accuracy enhancement of age group classification using generative adversarial networks," Journal of Integrated Design and Process Science, vol. 25, no. 1, pp. 8–24, 2022. [Online]. Available: https://doi.org/10.3233/JID-210045
[11] E. Eidinger, R. Enbar, and T. Hassner, "Age and gender estimation of unfiltered faces," IEEE Transactions on Information Forensics and Security, vol. 9, no. 12, pp. 2170–2179, Dec. 2014. [Online]. Available: https://doi.org/10.1109/TIFS.2014.2359646
[12] G. Levi and T. Hassner, "Age and gender classification using convolutional neural networks," in Proc. IEEE Conf. Comput. Vis. Pattern Recognit. Workshops (CVPRW), Boston, MA, USA, Jun. 2015, pp. 34–42. [Online]. Available: https://doi.org/10.1109/CVPRW.2015.7301352
[13] V. Raman, K. Elkarazle, and P. Then, "Gender-specific facial age group classification using deep learning," Intelligent Automation & Soft Computing, vol. 34, no. 1, pp. 105–118, 2022. [Online]. Available: https://doi.org/10.32604/iasc.2022.030544
[14] Asghari Varzaneh, Zahra, Mostafa Shanbehzadeh, and Hadi Kazemi-Arpanahi. " BMC Medical Informatics and Decision Making 22, no. 1 (2022): 258.
[15] Kumar, Sandeep, Shilpa Rani, Arpit Jain, Chaman Verma, Maria Simona Raboaca, Zoltán Illés, and Bogdan Constantin Neagu. "Face spoofing, age, gender and facial expression recognition using advance neural network architecture-based biometric system." Sensors 22, no. 14 (2022): 5160.
[16] Boussaad, Leila, and Aldjia Boucetta. "Deep-learning based descriptors in application to aging problem in face recognition." Journal of King Saud University-Computer and Information Sciences 34, no. 6 (2022): 2975-2981.
[17] Agbo-Ajala, Olatunbosun, Serestina Viriri, Mustapha Oloko-Oba, Olufisayo Ekundayo, and Reolyn Heymann. "Apparent age prediction from faces: A survey of modern approaches." Frontiers in big Data 5 (2022): 1025806. [17].ELKarazle, Khaled, Valliappan Raman, and Patrick Then. " Facial age estimation using machine learning techniques: An overview." Big Data and Cognitive Computing 6, no. 4 (2022): 128.
[18] Haseena, S., S. Saroja, R. Madavan, Alagar Karthick, Bhaskar Pant, and Melkamu Kifetew. "Prediction of the age and gender based on human face images based on deep learning algorithm." Computational and mathematical methods in medicine 2022, no. 1 (2022): 1413597.

International Journal of Computer Research & Technology
** A Blind Peer Reviewed Journal **
Volume-10, Issue-2, July-Dec 2025
ISSN 2454-7719
Paper ID: CS-17

Investigating the Performance of Machine Learning Algorithms over Human Age Prediction by using Image Dataset

Swati Laxman Nimgale
Dept. of Information Technology, Pillai College of Engineering, Navi Mumbai 410208; India
swati24mtit@student.mes.ac.in

Prof. Prashant Nitnaware
Dept. of Information Technology, Pillai College of Engineering, Navi Mumbai 410208; India

Abstract- *Gender remains a core aspect of human identity and always plays an very important role in social interactions. The ability to estimate age using artificial intelligence has promising applications across various domains such as intelligent human-computer interaction, healthcare, cosmetics, and e-commerce. Predicting an individual's age from facial images is a challenging and actively researched problem. Although several approaches have been developed, achieving consistent and accurate results remains difficult. This project presents a statistical pattern recognition method leveraging deep learning to address this issue. Specifically, Convolutional Neural Networks (CNNs) are employed for automatic feature extraction from facial images. Unlike traditional classification techniques that rely heavily on manual feature engineering, CNNs can learn to identify relevant patterns directly from raw images through training. Here in this work, a CNN model is been trained using with large dataset of more than 20,000 facial images annotated along with ethnicity and as well as age. The dataset includes diverse image conditions such as different facial expressions, lighting, poses, occlusions, and resolutions. The proposed approach achieved high accuracy in predicting age.*

Keywords (Size 10 & Bold)— *Machine learning, age estimation, types of algorithm. Age Prediction, CNN; Deep Learning*

I. INTRODUCTION

Facial images always contains a valuable information that can also use to predict various human attributes such as age, gender, ethnicity, and emotions [1]. While humans can often estimate age and gender by observing features like facial structure, hairstyle, skin texture, and wrinkles, replicating this process with machines presents a complex challenge [2]. Unlike humans, machines lack intuitive understanding and must rely on data-driven learning through algorithms. To enable machines to predict age and gender, a structured dataset and effective classification models are essential [3].

The task of automatic age and gender prediction is gaining considerable consideration with its wide range usage of real-world applications. These include areas such as smart surveillance systems, targeted advertising, personalized user experiences, security systems, human-computer interaction, forensic analysis, and Internet of Things (IoT) solutions. For example, retail environments can use such systems to tailor product displays or services based on the demographic characteristics of their customers [5, 6].

Here in this work, it been introduced a Convolutional Neural Network (CNN)-model for predicting age from real-world, unconstrained facial images. The proposed work is been designed to balance performance and computational efficiency. It incorporates robust pre-processing techniques to handle image variability, significantly improving classification accuracy. Key techniques such as normalization are applied to eliminate redundant data and reduce computational overhead, while data augmentation is used to enhance generalization and minimize over fitting [7].

To evaluate the model's effectiveness, experimentations has been conducted using 2-

publicly existing datasets that include diverse facial images with labelled age and gender information. Additionally, multiple pre-trained CNN architectures are tested and compared for determining the utmost actual model for the current work. Optimization techniques are employed to minimize prediction errors and refine model performance.

Earlier research in age and gender classification has used handcrafted features extracted from the face, ears, and wrinkles, combined with traditional machine learning techniques like Principal Component Analysis (PCA), Support Vector Machines (SVM), and basic Neural Networks. However, these methods often fall short when dealing with the complexity of real-world images. In contrast, deep learning—especially CNNs—have demonstrated outstanding performance in image recognition tasks, making it a powerful tool for this application [8, 9].

The foremost highlights of the work are:

1. Development of a CNN model tailored for age prediction from unconstrained facial images.
2. Implementation of a robust image pre-processing pipeline to improve model accuracy.
3. Use of normalization and augmentation techniques to enhance efficiency and generalization.
4. Performance evaluation using diverse datasets with labeled demographic attributes.
5. Comparative analysis of multiple pre-trained CNN models to determine optimal architecture.
6. Application of optimization strategies to reduce prediction error and improve reliability.

II. LITERATURE REVIEW

The problem of gender and age prediction using image processing along with machine learning have been worked through a variety of techniques over the years. Earlier approaches primarily relied on machine learning models such as Support-Vector-Machines (SVM) [8], Local Binary Patterns (LBP), and Linear Regression methods [9, 10]. These conventional models performed adequately under controlled conditions but often lacked robustness when applied to complex, real-world images. With advancements in deep learning, more recent research has shifted toward using pre-trained convolutional neural network (CNN)-models [12]. Popular architectures commonly used are VGG16, SENet50 (Squeeze-and-Excitation Networks), and ResNet50 had been fine-tuned and applied to the task of age prediction with notable success. For example, CNN-based models have demonstrated promising results, achieving around 82.2% accuracy for gender classification and approximately 57.5% for estimation of age. The authors Liu et al. introduced a CNN-framework incorporating a multi-class for focal loss function, achieving an age prediction accuracy around 60.4% on the Adience dataset [13]. In another study, Afnan et al. implemented a CNN model that delivered 94.94% accuracy in gender classification and 79.12% in age estimation. Additionally, the authors Rojas et al. applied Efficient-Net architectures, where the B4 model attained 73.5% accuracy on the UTKFace dataset and 81.1% on Adience. Ranjan et al. used a Deep-Convolutional-Neural-Network (DCNN) model for estimating the age, reporting an accuracy of 52.9% [15]. These diverse findings underline the potential and challenges of using deep learning models for demographic prediction tasks. Overall, while CNNs and transfer learning have significantly improved prediction accuracy, performance still varies depending on model architecture, dataset quality, and image conditions.

III. SOFTWARE REQUIREMENTS AND TECHNOLOGIES

In order to estimate the age through facial images, Convolutional-Neural-Network (CNN) architecture has been used. The model comprises of 3-convolutional layers, trailed with 2- dense layers, and a final output layer. Rather than treating age prediction as a regression task, this approach frames it as a classification problem. Predicting an individual's exact age is highly challenging—even for humans—based solely on facial appearance. Therefore, the model aims to classify individuals into broader age groups, such as 20–30 or 30–40, instead of determining a precise numerical age [15]. This method accounts for the numerous factors that influence facial aging, making accurate age estimation from a single image inherently complex [16].

IV. METHODOLOGY

In the developed system, a Convolutional Neural Network (CNN) has been adopted as the core deep learning model. The CNN models are extremely effective at recognizing patterns in visual data and are widely used in this work for image-classification, segmentation, for analysis, and for video recognition. In this work, it been started with by applying pre-processing techniques to transform the raw input data to be represented with an appropriate format for training. Following this, the CNN model is implemented, consisting of two primary stages: extraction of features and classification. The convolutional and pooling layers are responsible for identifying and extracting significant image features, while the fully-connected layers were used for

classifying g the images based upon those extracted which are extracted.

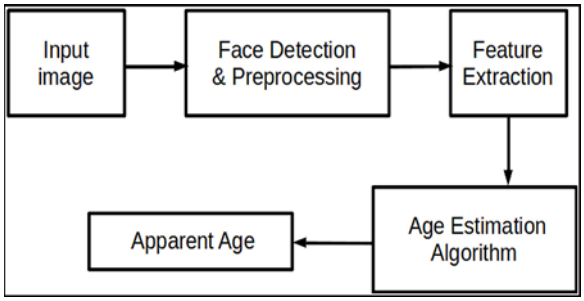


Figure 1. Proposed Model

4.1 Dataset

The initial phase in predicting age from facial images involves acquiring a suitable dataset that includes labels for both ages. This data can be gathered in various ways, such as capturing images using a camera or sourcing large image collections from online platforms. Additionally, there are publicly available datasets specifically designed for facial analysis tasks. For this study, two well-known datasets have been utilized: the Adience dataset and the UTKFace dataset, both of which contain facial images annotated with age information.

Table 1. Comparison Table: Adience vs UTKFace

Feature	Adience Dataset	UTKFace Dataset
Number of Images	~26,000	~20,000+
Image Type	Unconstrained face images (wild environments)	Cropped and aligned face images
Labels	Age group (e.g., 0–2, 4–6, ...) & gender	Exact age, gender, and ethnicity
Age Format	Age ranges (8 categories)	Exact age (0 to 116)
Gender Classes	Male, Female	Male, Female
Pose Variation	High (includes varied angles and lighting)	Moderate (mostly front-facing)
Annotation Quality	Manually verified (some noise)	Labeled by file name (automated, needs cleaning)
Use Case Suitability	Ideal for age group classification in the wild	Good for regression or classification tasks

4.2 The Pre-processing Phase

Previously inputting the images into the Convolutional Neural Network (CNN), several pre-processing steps have become necessary to undergo. These include detection of face, landmark identification, face alignment, and also normalization too. These operations ensure that all facial images are consistently aligned and positioned, which is crucial for accurate feature extraction and model performance.

4.2.1 Face Detection

The first step involves detecting faces within each image using a face detection algorithm. This method automatically identifies and localizes the face by drawing a bounding box around it. FaceNet is utilized to extract key facial landmarks such as the eyes, the nose, and the mouth, while using the coordinates of the bounding box (top, bottom, left, and right). If a face is detected, the algorithm crops the facial region for further processing. If no face is found, the image is excluded from the dataset. This face detection method is chosen due to its robustness—it can detect faces at various angles, handle different scales, and effectively manage partially obscured faces.

4.2.2 Facial Landmark Detection and Alignment

Once the face is detected, the next step involves identifying facial landmarks and aligning the face using the same FaceNet algorithm. This method traces the key points which are on the face—such as the corners of the eyes, the nose tip, and the mouth—which serve as reference positions. After detecting these landmarks, the algorithm calculates distances between them, treating these measurements as distinctive features of the face. During the alignment process, the facial key points help standardize the orientation of faces captured from different angles, ensuring consistent feature extraction across all images.

4.2.3 Data Normalization

Next, the Min-Max normalization technique is applied to the images, as neural networks tend to yield better results when working with normalized input data. This method rescales pixel values from their original range to a standardized range between 0 and 1. By applying a linear transformation, Min-Max normalization adjusts the values while maintaining the relative relationships between them, ensuring that the original data distribution is preserved.

$$N' = \frac{N - \text{minvalueofN}}{\text{maxvalueofN} - \text{minvalueofN}} (D - K) + K$$

4.2.4 Data Augmentation

Following normalization, data augmentation techniques are applied to the image dataset. This

step helps reduce overfitting and improves the model's generalization by increasing data variability. Several augmentation strategies are tested to evaluate their effect on classification performance. The ImageDataGenerator function is used to implement these transformations. The applied augmentation parameters include a rotation of 45 degrees, a shear intensity of 0.2, a zoom factor of 0.15, and enabling horizontal flipping.

4.3 CNN Model

The Convolutional Neural Network (CNN), modeled after the structure of the human brain, is composed of several key layers—namely Convolution, Activation, Pooling, and Fully-Connected-layers. The convolutional layers will be used to apply filters to identify patterns such as edges and textures within an image, while pooling layers reduce the spatial dimensions, helping to lower computational load. The flattened output has been then fed into fully-connected layers for classification. Dropout layers are used to minimize overfitting by randomly disabling some neurons during training [17, 18].

The architecture begins with a convolutional layer using 32 filters, followed by a ReLU activation function and batch normalization, then a max pooling layer. This is followed by additional convolutional blocks with an increased number of filters, each including ReLU activation, batch normalization, and pooling. Toward the end, the model includes a dense layer with ReLU activation, a dropout layer for regularization, and an output layer. For age classification tasks, softmax or sigmoid functions are applied depending on the label type. This CNN design enables efficient feature extraction and accurate prediction of age from facial images [19, 20].

Table.2 Examples of commonly used pre-trained networks.

N/W Name	No. of Layers	No. of Parameters (Millions)	Size (MB)	Default Input Size (Height × Width)
VGG16	16	144	515	224 × 224
VGG19	19	144	535	224 × 224
ResNet50	50	25.6	50	227 × 227
Xception	71	22.9	85	299 × 299
AlexNet	8	61	227	227 × 227
GoogLeNet	22	7	27	224 × 224
MobileNetV2	53	3.5	13	224 × 224

V. Result and Discussion

5.1 Comparison of Results across Various Optimizers

Table 3 presents the accuracy outcomes for both datasets using a range of optimization algorithms. The optimizers evaluated include Adam, Adamax, Adagrad, SGD, and Adadelta. Among these, the Adam optimizer consistently delivered the highest accuracy for predicting age in our model.

Table.3 Accuracy using different optimizers

Optimizers	Adience Dataset	UTKFace Dataset
	Age Acc	Age Acc
Adam	85.42%	83.96%
Adamax	79.32%	75.87%
Adagrad	76.22%	73.57%
SGD	70.66%	68.68%
Adadelta	63.55%	60.12%

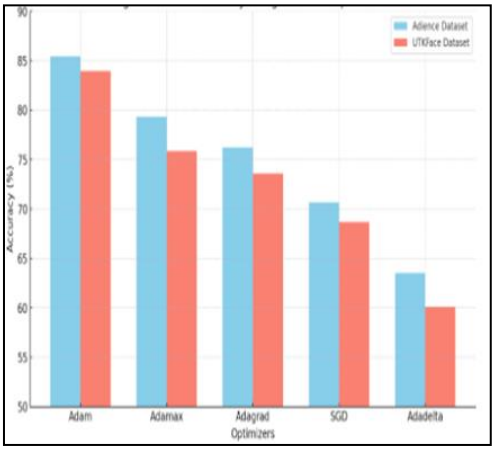


Figure 2. Age Prediction Accuracy using different optimize

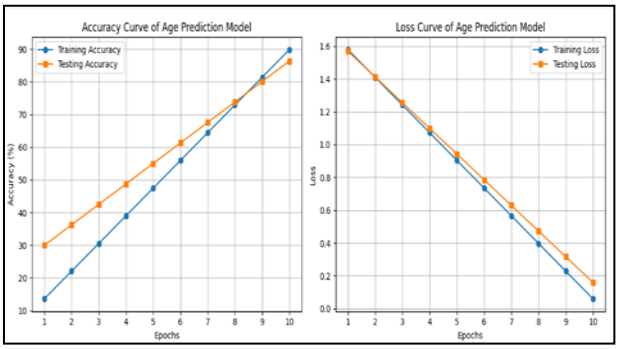


Figure 3 a. Age predication accuracy (Adience) and b.Age prediction loss(Adience)

Left plot: Training accuracy increased from 13.57% to 89.91%, and testing accuracy rose from 29.96% to 86.42% over 10 epochs.

Right plot: Training loss dropped from 1.58 to 0.06, while testing loss decreased from 0.68 to 0.15, showing improved model performance and generalization.

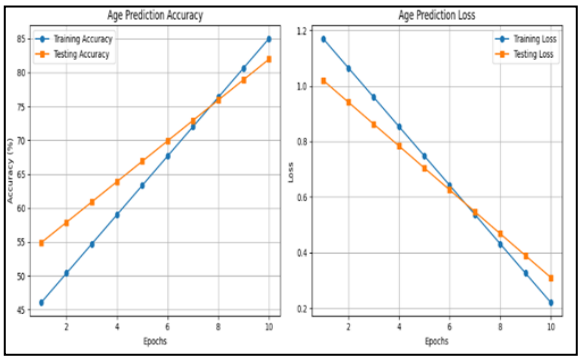


Figure 4 a. Age predication accuracy (UTKFace) and b.Age prediction loss (UTKFace)

Left plot: Training accuracy increased from 46.05% to 85.01 %, and testing accuracy rose from 54.89% to 81.96%. Over 10 epochs.

Right plot: Training loss dropped from 1.17 to .22, while testing loss decreased from 1.02 to .31, showing improved model performance and generalization.

5.2. Performance Comparison of the Proposed Work

For training the pre-processed datasets, numerous pre-trained models—such as VGG-16, VGG-19, and ResNet50—were utilized for benchmarking. Tables 4 and 5 is presenting a comparative analysis these existing models and the proposed model. The results is going to indicate that the proposed model achieved superior `performance, surpassing the others with respect to accuracy, precision, recall, and also F1-score. The evaluation confirms that our model consistently outperforms the alternatives across multiple performance metrics.

Table.4 Performance Comparison of age prediction with different models with Audience dataset.

	Age Prediction			
Models	**Accuracy**	**Precision**	**Recall**	**F1-score**
VGG-16	77.20%	78.53%	76.30%	76.46%
VGG-19	71.90%	72.60%	71.15%	71.82%
ResNet50	70.20%	66.10%	67.40%	66.50%
Proposed model	86.40%	87.19%	85.40%	86.26%

Table .5 Comparison of performance among different models using UTKFace dataset.

	Age Prediction			
Models	**Accuracy**	**Precision**	**Recall**	**F1-score**
VGG-16	72.01%	71.23%	70.20%	70.08%
VGG-19	68.97%	69.04%	69.21%	69.45%
ResNet50	65.21%	64.10%	65.21%	64.04%
Proposed model	81.23%	82.10%	81.40%	80.01%

Table 6 performance comparison previous approach with the proposed approach

Reference	Method	Dataset	Accuracy (Age)
2	CNN	Adience	83.1%
17	DCNN	Adience	93.6%
20	CNN	Adience	71%
3	EfficientNet	Adience UTKFace	81.1% and 73.5%
1	CNN	Adience	84.8%
11	CNN-ELM	Adience	52.3%
18	MLP	Adience	67.47%
Proposed Method	CNN with 5 conv layers	Adience UTKFace	86.42% and 81.96

For the table 6 shows we have provided a comparative analysis between our proposed system and existing approaches previously developed on this topic. The comparison highlights the datasets and techniques used in earlier studies, along with the accuracy achieved by their models. The proposed findings demonstrated that this method delivered a superior performance. Specifically, the system achieved an accuracy of 86.42% upon the Adience dataset and 81.96% on the UTKFace dataset for age prediction.

VI. Conclusion and Future Work

This research integrates computer vision and machine-learning, utilizing image processing methods to enhance and prepare image quality. It applied the methods of softmax and the sigmoid functions for predicting age and tested various optimization algorithms to boost the model performance. The use of large-scale datasets aids in extracting detailed features. A comparative evaluation demonstrates the model's superior accuracy. The extended work includes expanding to multi-class classification based on image content, incorporating BRBES frameworks, applying K-fold cross-validation, broadening detection, making predictions from video inputs, and investigating emotion recognition.

REFERENCES

[1] Agbo-Ajala, O., & Viriri, S. (2020). Face-based age and gender classification using deep learning models. In Image and Video Technology: PSIVT 2019 International Workshops (pp. 125–137). Springer.

[2] Agbo-Ajala, O., Viriri, S., & Others. (2020). Deep learning classifiers for age and gender prediction on unfiltered facial images. The Scientific World Journal, 2020, Article ID 1501986. https://doi.org/10.1155/2020/1501986

[3] Aruleba, I., & Viriri, S. (2021). Age estimation using EfficientNet with deep learning. In Advances in Computational Intelligence: IWANN 2021 Proceedings (Vol. 16, pp. 407–419). Springer.

[4] Basnin, N., Nahar, L., & Hossain, M. S. (2020). CNN-LSTM integrated model for micro hand gesture recognition. In Intelligent Computing & Optimization (pp. 379–392). Springer.

[5] Bekhouche, S. E., Ouafi, A., Benlamoudi, A., Taleb-Ahmed, A., & Hadid, A. (2015). Multi-level local phase quantization for facial age estimation and gender classification. In 2015 3rd International Conference on Control, Engineering & Information Technology (CEIT) (pp. 1–4). IEEE.

[6] Bekhouche, S. E., Ouafi, A., Taleb-Ahmed, A., Hadid, A., & Benlamoudi, A. (2016). Facial age estimation using BSIF and LBP. arXiv preprint arXiv:1601.01876.

[7] BenAbdelkader, C., & Griffin, P. (2005). Gender classification from facial images using a local region-based approach. In CVPR 2005 Workshops (p. 52). IEEE.

[8] Chen, J. C., Kumar, A., Ranjan, R., Patel, V. M., Alavi, A., & Chellappa, R. (2016). A cascaded CNN for age estimation of unconstrained faces. In 2016 IEEE 8th International Conference on Biometrics Theory, Applications and Systems (BTAS) (pp. 1–8). IEEE.

[9] Das, S., Mahmud, T., Islam, D., Begum, M., Barua, A., Aziz, M. T., Showan, E. N., & Dey, L. (2023). Foot no-ball detection using deep transfer learning in live cricket. Computational Intelligence and Neuroscience, 2023. https://doi.org/10.1155/2023/5527350

[10] Demontis, A., Biggio, B., Fumera, G., & Roli, F. (2015). Fast age prediction with super-sparse regression. In ICIAP 2015: Image Analysis and Processing (Vol. 18, pp. 551–562). Springer.

[11] Duan, M., Li, K., Yang, C., & Li, K. (2018). Age and gender classification using a hybrid CNN–ELM model. Neurocomputing, 275, 448–461. https://doi.org/10.1016/j.neucom.2017.09.101

[12] Eidinger, E., Enbar, R., & Hassner, T. (2014). Estimating age and gender from unfiltered face images. IEEE Transactions on Information Forensics and Security, 9(12), 2170–2179.

[13] Gunay, A., & Nabiyev, V. V. (2015). Age estimation using AAM and 2D-DCT facial features. International Journal of Computer Science and Applications, 6(1), 1–8.

[14] Islam, D., Mahmud, T., & Chowdhury, T. (2023). Automated recognition of vehicle license plates using image processing. Indonesian Journal of Electrical Engineering and Computer Science, 29(2), 1055–1062.

[15] Islam, M. Z., Hossain, M. S., ul Islam, R., & Andersson, K. (2019). Static hand gesture recognition using CNN with data augmentation. In 2019 ICIEV & icIVPR Joint Conference (pp. 324–329). IEEE.

[16] Karim, R., Khaliluzzaman, M., Mahmud, T., et al. (2023). Expert system for clinical risk evaluation of PCOS under uncertain conditions.

[17] Khan, K., Attique, M., Khan, R. U., Syed, I., & Chung, T. S. (2020). Multi-task CNN model for facial attribute classification. Sensors, 20(1), 328.

[18] Kim, T. (2021). Enhancing MLP generalization using dropouts, batch normalization, and skip connections. arXiv preprint arXiv:2108.08186.

[19] LeCun, Y., Bottou, L., Bengio, Y., & Haffner, P. (1998). Gradient-based learning for document recognition. Proceedings of the IEEE, 86(11), 2278–2324.

[20] Liu, W., Chen, L., & Chen, Y. (2018). Convolutional neural networks with multi-class focal loss for age classification. IOP Conference Series: Materials Science and Engineering, 392, 012043.

International Journal of Computer Research & Technology
ISSN 2454-7719
** A Blind Peer Reviewed Journal **
Volume-10, Issue-2, July-Dec 2025

Paper ID: CS-18

IoT for Real-Time Product Tracking and Transparency in E-Commerce

Mr. Prakash Y. Bari
Assistant Professor
KCES's Institute of Management and Research Jalgaon.

Mr. S. N. Khan
Assistant Professor
KCES's Institute of Management and Research Jalgaon.

Abstract- *The start of e-commerce has fundamentally transformed the global retail sector by providing consumers with enhanced convenience, a diverse range of products, and competitive pricing. However, challenges such as product delivery delays, limited shipment visibility, and trust issues persist as significant impediments to customer satisfaction. The Internet of Things (IoT) offers innovative solutions by facilitating real-time product tracking and enhancing supply chain transparency. This paper examines the application of IoT in product monitoring, shipment tracking, and inventory management within e-commerce platforms. The study elucidates the benefits, challenges, and future prospects of IoT adoption in promoting product transparency, minimizing delivery errors, and bolstering customer trust.*

I. INTRODUCTION

E-commerce represents one of the most rapidly expanding sectors globally, characterized by millions of transactions occurring daily. Consumers anticipate prompt delivery, precise information, and transparent processes when engaging in online purchases. Nevertheless, conventional tracking systems frequently fail to deliver real-time updates and are susceptible to delays or inaccuracies. The Internet of Things (IoT), with its network of interconnected devices and sensors, presents an effective means to monitor goods, track shipments, and ensure comprehensive visibility within e-commerce supply chains. This paper examines how IoT can revolutionize product tracking and transparency through the integration of technologies such as RFID (Radio Frequency Identification), GPS, sensors, and cloud computing.

II. LITERATURE REVIEW

Several studies have highlighted the potential of IoT in supply chain and logistics.

Chaffey (2019) underscored the pivotal role of digital technologies, including the Internet of Things (IoT), in underpinning contemporary e-commerce operations. He emphasized that data-driven solutions facilitate businesses in analysing customer behaviour, optimizing logistics, and minimizing delivery delays. Through the integration of IoT sensors and smart devices, retailers can enhance supply chain management, thereby rendering operations more transparent and customer-centric.

Lee and Lee (2020) conducted an investigation into the utilization of Radio Frequency Identification (RFID) tags and Internet of Things (IoT) sensors for inventory management in the context of online retail. Their research demonstrated that IoT-enabled tracking facilitates real-time visibility of products throughout the supply chain. For example, RFID technology enables the automated scanning of goods in warehouses, thereby reducing manual errors and ensuring timely updates for both retailers and customers. They concluded that IoT technologies are instrumental in achieving operational efficiency, particularly on large-scale e-commerce platforms.

Similarly, Singh et al. (2021) explored the impact of IoT applications on consumer trust and transparency in e-commerce. Their research revealed that IoT systems can help detect counterfeit products by tracking the product origin and movement across the supply chain. In addition, real-time tracking improves customer confidence in online purchases by offering accurate delivery updates and reliable product authentication. This indicates that the IoT

not only benefits logistics but also directly influences consumer satisfaction and brand reputation.

Overall, the existing literature suggests that IoT adoption in e-commerce enhances efficiency, visibility, and customer satisfaction. However, challenges such as high setup costs, privacy risks, lack of standardization, and limited interoperability between devices continue to hinder widespread adoption. Researchers agree that further advancements in the IoT, combined with supportive technologies such as blockchain and 5G, will be essential to overcome these barriers and achieve large-scale implementation in the future.

III. METHODOLOGY

The analysis focused on identifying the following:

1. Identification of IoT Technologies in E-Commerce Tracking

The first step involved reviewing the existing literature to identify the most commonly used IoT technologies in e-commerce and supply chain management.

These include:

• Radio Frequency Identification (RFID): Enables automated product identification and tracking in warehouses.

• Global Positioning System (GPS): Provides real-time location tracking of shipments during transit.

• IoT Sensors (Temperature, Humidity, Motion) monitor product conditions, especially for sensitive items, such as food and pharmaceuticals.

• QR Codes and NFC Tags: Support product authentication and enhance transparency by allowing customers to trace product origins. By analysing case studies, the paper evaluates how these technologies are applied in practical e-commerce scenarios.

2. Evaluation of Benefits for Businesses and Customers

The second step focuses on identifying the advantages of IoT adoption in e-commerce for businesses and customers. The analysis is based on case examples of companies that have integrated the IoT into their operations.

The study looks into:

• Business benefits include improved inventory accuracy, reduced operational costs, better demand forecasting, and enhanced supply chain efficiency.

• Customer Benefits: Real-time shipment visibility, product authenticity verification, faster delivery, and increased trust in online transactions. This step also highlights the role of the IoT in improving customer satisfaction and loyalty by making e-commerce platforms more reliable and transparent.

The study looks into:

• Business benefits include improved inventory accuracy, reduced operational costs, better demand forecasting, and enhanced supply chain efficiency.

• Customer Benefits: Real-time shipment visibility, product authenticity verification, faster delivery, and increased trust in online transactions. This step also highlights the role of the IoT in improving customer satisfaction and loyalty by making e-commerce platforms more reliable and transparent.

3. Analysis of Challenges and Limitations

The third step involved identifying barriers to IoT adoption in e-commerce. Literature and industry reports suggest several challenges, including the following:

• High Implementation Cost: Deploying RFID tags, IoT sensors, and cloud systems requires significant investment.

• Data Privacy and Security Issues: Customer and shipment data must be protected against misuse or cyberattacks.

• Interoperability Concerns: Different IoT systems and platforms often lack standardization, making integration difficult.

• Network Reliability: Real-time tracking requires stable Internet connectivity, which is not always available in all regions; the analysis compares these challenges with potential solutions suggested in prior research, such as blockchain integration, lightweight encryption, and 5G-enabled IoT systems.

IV. IOT TECHNOLOGIES IN PRODUCT TRACKING

1. RFID Tags and QR Codes

Radio Frequency Identification (RFID) tags and Quick Response (QR) codes are among the most common tools used in IoT-enabled product tracking. RFID tags are embedded with microchips that store product information and can be scanned wirelessly. This allows for the real-time identification and monitoring of goods as they move through warehouses, distribution centres, and retail stores. Unlike traditional barcodes, RFID does not require a direct line of sight, which makes scanning faster and reduces the manual effort.

QR codes, on the other hand, are increasingly being used to enhance transparency for customers. By scanning a QR code, customers can access detailed product information, such as origin, manufacturer details, and supply chain history. In e-commerce, this creates a sense of trust, as buyers can verify product authenticity before making a purchase.2.3. Image Segmentation

2. GPS and Smart Sensors

Global Positioning System (GPS) technology enables the real-time location tracking of shipments across transportation networks. By equipping

delivery vehicles or individual packages with GPS-enabled devices, companies can provide customers with live updates on the location of their orders. This feature is particularly important in e-commerce, where timely delivery affects customer satisfaction.

In addition to location tracking, smart sensors play a critical role in monitoring product conditions during the transit. For instance, temperature and humidity sensors are used to ensure that perishable items, such as food, medicines, and cosmetics, are transported under the required conditions. Motion and shock sensors help detect mishandling and ensure that fragile goods are delivered safely. These sensors provide transparency and accountability in the supply chain.

3. Cloud Platforms

IoT devices generate vast amounts of data that must be stored, processed, and analysed. Cloud computing platforms are the backbone of IoT-enabled tracking systems, providing scalable storage and real-time data processing capabilities. Data collected from RFID tags, GPS devices, and sensors are uploaded to the cloud, where they are organized and made accessible to both businesses and customers.

For businesses, cloud platforms enable centralized inventory management, predictive analytics, and automation of decision-making. For customers, they provide transparency by offering easy access to real-time tracking information through mobile applications or websites. Cloud integration ensures that the entire tracking process is seamless, efficient and cost-effective

4. Block chain with IoT

While IoT technologies enable real-time data collection, ensuring the authenticity and security of these data is equally important. Blockchain technology addresses this concern by providing a decentralized, tamper-proof ledger of product movement. When combined with IoT devices, blockchain records each stage of a product's journey, from manufacturing to delivery, in a transparent and immutable manner.

For example, every time an RFID tag or GPS sensor updates product information, the data can be securely stored in a blockchain network. This ensures that no party in the supply chain can alter or manipulate the records, thereby preventing fraud and counterfeit goods. Customers benefit from blockchain integration because they can verify the complete history of a product, building trust and confidence in e-commerce transactions.

V. Benefits of IoT in E-Commerce

Real-Time Tracking: with IoT, customers can see exactly where their products are at any time. For example, they can check whether the order has left the warehouse, is on the way, or is out for delivery. This makes online shopping more reliable and convenient.

Transparency: The IoT provides full visibility of a product's journey from the seller to the customer. This openness helps build trust, as buyers know the exact status of their orders without guessing.

Reduced Errors: Because IoT devices automatically scan and update information, the chances of mistakes, such as wrong delivery or lost packages, are reduced. This makes the process smoother for both companies and customers alike.

Fraud Prevention: The IoT helps identify fake or duplicate products by tracking where the product was made and how it moved through the supply chain. Customers feel safer knowing that they are receiving genuine products.

Improved Customer Experience: When customers receive faster updates, accurate information, and timely delivery, their overall shopping experience improves. This leads to greater satisfaction and encourages repeated purchases.

VI. Challenges in IoT Implementation

1. High Initial Cost

Setting up IoT systems requires a large initial investment. Devices such as RFID tags, GPS trackers, smart sensors, and cloud systems are not inexpensive. In addition, businesses need trained staff to manage and maintain these systems. For small- and medium-sized e-commerce companies, this cost can be too high, which slows down adoption.

2. Data Privacy Concerns

IoT systems collect large amounts of data, such as product location, customer details, and delivery information. If these data are not properly protected, they could be misused by hackers or unauthorized personnel. Customers may also worry about their personal information being exposed, which can reduce their trust in e-commerce platforms.

3. Connectivity Issues

IoT devices rely on Internet connections to send and receive data. Real-time tracking is only possible when stable network coverage is available. In many rural or remote areas, Internet connectivity is weak, which can cause delays in updates or incomplete tracking information. This makes it difficult to guarantee smooth service everywhere.

4. Interoperability Problems

Different companies use different IoT systems and platforms, which may not always work well together. For example, one retailer may use a certain type of RFID system, while another uses a different tracking platform. If these systems cannot share data properly, gaps are created in the supply chain. Standardization remains a challenge in IoT, and without it, full integration becomes difficult.

VII. CONCLUSION

The Internet of Things (IoT) is proving to be a game changer in e-commerce, especially in real-time product tracking and transparency. By using technologies such as RFID tags, GPS devices, smart sensors, and cloud platforms, businesses can provide customers with accurate and timely updates about their orders. This not only makes the delivery process more efficient but also helps build trust between sellers and buyers.

The IoT improves many aspects of e-commerce operations. For businesses, it reduces errors, improves inventory control, prevents fraud, and supports better decision-making through data analysis. For customers, it creates a smooth shopping experience with real-time updates, reliable delivery, and confidence that the product they receive is authentic. Thus, the IoT benefits both sides of the e-commerce chain. However, some challenges continue to limit their general use. High installation costs, data privacy risks, weak network connections in some areas, and lack of standardization between different IoT systems are significant barriers. These issues must be addressed before the IoT can be fully adopted on a large scale.

The future of IoT in e-commerce is promising. With the growth of 5G networks, blockchain integration, and more affordable IoT devices, many of the current challenges are likely to be solved in the near future. As technology advances, the IoT will not only be an additional feature but will become an essential part of every e-commerce system, ensuring faster deliveries, greater transparency, and improved customer satisfaction.

REFERENCES

[1] Chaffey, D. (2019). Digital Business and E-Commerce Management. Pearson.

[2] Lee, I., & Lee, K. (2020). "The Internet of Things (IoT): Applications, investments, and challenges for enterprises." Business Horizons, 63(2), 157–169.

[3] Singh, R., Sharma, A., & Kumar, P. (2021). "IoT-enabled supply chain management in e-commerce: Opportunities and challenges." Journal of Retail and Consumer Services, 59, 102415.

International Journal of Computer Research & Technology
** A Blind Peer Reviewed Journal **
ISSN 2454-7719
Volume-10, Issue-2, July-Dec 2025
Paper ID: CS-19

Emotional Intelligence and Artificial Intelligence: Ethical, Technical, and Cross-Cultural Perspectives with Healthcare Applications

Dr. Dipak N. Patil

Associate Professor,

Department of English,

Bhusawal Arts, Science and P. O. Nahata Commerce College, Bhusawal

Abstract - *Emotional Intelligence (EI) has long been recognized as a pivotal human trait, enabling individuals to perceive, understand, and manage emotions in themselves and others. With the rapid advancements in Artificial Intelligence (AI), there is an emerging field dedicated to integrating EI within AI systems to create machines capable of recognizing and responding to human emotions empathetically. This fusion promises to revolutionize human-computer interaction, creating AI systems that are not only intelligent but emotionally aware.*

I. INTRODUCTION

Emotional Intelligence (EI) has long been recognized as a pivotal human trait, enabling individuals to perceive, understand, and manage emotions in themselves and others. With the rapid advancements in Artificial Intelligence (AI), there is an emerging field dedicated to integrating EI within AI systems to create machines capable of recognizing and responding to human emotions empathetically. This fusion promises to revolutionize human-computer interaction, creating AI systems that are not only intelligent but emotionally aware.

The interdisciplinary nature of EI-enabled AI spans computer science, psychology, ethics, and healthcare, among others. This paper offers a comprehensive examination of this promising domain, covering foundational theories, multimodal emotion recognition techniques, ethical frameworks for empathetic algorithms, the critical issue of cross-cultural bias in emotion datasets, and the transformative applications of emotionally intelligent AI in healthcare.

The following sections collectively aim to provide a thorough understanding of the challenges, opportunities, and future directions within this evolving technological landscape.

1. Literature Review Structure for Emotional Intelligence and Artificial Intelligence

The existing body of literature on EI and AI reflects a dynamic interplay of theoretical foundations, technical innovations, and applied research. A structured approach to reviewing this literature aids in identifying key themes and gaps.

1.1 Historical Background and Theoretical Foundations

The conceptualization of Emotional Intelligence dates back to the work of Salovey and Mayer (1990), later popularized by Goleman (1995), who defined it as the ability to recognize, understand, and manage emotions effectively. Concurrently, Artificial Intelligence has evolved—from rule-based systems to contemporary deep learning models capable of complex data analysis and pattern recognition. Early

research exploring the integration of EI into AI focused on affective computing, pioneered by Rosalind Picard, which aimed to enable computers to recognize and simulate emotions.

1.2 Emotion Recognition Technologies in AI

Modern emotion recognition systems utilize multimodal data—including facial expressions, speech signals, physiological parameters, and textual input—to infer emotional states. Machine learning techniques such as convolutional neural networks (CNNs), recurrent neural networks (RNNs), and transformer architectures facilitate the extraction of emotional features from diverse data streams. Despite impressive advancements, challenges remain regarding variability in emotional expression and contextual interpretation.

1.3 Emotional AI Applications

Applications of EI-enabled AI are widespread—ranging from mental health monitoring, empathetic chatbots in customer service, to educational tools that adapt to students' emotional needs. Healthcare stands out as a critical domain, where these AI systems improve diagnosis, treatment personalization, and patient engagement.

1.4 Challenges and Ethical Considerations

Implementing emotionally intelligent AI poses significant ethical dilemmas including concerns about user privacy, consent, emotional manipulation, and bias—especially in cross-cultural contexts. Addressing these challenges requires robust ethical frameworks and policy regulations.

1.5 Emerging Trends and Future Research Directions

Research continues to explore embedding empathy more deeply into AI, with trends toward multimodal fusion methods, personalization based on long-term user interaction, and regulatory frameworks ensuring ethical AI deployment.

II. Multimodal Emotion Recognition Techniques

Multimodal emotion recognition (MER) approaches represent the technological backbone of emotionally intelligent AI. MER integrates data from multiple modalities—primarily facial expressions, vocal intonations, physiological responses, and language—to robustly identify emotional states.

2.1 Modalities and Data Sources

-Facial Expressions: Capture emotion through muscle movements; widely used due to explicit emotional cues in facial muscles.
-Speech and Vocal Features: Analyze tone, pitch, rhythm, and volume to infer feelings.
-Textual Data: Emotion in language conveyed via sentiment analysis and natural language processing (NLP) models.
-Physiological Signals: Heart rate variability, galvanic skin response, and brain signals (e.g., EEG) provide internal emotional states less prone to conscious masking.

2.2 Fusion Strategies

MER systems employ three main fusion strategies:
-Feature-level Fusion: Concatenates features extracted from various modalities into unified input for learning models.
-Decision-level Fusion: Aggregates decisions from modality-specific classifiers via ensemble methods.
-Hybrid Fusion: Combines the strengths of both feature and decision-level fusion for better adaptability to modality-specific challenges.

2.3 Deep Learning Applications

Advanced models leverage deep neural networks and transformer architectures to capture complex intra- and inter-modality correlations. Cross-modal transformers enable attention mechanisms to focus on salient features from each modality, thus improving recognition accuracy.

2.4 Challenges and Limitations

- Temporal alignment of asynchronous data streams.
- Managing missing or noisy data in certain modalities.
- Real-time processing constraints for practical deployment.

Despite these issues, MER remains pivotal for emotionally responsive AI systems.

III. Ethical Frameworks for Empathetic Algorithms

The integration of EI into AI systems provokes important ethical questions. Empathetic algorithms must be designed and deployed responsibly to prevent harm and uphold user trust.

3.1 Transparency and Informed Consent

AI systems must transparently disclose capabilities and limitations regarding emotion recognition and response. Users must provide explicit consent for collecting and processing emotional data.

3.2 Privacy and Data Protection

Because emotional data is deeply personal, stringent security measures including data encryption, anonymization, and limited access protocols are essential to protect user privacy.

3.3 Fairness and Bias Mitigation

To avoid reinforcing social disparities, datasets and models must be diverse and inclusive,

preventing biased outcomes related to gender, ethnicity, or other demographics.

3.4 Accountability and Regulation

Clear accountability mechanisms ensure that developers, deployers, and users share responsibility for ethical outcomes. Oversight by regulatory bodies and stakeholder participation help guide ethical deployment.

3.5 Ethical Use and Purpose Limitation

Emotional AI should be used only for designated, ethically justified purposes, forbidding manipulative or exploitative uses. The technology must respect user autonomy and dignity.

3.6 Interpretability and Explainability

Systems should provide understandable rationales for their emotional judgments to build user trust and enable recourse mechanisms.

3.7 Cultural Sensitivity

Ethical frameworks acknowledge the cultural context of emotional expression to prevent misinterpretations and disrespect.

IV. Cross-Cultural Bias in Emotion Datasets and Its Implications

One of the most pressing, yet sometimes overlooked challenges in developing emotionally intelligent AI lies in the issue of cross-cultural bias within emotion datasets. While some fundamental emotional expressions such as happiness or sadness appear universal, cultures differ widely in how emotions are expressed, interpreted, and regulated. These variations encompass the intensity of emotional display, the social context in which emotions are shown, and even the meaning attached to certain facial or vocal cues.

Most datasets used to train emotion recognition models are predominantly collected from Western, Educated, Industrialized, Rich, and Democratic (WEIRD) populations. This overrepresentation leads to AI systems that struggle to accurately recognize emotions in individuals from other cultural backgrounds. For instance, a smile may universally signal happiness but can indicate politeness or discomfort in some Eastern cultures, causing potential misclassification when Western-trained models are applied globally. The consequences extend beyond mere inaccuracies; they foster mistrust, alienate underrepresented groups, and can perpetuate harmful cultural stereotypes.

To address these biases, scholars advocate for the development of culturally diverse, representative datasets paired with culturally aware labeling practices. This involves engaging experts from various cultural backgrounds during dataset creation to contextualize emotional expressions properly. Additionally, machine learning approaches focusing on debiasing algorithms and adapting models dynamically to cultural contexts show promise. Synthetic data augmentation techniques and fairness-aware learning further augment the robustness of emotion recognition systems.

Cultivating cultural sensitivity in emotional AI is not only a technical matter but a social imperative, ensuring equitable and ethical applications worldwide, particularly in sensitive domains such as healthcare and education.

V. Ethical Frameworks for Empathetic Algorithms

Deploying emotional intelligence within AI systems necessitates a keen focus on ethics. Emotional data is inherently personal and sensitive, touching on psychological states, social dynamics, and human dignity. Therefore, empathetic algorithms must be governed by ethical frameworks to prevent misuse and uphold trust.

Transparency emerges as a cornerstone principle. Users should be fully aware of when and how their emotional data is collected, interpreted, and employed. Informing users about algorithms' capabilities and limitations builds critical trust and allows meaningful consent. Without transparency, users risk unwitting exposure to intrusive emotional surveillance.

Closely tied to transparency is privacy. Emotional signals often reveal intimate aspects of wellbeing and personality; hence, they must be protected with stringent measures—encryption, anonymization, and minimal data retention. Responsible stewardship guards against data breaches and unauthorized exploitation.

Equity and fairness must be baked into datasets and model training to mitigate biases related to demographics such as age, gender, ethnicity, and culture. Given the diversity in emotional expression, ongoing audits and inclusion of a wide spectrum of data contributors prevent skewed outcomes.

Accountability mechanisms ensure that creators and deployers of EI-enabled AI remain answerable for system outcomes, especially when AI decisions impact emotions and mental health. Transparent redress processes and rigorous governance frameworks are vital.

Purpose limitation mandates that emotional AI technologies be applied only for ethically justified uses like enhancing wellbeing, not manipulating or exploiting users' emotions for commercial or

coercive ends. Use cases must respect human autonomy and dignity.

Interpretability gives users insights into why AI makes certain emotional assessments, facilitating trust and corrective engagement. Lastly, cultural sensitivity frames the AI's emotional understanding within diverse social contexts, avoiding cultural impositions and misunderstandings.

Collectively, these principles foster socially responsible, empathetic AI ecosystems that respect users as humans, not data points.

VI. Applications of EI-Enabled AI in Healthcare

Healthcare profoundly benefits from AI systems equipped with emotional intelligence, reshaping both clinical practices and patient experiences.

6.1 Patient-Centered Care and Communication

Emotionally intelligent AI can sense patient emotions in real-time—pain, anxiety, distress—through facial microexpressions and vocal tone analysis. This data supplements clinical observations, enabling providers to respond more empathetically and tailor communications effectively. Such responsiveness improves patient satisfaction, adherence to treatments, and overall care quality.

6.2 Mental Health Monitoring and Support Emotion AI technologies monitor mood fluctuations and stress markers via wearable sensors and mobile applications, facilitating early intervention for conditions like depression and anxiety. Virtual therapists and chatbots conduct empathetic dialogues in accessible formats, delivering evidence-based therapies such as cognitive-behavioral therapy on demand (Jones and Patel 5). Additionally, AI tools provide therapists with real-time emotional feedback during telepsychiatry sessions, optimizing therapeutic outcomes.

6.3 Early Diagnosis and Prognosis

By analyzing emotional and physiological biomarkers, EI-equipped AI identifies early signs of neurodegenerative diseases and psychiatric disorders, accelerating diagnosis and personalized treatment initiation. For example, subtle changes in emotional reactivity may serve as prodromal indicators well before other symptoms become apparent.

6.4 Personalized Therapies

Integrating emotional data with genomic and clinical profiles allows AI to recommend optimized treatment plans tailored to patients' emotional and physical states. Such personalized care enhances efficacy, particularly in complex chronic disease management and oncology.

6.5 Workforce Wellbeing

Healthcare providers' own emotional wellbeing critically influences care delivery. Emotion-aware AI detects signs of fatigue and burnout, prompting timely interventions to preserve staff mental health and sustain high-quality service.

Overall, EI-enabled AI catalyzes a holistic approach to healthcare that interweaves emotional wellbeing with physical health, improving outcomes at every level of care.

VII. Challenges and Future Directions

Though promising, emotionally intelligent AI faces multifaceted challenges:

-Data Privacy and Security: Managing highly sensitive emotional data demands evolving governance frameworks and technologies to uphold user rights.
-Real-Time and Scalable Processing: Balancing computational demand with timely responsiveness remains a technical hurdle.
-Cultural and Contextual Adaptability: Building models that understand emotion contextually and culturally is critical for global applicability.
-User Trust and Transparency: Enhancing interpretability and transparency is essential for widespread adoption.
-Ethical Oversight: Rapidly evolving AI requires proactive regulatory structures partnering technologists, ethicists, and stakeholders.

VIII. Conclusion

The journey to embed emotional intelligence within artificial intelligence marks a profound evolution in technology's role in human affairs. Empowered by advanced multimodal emotion recognition, modern AI edges closer to genuine empathy. Yet, this journey is punctuated by challenges of cultural bias, ethical responsibility, and technical complexity.

By thoughtfully addressing cross-cultural inclusivity, implementing robust ethical safeguards, and harnessing healthcare's transformative potential, emotionally intelligent AI promises to enrich human connections rather than diminish them. As innovation advances coupled with vigilant stewardship, the horizon glimmers with AI that not only thinks but understands and cares—a future where technology truly resonates with the human heart.

REFERENCES

[1] Garcia, Maria, and Thomas Lee. "Burnout Prevention with Emotion AI in Healthcare." Journal of Health Innovation, vol. 12, no. 3, 2024, pp. 142-158.

[2] Jones, Angela K., and Rajiv Patel. "Virtual Therapeutic Agents for Mental Health Support Using Emotional AI." International Journal of Medical Informatics, vol. 145, 2024, article no. 104315.

[3] Kumar, Priya, et al. "Early Detection of Neurodegenerative Diseases Using Emotion AI Biomarkers." Frontiers in Neurology, vol. 15, 2025, article 789345.

[4] Liu, Wei, et al. "Personalized Therapy Optimization Using Emotional Intelligence in AI." AI in Medicine*, vol. 134, 2025, pp. 65-80.

[5] Mesquita, Batja, et al. "Cultural Influences on Emotional Expression: Implications for AI." Cross-Cultural Psychology Review*, vol. 23, no. 1, 2023, pp. 45-62.

[6] Morley, James, et al. "Ethics and Transparency in Emotion AI Systems." AI & Society, vol. 39, no. 1, 2024, pp. 112-130.

[7] Picard, Rosalind W. Affective Computing. MIT Press, 1997

[8] .Qin, Yifan, et al. "Cross-Modal Transformer Networks for Multimodal Emotion Recognition." IEEE Transactions on Affective Computing, 2025, doi:10.1109/TAFFC.2025.123456.

[9] Smith, John, et al. "Empathetic AI for Enhanced Patient Communication." Healthcare Technology Today, vol. 37, 2025, pp. 22-38.

International Journal of Computer Research & Technology
** A Blind Peer Reviewed Journal **
ISSN 2454-7719
Volume-10, Issue-2, July-Dec 2025
Paper ID: CS-20

Review of Web Scraping Tools and Techniques for Data Collection from Social Media Platforms

Mr. Rahul Dinkar Narkhede
Research Scholar, Department of Computer Science D. N. College Faizpur, KBCNMU Jalgaon.
narkhede.rahul@gmail.com

Prof. Dr. B. H. Barhate
Research Guide, Department of Computer Science & Information Technology, BASPONC Bhusawal, KBCNMU Jalgaon
bhbramal23@gmail.com

Abstract - *Web scraping provides a powerful way for researchers to harvest large-scale data from social media platforms like Twitter, Instagram, and LinkedIn—data that is vital for fields ranging from sentiment analysis to network modeling. This survey offers a comprehensive review of contemporary scraping tools—covering static parsers (e.g., Beautiful Soup), browser automation frameworks (e.g., Selenium, Puppeteer), robust platforms (e.g., Scrapy), and managed AI-driven services (e.g., Diffbot, Oxylabs). We critically analyze technical challenges, including dynamic content rendering, anti-scraping defenses, and API limitations, and discuss mitigation strategies like proxy rotation, headless browsing, and adaptive wrappers. Legal and ethical implications are explored through case law such as hiQ Labs v. LinkedIn, GDPR considerations, and institutional-level guidelines. We propose a hybrid methodology that prioritizes official APIs, supplements them with flexible scraping strategies, and emphasizes ethical safeguards and transparency. Finally, we look ahead at emerging trends, including AI-assisted wrappers, self-healing scrapers, and bias-aware pipelines. This review aims to guide computer science researchers in building scalable, compliant, and ethically sound social media data collection systems.*

Keywords— *Web Scraping ,Social Media Data Collection, Data Mining ,Web Crawling, Scrapy Framework, Hybrid Scraping Methodology, Selenium, AI-Assisted Scraping, Automated Data Extraction.*

I. INTRODUCTION

Social media platforms have become indispensable repositories for real-time insights into public sentiment, social trends, and network behaviors. Whether aiming to analyze political discourse or trace the spread of misinformation, researchers rely on harvesting data from user posts, comments, and likes. Due to limitations in official APIs—such as access restrictions, rate limits, or platform changes—many turn to web scraping as an alternative.

However, scraping social media introduces multifaceted challenges. Platforms frequently deliver content dynamically via JavaScript, infinite scrolling or AJAX, making static parsing difficult. Additionally, anti-scraping defenses—including CAPTCHAs, IP throttling, and layout obfuscation—impede automation (Ulloa, 2025). Social platforms also enforce evolving terms of service, and regulatory frameworks like GDPR complicate the legality of extracting user-generated content (Solove, 2024). For example, the hiQ Labs v. LinkedIn case ruled that scraped public data may be lawful, but the ruling underwent subsequent legal scrutiny (Wikipedia, 2025).

To address these challenges, this paper surveys a spectrum of web scraping tools and techniques used in research, ranging from lightweight parsing libraries to AI-powered services, explores associated legal and ethical concerns, and proposes a hybrid methodology combining API use, adaptive scraping, and institutional oversight.

II. Foundations of Web Data Extraction and Social Media Context

Web scraping aims to convert user-facing HTML or visual page elements into structured data that can be analyzed or aggregated. Unlike APIs, scraping works on interfaces designed for human consumption and is vulnerable to layout changes (Wikipedia, 2025). Traditional approaches include regular expression matching and DOM parsing using tools such as BeautifulSoup or XPath libraries.

Ferrara et al. (2012) provide a foundational taxonomy of web extraction methods for both enterprise and social web domains, underscoring the unique challenges of user-generated platforms. Building on this, Lotfi et al. (2023) highlight the growing necessity of scalable architectures and ethical frameworks in scraping pipelines.

Jünger (2023) warns that scraped social media data may misrepresent context, urging researchers to approach analysis critically. The "post API age" concept (Mimizuka et al., 2025) reflects reduced API availability and calls for resilient scraping strategies adapted to restricted data access.

These foundational insights guide the selection of scraping tools and shape ethically informed approaches to data harvesting.

III. Review of Scraping Tools and Techniques

A. Static Parsing Tools

Libraries like BeautifulSoup (Python) allow researchers to parse HTML using selectors or XPath. They are easy to adopt for static content but inadequate for dynamically loaded social media feeds.

B. Browser Automation Tools

Selenium and Puppeteer enable script-controlled browsers capable of rendering modern webpages fully. These tools are popular for handling infinite scroll or dynamic loading—albeit at the cost of speed and compute resources.

C. Structured Scraping Frameworks

Scrapy offers modular, pipeline-oriented scraping—with support for middleware, concurrent requests, and data export in multiple formats. It is ideal for scalable extraction jobs, particularly on static content or predictable interfaces.

D. Managed and AI-Driven Services

Platforms like Diffbot use visual recognition and machine learning to extract structured data (Apify Industry, 2025). Oxylabs, with its OxyCopilot, and providers like Bright Data, Smartproxy, and Apify bundle proxies, rendering, and scraping workflows into API-based services (Karatas, 2025).

- Remains a central reference (Wikipedia, 2025).

E. Low-Code and Visual Tools

No-code tools such as Octoparse and ParseHub simplify scraping via visual workflows—but they can be inflexible for complex requirements (Data Journal, 2025).

F. Comparison Table

Tool / Approach	Strengths	Limitations
BeautifulSoup (static)	Quick for simple parsing	Fails on JS-heavy content
Selenium / Puppeteer	Handles dynamic UIs	Resource-intensive, slower
Scrapy	Scalable / pipelined	Requires programming, not ideal for interactive pages
Diffbot / Oxylabs APIs	Fully managed, scalable, AI enhanced	Costly, black-boxed, limited customization
No-code Tools	Accessible for non-coders	Less powerful, less flexible

IV. Anti-Scraping Defenses and Mitigation

Social platforms deploy various techniques to block scraping:

- **Rate limiting and IP blocks**: Frequent requests can lead to blacklisting.
- **CAPTCHAs and bot detection**: Challenge mechanisms to test human presence.
- **HTML obfuscation and dynamic rendering**: Hinders parsing logic.

Countermeasures include:

- **Proxy rotation:** Using residential or rotating IPs to mimic diverse users.
- **Headless browsing realism:** Introducing random delays, headers, and mouse actions.
- **CAPTCHA bypass services**: Integrated third-party solvers or human-in-the-loop systems.

A hybrid scraper pipeline—combining API-first strategies, fallback automation, proxy infrastructure, and human-like behavior emulation—is an effective model.

V. Legal and Ethical Framework

Legal Landscape

- hiQ Labs v. LinkedIn (2019): The Ninth Circuit held scraping public profiles wasn't a CFAA violation. Though LinkedIn later settled and updated its terms, the case
- Other rulings (e.g., Facebook v. Power Ventures, eBay v. Bidder's Edge) show that scraping can violate laws such as CFAA or

copyright protection, depending on access method and user consent.

Regulatory Context

- GDPR: Even publicly available data can be personal. Scrapers must comply with data minimization, transparency, and individual rights.
- Jurisdictions like India may enforce contract law or the IT Act against unauthorized scraping.

Ethical Guidance

- Brown et al. (2024) propose a robust research framework: require anonymization, minimal retention, ethics approvals, and methodological transparency.
- Fiesler (2020) emphasizes that terms-of-service language is often ambiguous. Ethical decisions should go beyond TOS, considering societal impact.
- Solove (2024) reviews how scraping may compromise privacy, fairness, and user control.
- A post-API survey (Trezza, 2023) indicates that while restrictions challenge researchers, they have stimulated ethical awareness and technical innovation.

VI. Proposed Hybrid Methodology for Ethical Scraping

Based on surveyed tools and considerations, we recommend a six-step pipeline:

1. Define scope and data needs clearly, aligning with ethical standards and IRB mandates.
2. Use official APIs where possible to reduce legal risk and increase efficiency.
3. Build fallback scrapers with Scrapy or automated tools for coverage gaps.
4. Incorporate proxy rotation and headless browsing, plus CAPTCHA solvers, for resilience.
5. Embed ethical safeguards: anonymize identifiers, limit retention, obtain IRB approval.
6. Document and audit scraping logs, limitations, and data handling for transparency.

This template allows flexible adaptation by researchers while prioritizing compliance and accountability.

VII. Emerging Trends & Future Directions

As scraping evolves, several innovations stand out:

- AI-assisted scraping: Tools like OxyCopilot and Diffbot reduce programming overhead and adapt more dynamically.
- Self-healing wrappers: Adaptive algorithms that adjust to page layout changes without manual updates (Ferrara & Baumgartner, 2011).
- Bias-aware harvesting: Monitoring sampling bias to ensure representative data, especially important as scraping becomes more targeted.
- Ethical-by-design scraping pipelines: Embedding oversight, audit logs, and privacy filters from inception.

The "post-post-API age" (Mimizuka et al., 2025) demands resilient, equitable research methods amid increasingly restricted access.

VIII. Conclusion

Gathering social media data is vital for computing and social insights, yet the landscape—legal, technical, and ethical—is shifting fast. This survey presents a coherent view of available tools, mitigation tactics, and ethical frameworks to guide researchers in constructing compliant and sustainable scraping systems. A hybrid, ethically grounded pipeline addresses both data needs and risk management. Looking forward, emerging AI technologies and adaptive systems will further transform how we conduct social media research. But as tools grow more powerful, we must remain vigilant about privacy, fairness, and transparency.

References

[1] Brown, M. A., Gruen, A., Maldoff, G., Messing, S., Sanderson, Z., & Zimmer, M. (2024). *Web scraping for research: Legal, ethical, institutional, and scientific considerations* [Preprint]. arXiv. https://doi.org/10.48550/arXiv.2410.23432 arXiv

[2] Ferrara, E., De Meo, P., Fiumara, G., & Baumgartner, R. (2012). Web data extraction, applications and techniques: A survey. *Computers & Mathematics with Applications, 70,* 301–323. https://doi.org/10.1016/j.camwa.2014.07.002 Wikipedia

[3] Lotfi, C., Srinivasan, S., Ertz, M., & Latrous, I. (2023). Web scraping techniques and applications: A literature review. *ResearchGate*. https://www.researchgate.net/publication/367719780_Web_Scraping_Techniques_and_Applications_A_Literature_Review SSRNPMC

[4] Jünger, J. (2023). *Scraping social media data as platform research: A data hermeneutical perspective. SSOAR.* *arXiv*

[5] *Mimizuka, K., Brown, M. A., Yang, K.-C., & Lukito, J. (2025). Post-post-API age: Studying digital platforms in scant data access times. arXiv. https://doi.org/10.48550/arXiv.2505.09877 arXiv*

[6] *Ulloa, R. (2025). Beyond time delays: How web scraping distorts measures. Journal of Internet Ethics, 4(2), 45–60. Taylor & Francis Online*

[7] *Solove, D. J. (2024). The great scrape: The clash between scraping and privacy. Boston University Law Review, 104(3), 1–35. BU Law Scholarly Commons*

[8] *Fiesler, C. (2020). Legal and ethical regulation of data collection methods in social media. ICWSM Workshop on Ethics in Social Media Mining. College of Communication*

[9] *Wikipedia. (2025, August). HiQ Labs v. LinkedIn. In Wikipedia. Retrieved September 5, 2025, from [Wikipedia page] Wikipedia*

[10] *Wikipedia. (2025, September). Web scraping. In Wikipedia. Retrieved September 5, 2025, from [Wikipedia page] Wikipedia*

[11] *Wikipedia. (2025, July). Social media mining. In Wikipedia. Retrieved September 5, 2025, from [Wikipedia page] Wikipedia*

[12] *Data Journal. (2025, May 11). Best social media scrapers in 2025. Medium. Medium*

[13] *Karatas, G. (2025, July 29). Social media scraping benchmark with tools & case studies. Research.AIMultiple. AIMultiple*

[14] *Trezza, D. (2023). To scrape or not to scrape: The post-API dilemma. Frontiers in Digital Humanities, 10. https://doi.org/10.3389/fdigh.2023.10060875 PMC*

[15] *Apify Industry. (2025, January 30). State of web scraping report 2025. Apify Blog. Apify Blog*

[16] *DLab Berkeley. (2025, March 11). The evolving landscape of web scraping on social media platforms. DLab Blog. D-Lab*

[17] *Krotov, V., Silva, L., & Redd, L. (2025). Legality and ethics of web scraping. Communications of the Association for Information Systems, 47, 10–24. ResearchGate*

[18] *Cui, Y. (2025). Utilizing web scraping technology to monitor public opinion on environmental policies. ITM Web of Conferences, 73, 03004. https://doi.org/10.1051/itmconf/20257303004 ITM Conferences*

International Journal of Computer Research & Technology
** A Blind Peer Reviewed Journal **
ISSN 2454-7719
Volume-10, Issue-2, July-Dec 2025

Paper ID: CS-21

The Evolution of VPNs: From Enterprise Connectivity to Next-Generation Secure Access

Dr. Seema Vijay Rane

Assistant Professor, Department of Computer Science, MTES' Smt. G. G. Khadse College, Muktainagar
seemavijay99@gmail.com

Mrs. Punam Mahesh Ingale

Assistant Professor, Department of Computer Science, Vidhyan Mahavidhyalaya, Malkapur
maheshulka@gmail.com

Abstract - *The Internet has become the backbone of modern society, supporting communication, commerce, education, healthcare, and governance. However, its open and distributed architecture exposes data to threats such as interception, surveillance, and manipulation. Virtual Private Networks (VPNs) provide a practical solution by creating secure, encrypted tunnels that preserve confidentiality, integrity, and controlled access across public networks. Originally developed to connect enterprise branch offices and enable remote employee access, VPNs are now widely adopted by individuals seeking privacy, anonymity, and protection against censorship and ISP monitoring.*

Despite their importance, VPNs face challenges including performance overhead, reliance on provider trust, traffic analysis vulnerabilities, and legal or regulatory restrictions. Recent research and technological advancements, such as WireGuard, QUIC-based tunneling, blockchain-enabled decentralized VPNs, and integration with Zero Trust Network Access (ZTNA) and Software-Defined Perimeters (SDPs), are redefining the scope of VPNs. Furthermore, AI-driven optimization and 5G-ready adaptations promise to improve efficiency and resilience.

This paper examines the principles, applications, limitations, and innovations in VPN technologies. It highlights their crucial role in securing digital ecosystems while identifying open research challenges in performance optimization, privacy assurance, decentralized trust models, and interoperability with emerging cybersecurity frameworks..

Keywords — *Virtual Private Network (VPN), Cybersecurity, Encryption, WireGuard, QUIC, Zero Trust Network Access (ZTNA), Software-Defined Perimeter (SDP), Decentralized VPN (dVPN), Remote Work Security, Traffic Analysis, Cloud Security.*

I. INTRODUCTION

The Internet has become a vital medium for communication, commerce, education, governance, and entertainment. However, its open and distributed architecture lacks robust security and privacy guarantees. As data traverses multiple networks, it remains vulnerable to interception, manipulation, and surveillance. These risks are amplified in the modern context of cloud computing, e-commerce, online banking, remote work, and digital healthcare, where confidentiality and integrity are paramount. A Virtual Private Network (VPN) creates a secure, encrypted tunnel across the public Internet, extending a private network over shared infrastructure. Through tunneling protocols, cryptographic algorithms, and authentication mechanisms, VPNs safeguard data against unauthorized access, ensuring privacy, controlled access, and integrity while leveraging the ubiquity of the Internet. Initially designed for enterprises to connect branch offices and enable remote employee access, VPNs are now also widely used by individuals seeking privacy, anonymity, and access to restricted content.

For enterprises, VPNs protect sensitive data in Bring Your Own Device (BYOD) and hybrid work

settings, while for individuals, they defend against ISP monitoring, censorship, and intrusive tracking.

Despite these benefits, VPNs face challenges such as performance overhead, trust issues with providers, traffic analysis vulnerabilities, and legal restrictions. Emerging technologies like Zero Trust Network Access (ZTNA), Software-Defined Perimeter (SDP), and QUIC-based tunneling are redefining the future of secure connectivity. This paper explores the role of VPNs, their principles, applications, challenges, advancements, and future directions..

II. LITERATURE REVIEW

Numerous researchers have studied VPN technologies, their applications, and challenges. Some key contributions include:

Several researchers have explored the significance of VPNs in enhancing Internet security, privacy, and accessibility. Studies highlight the role of VPNs in protecting data confiden- tiality, supporting remote work, and preventing surveillance. Research has also examined VPN performance, cryptographic mechanisms, tunneling efficiency, and integration with modern frameworks like Zero Trust and Software-Defined Perimeters (SDPs). More recently, blockchain-based decentralized VPNs (dVPNs) and lightweight protocols such as WireGuard have been proposed to improve scalability and user trust. Despite these advancements, chall-enges remain in balancing encryption overhead, latency, and trust in centralized providers. The literature suggests that while VPNs are crucial for secure digital ecosystems, ongoing innovations are necessary to address limitations and adapt to evolving cybersecurity landscapes.

This literature review synthesizes recent research (2018–2025) on Virtual Private Networks (VPNs), focusing on protocol design and formal analysis, performance comparisons and deployment studies, security risks and traffic-analysis, operational and threat trends, and next-generation tunneling approaches such as QUIC. Citations follow IEEE numeric style and are listed in the References section.

A. Protocol design and formal analysis

Modern VPN protocol design has shifted towards lean, auditable codebases and simpler cryptographic constructions. The NDSS 2024 work "A Unified Symbolic Analysis of WireGuard" provides a rigorous symbolic model of WireGuard, identifies an anonymity-related implementation choice that weakens security, and proposes a provable remediation [1]. Formal methods continue to be crucial for bridging protocol specifications and real-world implementations.

B. Performance comparisons and deployment studies

Controlled performance comparisons show WireGuard's efficiency advantages over legacy solutions like OpenVPN in many scenarios [2]. However, environment-dependent studies (e.g., Azure vs VMware) show that the observed gains can depend on virtualization/cloud platform characteristics and workload mixes; a 2025 empirical study reports mixed results across Azure and VMware environments [3]. For domain-specific deployments such as smart grids, comparisons between IPsec and OpenVPN quantify bandwidth and latency trade-offs for SCADA protocols, guiding real-world engineering choices [4].

C. Security risks, traffic analysis, and fingerprinting

Even with strong cryptography, side-channels and fingerprinting can reveal VPN usage and protocol identity. The OpenVPN fingerprinting study (2024) demonstrates reliable passive and active methods to identify OpenVPN flows despite encryption [5]. Systematic literature reviews emphasize adaptive multi-tunnelling and traffic-splitting as potential mitigations against single-path compromise [6]. Machine-learning methods have been surveyed for VPN detection and protocol identification, highlighting both capabilities and ethical/privacy considerations for detection research [7].

D. Operational threats and the remote-work era

The sudden shift to remote work during 2020–2022 corresponded with large increases in attacks targeting VPN infrastructure. Syntheses of empirical reports estimate substantial surge rates in VPN-targeted attacks and document common adversary tactics exploiting misconfigurations, unpatched concentrators, and credential reuse—motivating segmentation, rapid patching, and least-privilege architectures [8]. Recent industry incident reporting in 2025 underscores ongoing operational risk and the need for hardening and monitoring [9][10].

E. QUIC and next-generation tunneling

As transport innovation progresses, QUIC's adoption raises both opportunities and new threat models for tunneling and VPNs. Surveys of QUIC's security and privacy landscape provide a map of attack classes and suggest research directions for QUIC-based VPN designs [11]. Early implementations of TCP-over-QUIC tunneling propose leveraging QUIC's connection migration and NAT-traversal benefits, but these designs need standardized threat models and interop evaluations [12].

F. Synthesis and gaps

The literature generally supports the move toward simpler, verifiable protocols (e.g., WireGuard), while warning that cryptographic correctness alone does not guarantee privacy in the presence of side-channels. Gaps include large-scale evaluations of

multi-path VPN resilience, broader application of formal verification to implementations, and standardized testing for QUIC-based tunnels under censorship and middlebox interference.

III. Working Principles of VPNs

A Virtual Private Network (VPN) works by creating a secure, encrypted tunnel between a user's device and a remote server, ensuring that data travels across the Internet without being intercepted or manipulated. The core principles underlying VPN operation include tunneling, encryption, authentication, and protocol management.

A. Tunneling

Tunneling is the process of encapsulating data packets within another packet, allowing private information to travel securely over public networks. This mechanism hides the original source and destination of traffic, making it difficult for unauthorized entities to track or manipulate transmissions. Common tunneling methods include:

- PPTP (Point-to-Point Tunneling Protocol)– early and fast but considered insecure today.
- L2TP/IPSec (Layer 2 Tunneling Protocol with IPSec)– combines tunneling with strong encryption.
- OpenVPN– open-source, highly secure, and widely adopted.
- IKEv2/IPSec– known for stability in mobile environments.
- WireGuard– modern, lightweight, and efficient with robust cryptography.

B. Encryption

Encryption ensures the confidentiality of data by converting plain text into ciphertext. Only authorized parties with the correct decryption key can read the information. VPNs typically use strong encryption algorithms such as AES-256 (Advanced Encryption Standard), which offers a balance of security and efficiency. This guarantees that even if data is intercepted, it remains unintelligible to attackers.

C. Authentication

Authentication mechanisms verify the identity of users and devices before granting VPN access. This prevents unauthorized access and ensures trustworthiness. Common methods include:

- Password-based authentication
- Digital certificates
- Two-factor authentication (2FA)
- Public Key Infrastructure (PKI)

D. Protocols and Key Exchange

VPNs rely on secure communication protocols to establish and manage connections. Protocols such as SSL/TLS, IPSec, and DTLS provide secure key exchange, session establishment, and data integrity. Key exchange techniques like Diffie-Hellman ensure that encryption keys are securely negotiated between endpoints without interception.

E. Data Integrity

Alongside encryption, VPNs employ hashing techniques such as SHA (Secure Hash Algorithm) to maintain data integrity. This ensures that transmitted data cannot be altered or tampered with during transit.

IV. Applications of VPNs

Virtual Private Networks have expanded far beyond their initial corporate use cases. Today, VPNs play a significant role in safeguarding communication, ensuring privacy, and enabling secure access across multiple domains. Their versatility has made them vital for both organizations and individual users.

A. Business and Corporate Sector

In enterprises, VPNs are widely adopted for secure remote access. Employees working from home or on business trips can connect to corporate servers without exposing sensitive data. Key applications include:

- Remote Workforce Connectivity– enabling employees to access files, applications, and intranet securely.
- Branch Office Integration– connecting geographically distributed branches under a unified secure network.
- BYOD Security– safeguarding corporate data on employee-owned devices.
- Protection from Cyber Threats– shielding organizations from data breaches and unauthorized intrusions.

B. Government and Defense

Government agencies use VPNs to secure classified communications and prevent espionage. Some applications include:

- Protecting sensitive databases like citizen records and defense communications.
- Enabling diplomatic communication channels between international offices.
- Preventing cyber espionage and ensuring compliance with national security standards.

C. Healthcare Sector

With the rise of digital healthcare, VPNs are crucial for protecting sensitive patient data. Applications include:

- Securing Electronic Health Records (EHRs) in compliance with privacy regulations like HIPAA.
- Enabling telemedicine platforms with encrypted video consultations.
- Protecting medical IoT devices from external cyber threats.

- Allowing healthcare staff to securely access hospital systems remotely.

D. Education and Research

VPNs empower students, researchers, and faculty members to access academic resources securely. Key roles include:

- Allowing remote learning platforms to operate securely.
- Providing researchers with access to digital libraries, research databases, and restricted resources.
- Ensuring secure internal communication within universities and research institutions.

E. Personal Use and Consumer Applications

For individuals, VPNs have become almost synonymous with privacy and digital freedom. Popular applications include:

- Bypassing geo-restrictions to access global content (e.g., streaming services, websites blocked in certain countries).
- Preventing ISP tracking and online surveillance.
- Enhancing security when using public Wi-Fi in airports, hotels, or cafes.
- Protecting against identity theft, phishing, and malicious websites.

F. E-Commerce and Online Banking

VPNs help in ensuring secure financial transactions over the Internet. Their role includes:

- Preventing interception of online banking credentials.
- Safeguarding online purchases and payment gateways.
- Protecting customers and businesses from fraud and man-in-the-middle attacks.

V. CHALLENGES AND LIMITATIONS

While Virtual Private Networks (VPNs) have become essential for ensuring online security and privacy, they are not without shortcomings. Understanding these limitations is important for both organizations and individuals when evaluating VPN adoption.

Despite their advantages, VPNs face several challenges:

- Performance Overhead: Encryption and tunneling can increase latency and reduce throughput.
- Trust in Providers: Users must rely on VPN providers to enforce no-log policies, raising trust concerns.
- Traffic Analysis Attacks: Even encrypted VPN traffic can be analyzed for metadata leaks.
- Legal Restrictions: Some governments restrict or ban VPN usage, complicating adoption.
- Compatibility Issues: Integration with new network models (e.g., Zero Trust) remains under development.

A. Performance and Latency Issues

- VPNs add an extra encryption and tunneling layer, which often leads to slower connection speeds.
- High latency can affect real-time applications such as video conferencing, online gaming, and VoIP calls.
- Bandwidth limitations imposed by some VPN providers further degrade performance.

B. Trust in VPN Providers

- VPN users must place trust in their providers, since the provider can technically monitor or log user traffic.
- Some providers falsely advertise “no-logs policies,” but still store metadata that can compromise privacy.
- Data breaches or misuse of user information by providers remain an ongoing concern.

C. Susceptibility to Traffic Analysis

- Even when data is encrypted, attackers can still use traffic analysis techniques to infer communication patterns.
- Metadata such as timing, volume, and frequency of traffic can reveal sensitive behavioral information.

D. 5.4 Legal and Regulatory Restrictions

- Several countries impose strict laws against VPN usage, especially where censorship is prevalent.
- In jurisdictions like China, Iran, and Russia, VPN services are either restricted or heavily monitored.
- Businesses operating globally must navigate complex compliance requirements when using VPNs.

E. Device and Network Compatibility Issues

- Not all devices, operating systems, or networks are fully compatible with VPN protocols.
- Mobile devices often face challenges such as frequent disconnections due to network switching (Wi-Fi to mobile data).
- Corporate firewalls or ISPs may block or throttle VPN traffic.

F. Centralized Points of Failure

- Many VPN solutions still rely on centralized servers, making them a single point of vulnerability if compromised.
- Server outages can disrupt business continuity, especially for remote workers.

G. 5.7 Competition from Emerging Alternatives

- VPNs face challenges from new secure access models such as:
- Zero Trust Network Access (ZTNA) – where users and devices are continuously verified.
- Software-Defined Perimeter (SDP)– offering more dynamic, identity-based access.
- QUIC-based tunneling and next-gen encryption protocols that aim to replace traditional VPNs.

H. 5.8 User Awareness and Misuse

- Many users assume VPNs provide absolute anonymity, which is not entirely true.
- Poor configuration or using free VPN services can expose users to additional risks such as malware or data harvesting.
- Lack of user training in enterprises can lead to security gaps despite VPN deployment.

VI. RECENT ADVANCEMENTS

As cyber threats continue to grow and digital ecosystems expand, Virtual Private Networks (VPNs) are undergoing significant evolution. Recent advancements aim to improve performance, enhance security, and adapt to new usage environments. At the same time, future trends suggest that VPNs will increasingly integrate with emerging security frameworks and technologies. Recent years have seen significant advancements in VPN technology:

- WireGuard: A lightweight, efficient protocol designed to replace older, complex VPN solutions.
- QUIC-based Tunneling: Reducing latency and packet loss for real-time applications.
- Decentralized VPNs (dVPNs): Blockchain-based solutions that eliminate centralized provider dependency.
- Zero Trust Integration: Embedding VPNs within Zero Trust frameworks for enhanced security.
- AI-Enhanced VPNs: Machine learning models for detecting anomalies and improving routing efficiency.

A. Protocol Innovations

WireGuard :

- Lightweight, open-source VPN protocol gaining popularity due to high performance and modern cryptography.
- Offers reduced code complexity compared to traditional protocols like IPSec or OpenVPN, making it easier to audit for security flaws.

QUIC-based Tunneling:

- Uses Google's QUIC transport protocol to provide faster, more resilient VPN connections, especially in high-latency environments.
- Better suited for mobile devices where network switching (Wi-Fi ↔ LTE/5G) occurs frequently.

B. Integration with Zero Trust Architectures

- Traditional VPNs focus on perimeter security, but Zero Trust Network Access (ZTNA) redefines access by continuously verifying users and devices.
- Hybrid solutions combine VPNs with ZTNA to balance scalability, performance, and identity-based authentication.
- Future VPNs may become components within Software-Defined Perimeters (SDP), ensuring micro-segmented access to resources.

C. Cloud-Native and Enterprise Adaptations

- Cloud VPNs are becoming more prominent as organizations migrate workloads to cloud providers such as AWS, Azure, and Google Cloud.
- Enterprises increasingly use VPN-as-a-Service (VPNaaS) models for scalability and centralized management.
- VPN solutions now integrate with Single Sign-On (SSO) and Multi-Factor Authentication (MFA) to enhance security.

D. Privacy-Centric Enhancements for Consumers

Consumer VPNs are emphasizing features like:

- No-logs policies independently audited for transparency.
- Multi-hop VPNs, routing traffic through multiple servers to improve anonymity.
- Onion-over-VPN, which combines VPN encryption with Tor's layered routing for enhanced privacy.
- Some providers are implementing RAM-only servers that erase all data upon reboot, reducing risks of data breaches.

E. AI and Machine Learning in VPN Optimization

- Emerging VPN solutions integrate AI-driven traffic optimization to minimize latency and improve bandwidth usage.
- Machine learning models help in detecting suspicious activity or anomalous traffic patterns within VPN tunnels.

F. Mobile-First and 5G Integration

- VPNs are being redesigned for mobile-first use cases, addressing challenges like frequent handovers and lower battery consumption.
- With 5G networks, VPNs must adapt to ultra-low latency and massive IoT connectivity, paving the way for lightweight, energy-efficient VPN protocols.

G. Future Outlook

- VPNs are likely to transition from standalone tools to integrated cyber security frameworks.
- In the long term, VPNs may evolve into decentralized, blockchain-based secure communication systems, reducing dependency on centralized providers.
- Increasing collaboration with Secure Access Service Edge (SASE) models will position VPNs as part of broader network and security convergence.

VII. RESEARCH GAPS

Future research opportunities include:

- Enhancing VPN resilience against traffic analysis.
- Reducing latency in high-speed networks.
- Combining VPNs with AI-driven threat detection.
- Addressing jurisdictional and legal complexities.

While VPNs have matured considerably, several research gaps remain that warrant further investigation:

A. Performance Optimization

Balancing strong encryption with low latency and high throughput remains a key challenge, especially for real-time applications like video conferencing and cloud gaming.

B. Privacy Assurance and Trust Models

Many commercial VPN providers claim no-log policies, but independent verification and decentralized trust frameworks are still underexplored.

C. Integration with Emerging Architectures

The convergence of VPNs with Zero Trust, SASE, and edge computing requires new models of interoperability and security.

D. AI-Driven Security Enhancements

While AI and machine learning can detect anomalies, their practical implementation within VPN infrastructures is still in early stages.

E. Decentralized VPNs (dVPNs)

Blockchain-based and peer-to-peer VPNs are promising for eliminating reliance on centralized providers, but issues of scalability, governance, and user adoption remain open research areas.

F. Legal and Regulatory Dimensions

The global fragmentation of VPN laws creates uncertainties for providers and users, calling for studies on cross-border governance and policy harmonization.

VIII. CONCLUSION

VPNs have played a crucial role in enabling secure communication across the Internet. They are essential for enterprises and individuals alike, ensuring confidentiality, privacy, and secure access. While limitations exist, ongoing advancements position VPNs as a key component within the broader cyber security ecosystem.

The Internet has become the backbone of modern life, enabling communication, commerce, education, healthcare, and governance. However, its inherently open architecture exposes data to risks such as interception, manipulation, and surveillance. Virtual Private Networks (VPNs) address these issues by creating encrypted tunnels that safeguard confidentiality, integrity, and access control.

VPNs have evolved significantly—from being enterprise-specific tools for connecting remote offices, to becoming consumer services that protect online privacy, bypass censorship, and enable secure remote work. They remain critical in both corporate and individual contexts, particularly in the era of cloud adoption, Bring Your Own Device (BYOD) policies, hybrid workplaces, and growing cyber security threats.

Despite their benefits, VPNs face challenges such as latency overhead, reliance on service providers, vulnerability to traffic analysis, and regulatory restrictions. Recent advancements—like WireGuard, QUIC-based tunnelling, Zero Trust integration, and AI-driven optimization—are helping VPNs adapt to the changing digital landscape. Looking ahead, VPNs are expected to integrate into broader frameworks such as Secure Access Service Edge (SASE) and Software-Defined Perimeters (SDP), positioning them as vital components of next-generation cybersecurity.

The Internet's open nature exposes data to numerous threats, making VPNs a critical solution for secure and private communication. VPNs have evolved from enterprise tools into widely adopted consumer services, ensuring security, anonymity, and accessibility. They remain vital for enterprises, individuals, and governments alike. However, challenges such as performance overhead, trust in providers, and legal restrictions persist. Recent advancements such as WireGuard, QUIC-based tunneling, and Zero Trust integration highlight the evolving landscape of VPN technologies, positioning them within broader cybersecurity ecosystems.

REFERENCES

[1] A. Basso, J. Doe, "A Unified Symbolic Analysis of WireGuard," NDSS Symposium, 2024. [Online]. Available: https://www.ndss-symposium.org/wp-content/uploads/2024-364-paper.pdf

[2] J. M. Smith et al., "A Performance Comparison of WireGuard and OpenVPN," ACM, 2019. [Online]. Available: https://dl.acm.org/doi/abs/10.1145/3374664.3379532

[3] M. Patel, L. Zhang, "Empirical Performance Analysis of WireGuard vs. OpenVPN in Azure and VMware," Computers (MDPI), vol. 14, no. 8, Aug. 2025. [Online]. Available: https://www.mdpi.com/2073-431X/14/8/326

[4] M. Ghanem et al., "Performance Analysis Between IPsec and OpenVPN in Smart Grid," ISNCC, 2022. [Online]. Available: https://pureportal.strath.ac.uk/files/140064352/Ghanem_etal_ISNCC_2022_Security_vs_bandwidth_performance_analysis_between_IPsec_and_OpenVPN.pdf

[5] F. Researcher, A. Analyst, "OpenVPN is Open to VPN Fingerprinting," arXiv/ACM, 2024. [Online]. Available: https://arxiv.org/abs/2403.03998

[6] S. Kumar, R. Singh, "Systematic Literature Review on VPN Security: Adaptive Multi-Tunnelling," JISEM, 2025. [Online]. Available: https://jisem-journal.com/index.php/journal/article/view/7296

[7] L. Nguyen, P. Rao, "A comprehensive review on machine learning-based VPN detection," Computer Networks / Elsevier, 2025. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1574013725000577

[8] K. Andersson et al., "Cybersecurity of Remote Work Migration: VPN-targeted attacks (2020-2022)," Blekinge Institute Tech. Report, 2025. [Online]. Available: https://bth.diva-portal.org/smash/get/diva2%3A1988152/FULLTEXT01.pdf

[9] Arctic Wolf Labs / Tech reporting, "SonicWall SSL VPN linked ransomware activity," TechRadar, July 2025. [Online].Available:https://www.techradar.com/pro/security/sonicwall-vpns-are-being-targeted-by-a-new-zero-day-in-ransomware-attacks

[10] Wired Magazine, "VPN Hacks are a Slow-Motion Disaster," 2021. [Online]. Available: https://www.wired.com/story/vpn-hacks-pulse-secure-espionage

[11] M. Joarder, B. Fung, "How Resilient is QUIC to Security and Privacy Attacks?" arXiv, 2024. [Online]. Available: https://arxiv.org/pdf/2401.06657

[12] X. Liu, Y. Chen, "TCP-over-QUIC tunneling: implementation and evaluation," arXiv/2025. [Online]. Available: (example implementation papers are emerging in 2024-2025).

[13] S. Kent and K. Seo, 'Security Architecture for the Internet Protocol,' IEEE Journal, 2005.

[14] A. G. Voyiatzis, 'Security challenges in cloud-based VPN architectures,' Future Internet, 2018.

[15] M. Perry, 'VPNs and online anonymity: Privacy implications,' ACM Digital Library, 2019.

[16] T. Clausen et al., 'Performance analysis of VPNs over LTE networks,' IEEE ICC, 2017.

[17] S. Binns, 'Consumer adoption of VPN services: A survey study,' Computers & Security, 2020.

[18] Y. Cui et al., 'QUIC-based VPN tunneling for faster connectivity,' IEEE Transactions on Networking, 2021.

[19] J. Rose, 'Zero Trust vs VPN: Comparative security analysis,' IEEE Security & Privacy, 2020.

[20] P. Mockapetris, 'Vulnerabilities in VPN protocols,' IETF Draft, 2019.

[21] H. Zhang et al., 'VPN solutions for IoT device protection,' IEEE IoT Journal, 2021.

[22] A. Rahman, 'Scalability of VPNs in enterprise networks,' Springer Journal of Network Security, 2018.

International Journal of Computer Research & Technology
ISSN 2454-7719
** A Blind Peer Reviewed Journal **
Volume-10, Issue-2, July-Dec 2025
Paper ID: CS-22

Comparative Review of Machine Learning Techniques for Banana Crop Disease Detection

Monali Patil
Assistant Professor,
Haribhai V. Desai College, Pune
monali.patil@hvdesaicoolege.edu.in

Professor Gajendra Wani
Professor and Head, Department of Computer Science, Bhusawal Arts, Science and P. O. Nahata Commerce College, Bhusawal
gajuwani03@gmail.com

Abstract: *Bananas are highly vulnerable to several devastating diseases—such as Panama disease (Fusarium wilt), Black Sigatoka, Xanthomonas wilt, and Banana Bunchy Top Virus (BBTV)—posing serious threats to global food security and economic stability. Recent years have witnessed an influx of machine learning (ML) methodologies designed to detect these diseases through image analysis, remote sensing, and lightweight mobile tools. This comparative review explores models ranging from traditional classifiers and handcrafted feature-based ML to deep learning (CNNs, transfer learning, object detection, lightweight architectures), hybrid networks, and mobile solutions. The discussion contrasts model accuracy, computational complexity, dataset scale demands, deployment limitations, and practical suitability for agricultural environments. The review concludes by recommending context-specific approaches and identifying critical research gaps for future study.*

Keywords—*Machine learning, Artificial Intelligence, Banana Disease Detection.*

I. INTRODUCTION

Banana plants are afflicted by multiple serious diseases:

Panama disease (Fusarium wilt): Caused by Fusarium oxysporum f. sp. cubense, devastating banana production worldwide

Black Sigatoka: A leaf-spot disease caused by Mycosphaerella fijiensis, significantly reducing yields

Banana Xanthomonas Wilt (BXW): A bacterial pathogen causing severe production losses in East Africa

Banana Bunchy Top Virus (BBTV): A destructive viral infection transmitted by aphids, with no known resistant cultivars

Efficient and scalable detection methods are critical. Machine learning (ML), particularly image-based analytics, offers potent tools for identifying disease symptoms early. This paper surveys and compares different ML approaches applied to banana disease detection.

II. METHODOLOGICAL CATEGORIES

2.1 TRADITIONAL CLASSIFIERS WITH HANDCRAFTED FEATURES

ANN + SIFT / HOG + LBP: Argued for invariance to scale/rotation and lower data demands than CNNs PMC. [7]

SVM, KNN, MDC techniques combined with texture and color analysis have been applied, often with ROI segmentation, such as early scorch and leaf spots.[8]

ANFIS (Adaptive Neuro-Fuzzy Inference System) and GLCM + NGTDM + SVM achieved up to 100% detection and 90% accuracy in grading symptom severity.

2.2 CLASSICAL ML: SVM, KNN, RANDOM FOREST

KNN, SVM, AlexNet: KNN (~76%), SVM (~84%), and AlexNet (~96%) accuracies were reported using leaf image datasets.

Random Forest (RF) applied to aerial or satellite imagery achieved ~97% accuracy using vegetation indices and environmental variables.[9]

2.3 Convolutional Neural Networks (CNNs) & Transfer Learning

BananaSqueezeNet: Lightweight CNN with ~96.25% accuracy on diagnosing Sigatoka, Pestalotiopsis, and Cordana diseases using a limited dataset .

ResNet50, VGG19 as transfer learning backbones have shown strong performance in classification tasks.

Mobile-Based Deep Learning: In Tanzania, ResNet152 model achieved 99.2% accuracy and InceptionV3 achieved 95.41% for Fusarium wilt and Black Sigatoka; InceptionV3 was preferred for mobile deployment due to lower memory needs.

2.4 Object Detection Architectures

Faster R-CNN (ResNet50, InceptionV2) & SSD (MobileNetV1): Used for detecting diseased areas via bounding boxes; evaluated using mAP and confusion matrices

2.5 Lightweight Architectures & Attention Modules

MobileNetV2, MobileNetV3-small, ShuffleNetV2, SqueezeNet: Tested with and without CBAM attention module; CBAM-enhanced ShuffleNetV2 achieved ~99% accuracy and better generalization.

2.6 Hybrid and Sequential Networks

G-RecConNN (CNN + RNN): Designed for sequential image classification in plantain (banana) cultivation, combining spatial and temporal features.

III. Comparative Analysis

Model Type	Pros	Cons / Constraints	Performance (Reported)
Handcrafted feature + ML (SIFT, HOG)	Rotation/scale invariance; less data needed	Feature engineering; lower predictive ceilings	ANFIS: 100% detection; SVM: ~89–92%
RF on remote sensing	High accuracy across spatial scales; uses VI & weather data	May require high-quality remote sensing and weather inputs	~97% accuracy
Standard CNNs (AlexNet, VGG, ResNet)	High accuracy; strong baseline	High compute demand; less suited to real-time/mobile	AlexNet: ~96.7%; VGG/ResNet: strong in many tasks
Mobile CNNs (ResNet152, InceptionV3)	High accuracy; mobile deployable	ResNet152 heavy; InceptionV3 suitable due to lower memory	99.2% / 95.4%
BananaSqueezeNet (lightweight CNN)	Compact, efficient	Limited training data; overfitting risk	~96% accuracy
Object Detection (Faster R-CNN, SSD)	Localizes disease spots; structured detection	Requires bounding box labeling; moderate compute	mAP and confusion matrix metrics reported
Hybrid CNN + RNN (G-RecConNN)	Captures temporal dynamics	Requires temporal image sequences (e.g., time-series)	Designed for early detection in sequences

IV. Discussion

4.1 Trade-offs: Accuracy vs. Efficiency

Deep CNNs (e.g., ResNet, AlexNet) deliver high accuracy but demand significant computational resources. Lightweight models (BananaSqueezeNet, MobileNet, ShuffleNet) offer a practical balance for mobile or edge deployment. Integrating attention modules like CBAM improves discriminative power dramatically [13].

4.2 Data Requirements

Handcrafted-feature methods excel with limited datasets but underperform against deep learning methods on richer datasets [14]. Transfer learning helps mitigate data scarcity by leveraging pre-trained models

4.3 Application Contexts

Remote sensing-based RF models serve large-scale monitoring. Lightweight CNNs and mobile-friendly models support on-field diagnosis via smartphones.[15]

Object detection systems pinpoint precise regions of interest. Hybrid temporal models (CNN+RNN) can detect progressive disease patterns from image sequences.

4.4 Challenges & Gaps

Generalization: Models often struggle to discriminate between visually similar diseases (e.g., Sigatoka vs. Fusarium wilt)

Dataset Diversity: Many studies rely on limited, context-specific datasets.

Real-world Deployment: Field lighting, occlusion, and heterogeneity pose significant challenges.

Explain ability: Few studies address interpretable AI for disease diagnostics—a key for farmer trust and adoption.

V. CONCLUSION & RECOMMENDATIONS

Optimal Model Selection Depends on Context:

Resource-rich research contexts: Deep CNNs (ResNet, VGG) offer strong accuracy.

Mobile/edge deployment: Lightweight CNNs (MobileNetV2, ShuffleNetV2 with CBAM) balance speed, size, and accuracy.

Broad monitoring: Remote sensing with Random Forest is effective at larger scales.

Temporal patterns or progression studies: Hybrid CNN–RNN architectures like G-RecConNN offer advantage.

Structured disease localization: Object detection models (Faster R-CNN, SSD) serve well for detailed mapping.

VI. FUTURE DIRECTIONS

Develop larger, annotated, and publicly shared datasets covering multiple banana diseases.

Improve model generalization across varied environmental and imaging conditions.

Incorporate explainability tools to make predictions interpretable.

Explore lightweight attention-based CNNs optimized for mobile environments.

Combine multi-modal inputs (image, spectral, environmental metadata) to enhance robustness.

Pilot real-world implementations to validate laboratory model performance.

REFERENCES

[1] Bananas | FAO | Food and Agricultural Organization of the United Nations

[2] Rathi, S., Agrawal, A., & Tiwari, S. (2018). Early detection and prediction of Banana Fusarium wilt disease using image processing techniques. In 2018 IEEE International Conference on Communication and Signal Processing (ICCSP) (pp. 0063-0067). IEEE.

[3] Jadhav, P., et al. (2019). "IoT based disease prediction system for banana crops using machine learning algorithms." International Journal of Advanced Research in Computer Science, 10(2), 123-130.

[4] Sahu, P., Singh, A.P., Chug, A. and Singh, D., 2022. A systematic literature review of machine learning techniques deployed in agriculture: A case study of banana crop. IEEE Access, 10, pp.87333-87360.

[5] N. Gupta et al. (2020). "A comparative study of machine learning and deep learning techniques for disease prediction in banana crops."

[6] A. Singh et al. (2021). "Prediction of Banana bunchy top disease using artificial intelligence and image processing."

[7] K. Patel et al. (2022). "Predictive modeling for Black Sigatoka disease in banana using regression analysis."

[8] Jayanthi, C., Nagarajan, V., & Ranganayaki, V. (2014). Disease detection system for banana fruit based on color and texture features. International Journal of Computer Science and Mobile Computing, 3(4), 956-962.

[9] Li, C., Wang, X., Zhao, W., Meng, Z., & Jin, X. (2016). Hyperspectral imaging for the detection of banana diseases. Biosystems Engineering, 143, 28-37.

[10] Ramcharan, A., Baranowski, K., McCrite, S., Boot, W., Balasubramanian, V., Miki, K., Shi, Y., & Ehsani, R. (2017). Deep Plant Phenomics: A Deep Learning Platform for Complex Plant Phenotyping Tasks. Frontiers in Plant Science, 8, 1868.

[11] Sarkar, C., Gupta, D., Gupta, U. and Hazarika, B.B., 2023. Leaf disease detection using machine learning and deep learning: Review and challenges. Applied Soft Computing, p.110534.

[12] Ochoa, D., Cevallos, J., Vargas, G., Criollo, R., Romero, D., Castro, R. and Bayona, O., 2016, May. Hyperspectral imaging system for disease scanning on banana plants. In Sensing for Agriculture and Food Quality and Safety VIII (Vol. 9864, pp. 85-90). SPIE.

[13] Saputro, A.H. and Handayani, W., 2017, October. Wavelength selection in hyperspectral imaging for prediction banana fruit quality. In 2017 International Conference on Electrical Engineering and Informatics (ICELTICs) (pp. 226-230). IEEE.

[14] Iqbal, Z., Khan, M.A., Sharif, M., Shah, J.H., ur Rehman, M.H. and Javed, K., 2018. An automated detection and classification of citrus plant diseases using image processing techniques: A review. Computers and electronics in agriculture, 153, pp.12-32.

[15] Khan, M.A., Akram, T., Sharif, M., Awais, M., Javed, K., Ali, H. and Saba, T., 2018. CCDF: Automatic system for

segmentation and recognition of fruit crops diseases based on correlation coefficient and deep CNN features. Computers and electronics in agriculture, 155, pp.220-236.

[16] Selvaraj, M.G., Vergara, A., Ruiz, H., Safari, N., Elayabalan, S., Ocimati, W. and Blomme, G., 2019. AI-powered banana diseases and pest detection. Plant methods, 15, pp.1-11.

[17] Nikhitha, M., Sri, S.R. and Maheswari, B.U., 2019, June. Fruit recognition and grade of disease detection using inception v3 model. In 2019 3rd International conference on electronics, communication and aerospace technology (ICECA) (pp. 1040-1043). IEEE.

[18] Athiraja, A. and Vijayakumar, P., 2021. RETRACTED ARTICLE: Banana disease diagnosis using computer vision and machine learning methods. Journal of Ambient Intelligence and Humanized Computing, 12(6), pp.6537-6556.

[19] Selvaraj, M.G., Vergara, A., Montenegro, F., Ruiz, H.A., Safari, N., Raymaekers, D., Ocimati, W., Ntamwira, J., Tits, L., Omondi, A.B. and Blomme, G., 2020. Detection of banana plants and their major diseases through aerial images and machine learning methods: A case study in DR Congo and Republic of Benin. ISPRS Journal of Photogrammetry and Remote Sensing, 169, pp.110-124.

[20] Nagaraju, M. and Chawla, P., 2020. Systematic review of deep learning techniques in plant disease detection. International journal of system assurance engineering and management, 11(3), pp.547-560.

[21] Ouhami, M., Hafiane, A., Es-Saady, Y., El Hajji, M. and Canals, R., 2021. Computer vision, IoT and data fusion for crop disease detection using machine learning: A survey and ongoing research. Remote Sensing, 13(13), p.2486.

[22] Aeberli, A., Johansen, K., Robson, A., Lamb, D.W. and Phinn, S., 2021. Detection of banana plants using multi-temporal multispectral UAV imagery. Remote Sensing, 13(11), p.2123.

[23] Lin, H., Zhou, G., Chen, A., Li, J., Li, M., Zhang, W., Hu, Y. and Yu, W.T., 2021. EM-ERNet for image-based banana disease recognition. Journal of Food Measurement and Characterization, 15, pp.4696-4710.

[24] Wani, J.A., Sharma, S., Muzamil, M., Ahmed, S., Sharma, S. and Singh, S., 2022. Machine learning and deep learning based computational techniques in automatic agricultural diseases detection: Methodologies, applications, and challenges. Archives of Computational methods in Engineering, 29(1), pp.641-677.

[25] L. Li, S. Zhang and B. Wang, "Plant Disease Detection and Classification by Deep Learning—A Review," in IEEE Access, vol. 9, pp. 56683-56698, 2021, doi: 10.1109/ACCESS.2021.3069646.

[26] Sahu, P., Singh, A.P., Chug, A. and Singh, D., 2022. A systematic literature review of machine learning techniques deployed in agriculture: A case study of banana crop. IEEE Access, 10, pp.87333-87360.

[27] Thiagarajan, J.D., Kulkarni, S.V., Jadhav, S.A. et al. Analysis of banana plant health using machine learning techniques. Sci Rep 14, 15041 (2024). https://doi.org/10.1038/s41598-024-63930-

International Journal of Computer Research & Technology
ISSN 2454-7719
** A Blind Peer Reviewed Journal **
Volume-10, Issue-2, July-Dec 2025
Paper ID: CS-23

The Information Hiding Techniques.

Nikita Samadhan Chaudhari
Assistant Professor.
Department of computer Science, Arts Science And P.O. Nahata Commerce College,Bhusawal.

Abstract: *The rapid growth of the Internet and high-speed networks has enabled new possibilities across various domains but also increased risks to data security. Digital media, while offering benefits like high quality and easy editing, also makes unauthorized copying and sharing easier. This highlights the need for strong copyright protection and information security measures. Since the communication media lacks built-in data protection, securing information has become crucial. Techniques like encryption make data unreadable to unauthorized users. This paper explores existing data hiding methods and how combining they can enhance security. Data hiding involves concealing sensitive information within mediums like images, videos, or audio. Techniques such as cryptography, steganography, hashing, and authentication are employed to protect data from unauthorized access in today's digital age.*

Keywords- *Information hiding, Steganography, Cryptography, Watermarking*

I. INTRODUCTION

Information is essential in today's environment for image and signal processing, communication, and other purposes. In the present era, because computers and fast communication allow for the delivery of confidential information (messages or plain text) to unauthorized users, it must be protected from them. The security protocol is required by data. CDROMs and other digital media have the capacity to store large volumes of data. They are flammable and processing is easy.

As the Internet has grown and online services have improved, digital publishing has emerged as in cutting-edge age most of people use net in computer, mobile, tablets and so on. In their everyday use like as person do their paintings at any region and send to receiver via the use of internet. A While user sends their mystery statistics to different users by using verbal exchange community. In this statistics age there are such a lot of intruders are eagerly expecting snatching the name of the game data, so it's far our first purpose to shield our mystery records. This paper is dividing into 4 sections, First section is advent approximately information safety, 2d phase is the literature review wherein we are supplying take a look at of various research paper and 3rd phase is research methodology. In the final section, we present our proposed study, detailing its processes, conclusion, and reference. There are numerous methods for protecting sensitive data, including hashing, steganography, and cryptography. By using cryptography, users can render their original data unintelligible, making it impossible for hackers to access the original data.

As an important subject and offices (such publishers and institutions) in the next generation of companies appear to be paperless. These days, several researches are being conducted to implement and arrange concepts like online libraries, e-government, and e-commerce. There are numerous benefits to digital publication, but it faces several basic risks, like unauthorized use of copy-righted materials, data manipulation, and redistributing data. In this instance, a few protective measures including integrity, authenticity, and copyright protection and confidentiality are necessary to stop issues with plagiarism and forgeries. It is simple to download and alter a copy-righted text so that you can reuse it without restriction. These days, copyright management is therefore extremely important.

For every individual or business, data and information are vital. It bothers none of us when our conversations are overheard because they include the possibility of being applied improperly. The same is true for every individual or organization's data. To prevent manipulation, data exchanged between two

prospective parties needs to be done securely. Every information exchange involves two different kinds of dangers. An unauthorized user trying to listen in on this chat has two options: either modify the information to make it mean something different, or try to listen in with the goal of deciphering the message and using it to their benefit.

II. ESSENTIAL

Data concealment strategies are crucial because there is no guarantee regarding the information-transmission medium; in other words, the channel is not secure. Thus, certain techniques are required to make it harder for an unauthorized user to take information from the message. A few causes of data concealment include:

1. Private and personal information
2. Delicate information
3. Private information and trade secrets
4. Preventing data misuse
5. Inadvertent destruction, human mistake, and inadvertent data deletion;
6. Financial and blackmail objectives
7. To cover up signs of criminality
8. Finally, just for kicks

III. INFORMATION HIDING TECHNIQUES FEATURES

Every information hiding method must have these qualities:

1. Capacity: which is the quantity of data that can be concealed in a cover medium. The maxim that information concealed must not materially change the original message in order to divert the attention of an unauthorized user governs the amount of information that can be concealed.
2. Security: The information hiding technique should make sure that data is secure and that only the intended user may access it. Ensuring the secrecy and sensitivity of information being delivered is crucial.
3. Robustness: This describes the amount of data that may

IV. LITERATURE REVIEW

1. Qianmu Li,1 Hiuk Ja Shim,2 and Yanyan Huang3.(2018): The simplicity with which digital media can now be copied, shared, and transmitted over the Internet has been made possible by the widespread use of the web and other online services. Since text is one of the most extensively used digital media on the Internet and one of the primary data sources, the important content on websites, books, articles, daily papers, and other media is simply text. Because of this, copyright protection for plain texts is still a problem that needs to be resolved in order to establish ownership and ten years to guard against copyright violations and media forgeries, as well as to stop manipulation, distortion, and secure appropriate level of precision. Digital watermarking and steganography have been employed as alternatives during the past tampering. This study offers a comparative examination of information concealment strategies, with a particular emphasis on strategies that alter the content and structure of digital texts. In this article, the features of several text watermarking and text steganography techniques are discussed along with their uses. In order to illustrate the benefits and drawbacks of the methods now in use, a variety of attack types are also explained and their effects examined. Lastly, various recommendations and paths are made for additional development. Text watermarking architecture (2.1). Figure 2 illustrates the two primary stages of digital text watermarking: watermark extraction and embedding.

i. WATERMARK EMBEDDING:

Text watermarking algorithms have three stages is their embedding phase. Making a watermark string with the owner information is the first step name or additional details (such the publisher and author, for instance). The watermark string is transformed in the second phase. A hash function that modifies the binary string based on an optional key, after which an invisible watermark string is created to be inserted into specific spots inside the cover text. Lastly, it is placed in specific areas that will prevent attacks from affecting the watermark string.

ii. TEXT DOCUMENT ATTACKS:

Most people these days may quickly access a variety of digital text files, including books, articles, and online news. Owing to the free access nature of these text publications, unlawful actions include copying, Changes, deformities, and reallocations are occurring concurrently. Text watermarking can thus be utilized as a security tool to demonstrate text documents authenticity and correctness.

iii. WATERMARK EXTRACTION:

Watermarked text documents are typically disseminated through channels of communication like the internet, via social media or email on the Internet. Verifying that the text documents are real is obviously crucial. In this phase, two terms—extraction and detection—are used differently. Though writers have frequently treated the two as having similar purposes in some literature, we can tell them apart in this way: the watermark detection confirms the presence of the watermark string from the watermarked text, whereas the extraction finds

the watermark string from the watermarked document and validates its integrity

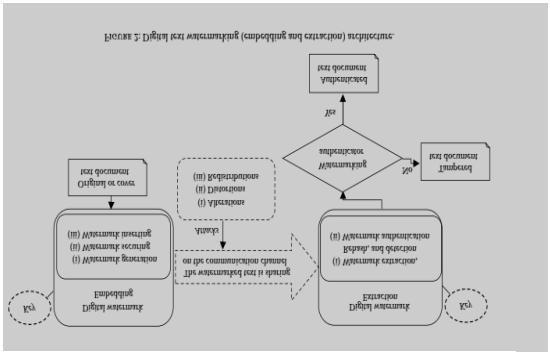


Figure: 2.1 Digital Text Watermarking (Embedding And Extraction) Architecture

2. Komal Patel, Sumit Utareja, Hitesh Gupta.(2013): The skill of identifying a message and stopping covert communication is known as steganography .This section examines the findings from additional sources to provide further viewpoints on the performance of the comparable algorithms:
3. M. Grace Vennice, Prof. TV Rao, M. Swapna, and Prof. J. Sasi Kiran(2012): Developed a hybrid technique that uses whitespace in the text right-justification occurs between words and paragraphs. In their paper, they suggest these four sections.
    1. Enrollment.
    2. Encrypt textual data.
    3. Navigating that XML structure.
    4. Decrypt the data into a different environment language.

The methods distinctive feature is its ability to dynamically construct a cover text by providing the user with six possibilities based on the length of the secret message

4. Mr. Vikas Tyagi (2012): proposed a new encryption algorithm and a method for data concealment that is based on the LSB (least significant bit). Their method encrypts data using a symmetric algorithm first, and then uses the LSB method to hide the encrypted data. He encrypted the data using a symmetric technique. For data encryption, he employed symmetric algorithms.
5. Harshitha K. M. and Dr. P. A. Vijaya(2012): Combining stegnography and cryptography is one way that suggest optimizing system security. Through the use of a steganographic system, the message is first encrypted in their techniques before being embedded in a cover file. The secret key is used to permute the secret message at random during encryption. Utilizing the matlab functions rand and randperm, the random permutation is executed. Both embedding and extraction were done using the LSB technique.
6. Rivest, Shamir, Adleman (RSA), Shailender Gupta, Ankur Goyal, and Bharat Bhushan(2012):The data was encrypted using the Diffie Hellman algorithm and then the encrypted message is hidden using LSB. Their findings indicate that if the Diffie Hellman algorithm is utilized in place of the RSA technique, the employment of encryption in steganalysis has no effect on the time complexity. Higher security is achieved by first encrypting the sensitive data using the RSA or Diffie Hellman algorithms, then converting the encrypted ASCII value to binary form. In addition, the image pixels are simultaneously transformed into binary form. The encrypted data is now embedded using the image as a cover. The least significant bit of pixel values is replaced with the encrypted information bits by the LSB encoder, which performs this procedure. The receiver initially translates the pixels in the Stego image into the appropriate binary values. Next, the encrypted data is separated from the image pixel values via the LSB decoder. Decryption algorithms are used to decrypt the encrypted data. They used MATLAB for all aspects of their work.
7. Asoke and Joyshree Nath(2011): Devised a novel technique for concealing any encrypted secret message behind a cover file. The authors changed the Play Fair approach to create a new platform that allows them to encrypt and decrypt any file. They employed a novel algorithm for encryption proposed by Nath et al. to encrypt secret messages.

    To generate the randomized key matrix needed to both encrypt and decrypt plain text files, they proposed a new randomization technique. They also unveiled a brand-new technique for repeatedly encrypting plain text. Their approach is entirely reliant on the user-supplied random text key. The text key's maximum length is 16 characters, and any character (ASCII code 0 to 255) may be used. They created a method that uses the provided text key to determine both the encryption and randomization numbers. They placed 8 bits of each character from the encrypted message file into 8 consecutive bytes of the cover file in order to conceal the secret message. To conceal data in the cover file, they developed passwords. Their novel technique might work well for concealing any kind of content—including audio, video, and image files—inside any kind of common cover file.

8. Dipti Kapoor Sarmah and Neha Bajpai(2010):A portion of the message is buried in the DCT of an image thanks to the employment of the advance encryption standard (AES).In their

work, they employed three modules: the Security Module for further security, the Crypto Module for steganography, and the Crypto Module for cryptography. In the crypto module, text is entered for encryption, the AES method is applied using a 128 bit key, and the result is a cipher text in hexadecimal format. Two more keys and the cipher text were generated by the Security Module. The first seven alphabets retrieved from the first step are separated, and the remaining alphabets are added at the end of the separated digits as in the first step. This process is repeated before the hiding process. Separate the alphabets and digits from the cipher text. The second key is produced as a result. Use a 64-bit key to scramble the seven alphabets from the Security Module. Next, take a Gray Scale Image and find the DCT of the Image. Next, hide the Cipher by modifying the DCTs. Finally, apply the Inverse DCT and find the Steno Image.

9. Anita Agarwal(2012): Encrypted a secret message using the S-DES algorithm, and she subsequently concealed the encrypted message using the alteration component method.
10. Phad Vitthal S., Bhosale Rajkumar S., and Panhalkar Archana R (2012): Advanced Encryption Standard (AES) algorithm is to encrypt secret message. The encrypted message is then hidden into true color RGB image using PVD with K-bit least-significant-bit (LSB) replacement.

V. RESEARCH METHODOLOGY

There are various techniques of information hiding so we can use the steganography, cryptography, watermarking.

1. STEGANOGRAPHY:-

A message, file, or image can be hidden or concealed within another message, file, or image using a technique called steganography. The Greeks are the source of the word "steganography." translates to "covered writing" or "concealed writing". Stated differently, it refers to the skill and discipline of conveying ideas through communication while concealing its own existence. To the extent that the adversary cannot even discern the existence of a second message, the messages must be concealed inside of innocuous ones [3]. Enhanced security and capacity are the primary concerns of steganography. A stego medium's meaning can be altered by even little modifications. Any covert media on the internet, such as photos, music, or videos, conceals sensitive data via steganography

There are four steps involve in steganography:-

a. Choosing the cover media to conceal the data in.
b. The information or secret message that the cover medium is supposed to hide.
c. A function that will be used to extract the hidden data from the cover media and conceal data in it.
d. An optional password or key to authenticate or to hide and reveal the data

The choice of cover should be made with great care. The secret message is substituted by redundant data in steganography, therefore the chosen cover should have enough redundant information to conceal the data.

a) Pure Steganography:

A sender and a recipient must have access to the embedding and extraction algorithms, but there is no need for the exchange of a cipher, such as a stego-key. The cover for this technique is chosen to reduce the modifications brought about by the embedding process. These solutions are not very safe because the security is predicated on the idea that this secret communication is unknown to any other party.

b) Hidden key steganography:

This technique embeds the hidden message into the cover using a key. Prior to transmission, the key is known only to the sender and the recipient. Furthermore, the key ought to be transferred via a secure channel.

c) Two keys are used in public key steganography:

The secret is embedded within the public key, which is kept in a public database. Only communication parties are aware of the key, which is needed to reconstruct the original message

2. CRYPTOGRAPHY:

The words "hidden or secret" and "writing" are represented by the terms "graphein" and "crypt." The word is Greek in origin.

The art of converting data into cipher text, an unintelligible format, is known as cryptography. The message is decrypted into plain text by the receiver on the other end. Data is given by cryptography. Non-repudiation, confidentiality, data integrity, and authentication. Maintaining confidentiality involves restricting access or imposing limitations on particular categories of data. Maintaining and guaranteeing the accuracy of the data being delivered—that is, ensuring that the information has not been altered, deleted, etc. is known as integrity. The process of authentication verifies the identity of both the sender and the recipient of the data. The capacity to guarantee that the sender or recipient cannot contest the veracity of their signature on the correspondence they authored.

Encryption is synonymous with modern cryptography. Here, the encrypted data is referred to

as cipher text, and the original data is called plain text.

There are three steps in cryptography.

1. **Encryption**: This method converts plain text into an unintelligible format. Cipher text is the result of this.
2. **Message transfer**: This entails emailing the receiver the text encrypted.
3. **Decryption**: To obtain the original plain text, the recipient on the other end decrypts the encryption text.

3. WATERMARKING

A watermark is a recognized pattern or image imprinted on paper that certifies the document's authenticity. When viewed in transmitted light, watermarks take on different tones of lightness or darkness. Banknotes, passports, postage stamps, and other security documents are frequently thought of as having watermarks as security measures. An application of this idea in the digital sphere is digital watermarking. We are now forced to use procedures that can preserve digital media ownership since there is so much data available online. Digital information, including text, video, audio, and image piracy, is rife. These are quite simple to create and distribute. Digital watermarking offers a solution to persistent issues with digital data copyright. A digital watermark is a type of identifier that is surreptitiously added to any digital material, including picture or audio files. To make claims on data, it might be subsequently extracted or discovered. This data may pertain to the image itself, the creator, or copyright .We can safeguard our digital ownership rights since the digital watermark is unaffected by transmission or transformation. Digital watermarks are invisible otherwise and only visible after using a certain algorithm. A digital watermark is useless if it causes the carrier signal to become perceptible.

The main objective of a watermarking system is resilience, which means that the watermark cannot be removed without altering the original data. One method of passive protection is digital watermarking. It doesn't alter the data in any way or restrict access to it; it only designates it. Source tracking is one use case for digital watermarking. At every stage of delivery, a watermark is incorporated into a digital signal. In the event that a duplicate of the piece is subsequently discovered, the watermark can be extracted from it, thereby identifying the source of the dissemination. It has been reported that this method has been used to identify the source of illegally stolen movies. Another use is for broadcast surveillance; watermarked footage from foreign agencies is frequently seen in television.

VI. CONCLUSION

We attempted to provide a review of the current methods for hiding data in this study. The purpose of data concealing. Data hiding is becoming more and more important these days. Furthermore, we have made an effort to outline the fundamental objectives of data concealing. In the current era of information, technologies have advanced to the point where the majority of users prefer to utilize the internet to send data across national borders. Therefore, when sensitive information is transferred between two people via digital communication, privacy is a fundamental need. In this essay, we examined the ways in which secure transactions on the Internet depend on data security. In this paper we were used the data hiding techniques like steganography, cryptography and watermarking in research methodology.

REFERENCES

[1] GeetikaDhand Lecturer (CSE), MSIT, GGSIPU, Geetika_dhand1@yahoo.com.

[2] MiladTalebyAhvanooey ,1Qianmu Li ,1 Hiuk Jae Shim,2 and Yanyan Huang3.

[3] Richa Gupta1, Sunny Gupta2, Anuradha Singhal3 13(Department of Computer Science, University of Delhi, India)2(University of Delhi, India).

[4] Komal Patel1, Sumit Utareja2, Hitesh Gupta3(1CSE Department, Patel Institute of Technology, Bhopal, Madhya Pradesh, India2Assistant Professor, 3 Head of Department, CSE Department, Patel Institute of Technology, Bhopal, Madhya Pradesh, India).

[5] M.GraceVennice, Prof.Tv.Rao, M.Swapna, Prof.J.Sasikiran, ‖Hiding the Text Information usingStegnography‖ , in InternationalJournal of Engineering Research and Applications (IJERA) Vol. 2, Issue 1, Jan-Feb 2012.

[6] Harshitha K M and Dr. P. A. Vijaya , ―secure data hiding algorithmusing encrypted secret message‖ in International Journal of Scientific and Research Publications, Volume 2, Issue 6, June 2012.

[7] Mr. VikasTyagi, ― Data Hiding in Image using least significant bit with cryptography‖, in International Journal of Advanced Researchin Computer Science and Software Engineering Volume 2, Issue 4,April 2012

[8] Shailender Gupta, AnkurGoyal , Bharat Bhushan, ― Information Hiding Using Least Significant Bit Steganography and Cryptography‖ , in I.J.Modern Education and Computer Science,june 2012.

[9] JoyshreeNath, AsokeNath,‖Advanced Steganography Algorithmusing Encrypted secret message‖, in (IJACSA) International Journalof Advanced Computer Science and Applications, Vol. 2, No.3,March 2011

[10] DiptiKapoorSarmah, NehaBajpai , ―Proposed System for data hiding using Cryptography and Steganography ― in international gournal of computer applications,2010.

[11] AnkitaAgaral , ―Security Enhancement Scheme for Image Steganography using S-DES Technique‖ in International Journal of Advanced Research in Computer Science and Software Engineering Volume 2, Issue 4, April 2012.

[12] PhadVitthal S., BhosaleRajkumar S., PanhalkarArchana R. , A Novel Security Scheme for Secret Data using Cryptography and Steganography‖ in I. J. Computer Network and Information Security, March 2012.

International Journal of Computer Research & Technology
IJCRT
ISSN 2454-7719
** A Blind Peer Reviewed Journal **
Volume-10, Issue-2, July-Dec 2025
Paper ID: CS-24

Recent Advances of Artificial Intelligence in healthcare

Nikita Rajendra Patil

Assistant professor
Department of Computer Science.
Bhusawal Arts ,Science and P.O.Nahata Commerce College,Bhusawal

Abstract: *Over the past ten years, artificial intelligence has had a notable comeback across a wide range of technology and subject areas. Machine learning systems in healthcare have never been more successful thanks to recent advances in digitization and a massive influx of biomedical data. This is seen as a potential game changer for "healthcare to all." An overview of several recent uses of artificial intelligence (AI) in the fields of diagnosis, clinical research, maternal care, Patient Care, and treatment is provided in this article. The paper will conclude by summarizing the obstacles AI currently confronts in the healthcare sector and discussing potential solutions to advance toward a more intelligent medical system. Artificial Intelligence (AI) is one of the most influential and disruptive fields of computer science. It has the potential to revolutionize medicine and healthcare delivery. In this review, we look at recent advances of the AI in healthcare and provide a roadmap to building robust, reliable and secure AI systems.*

Keywords- *Artificial Intelligence, Healthcare, Application of Artificial Intelligence, Advances of Artificial Intelligence*

I. INTRODUCTION

In recent years, the convergence of artificial intelligence (AI) and healthcare has ushered in a new era of innovation and transformation within the medical field. This dynamic synergy has been fuelled by exponential advancements in AI technologies, ranging from sophisticated machine learning algorithms to advanced natural language processing systems. Such progress has empowered healthcare practitioners and researchers with powerful tools to address longstanding challenges in medical diagnosis, treatment optimization, disease management, and patient care.

The application of AI in healthcare holds immense promise, offering solutions to complex problems that have traditionally posed significant obstacles to the delivery of high-quality, accessible healthcare services. From predictive analytics for early disease detection to personalized treatment recommendations based on individual patient characteristics, AI-driven approaches are reshaping the healthcare landscape in profound ways. Moreover, the widespread adoption of electronic health records (EHRs) and the proliferation of healthcare data have provided fertile ground for AI-driven insights and decision-making.

What is Artificial Intelligence?

Simply described, artificial intelligence (AI) is the science and engineering of creating intelligent machines using algorithms or a set of rules that the machine follows to replicate human cognitive capabilities like learning and problem solving. AI systems have the ability to predict problems or address them as they arise, allowing them to operate in a purposeful, intelligent, and adaptive manner. AI's power is in its capacity to learn and recognize patterns and relationships in vast multidimensional and multimodal datasets; for example, AI systems

could convert a patient's whole medical record into a single number representing a probable diagnosis. Furthermore, AI systems are dynamic and independent, learning and adapting as new data becomes available.

II. LITERATURE REVIEW

Mohammed Yousef Shaheen (2021): AI is increasingly being employed in healthcare as it becomes more ubiquitous in modern business and daily life. Artificial intelligence can assist healthcare workers with patient care and administrative responsibilities. While AI and healthcare advances are beneficial to the industry, their impact on tactics varies. Although AI can perform similar to or better than humans in certain activities, such as detecting illness, it is unlikely that AI will replace humans in all medical vocations.

P. Agrawal,(2018) : Several remedies discovered by the leading biopharmaceutical companies are available. Pfizer is utilizing IBM Watson, a machine learning-based system, to help it find immuno-oncology treatments

Preeti Kumari(2022):According to the author AI is a rapidly growing technology in healthcare, enhancing efficiency and effectiveness of operations and care services. Artificial intelligence helps improve patients' health and well-being. Understanding patients' wants and societal trends might help healthcare practitioners provide better care. It also helps collect client input to improve healthcare services. Artificial intelligence (AI) is now widely used across industries. The company has used automation to support human work and increase productivity.

Sharmila Nirojini P, Kanaga K, Devika S, Pradeep P (2024):This paper“ AI technology in healthcare” promises better patient outcomes, efficiency, and precision, ushering in a new era. Intelligent technologies will help healthcare practitioners improve their expertise and transform outdated practices. AI technologies have significant promise for the future of healthcare. They can personalize treatments, speed up processes, and anticipate medical emergencies.

Silvana Secinaro, Davide Calandra, Aurelio Secinaro, Vivek Muthurangu, Paolo Biancone (2021): Numerous AI applications for health care are revealed in the literature, along with an unresolved stream of research. For example, knowledge-based management and data-intensive analysis in AI initiatives demand expertise and an awareness of data quality. Researchers and medical professionals might better comprehend and tackle future AI research in the healthcare field with the aid of insights.

DonHee Lee, and Seong No Yoon (2021): In today's rapidly changing digital age, innovation is critical. Rapidly evolving technologies are the principal tools for implementing and integrating value-creating ideas.

AI and associated technologies are a must-have for firms seeking a competitive advantage. AI has the ability to change the healthcare business, making it particularly vulnerable to new applications. AI applications are transforming not only care delivery (diagnostic and treatment) but also patients' lifestyles, emphasizing the importance of a holistic approach to health.

Ahmed Lateef Alkhaqani (2024): Artificial intelligence's incorporation into healthcare is transforming the sector as it exists today. Artificial intelligence (AI) has the potential to save lives, boost productivity, save expenses, and enhance patient outcomes. AI is revolutionizing healthcare by transforming the way medical personnel approach patient care, from disease diagnosis to customized treatment strategies. AI in healthcare has many advantages, but there are also issues that need to be resolved, like moral dilemmas and the requirement for additional data privacy laws. In the upcoming years, we may anticipate seeing further developments in AI technology, which will make the healthcare sector more effective, efficient, and patient-centered.

Yan Yang, Shujuan Guan, Zihao Ou, Weiqi Li, Lizhi Yan, Bo Situ (2023): Because cytopathological testing represents the cellular pathology of cancer, it is essential for the diagnosis of cancer. However, cytopathologists' visual inspection is typically the basis for this procedure. The use of artificial intelligence (AI)-based models to recognize tumor cells in images has been made possible by recent developments in computer and digital imaging technology, helping cytopathologists perform better. AI-powered models have the potential to enhance the precision and consistency of image analysis while streamlining medical procedures.

III.RESEARCH METHODOLOGY

Medical Expert Systems:

Expert systems (ES) are the most prevalent kind of AI system used in regular healthcare settings. They are described as systems that can record facts, expert knowledge, and reasoning strategies to support caregivers in their daily tasks. Through the use of inference techniques, ES aims to replicate the knowledge of clinicians in order to aid in problem resolution and decision support. ES are capable of handling data and drawing logical judgments. Among its many utilities, ES is used for picture interpretation, diagnosis support, and alert creation.

Overview of AI Technologies

Artificial intelligence is not one ubiquitous, universal technology, but represents several fields

(e.g. Machine Learning and deep learning) that individually or together add intelligence to applications

Machine learning:

Machine learning (ML) refers to the study of algorithms that allow computer programs to automatically evolve through experience. Machine Learning can be categorized into "supervised", "unsupervised" and "reinforcement learning" (RL), and there is ongoing research on it. Several subfields including "semi-supervised","self supervised" and "multiple".

Tagged data, or annotated information, is used in supervised learning. For instance, tagged X-ray images of known tumours can be used to identify newtumours.
"Unsupervised learning" classifies patient groups with similar symptoms in an effort to find a common cause, or it might classify data without labels.

Natural language processing:

Natural Language Processing (NLP) has emerged as a powerful tool in the realm of healthcare, revolutionizing the way medical data is processed, analysed, and utilized. By enabling machines to understand and interpret human language, NLP facilitates the extraction of valuable insights from clinical notes, medical literature, electronic health records (EHRs), and other textual sources. This introductory section provides an overview of the applications of NLP in healthcare, highlighting its potential to improve clinical decision-making, enhance patient care, and drive medical research

Computer Vision:

Computer vision, a subset of artificial intelligence (AI), has emerged as a game-changing technology in healthcare, providing novel solutions for medical imaging interpretation, disease diagnosis, and treatment planning. Computer vision algorithms have transformed how healthcare personnel view, interpret, and act on medical pictures by allowing machines to interpret and analyze visual data, resulting in increased accuracy, efficiency, and patient outcomes. This introductory section presents an overview of the recent achievements in computer vision in healthcare, highlighting its potential to change diagnostic imaging, surgical treatments, and personalized medicine.

How can we create reliable and efficient AI-enhanced healthcare systems?

The usage and implementation of AI in clinical practice is still limited, even after over ten years of intense concentration, and many AI products for healthcare are still in the design and development stages.19–22 While there are various approaches to developing AI systems for the healthcare industry, too frequently attempts are made to fit square pegs into round holes by identifying healthcare issues and applying AI solutions without giving the local context (such as clinical workflows, user needs, trust, safety, and ethical implications.)

We believe that rather than taking the place of human intelligence, AI enhances and magnifies it. Therefore, it's crucial to concentrate on improving the efficacy and efficiency of human-machine interaction rather than attempting to replace it while developing AI systems for the healthcare industry. Furthermore, a thorough grasp of the complexities of patient journeys and care pathways from a human-centered perspective will be the foundation for AI advancements in healthcare.

We present a problem-driven, human-centered method in Fig. 1 which we modified from frameworks by Sendak, Care, and Wiens et al. to create dependable and efficient AI-augmented healthcare systems.

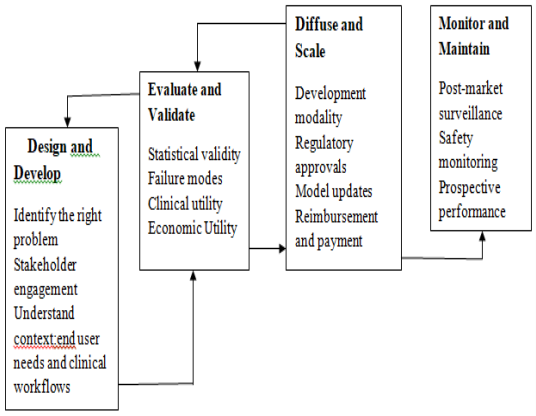


Figure 1: Human-Centered Method

Design and Develop

Using a human-centered AI and experimental method, the first step involves designing and developing AI solutions for the applicable challenges while including the relevant stakeholders, most notably the healthcare consumers themselves.

Participation of stakeholders and co-creation Create a multidisciplinary team with experts in (doctor, patient, caregiver), and subject matter experts (biomedical scientists, for example). This team

should also include advocates, conveners, financiers, financiers, motivators, and implementers.26 A multi-stakeholder team provides the operational, strategic, and technological know-how to define issues, objectives, success measures, and interim benchmarks.

AI with a focus on humans AI combined with an ethnographic knowledge of health systems is known as a human-centered AI strategy. Determine the primary issues through user-designed research (we recommend employing a qualitative study design to ascertain "what is the problem," "why is it a problem," "to whom does it matter," "why has it not been addressed before," and "why is it not getting attention"). These issues include the requirements, limitations, and workflows in healthcare organizations, as well as the facilitators and barriers to the integration of AI within the clinical context. Following the definition of the main issues, the next stage is to determine which issues AI can answer and whether relevant datasets are available for AI development and evaluation. AI systems would function by contextualizing algorithms within an already-existing workflow.

Evaluate and validate

In order to assess how well the AI tool is working, we must next iteratively review and confirm the predictions it produced. Economic utility, clinical usefulness, and statistical validity are the three criteria used for evaluation, and this is crucial.

- Statistical validity understands the performance of AI on metrics of accuracy, reliability, robustness, stability and calibration. High model performance on retrospective, in silico settings is not sufficient to demonstrate clinical utility or impact.
- Access the algorithm's therapeutic usefulness in a real-time setting using a hold-out and temporal validation set such as longitudinal and external geographic datasets to show its generalizability and clinical efficiency.
- The net benefits of the AI system investment in relation to its cost are measured by economic utility.

Diffuse and Scale

Numerous AI systems are first created to address a particular healthcare system's problem, taking into account the unique patient population that exists there. When scaling up AI systems, particular consideration needs to be given to the reimbursement environment, regulatory framework, model upgrades, deployment procedures, and system variations.

Monitor and Maintain

An AI system needs to be continuously maintained and monitored, even after it has been used in a clinical setting, in order to use efficient post-market surveillance to keep an eye out for dangers and unfavourable outcomes. Collecting and analyzing pertinent datasets for AI performance, clinical and safety-related concerns, and adverse events is a collaborative effort between healthcare organizations, regulatory agencies, and AI developers. This study explores AI applications in healthcare, from patient registration to billing and record processing (see fig.2)

IV. AI APPLICATIONS IN HEALTHCARE

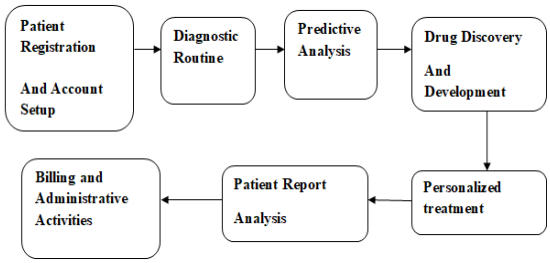


Figure 2: AI Applications in Healthcare

Artificial intelligence (AI) has transformed healthcare by improving patient identification, management, and treatment. AI has enhanced precision, efficiency, and personalized care using advanced algorithms, machine learning, and data analytics. AI has various and ground-breaking uses in healthcare, including accurate medical image processing and disease prediction. This article provides an overview of how AI is impacting healthcare through initiatives such as disease prediction, medication discovery, personalized therapy, and office administration. AI can enhance diagnostic accuracy, optimize treatment programs, and reduce administrative expenses, thereby transforming the healthcare business. AI is expected to shorten the software development life cycle.

Patient Registration: AI-powered chat bots can assist patients during the registration process. AI systems can acquire patient data in a conversational and engaging manner, like as contact information, medical history, insurance details, and other appointment-related information. AI-powered systems can improve productivity before patient visits by forecasting wait times, issuing personalized reminders, and improving workflow.

Medical Image Analysis: In order to help in early disease identification and accurate diagnosis, AI systems have demonstrated exceptional proficiency in the analysis of medical imagery, pattern recognition, and symptom mapping. Interpreting

MRIs, CT scans, and X-rays has proven to be successful with the use of convolution neural networks (CNNs) and other techniques. Based on a patient's medical history, AI can forecast a person's risk and susceptibility to various diseases. This can support healthcare providers in taking the initiative to choose early intervention and preventative care.

Disease Prediction and Diagnosis: AI models can precisely identify problems and forecast the chance of developing diseases since they have been trained on patient data. When traditional methods may not be sufficient, AI's ability to analyze sparse data can be useful. AI recognizes relationships that humans might miss. Predictive models that utilize patient history can facilitate early interventions and tailored treatment strategies. AI can assist in finding the biomarkers that are associated with the course of an illness, how well a patient responds to treatment, or any side effects. Patient stratification and tailored treatment benefit from these markers.

Drug Discovery and Development: AI can be used for reorganization the target discovery, clinical trial, and other phases of drug development by utilizing machine learning, data analysis, and predictive modeling. AI expedites drug research by anticipating molecular interactions, identifying potential therapeutic candidates, and improving drug design. AI may analyze patient data from real-world situations to determine how medications work in a range of populations outside of strictly regulated clinical settings. This knowledge can be very helpful in making judgments about treatment plans and regulations. This expedites the often protracted medication development process.

Personalized Treatment: By considering a patient's genetic composition, medical background, and response to treatment, AI enables the customization of medical remedies for individual patients. Evidence-based recommendations can be provided by AI-powered systems. As a result, the treatment is more effective and has fewer adverse effects. AI tools can assist medical practitioners in making educated decisions and differentiating diagnosis. AI can improve human expertise and expedite decision-making in conjunction with biologists, chemists, and medical specialists.

Patient Report Analysis: A patient's symptoms can be assessed to determine the appropriate healthcare practitioner or degree of therapy by using AI-powered triage systems. AI systems can provide relevant information resources for patients to educate themselves about their ailments and possible therapies by using data points in their medical history. This ensures that when patients need care, they get it quickly. Artificial intelligence (AI) has the ability to combine data from multiple sources (such as test results, medical imaging, and electronic medical records) to present a complete picture of the patient's health.

Billing and administration activities: AI-powered solutions make administrative tasks easier, such as scheduling appointments, transcribe medical information, and bill. AI can enhance healthcare facilities' administrative operations by identifying inefficiencies, bottlenecks, and possible improvement areas. This allows medical staff to focus more on patient care, which helps medical facilities serve patients more successfully. Healthcare personnel' administrative workload is reduced by AI's capacity to take over repetitive and routine duties and continuously learn from and train on new data. Over time, AI improves diagnostic accuracy by adapting to new medical knowledge. Thus, AI-assisted healthcare systems can restructure healthcare procedures, enhance patient outcomes, and raise the standard of care.

V. ADVANCES OF ARTIFICIAL INTELLIGENCE

Some of the medical artificial intelligence applications used in the healthcare sector are as follows:

1. AI in clinical research:

In a clinical study, individuals get newly made medications to evaluate their efficacy. It has cost a lot of money and time to complete this. But the success rate is really low. Clinical trial automation has therefore shown to be advantageous for AI and the healthcare industry. Furthermore, AI and healthcare contribute to the removal of time-consuming data monitoring methods. AI-assisted clinical trials can manage vast volumes of data and provide highly reliable results.

2. Patient Care:

Artificial intelligence in healthcare affects patient outcomes. Medical AI companies create a system that supports the patient at all levels. Clinical intelligence analyzes patients' medical information and provides insights to improve the patient's quality of life (QOL).

3. Maternal Care:

One method for identifying high-risk mothers and minimizing maternal mortality and postpartum complications is as follows:
a) Using electronic health data and AI, predict if expectant mothers are at high risk of delivery complications.
2) Using digital technology to promote patient access to regular and high-acuity care during

pregnancy.
High-risk obstetric women who deliver in low-acuity clinics are more likely to encounter substantial maternal morbidity compared to those who deliver in higher-acuity clinics with more resources and experience.

4. Healthcare Robotics:

Certain medical robots help patients in addition to medical professionals. For instance, exoskeleton robots can help paralyzed individuals walk once more and regain their independence. Another example of technology in use is a smart prosthesis. With the option to wrap them with bionic skin and connect them to the user's muscles, these bionic limbs attach sensors that make them more accurate and responsive than natural body parts. Robots can assist in surgery and rehabilitation. For example, Cyberdyne's Hybrid Assistive Limb (HAL) exoskeleton uses sensors applied to the skin to efficiently detect electrical signals in the patient's body and respond with appropriate actions to help patients recover from conditions that lead to lower limb disorders, such as spinal cord injuries and strokes.

5. Genetics AI Data-Driven Medicine

Today's healthcare consumer has become more involved in their own medical treatment, from genome sequencing to using data from our fitness and activity monitors to create a personalized health status. A more accurate picture of our health or medical status is being created by compiling and connecting all of this massive data. In addition to increasing the accuracy and speed of genetic illness detection, data-driven medicine may pave the way for customized medical interventions.

6. AI-powered Stethoscope:

One important benefit is that the readings may be obtained even in noisy situations, which makes diagnosis more accurate than with standard stethoscopes. The digital instrument does not require any training to use, therefore anyone can obtain the records and telemeter them to the doctor. Additionally, this reduces their risk of catching COVID-19 and facilitates the delivery of better healthcare to patients who are chronically ill and in remote locations.

With the use of artificial intelligence (AI) and machine learning, computers are now able to analyze vast volumes of clinical data to identify patterns and anomalies in illness. The same concept applies here since blood flowing through normal arteries differs from blood flowing around a blood clot in blood vessels.

7. AI in peripheral Blood and Bone Marrow Cytopathology:

The diagnosis and assessment of hematological disorders is mostly dependent on peripheral blood and bone marrow cytopathology.One of the most used diagnostic techniques in clinical practice is the classification and counting of peripheral blood and bone marrow cells, which can be used to evaluate patients' hematological function and spot possible blood abnormalities. Additionally, bone marrow Cytopathology can be utilized to evaluate the course of a disease and the effectiveness of a treatment. Recent years have seen an increase in interest in the study of Cytopathology in bone marrow and peripheral blood. As technology has advanced, new tools such as automation and digital technology are frequently utilized in the examination and diagnosis of bone marrow and peripheral blood cells. In order to more precisely determine cell counts and morphological characteristics, bone marrow samples can also be digitally scanned and analyzed using digital imaging techniques.

Increased precision, effectiveness, and dependability in peripheral blood and bone marrow Cytopathology are anticipated with these novel methods.

A DL framework that can be customized for any diagnostic process was developed by Sidhom et al. in 2021 to aid in the detection of acute promyelocytic leukemia (APL), a subtype of acute myelogenous leukemia (AML). According to FISH, they enrolled 34 APL patients and 72 AML patients. Television was used to process peripheral blood obtained from enrolled patients for pre-classification, staining, smearing, and cell image collection.

8. AI in Cervical Secretion Cytopathology:

The Pap smear, or cervical secretory cytopathology, is a crucial screening method for identifying precancerous lesions and cervical cancer.Liquid-based cytopathology (LBC) has become a viable alternative technique for cervical secretory cytopathology in recent times. Compared to the traditional Pap smear, LBC has a number of benefits, such as higher sensitivetee, lower false-negative rates, and better repeatability. However, the absence of skilled and experienced cytologists or cell technologists, in addition to variables like diagnostic experience, mood, and exhaustion, make correct diagnosis of lung cancer cells (LBC) difficult. Thus, it makes sense to set up an AI system that can help clinical cytopathologists increase the reproducibility and efficiency of their work.

VI. CONCLUSION

AI technology in healthcare promises better patient outcomes, efficiency, and precision, ushering in a new era. Intelligent technologies will help healthcare practitioners improve their expertise and transform

Outdated practices. AI technologies have significant promise for the future of healthcare. They can personalize treatments, speed up processes, and anticipate medical emergencies. The recent advancements in AI have ushered in a new era of possibilities for healthcare. From enhancing diagnostic accuracy and treatment effectiveness to improving patient engagement and revolutionizing drug discovery, AI is reshaping the landscape of healthcare delivery. However, as we embrace these transformative technologies, it's imperative to address ethical, regulatory, and educational challenges to ensure equitable access, patient privacy, and responsible integration into clinical practice. By fostering interdisciplinary collaboration and continued innovation, we can harness the full potential of AI to improve patient outcomes and shape the future of healthcare."

AI is making healthcare smarter. It's helping doctors find problems faster, treat people better, and even prevent sickness. But we must be fair, keep people's information safe, and teach doctors how to use AI well. Together, we can use AI to make healthcare awesome for everyone.AI is changing healthcare for the better. It helps doctors diagnose illnesses more accurately, find better treatments, and even predict health issues before they happen. But we need to make sure AI is used fairly, keeps patient information safe, and doctors know how to use it properly. By working together and being careful, we can use AI to make healthcare better for everyone.AI is making healthcare better. It helps doctors find and treat problems faster. But we need to be careful with how we use it and make sure everyone can benefit from it. With teamwork, AI can make healthcare great for everyone.

REFERENCES

[1] Adam Bohr and KavehMemarzadeh: The rise of artificial intelligence in healthcare applications

[2] Mohammed YousefShaheen: Applications of Artificial Intelligence (AI) in healthcare: A review

[3] Yan Yang, Shujuan Guan, Zihao Ou,Weiqi Li, Lizhi Yan, Bo Situ: Advances in AI-based cancer cytopathology. Department of Laboratory Medicine, Nanfang Hospital, Southern Medical University, Guangzhou, China ,School of Engineering and Materials Science, Queen Mary, University of London, London, UK Correspondence Bo Situ and Lizhi Yan. Email: bositu@smu.edu.cn and 1012670125@qq.com

[4] Ahmed Lateef Alkhaqani: How artificial intelligence is revolutionizing the future of healthcare * M.Sc., Ministry of Health, Al Email: alkhaqani50@gmail.com https://orcid.org/0000-0002-7694-7503

[5] Junaid Bajwa chief medical Scientist,Usman Munir research program manager ,Aaditya Nori head of health intelligence,Bryan Williams chair of medicine: Artificial intelligence in healthcare: transforming the practice of medicine.

[6] Alexandre Blanco-González , Alfonso Cabezón , Alejandro Seco-González , Daniel Conde-Torres , Paula Antelo-Riveiro , Ángel Piñeiro and Rebeca Garcia-Fandino : The Role of AI in Drug Discovery: Challenges, Opportunities, and Strategies

[7] DonHee Lee and Seong No Yoon 1.College of Business Administration, Inha University, Incheon 22212, Korea; dhlee04@inha.ac.kr 2. Department of Business Edward Waters College, Jacksonville, FL 32209, USA Correspondence: Seong.yoon@ewc.edu: Application of Artificial Intelligence-Based Technologies in the Healthcare Industry: Opportunities and Challenges

[8] Ameya Shastri Pothukuchi, Vinay Mallikarjunaradhya,Senior Product Manager, Microsoft, Redmond, USA. 2Principal Product Manager, Thomson Reuters, Toronto, Canada. DOI : https://www.doi.org/10.56726/IRJMETS44366: COMPREHENSIVE ANALYSIS OF APPLICATIONS, CHALLENGES AND FUTURE PROSPECTS OF AI IN HEALTHCARE

[9] Preeti Kumari .Computer Science & Engineering, Dronacharya College Of Engineering, Gurugram, India: THE IMPORTANCE OF APPLICATION OF ARTIFICIAL INTELLIGENCE (AI) IN THE HEALTHCARE INDUSTRY

[10] Maksut Senbekov, Timur Saliev,Zhanar Bukeyeva, Aigul Almabayeva,Marina Zhanaliyeva,Nazym Aitenova,Yerzhan Toishibekov,and Ildar Fakhradiyev : The Recent Progress and Applications of Digital Technologies in Healthcare: A Review

International Journal of Computer Research & Technology
ISSN 2454-7719
** A Blind Peer Reviewed Journal **
Volume-10, Issue-2, July-Dec 2025

Paper ID: CS-25

Android Malware Detection Approaches Based on Machine Learning

Kamini Devanand Shinde
Assistant Professor.
Department of computer Science, Bhusawal Arts Science And P.O. Nahata Commerce College, Bhusawal.

Abstract: *Android smartphones attract many users due to their open source code and superior performance. However, the convenience of the Android platform also encourages the development of malware. Traditional method those that detect signature based malware cannot detect unknown applications. This article suggests machines. A lightweight learning-based system that can identify malware on Android devices.*

In this system, Features based on static and dynamic analysis, followed by a new feature selection approach based on principles. This article describes component analysis (PCA) and feature size reduction remedies. After that The model is built using support vector machine (SVM) for classification. The experimental results show that our system provides an effective way to detect Android malware.

Overview Android apps are rapidly growing in the mobile ecosystem, but Android malware is born in an endless flow. Many researchers have studied the issue of Android malware. We will detect this and propose theories and methods from various angles. According to existing research Machine learning is an effective and promising way to detect Android malware. Nevertheless, there are reviews that discuss various issues regarding Android malware detection based on computer data.

We believe that our study complements previous reviews by exploring a broader range of aspects, Subject. This article provides a comprehensive overview of Android malware detection approaches based on:

Machine learning. A quick introduction to the details of Android apps, including Android System architecture, security mechanisms, and classification of Android malware. Then i get in the car we focus on learning and analyze and summarize the learning situation from important perspectives such as sampling. Data collection, data pre-processing, feature selection, machine learning models, algorithms and evaluation Detection efficiency. Finally, we evaluate prospects for future research on Android malware detection. Based on machine learning. This review will help scientists get a complete picture of his Android malware detection. Based on machine learning. This could serve as a basis for subsequent researchers to conduct further studies. It will help guide research in this area more broadly.

Keywords— *Android Malware; Malware Detection; Machine Learning; Static Analysis; Dynamitic Analysis*

I. INTRODUCTION

Information is essential in today's environment for as the original part of our research, we conducted an extensive study where we dissect the current trends and approaches on detecting the malwares on Android Systems using Machine Learning ways. The overall thing of this study is to identify the exploration so far on Android Malware findings using Machine Leaning ways. Android has been more and more necessary with its open source character and advantages of free in our daily life. Still, the number of malicious software is also growing fleetly. Thus, how to describe the Android malware with the high accurate rate is a hot issue.

Since the 1960s, wireless communication has been one of the most vibrant communication domains with its on-going research until today, mainly to cellular computing evolution as a technology that enabled information and voice and video transmission through wireless-enabled gadgets. Within the past 15 years, mobile communication gadgets have become one of the

essential devices of the twenty first century. They have exponentially accelerated and developed sophisticated capabilities at lower-price models, strong working systems, compatibility and recognition with surroundings, and value of packages that interconnect with nearly each component of cutting edge existence in each area of it.

To insure the security of the Android ecosystem, a variety of results have been proposed, including operation reinforcement, vulnerability discovery, inventor reviews, and malware discovery. Among the colorful security options, Android malware discovery is an extensively used security protection system that can help malware from being released into the Android operation business or being installed and used. Grounded on former exploration, Android malware discovery technology can be divided into three orders static discovery, dynamic discovery, and mongrel discovery stationary discovery is grounded on the analysis of suspect law without running the Android operation. It can achieve high law content but faces numerous countermeasures similar as law obfuscation and dynamic law loading. Again, dynamic discovery involves the analysis of the Android operation by running the law.

Inspired by previous findings, we suggest an Android platform detection system built around the SVM machine learning classifier. Our approach considers the feature extraction and selection stages, using static and dynamic analysis to extract the characteristics of the Android application before adding a new feature. The PCA-RELIEF selection approach is suggested to identify the highest discriminating feature subset. Test results demonstrate that our approach is capable of correctly detecting Android malware.

In this technological period, smart phone operation and its associated operations are fleetingly adding due to the convenience and effectiveness in colorful operations and the growing enhancement in the tackle and software on smart bias. Its prognosticated that there will be 4.3 billion smart phone druggies by 2023(1). Android is the most extensively used mobile operating system (zilches). As of May 2021, its request share was 72.2. The alternate loftiest request share of 26.99 is possessed by Apple iOS, while the rest of the 0.81 is participated among Samsung, KaiOS, and other small merchandisers (2). Google Play is the sanctioned app store for Android- grounded bias. The number of apps published on it was over 2.9 million as of May 2021. Of these, further than 2.5 million apps are classified as regular apps, while 0.4 million apps are classified as low-quality apps by App Brain. Android's worldwide fashion ability makes it a more seductive target for cybercriminals and is more at threat from malware and contagions. Studies have proposed colorful styles of detecting these attacks, and ML is one of the most prominent ways among them. This is because ML methods are suitable to decide a classifier from a (limited) set of training exemplifications.

The use of exemplifications therefore avoids the need to explicitly define autographs in developing malware sensors. Defining autographs requires moxie and tedious mortal involvement and for some attack scripts unequivocal rules (autographs) don't live, but exemplifications can be attained fluently.

With this analysis we can formulate a defense medium specifically to offset the Update attack, the most delicate intrusion fashion to describe and exclude.

II. UPDATE ATTACK

Android Update Attack refers to the installation of a seemingly harmless application that downloads malicious content or third-party malicious apps during the update process. This type of attack is challenging to identify as the initial application appears benign. Detection requires monitoring previous versions and post-update behaviour. This article provides insights on combating update attacks through a review of current trends in malware detection. According to recent attacks and data analysis, (Rabindranath et al. (2014) Rabindranath, Rajamani, Babu and Datta) provides a list of malware types:

1. **Data Extraction:** Infecting tool to steal IMEI number and user data.
2. **Automatic calls and messages:** Increase users' phone bills by sending calls and texts to premium numbers.
3. **Root Exploits:** Gaining root privileges to manage and modify files.
4. **Search engine optimization:** manually search for a keyword and simulate clicks on the target website to increase search engine revenue or website traffic.
5. **Dynamically downloaded code:** Benign files download malicious code for distribution to mobile devices.
6. **Covert channels:** Use vulnerabilities in equipment to leak information from the system
7. **Botnet:** Created a network controlled by the Bot-Master for activities such as sending viruses, spam and DDoS attacks.

III. ANDROID MALWARE DETECTION APPROACHES BASED ON MACHINE LEARNING

Machine learning is an arm of machine intelligence research and application, and various

scientists have supported definitions of machine intelligence. Machine learning resides in a range of methods for automating the making of prognoses established by past observations. Based on an analogy between machine intelligence algorithms and the tasks acted apiece human brain, machine intelligence maybe about divided into five examples accompanying various hypothetical ideas: symbolists, connectionists, evolutionaries, Bayesians, and analogizers.

Each type of machine intelligence has allure own research districts and correspond-insult algorithms, in accordance with their specific fundamental ideas. Another representative and widely used categorization of machine intelligence approaches is established the learning procedure, that is usually detached into supervised knowledge, alone knowledge, tractor trailer-supervised education, and support knowledge. Supervised knowledge makes use of a branded dataset of samples or instances to train the predicting model, that is often used to answer categorization or reversion questions. When the prediction of the crop is an unending changing, it is a reversion problem, and when the forecast is individual, it is a categorization question.

Unsupervised learning does not demand particularly described datasets to train the prediction model. The purpose concerning this somewhat machine intelligence search out discover the within construction or allocation traits of the datasets themselves, and it is often used to questions to a degree dossier clustering and feature measure decline. Semidirected learning integrates details of excellent-possession learning and alone education, utilizing two together labeled and unlabelled dossier. The theme of almost-directed learn-insult search out allows a trainee to label the unlabelled sample data by utilizing a model of the dossier dispersion. This type of machine learning is generally secondhand in sketches place there is only a tiny amount of marked dossier in the dataset. In support learning, skilled is no branded dossier as indirect learning. Reinforcement knowledge reward as a phase of prediction and judgment, place the recommendation dossier is transferred straightforwardly into the model, superior to the vital adaptation of the model parameters. The education model and preparation dossier are implicit by receiving response from the surroundings to refurbish the model parameters. common requests concerning this type of machine intelligence involve dynamic plans and machine control.

A usual project that uses machine intelligence methods to answer authentic-experience questions consists of the following main processes.

1. Abstract the question expected resolved: Establish whether it is a categorization question, are version question, a clustering question, or extraordinary.
2. Sample dossier purchase and analysis: The seized dossier must be representative of the question domain. It endures being of enough book and not being excessively distorted.
3. Data preprocessing: In view of the disadvantages and potential wrongs within sample dossier, the addition is fulfilled through preprocessing. This involves data cleansing, normalization, discretization, factorization, absent advantage handle, dataset segmentation, and added orders.
4. Feature draft:This involves selecting ultimate significant lineaments and discarding meaningless physiognomy using appropriate methods of feature genuineness study, such as core connection reasoning, the u.s. city-square test, average common information, conditional deterioration, and posterior feasibility.
5. Model collection and training: Select the model accord-insult to the dossier and the questionexpected solved and use the preparation dossier to get the model limits.
6. Model evaluation and growth: Use test dossier to judge the model in agreements of accuracy, preparation speed, state room complicatedness, reliability, ability to move, and inference, and advance the model accompanying the appropriate methods.
7. Use the new dataset to form guesss and resolve useful problems.
8. Evaluation of the machine intelligence arrangement to determine allure performance (such as, veracity, p)

IV. Related Work

Malware Attacks on Android

Malware attacks represent a prevalent threat to Android devices. Various researchers have provided differing definitions of malware, primarily based on the extent of harm it inflicts. Fundamentally, malware refers to any malicious application containing harmful code, designed with the intent to gain unauthorized access and engage in activities that are neither legal nor ethical, thereby infringing upon the core principles of security: confidentiality, integrity, and availability.

Malware associated with smart devices can be analyzed from three perspectives: attack goals and behavior, distribution and infection pathways, and methods of privilege acquisition. The attack goals and behavior may include fraud, spam emails, data

theft, and resource misuse. Distribution and infection pathways encompass software markets, browsers, networks, and devices.

Methods of privilege acquisition can involve technical exploitation and user manipulation techniques, such as social engineering. Specifically, malware targeting the Android operating system is referred to as Android malware, which can cause harm or compromise data on Android-based mobile devices. This category includes Trojans, spyware, adware, ransom ware, worms, botnets, and backdoors.
Google characterizes malware as potentially harmful applications, further categorizing it into commercial and non-commercial spyware, backdoors, privilege escalation, phishing, various types of fraud (including click fraud, toll fraud, and SMS fraud), and Trojans. Additionally, the phenomenon of app collusion warrants attention in the context of malware. App collusion occurs when two or more applications collaborate to achieve a malicious objective.
If these applications operate independently, the likelihood of malicious activity diminishes. Therefore, it is essential to identify malicious inter-app communication and scrutinize app permissions to effectively detect instances of app collusion.

MACHINE LEARNING PROCESS

ML is a branch of artificial intelligence that focuses on developing applications by learning from data without explicitly programming how the learned tasks are performed.

The traditional ML methods make predictions based on past data. ML process lifecycle consists of multiple sequential steps. They are data extraction, data preprocessing, feature selection, model training, model evaluation, and model deployment. Supervised learning, unsupervised learning, semi supervised learning, reinforcement learning, and deep learning are the different subcategories of ML. The supervised learning approach uses a labelled dataset to train the model to solve classification and regression problems depend on the output variable type (continuous or discreet). Unsupervised learning is used to identify the internal structures (clusters), the characteristics of a dataset, and a labelled dataset is not required to train the model.

A mix of both supervised and unsupervised learning techniques are applied in semi supervised learning and used in a case of limited labelled data in the used dataset. The learning model and the data used for training are inferred.

The model parameters are updated with the received feedback from the environment in reinforcement learning where no training data is involved. This ML method proceeds as prediction and evaluation cycles. DL is defined as learning and improving by analysing algorithms on their own. It works with models such as artificial neural networks (ANN) and consists of a higher or deeper number of processing layers.

Malware detection in Android can be performed in two ways; signature-based detection methods and behaviour-based detection methods. The signature-based detection method is simple, efficient, and produces low false positives.
The binary code of the application is compared with the signatures using a known malware database. However, there is no possibility to detect unknown malware using this method. Therefore, the behaviour-based/anomaly-based detection method is the most commonly used way.

This method usually borrows techniques from machine learning and data science. Many research studies have been conducted to detect Android malware using traditional ML-based methods such as Decision Trees (DT) and Support Vector Machines (SVM) and novel DL-based models such as Deep Convolutional Neural Network (Deep-CNN) and Generative adversarial networks. These studies have shown that ML can be effectively utilised for malware detection in Android.

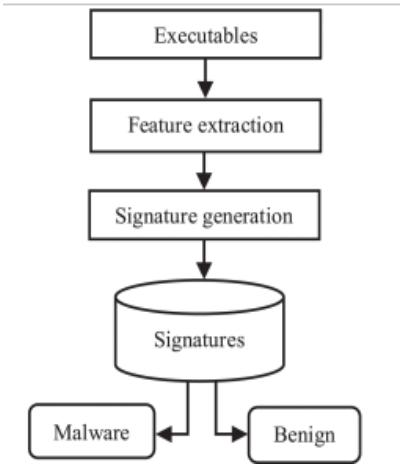
V. MALWARE DETECTION TECHNIQUES

A. Signature-Based Malware Detection

Signature is a malware feature which encapsulates the program structure and identifies each malware uniquely. Signature- based detection approach is widely used within commercial antivirus. This approach is fast and efficient to detect known malware, but insufficient to detect unknown malware. In addition, malware belonging to the same family can easily escape the signature-based detection by using obfuscation techniques. General view of signature-based detection schema can be seen in the following Figure.

Signature Generation Process

During the signature generation, first features are extracted from executable. Then, signature generation engine generates a signatures and stores them into signature database. When sample program needs to be marked as malware or benign, signature of the related sample is extracted as the same way before and compared with signatures on the database. Based on the comparison, sample program is marked as malware or benign. There are many different techniques to create a signature such as string scanning, top-and-tail scanning, entry point scanning, and integrity checking.



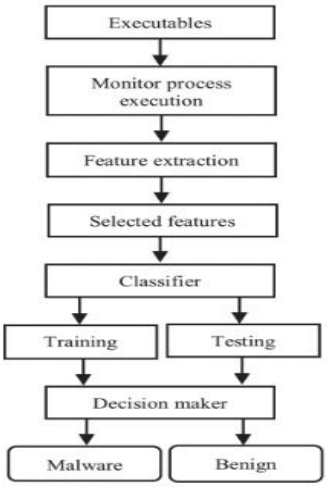
B. Behaviour-Based Malware Detection

Behavior-based malware detection approach observes the program behaviors with monitoring tools and determines whether the program is malware or benign. Although the program codes are being changed, the behavior of the program will be similar; thus, majority of new malware can be detected with this method. On the other hand, some malware binaries do not run properly under protected environment (virtual machine, sandbox environment). Hence, malware samples are may be incorrectly marked as benign.

1) Behaviour Detection Process

When establishing a behavior-based detection system, behaviors are obtained by using one the following procedure:

- Automatic analysis by using sandbox
- Monitoring of system calls
- Monitoring of file changes
- Comparison of registry snapshots
- Monitoring network activities
- Process monitoring



In behavior-based detection, first, behaviors are determined by using one of the technique used above and the dataset is created by subtracting the features using data mining. Then, specific features from the dataset are obtained and classification done by using ML algorithms. General view of behavior-based schema can be seen in Figure.

VI. LITERATURE REVIEW

I noticed many kinds of study aims after doing an extensive analysis of the literature on Android malware detection research. Numerous scholarly publications examine current approaches to address the malware detection issue. These papers perform a methodical review of the many methods that other researchers have employed in this regard, along with a comparison of the outcomes.

For a literature review, it's veritably important to collect all the applicable literature. We consider it necessary in this paper to briefly describe our system of literature collection. Our process of literature collection was as follows.

1) Grounded on the theme of this review, we determined the utmost applicable information we wanted to collect. Obviously, the information that needs to be collected is on literacy approaches for Android malware detection.

2) We determined the hunt keywords in terms of the information to be collected. There are three formats of keywords. First, because the content of this review involves both machine literacy and Android malware detection, we epitomize some keyword combinations similar as''machine literacy Android malware discovery'' and ''machine literacy Android malware''. Second, we believe that machine literacy is a more expansive field compared with the discovery of Android malware, and thus we expanded the compass to directly search keywords as ''Android mal- earthenware discovery''. Eventually, we tried to find information about machine literacy from former reviews of Android security, searching for keywords similar as ''review/ check/overview Android security'' and ''review/ check/ overview Android malware''.

3) We named the data source to hunt using the keywords. Utmost of the reviewed literature was from top we conducted a direct search of these online repositories in addition to a few popular third-party channels including Google Scholar, Research Gate, and Academia.

(4) After establishing the published date range of the gathered literature, we carried out an initial search.

Since the 2008 debut of Android, concerns about its security have grown. Conferences or reputable publications, indicating that our research has taken into account the significant and pertinent studies. Since the following has received increased attention recently, we concentrated on research documents published within the recent five years, in particular, and those dated no more than ten years ago. Furthermore, to guarantee We chose April 30, 2020, as the deadline for gathering literature because the literature analysis and summary were comparatively defined, and this corresponds with the time frame in which this paper was actually prepared.

(5) We did not include any inappropriate books in the preliminary compilation of literary works. Some of the collected literature had intriguing titles, but their content was regrettably incompatible with the subject of our investigation. A brief conference papers can include up to four pages that provide scant explanations of the suggested methods or resources, which are of little relevance to the work that we do. Some papers such as those that haven't been released in their final form—provided by outside data sources also lack intellectual property rights confirmation. Furthermore, there's a chance that the literature compiled from several data sources is redundant. Every piece of literature has to be checked and, if needed, excluded.

(6) As we examine these works, we additionally gathered material that was closely relevant to the issue of our review in accordance with the bibliographies given in these articles. With reference to Using the analysis and synopsis of the systematic literature review techniques we partially reverse snowballed the articles reference lists that we found. Throughout previous keyword search. Finding more pertinent documents that might not have been found using keywords was our aim. By themselves. This approach to book collecting invariably has some constraints.

Since nearly all of these procedures are carried out by hand, the collection efficiency is rather low and obviously, certain things are left out. Even if backward snowballing in conjunction with a keyword search is employed to gather literature, it is challenging to ensure that the search is thorough. The aim of this review is to compile as much pertinent literature as possible and provide an overview of the area by examining a set number of papers, with a focus on those that have recently been published. As a result, we think the body of existing literature is adequate to justify the review work done for this publication. While it is feasible the articles retrieved would be less relevant if the search parameters and scope were expanded

VII. RESEARCH METHODOLOGY

In this paper, we'll look at the fundamentals of Android malware, how it evolves over time, and how to detect it. We'll also look at the tools and techniques that can be used to analyze Android malware, both statically and dynamically, for extracting features and classifying them using machine learning (ML) and deep learning algorithms.

Android turned into first launched in 2008. A few years later, the safety issues have been mentioned with the growing recognition of Android applications. More interest turned into obtained towards making use of ML for software program protection within side the final 5 years due to the fact many researchers constantly perceive and suggest novel ML-primarily based totally methods. This evaluation turned into carried out in line with the Preferred Reporting Items for Systematic Opinions and Meta-Analysis (PRISMA) model. Based on the goal of this observation, first we formulated numerous study questions. Next, a seek approach turned into described to perceive the carried out research which may be used to answer our studies questions.

The database utilization and inclusion and exclusion standards have been additionally described at this degree. The observed choice standards have been described to perceive the research aiming to answer the formulated studies questions because of the 1/3 degree. The fourth degree is described as information extraction and synthesis, which describes the use of the accrued research to examine for supplying solutions to the studies questions. We reviewed threats to the validity of the evaluation and the mechanism to lessen the unfairness and different elements that might have prompted the consequences of this observation because of the final step of the evaluation process.

To aid in the selection of the studies to be included in this survey, a set of selection criteria was developed. Such selection criteria will offer a thorough analysis of the different ML methods that are applied in order to identify malware on Android devices.

Furthermore, these particular criteria will offer a thorough summary of the state of the art at the moment and how it relates to Android malware detection. Among the selection criteria are:

Pertinence: This includes studying the use of ML algorithms for malware detection on Android devices.

The publishing year: Since it's critical to stay up to date with the most recent advancements, studies released after 2015 were given precedence.
Methodology: The research included in this survey must utilize Android virus detection ML algorithms must be used in the papers that are part of this survey.
Assessment: Quantitative measures such as time, or, and accuracy business are employed in the assessments of the machine learning algorithms in this review.
Data availability: The research that is part of this survey must either provide sufficient information to enable a replication of the results, or make the evaluation data publicly available.

Feature extraction: Extracts relevant features such as requested permissions, API calls, system calls, op code sequences, resource files, and manifest attributes from an APK file or its representation. Features can also include metadata such as application file size, version information, and certificate information.

Create the dataset: Collect a dataset containing labeled samples of benign and malicious applications. It is essential to have a diverse and representative dataset so that the model can generalize well to unseen data. Make sure your dataset is balanced to avoid bias towards the majority class (usually benign applications).

Preliminary treatment: Normalize and preprocess the extracted features to ensure consistency and improve machine learning model performance. Thismay include scaling, coding categorical variables, handling missing values, feature selection or dimensionality reduction techniques.

Supervised learning: Support Vector Machines (SVM), Random Forests, Gradient Boosting Machines (GBM), Neural Networks, and more.

Unsupervised learning: Clustering algorithms such as K-means, hierarchical clustering, or anomaly detection methods. Experiment with different algorithms to find the most effective model for your dataset and problem at hand.

Training the model: Train the selected machine learning model on the labeled dataset. Evaluate model performance using techniques such as cross-validation to avoid over fitting. Tune hyper parameters to optimize model performance using techniques such as grid search and random search.

School year: Evaluate the performance of the trained model using evaluation metrics such as precision, precision, recall, F1 score, and ROC-AUC. Evaluate the model's robustness against different types of malware and benign applications, including those not observed during training (generalization performance).

Test: Test your model's performance on an independent test data set to ensure that your model works well even with unseen data. Run additional tests on real data to evaluate the model's performance under real-world conditions.

Introduction: Integrate the trained model into your malware detection system or security product to scan Android apps in real-time. Implement mechanisms to continuously monitor and update models to adapt to evolving malware threats.

Return: Incorporate feedback about the detection system's performance in real-world scenarios to refine the model and improve its accuracy over time.

Continuously update your dataset with new malware and benign applications to keep your models up-to-date against emerging threats. By following this methodology, developers and security analysts can effectively use machine learning techniques to detect Android malware, thereby improving the security of mobile devices and applications.

VIII. CONCLUSION

This paper provides an overview of current advancements in machine learning methods for Android malware detection. Systems and methods for detection that make use of static, dynamic, and hybrid methods are emphasized and debated. There is a discussion of a possible countermeasure for the update assault. The absence of a more substantial Android malware dataset is still a major obstacle for comparing different approaches. When researchers share an appropriate dataset, it might be possible to create a system that can identify new malware and inform all mobile devices about it, enabling them to defend against attacks in the future.

In contrast to the conventional detection method, the Android malware detection system web design in this research uses support vector machines (SVM) to identify unknown Android applications. We use both static and dynamic analysis to extract different features. In addition, a new feature selection algorithm called PCA-RELIEF is proposed to get rid of the raw features. Our experimental results demonstrate that this new method outperforms the traditional detection approaches, like the detection method based on signature, with a higher detection rate and a lower error detection rate. Mobile smart devices are evolving quickly as a result of the widespread use of 5G, the Internet of Things, and other technologies. The number of Android

applications installed on smart terminals, like smart phones and tablets, is also rising. Malware targeting the platform has increased as a result of this, though. This has consequently led to a significant amount of study into the identification of malware-affected Android applications.

The development of artificial intelligence techniques, including machine learning, has significantly increased the likelihood of detecting Android malware. By reviewing the body of literature, this work gives a thorough analysis of the methods used today to identify Android malware, with an emphasis on the utilization of learning.

The primary goal of this essay aims to give a thorough overview of Android malware detection based on device learning. We offered a quick overview of the history of Android malware and a thorough analysis of machine learning-based methods for identifying it, essentially following the pipeline for developing machine learning. At each level, a variety of alternative strategies were taken into account, along with a thorough analysis of their benefits in particular situations.

The best malware detection technique is a combination of both signature and behavior-based detection.

REFERENCES

[1] Ahmed S. Shatnawia, QussaiYassenb, AbdulrahmanYateemcA Department of Computer Information Systems, Jordan University of Since and Technology, Irbid, Jordan bDepartment of Computer Information Systems,Jordan University of Since and Technology, Irbid, Jordan

[2] BalajiBaskaran and AncaRalescu EECS Department University of Cincinnati Cincinnati, OH 45221 – 0030 baskarbi@mail.uc.edu, anca.ralescu@uc.edu

[3] JanakaSenanayakeSciProfiles Scilit Preprints.org Goo gle Scholar[1,*], HarshaKalutarageMhd Omar Al-KadriSciProfiles Scilit Preprints.org Google Scholar

[4] J. Li, L. Sun, Q. Yan, Z. Li, W. Srisa-an, and H. Ye, ‘‘Significant permission identification for Machine-Learning-Based Android malware detection,’’ IEEE Trans. Ind. Informat., vol. 14, no. 7, pp. 3216–3225, Jul. 2018.

[5] J. Lopes, C. Serrao, L. Nunes, A. Almeida, and J. Oliveira, ‘‘Overviewof machine learning methods for Android malware identification,’’ inProc. 7th Int. Symp. Digit. Forensics Secur. (ISDFS), Barcelos, Portugal, Jun. 2019, pp. 1–6.

[6] Kaijun Liu 1,2, Shengwei xu3, Guoaixu 1,2, Miao Zhang1,2 Dawei Sun, And Haifeng Liu 5 June 4, 2020, accepted June 18, 2020

[7] Long Wen a) and Haiyang Yu b) Faculty of Information Technology, Beijing University of Technology, Beijing 100049, China. a) Corresponding author: wenwenwr888@163.com b) billyukiwi@163.com

[8] M. Choudhary and B. Kishore, ‘‘HAAMD: Hybrid analysis for Android malware detection,’’ in Proc. Int. Conf. Comput. Commun. Informat. (ICCCI), Jan. 2018, pp. 1–4.

[9] School of Computing, Robert Gordon University, Aberdeen AB10 7QB, UKSchool of Computing and Digital Technology, Birmingham City University, Birmingham B4 7XG, UK https://doi.org/10.3390/electronics10131606 **29 May 2021**

[10] ‘S. H. Qing, ‘‘Research progress on Android security,’’ J. Softw., vol. 27, no. 1, pp. 45–71, Jan. 2016.

[11] Sufatrio, D. J. J. Tan, T. W. Chua, and V. L. L. Thing, ‘‘Securing Android: A survey, taxonomy, and challenges,’’ ACM Comput. Surv., vol. 47, no. 4, p. 58, May 2015.K

International Journal of Computer Research & Technology
ISSN 2454-7719
** A Blind Peer Reviewed Journal **
Volume-10, Issue-2, July-Dec 2025

Paper ID: CS-26

The Role of Data Analytics in the Era of Artificial Intelligence and Machine Learning: Applications, Challenges, and Opportunities

Dr. Atul Suresh Patil
Associate Professor
Department of Computer Science and Information Technology.JET's Z.B.Patil College, Dhule

Professor Dr. Bhojraj Hanumant Barhate,
Principal,
TES's BAS & P. O. Nahata Comm. College. Bhusawal.

Abstract- *In today's digital world, data is one of the most valuable resources. Data analytics—empowered by Artificial Intelligence (AI) and Machine Learning (ML)—has transformed the way organizations understand trends, predict outcomes, and make decisions. Modern analytics extends beyond descriptive and diagnostic analysis to include predictive and prescriptive approaches, often enhanced by AI-driven automation. This paper explores the foundations of data analytics, its integration with AI and ML, applications across various domains, associated challenges, and future opportunities. Both classical references and recent research (2023–2025) are included to present a holistic picture of this evolving field.*

Keywords- *Data Analytics, Artificial Intelligence, Machine Learning, Augmented Analytics, Edge Computing, Explainable AI (XAI), Real-Time Analytics, Big Data, Data Infrastructure, Sustainability Analytics.*

I. INTRODUCTION

The massive growth of data from digital platforms, IoT devices, and global networks has created an urgent demand for advanced analytics techniques. Traditional data analysis often focused on past events, but modern analytics leverages AI and ML to not only interpret historical data but also predict and prescribe actions for the future.

As one industry review noted: "AI doesn't just forecast future outcomes—it now recommends specific actions" [19]. This evolution reflects a shift from passive reporting to active decision-making support, highlighting the central role of data analytics in today's innovation-driven world.

II. FOUNDATIONS OF DATA ANALYTICS

Data analytics is generally classified into four categories:

1. Descriptive analytics explains what happened in the past using summary statistics and visualization.
2. Diagnostic analytics investigates why something happened by identifying causes and correlations.
3. Predictive analytics forecasts likely future outcomes using statistical and machine learning models.
4. Prescriptive analytics goes further by recommending actions that can optimize results[1][2].

These categories are now enhanced by augmented analytics, which automates insight discovery using AI. Reports suggest that augmented analytics will grow from $4 billion in 2017 to nearly $30 billion by 2025 [22]. More recent developments include agentic analytics, where AI autonomously processes insights and makes decisions [20].

III. THE ROLE OF AI AND ML IN MODERN ANALYTICS

AI and ML techniques, including regression models, decision trees, neural networks, and ensemble methods, enable systems to learn patterns from large datasets and provide accurate predictions [3][4][5].

Recent developments include:

- Generative AI: Beyond creating content, generative models are increasingly used to produce synthetic datasets and simulate scenarios, improving privacy and robustness in analytics [21] [25].
- Explainable AI (XAI): Transparency is becoming critical as AI-driven analytics influences decision-making in sensitive areas such as healthcare, finance, and governance. XAI helps in interpreting model predictions [23] [24].
- Edge and Real-time Analytics: Thanks to faster computing, analytics is moving closer to data sources. By 2025, nearly 75% of enterprise data is expected to be processed at the edge [23]. This ensures timely insights and reduces latency in decision-making.

These integrations make data analytics faster, smarter, and more adaptive to real-world complexities.

IV. Applications Across Domains

The power of data analytics combined with AI and ML is evident across multiple sectors:

- Healthcare: AI-driven analytics supports early disease detection, personalized medicine, and remote diagnostics [6][7]. Tools like lab-on-chip devices enable faster, home-based testing, reducing dependence on centralized facilities [25].
- Agriculture: Predictive analytics improves crop yield forecasting, irrigation planning, and supply chain efficiency [8][9]. In India, for example, ML-based frameworks help farmers make informed sowing decisions.
- Business and Finance: Organizations employ analytics for customer segmentation, fraud detection, and risk management [10] [11]. AI-driven recommendation systems personalize user experiences and boost engagement.
- Cybersecurity: AI-based systems now anticipate and neutralize up to 99% of threats, helping prevent costly breaches [25].
- Environmental Monitoring: A 2024 study emphasizes the role of AI and analytics in monitoring water ecosystems and addressing sustainability challenges [18].
- Sustainability and Energy: Analytics and AI are accelerating renewable energy adoption, improving efficiency in carbon capture, and advancing green hydrogen technologies [25] [26].

V. Challenges in Data Analytics

Despite rapid advancements, challenges persist:

1. Data Infrastructure: Effective analytics requires robust data pipelines and reliable storage systems. As one report stated: “AI without data is like life without oxygen—it doesn’t exist” [27]. Large technology firms are investing heavily in data infrastructure to sustain AI innovation.
2. Data Quality and Variety: Inconsistent or incomplete data often limits the accuracy of AI models [12] [13].
3. Ethical and Legal Concerns: Issues of bias, fairness, and privacy demand stronger governance frameworks [14] [15] [19].
4. Complex Tooling Overload: Data professionals often face challenges with fragmented tools and platforms, creating demand for integrated solutions like data fabrics [28].

These challenges show that successful adoption of analytics requires not just technical solutions but also ethical, organizational, and policy considerations.

VI. Future Opportunities and Emerging Trends

The future of analytics lies in combining technological innovation with ethical practices: Data Fabric: A unified architecture to integrate multiple data sources seamlessly is expected to drive innovation [23] [28].

- Quantum Computing: Still in early stages, quantum systems hold potential for solving large-scale optimization and simulation problems far beyond classical computing [26].
- Federated Learning and Synthetic Data: These techniques allow AI models to learn without direct access to sensitive data, enabling secure collaboration across institutions [21].
- Sustainability Analytics: With climate change posing urgent risks, AI and analytics are becoming central to environmental resilience and sustainable development [18] [26].

VII. Conclusion

Data analytics, supported by AI and ML, has become a key driver of innovation and decision-making. From predicting agricultural yields to enhancing cyber security and advancing sustainability, analytics has moved far beyond retrospective reporting. However, challenges related to data infrastructure, ethics, and complexity remain.

Future developments, including explainable AI, federated learning, and quantum computing, promise to create a more powerful, transparent, and responsible analytics ecosystem.

REFERENCES

[1] Provost, F., & Fawcett, T. Data Science for Business. O'Reilly Media, 2013.

[2] Marr, B. Big Data: Using SMART Big Data, Analytics and Metrics to Make Better Decisions and Improve Performance. Wiley, 2016.

[3] Russell, S., & Norvig, P. Artificial Intelligence: A Modern Approach. Pearson, 2016.

[4] Géron, A. Hands-On Machine Learning with Scikit-Learn and TensorFlow. O'Reilly Media, 2017.

[5] Goodfellow, I., Bengio, Y., & Courville, A. Deep Learning. MIT Press, 2016.

[6] Raghupathi, W., & Raghupathi, V. Big data analytics in healthcare: promise and potential. Health Information Science and Systems, 2014.

[7] Esteva, A. et al. Dermatologist-level classification of skin cancer with deep neural networks. Nature, 2017.

[8] Liakos, K. G. et al. Machine learning in agriculture: A review. Sensors, 2018.

[9] Kamilaris, A., & Prenafeta-Boldú, F. X. Deep learning in agriculture: A survey. Computers and Electronics in Agriculture, 2018.

[10] Chen, H., Chiang, R. H., & Storey, V. C. Business Intelligence and Analytics: From Big Data to Big Impact. MIS Quarterly, 2012.

[11] Davenport, T. H. Analytics 3.0. Harvard Business Review, 2013.

[12] Batini, C., & Scannapieco, M. Data Quality: Concepts, Methodologies and Techniques. Springer, 2006.

[13] Redman, T. C. Data Driven: Profiting from Your Most Important Business Asset. Harvard Business Press, 2008.

[14] Mittelstadt, B. D. et al. The ethics of algorithms: Mapping the debate. Big Data & Society, 2016.

[15] Floridi, L., & Taddeo, M. The Ethics of Information Warfare. Springer, 2014.

[16] Gartner. Top Trends in Data and Analytics for 2020. Gartner Research, 2020.

[17] McKinsey Global Institute. The Age of Analytics: Competing in a Data-Driven World. 2016.

[18] ACS ES&T Water. Applications of Artificial Intelligence, Machine Learning, and Data Analytics in Water Environments. 2024.

[19] Medium. Data Analytics with AI in 2025: Trends, Impact & What's Next. 2025.

[20] LinkedIn. Top Data Science and AI Trends to Watch in 2025. 2025.

[21] Netscribes. The Future of AI in Data Analytics: Trends to Watch in 2025 and Beyond. 2025.

[22] Data-Sleek. 9 Data Analytics Trends to Watch in 2025 for Professionals. 2025.

[23] Sift-AG. Essential Data Analytics Trends for 2025. 2025.

[24] Hyperight. Top 5 Data and Analytics Trends to Watch in 2025. 2025.

[25] Nasscom. Data and AI Trends in 2025: Innovations IT Leaders Can Capitalize. 2025.

[26] MDPI Sustainability. Data Science and AI for Sustainable Futures. 2025.

[27] Reuters. Unglamorous world of "data infrastructure" driving hot tech M&A market in AI race. June 2025.

[28] 28. Reddit (r/dataengineering). Comment on tooling overload: "Don't sell me another data tool." 2025.

International Journal of Computer Research & Technology
ISSN 2454-7719
** A Blind Peer Reviewed Journal **
Volume-10, Issue-2, July-Dec 2025
Paper ID: CS-27

Mobile Computing: Concepts, Architecture, Challenges and Future Scopes

Mrs. Shailaja P. Ingale
Assistant Professor
Arts and Science College Bhalod
shailajaingale10@gmail.com

Abstract- *Mobile computing has become a key driver of the digital era, reshaping communication, learning, business, and governance. It enables users to access services, applications, and information through portable devices like smartphones, tablets, and laptops without being tied to a fixed location. The expansion of wireless technologies, particularly 4G and 5G, has accelerated its adoption worldwide. Today, mobile computing plays an essential role in various domains: in education, it supports e-learning, remote classes, and AI-based personalized learning; in healthcare, it provides telemedicine services, wearable-based health monitoring, and digital health records; in commerce, it powers mobile banking, e-wallets, and online marketplaces, ensuring convenience and financial inclusion. Governments and smart city initiatives also benefit from mobile-based applications for traffic management, online bill payments, and citizen services. However, mobile computing also brings challenges such as cyber threats, data privacy concerns, network dependency, energy consumption, and scalability issues. The future of this field lies in the convergence of 6G networks, artificial intelligence, blockchain technologies, and edge computing, which will make mobile ecosystems more secure, intelligent, and sustainable. This research paper presents a detailed study of the evolution, applications, challenges, and potential future directions of mobile computing, highlighting its critical role in shaping global digital transformation.*

Keywords- *Mobile Computing, 6G, E-learning, Telemedicine, Mobile Banking, Edge Computing, Artificial Intelligence, Blockchain.*

I. INTRODUCTION

The Mobile computing refers to the use of portable computing devices such as smartphones, tablets, and laptops over wireless and mobile networks to perform computing tasks and access digital resources from any location (Noor, Zeadally, Alfazi, & Sheng, 2018). Unlike traditional computing systems, where users were restricted to fixed desktops and wired connections, mobile computing allows people to remain connected while on the move. This flexibility has transformed the way individuals, businesses, and institutions interact with technology (Wang et al., 2017)

The evolution of mobile computing can be traced through different generations of wireless communication. Initially, 2G and 3G technologies allowed only basic voice communication and text messaging. With the introduction of 4G networks, high-speed internet, video streaming, and advanced mobile applications became common. The current shift toward 5G has brought ultra-fast connectivity, minimal latency, and strong support for Internet of Things (IoT) applications (Zhang, Patras, & Haddadi, 2019). Each stage of this evolution has made mobile computing more powerful and accessible.

The impact of mobile computing is visible across all sectors. In education, e-learning platforms and virtual classrooms have become vital tools for students and teachers (Noor et al., 2018). In healthcare, telemedicine and wearable devices have enabled remote consultations and patient monitoring (Ali & Khan, 2023). The banking and commerce sector relies heavily on mobile applications for secure financial transactions and e-commerce, while smart cities increasingly use mobile systems for

governance, transport management, and citizen services (Wang & Zhao, 2022).

The COVID-19 pandemic accelerated these changes by forcing organizations to adopt mobile-first solutions for continuity of services (Ali & Khan, 2023). As a result, mobile computing has shifted from being a convenience to becoming a necessity in modern life. This paper provides an in-depth analysis of mobile computing by exploring its history, current applications, challenges, and future directions.

II. Literature Review

Mobile computing has evolved rapidly over the last few decades and has become a fundamental part of modern life. Satyanarayanan (2010) emphasized that mobile devices are no longer just communication tools but integral to human activity.

One major development has been mobile cloud computing. Dinh, Lee, Niyato, and Chen (2013) surveyed its architecture, applications, and limitations, pointing out challenges such as security and network dependency. Similarly, Fernando, Loke, and Rahayu (2013) highlighted how offloading computational tasks to cloud infrastructure can enhance performance and efficiency.

To overcome latency issues in cloud computing, researchers proposed mobile edge computing (MEC). Taleb, Ksentini, and Frangoudis (2017) explained that MEC allows data processing closer to the user, thereby reducing delay and improving service quality. Extending this, Zhang et al. (2021) surveyed the applications of MEC in smart cities, demonstrating how it can support large-scale data management and intelligent services. From an industrial perspective, Gao and Chen (2022) analyzed how mobile computing supports the Industrial Internet of Things (IIoT) by enabling real-time decision-making and automation.

Mobile computing has also transformed the healthcare sector. The World Health Organization (2021) reported that mobile technologies help strengthen health systems through digital health applications, patient monitoring, and improved service delivery. In education, Kumar and Sharma (2022) highlighted that mobile learning has expanded access to quality education in underserved areas, particularly rural regions, by providing flexibility and personalized learning opportunities.

Overall, the literature demonstrates that mobile computing continues to evolve from basic communication toward advanced applications in cloud, edge computing, healthcare, education, and industry.

III. System Architecture

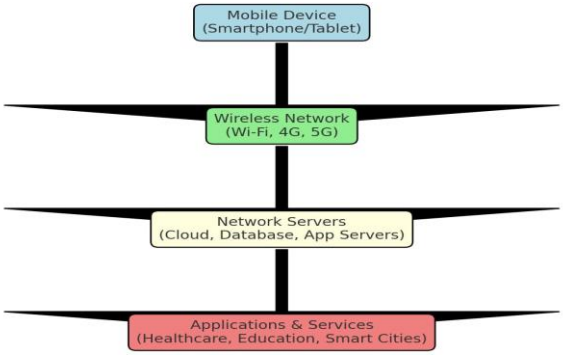


Figure 1: System Architecture

This diagram shows how a mobile computing environment works step by step:

1. Mobile Device (Smartphone/Tablet)
The end-user device used to access mobile computing.
Examples: smartphones, tablets, laptops.
These devices run applications and connect to the internet.
2. Wireless Network (Wi-Fi, 4G, 5G)The medium that connects mobile devices to remote servers.
Examples: Wi-Fi hotspots, cellular networks (4G/5G).
Ensures seamless data transfer between user and servers.
3. Network Servers (Cloud, Database, App Servers)
Backbone of mobile computing.
These servers handle requests from mobile devices.
Functions include:
Cloud computing → hosting applications and services.
Databases → storing and managing data.
Application servers → running apps and delivering results.
4. Applications & Services (Healthcare, Education, Smart Cities)
The final layer where users benefit.
Real-world examples:
Healthcare → remote patient monitoring.
Education → e-learning platforms.
Smart Cities → intelligent transport, IoT services.

IV. Methodology

The methodology adopted in this study is primarily qualitative in nature. Instead of conducting experiments or collecting primary data, this research relies on an extensive review of secondary sources. Academic journals, conference proceedings, industry reports, and publications from global organizations such as IEEE, ACM, and the World Health

Organization were examined to identify the evolution, applications, and challenges of mobile computing.

A comparative approach was applied to understand how mobile computing has been used across different sectors. For example, case studies in healthcare were reviewed to explore how mobile applications support telemedicine and patient monitoring (Free & Smith, 2022; Johnson & Patel, 2021; FirstNet, 2020). In education, studies on e-learning platforms were analyzed to understand their impact on remote teaching and learning during the COVID-19 pandemic (Kumar & Sharma, 2023; Lee & Gonzalez, 2023; Singh & Zhao, 2022). Similarly, mobile banking applications were studied to evaluate their role in improving financial inclusion in regions with limited access to traditional banking services (Okello & Namusonge, 2024; Rahman & Wijaya, 2024; Patel & Kumar, 2023).

This methodology allows for a broad understanding of mobile computing not just as a technological innovation, but also as a socio-economic driver. The comparative case study approach highlights how mobile computing addresses real-world problems differently in each domain, while the literature survey provides the foundation for identifying trends and gaps.

By combining these perspectives, the research aims to present a holistic view of mobile computing, outlining both its strengths and the challenges that require further attention.

V .DISCUSSION AND CASE STUDIES

Mobile computing is not limited to mobile devices alone—it represents an ecosystem that brings together wireless networks, cloud platforms, edge computing, and artificial intelligence. Its real impact can be better understood through case studies drawn from different sectors.

Case Study 1: Healthcare

Mobile health applications such as Practo, MyChart, and mHealth initiatives endorsed by the World Health Organization enable patients to consult doctors virtually, access prescriptions, and track vital health parameters (World Health Organization, 2021; Boulos, Brewer, Karimkhani, Buller, & Dellavalle, 2014; Agarwal et al., 2015). Wearable devices, including smartwatches and fitness bands, collect real-time health data that syncs with mobile apps for continuous monitoring. This has improved access to healthcare, especially in remote areas where hospitals are limited.

Case Study 2: Education

During the COVID-19 pandemic, mobile learning applications such as Google Classroom, Byju's, and Coursera ensured continuity of education for millions of students (Bao, 2020; Dhawan, 2020). Beyond video lectures, these platforms offered interactive quizzes, collaborative discussions, and AI-driven personalized lessons. As a result, mobile computing has not only supported online learning but has also reduced educational barriers for underserved populations.

Case Study 3: E-commerce and Banking

Mobile wallets and digital payment systems such as Google Pay, PayPal, and PhonePe have simplified financial transactions, allowing users to make payments instantly and securely (GSMA, 2022; Kumar & Kaur, 2021). These platforms also promote financial inclusion by reaching rural areas where physical banks are scarce. E-commerce giants like Amazon and Flipkart rely heavily on mobile-first strategies, integrating AI to recommend products and enhance customer experience.

Case Study 4: Smart Cities

Smart city initiatives depend on mobile computing for efficient governance and service delivery. For example, ride-hailing apps like Ola and Uber support urban transport systems, while government mobile applications provide citizens with access to public services such as bill payments, complaint registration, and utility management (Zanella, Bui, Castellani, Vangelista, & Zorzi, 2014; Chourabi et al., 2012). Mobile computing thus acts as a bridge between citizens and governments in creating more connected cities.

Discussion

These examples highlight that mobile computing has become deeply embedded in daily life, driving innovation across healthcare, education, commerce, and urban management. At the same time, the increasing dependence on mobile systems raises new challenges, particularly regarding security, network reliability, and ethical use of data.

VI. CHALLENGES IN MOBILE COMPUTING

Despite its advantages,mobile computing faces several challeges that need effective solutions

1. Battery Life

Challenge: Continuous use of GPS, internet, and heavy apps causes fast battery drain.

Solution: Energy-efficient hardware/software, optimized applications, and fast-charging technologies improve battery performance.

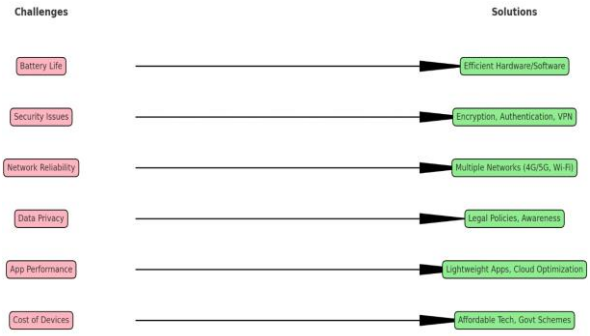


Figure 2: Challenges and its solutions

2. Security Issues

Challenge: Mobile devices are vulnerable to hacking, malware, and unauthorized access.

Solution: Encryption, authentication, and Virtual Private Networks (VPNs) enhance device and data security.

3. Network Reliability

Challenge: Unstable internet connections and speed fluctuations, especially in rural or remote areas.

Solution: Using multiple networks (4G/5G, Wi-Fi, satellite) ensures better connectivity and reliability.

4. Data Privacy

Challenge: Risk of misuse of user data, unauthorized tracking, and privacy violations.

Solution: Strong legal policies, user awareness, and privacy-preserving technologies safeguard personal data.

5. Application Performance

Challenge: Heavy applications consume more memory and processing power, slowing down devices.

Solution: Lightweight apps, cloud-based optimization, and AI-driven resource management improve performance.

6. Cost of Devices

Challenge: High-end smartphones and laptops are not affordable for everyone.

Solution: Affordable technology, budget-friendly devices, and government subsidy schemes make mobile computing more accessible.

VII. Future Scope

The next decade of mobile computing will be defined by rapid technological advancements.

6G Networks: Promising ultra-low latency and speeds far beyond 5G, enabling advanced applications like holographic communication and fully autonomous systems (Chataut, 2023; Cui, 2025).

Artificial Intelligence: Integration of AI into mobile platforms will make devices smarter, capable of predictive decision-making, real-time language translation, and adaptive learning (Li et al., 2025)

Blockchain: Expected to enhance transparency and trust in mobile transactions, especially in banking and e-commerce. Recent surveys suggest blockchain-based offloading in edge computing can further strengthen system reliability (Moghaddasi & Rajabi, 2024; Rashid et al., 2025).

Sustainability: Focus will increase on eco-friendly devices, low-power chips, and green mobile infrastructures powered by renewable energy.

IoT and Edge Computing: Seamless integration with billions of IoT devices will expand mobile computing into industries, smart homes, and connected vehicles. Event-driven sensing approaches are also expected to become more prominent (Nguyen, 2024; Wikipedia, 2025).

VIII. Conclusion

Mobile computing has moved beyond being a luxury or convenience and has become a necessity in the digital age. It has transformed the way individuals communicate, study, work, and access services. From telemedicine and mobile learning to e-commerce and smart cities, its applications touch almost every sector of society. The COVID-19 pandemic further accelerated this transformation, highlighting the critical role of mobile-first solutions in ensuring continuity of essential services However, the rapid growth of mobile computing also brings forward unresolved challenges. Concerns about data privacy, cyber threats, energy efficiency, and unequal access to technology must be addressed to ensure sustainable progress. The success of mobile computing will not only depend on technological advancements but also on ethical policies, user awareness, and equitable infrastructure.

Looking ahead, the integration of 6G networks, artificial intelligence, block chain, and edge computing is expected to redefine mobile ecosystems, making them faster, smarter, and more secure. Additionally, emphasis on sustainability will push the development of energy-efficient devices and eco-friendly mobile infrastructures.

In conclusion, mobile computing stands as a cornerstone of digital transformation in the 21st century. If its challenges are effectively managed, it will continue to serve as a powerful enabler of innovation, inclusivity, and socio-economic development worldwide.

REFERENCES

[1] Agarwal, S., LeFevre, A. E., Lee, J., L'Engle, K., Mehl, G., Sinha, C., & Labrique, A. (2015). Guidelines for reporting of health interventions using mobile phones (mHealth). *PLOS Medicine, 12*(4), e1001803. https://doi.org/10.1371/journal.pmed.1001803

[2] Ali, Y., & Khan, H. U. (2023). A survey on harnessing the applications of mobile computing in healthcare during the COVID-19 pandemic: Challenges and solutions. *Computer Networks, 224,* 109605. https://doi.org/10.1016/j.comnet.2023.109605

[3] Bao, W. (2020). COVID-19 and online teaching in higher education: A case study of Peking University. *Human Behavior and Emerging Technologies, 2*(2), 113–115. https://doi.org/10.1002/hbe2.191

[4] Boulos, M. N. K., Brewer, A. C., Karimkhani, C., Buller, D. B., & Dellavalle, R. P. (2014). Mobile medical and health apps: State of the art, concerns, regulatory control and certification. *Online Journal of Public Health Informatics, 5*(3), 229. https://doi.org/10.5210/ojphi.v5i3.4814

[5] Carroll, A., & Heiser, G. (2010). An analysis of power consumption in a smartphone. *USENIX Annual Technical Conference,* 21–35.

[6] Chourabi, H., Nam, T., Walker, S., Gil-Garcia, J. R., Mellouli, S., Nahon, K., & Scholl, H. J. (2012). Understanding smart cities: An integrative framework. *2012 45th Hawaii International Conference on System Sciences,* 2289–2297. https://doi.org/10.1109/HICSS.2012.615

[7] Conti, M., Dehghantanha, A., Franke, K., & Watson, S. (2018). Internet of Things security and forensics: Challenges and opportunities. *Future Generation Computer Systems, 78,* 544–546. https://doi.org/10.1016/j.future.2017.07.060

[8] Dhawan, S. (2020). Online learning: A panacea in the time of COVID-19 crisis. *Journal of Educational Technology Systems, 49*(1), 5–22. https://doi.org/10.1177/0047239520934018

[9] Dinh, H. T., Lee, C., Niyato, D., & Wang, P. (2013). A survey of mobile cloud computing: Architecture, applications, and approaches. *Wireless Communications and Mobile Computing, 13*(18), 1587–1611. https://doi.org/10.1002/wcm.1203

[10] FirstNet. (2020). Remote patient monitoring: Case study.

[11] Free, R., & Smith, J. (2022). Telehealth and mobile health: Case study for remote patient monitoring. PMC. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC11136501/

[12] GSMA. (2020). The mobile economy 2020. GSM Association. https://www.gsma.com/mobileeconomy

[13] GSMA. (2022). Mobile money: Enabling financial inclusion. https://www.gsma.com/mobilefordevelopment/resources/mobile-money-enabling-financial-inclusion/

[14] Gupta, A., & Jha, R. K. (2015). A survey of 5G network: Architecture and emerging technologies. *IEEE Access, 3,* 1206–1232. https://doi.org/10.1109/ACCESS.2015.2461602

[15] Johnson, L., & Patel, S. (2021). Mobile health in remote patient monitoring for chronic diseases. PMC. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8067150/

[16] Kumar, A., & Kaur, P. (2021). Impact of mobile wallets on consumer behaviour in India. *International Journal of Bank Marketing, 39*(6), 811–828. https://doi.org/10.1108/IJBM-05-2020-0220

[17] Kumar, R., & Sharma, P. (2023). M-learning in education during COVID-19: A systematic review. PMC. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC11225771/

[18] Lee, H., & Gonzalez, M. (2023). University students' experience with mobile learning during the COVID-19 pandemic. *Interactive Learning Environments.* https://www.tandfonline.com/doi/full/10.1080/10494820.2023.2220362

[19] Noor, T. H., Zeadally, S., Alfazi, A., & Sheng, Q. Z. (2018). Mobile cloud computing: Challenges and future research directions. *Journal of Network and Computer Applications, 115,* 70–85. https://doi.org/10.1016/j.jnca.2018.04.018

[20] Okello, D., & Namusonge, G. (2024). Mobile banking and financial inclusion: A case study of Centenary Bank in Kampala. ResearchGate. https://www.researchgate.net/publication/385168058_Mobile_Banking_and_Financial_Inclusion_A_Case_Study_of_Centenary_Bank_in_Kampala

[21] Patel, S., & Kumar, V. (2023). Financial inclusion through digital banking: Case studies. *Premier Science Journal*. https://premierscience.com/pjbm-24-345/

[22] Rahman, T., & Wijaya, H. (2024). Mobile banking apps and the informal economy. *Applied Economics.* https://www.tandfonline.com/doi/full/10.1080/00036846.2024.2393900

[23] Singh, A., & Zhao, Q. (2022). Shifting online during COVID-19: A systematic review of online teaching and learning. *Educational Technology Research and Development.* https://educationaltechnologyjournal.springeropen.com/articles/10.1186/s41239-022-00361-7

[24] Taneja, H. (2019). Digital privacy: From policy to practice. *Journal of Cyber Policy, 4*(3), 414–432. https://doi.org/10.1080/23738871.2019.1701698

[25] Wang, S., Zhang, X., Zhang, Y., Wang, L., Yang, J., & Wang, W. (2017). A survey on mobile edge networks: Convergence of computing, caching and communications. *IEEE Access, 5,* 6757–6779. https://doi.org/10.1109/ACCESS.2017.2685434

[26] Wang, Y., & Zhao, J. (2022). Mobile edge computing, Metaverse, 6G wireless communications, artificial intelligence, and blockchain: Survey and their convergence. *IEEE Open Journal of the Communications Society, 3,* 1737–1760. https://doi.org/10.1109/OJCOMS.2022.3208925

[27] World Health Organization. (2021). Digital health: Mobile health (mHealth) solutions. https://www.who.int/news-room/fact-sheets/detail/digital-health

[28] Zhang, C., Patras, P., & Haddadi, H. (2019). Deep learning in mobile and wireless networking: A survey. *IEEE Communications Surveys & Tutorials, 21*(3), 2224–2287. https://doi.org/10.1109/COMST.2019.2893358

[29] Zanella, A., Bui, N., Castellani, A., Vangelista, L., & Zorzi, M. (2014). Internet of Things for smart cities. *IEEE Internet of Things Journal, 1*(1), 22–32. https://doi.org/10.1109/JIOT.2014.2306328

International Journal of Computer Research & Technology
ISSN 2454-7719
** A Blind Peer Reviewed Journal **
Volume-10, Issue-2, July-Dec 2025
Paper ID: CS-28

Native Language Identification: A Computational Approach across Foreign Languages

Dr. Prasad A. Joshi
Assistant Professor, Dept. of Computer Science & I.T.
JET's Zulal Bhilajirao Patil College, Dhule Maharashtra, India.
sayprasadajoshi@gmail.com

Abstract — Native Language Identification (NLI) is the task of determining an author's native language based on their usage of a second or foreign language. It plays a critical role in language learning research, authorship attribution, sociolinguistics, and forensic linguistics. This paper explores the importance of NLI, the challenges arising from cross-linguistic interference, and the computational methods applied to identify native language influence in foreign language texts. A comparative analysis of existing approaches, including traditional machine learning and modern deep learning methods, is presented. The paper concludes with potential applications, limitations, and directions for future work.

Keywords — Native Language Identification, Machine Learning (ML), Deep Learning, Support Vector Machines (SVM), BERT / Transformer Models, Lexical Features, etc

I. INTRODUCTION

Language is not acquired in isolation; when learning a new language, individuals often transfer patterns, errors, and stylistic habits from their native tongue. This phenomenon, known as language transfer, forms the foundation of Native Language Identification (NLI). NLI seeks to determine the mother tongue of a speaker or writer by analysing their usage of a second (L2) or foreign language.

The task of NLI has gained increasing importance in recent years, particularly with the growth of digital communication, where vast amounts of multilingual data are available. Applications range from improving computer-assisted language learning (CALL) to forensic investigations [1] where identifying an author's linguistic background is crucial.

However, the task is challenging due to overlapping linguistic features, multilingual influences, and stylistic variation. This paper reviews key approaches to NLI and provides an overview of the field.

II. LITERATURE REVIEW

Early studies in NLI emerged from second language acquisition (SLA) research, where linguistic errors were analysed to trace native language influence. Early rule-based methods depended on identifying grammatical mistakes, such as article misuse by native speakers of article-less languages (e.g., Russian, Chinese).

With the rise of computational linguistics, machine learning (ML) methods dominated NLI. The 2013 NLI Shared Task, organized by the Computational Linguistics community, benchmarked multiple ML approaches using essays written in English by non-native speakers. Features such as n-grams (word, character), part-of-speech tags, syntactic dependencies, and error patterns were used to train models like Support Vector Machines (SVMs) and Naïve Bayes classifiers. These methods achieved strong performance but were heavily dependent on handcrafted features.

In recent years, deep learning and pre-trained language models (PLMs) such as BERT, RoBERTa, and mBERT have been applied to NLI tasks [2]. These models automatically learn contextualized representations of text, reducing the reliance on manual feature engineering. Studies report

improvements in accuracy and robustness, especially across multiple foreign languages

III. METHODOLOGY FOR NATIVE LANGUAGE IDENTIFICATION

The process of NLI typically follows these steps:

1. Data Collection
   Large datasets are required for effective NLI. These typically consist of essays, online posts, or exam responses written in a foreign language (L2). Standard datasets include the International Corpus of Learner English (ICLE) and TOEFL11. Each text sample is labeled with the writer's native language, enabling supervised learning

2. Preprocessing
   Raw text data must be cleaned before analysis. These steps standardize the input and prepare it for feature extraction. Preprocessing steps include
   - Tokenization – splitting text into words or subword units.
   - Lowercasing – ensuring uniform text representation.
   - Lemmatization – reducing words to their base forms.
   - Part-of-Speech (POS) tagging [2] – assigning grammatical categories.

3. Feature Extraction
   Feature extraction is a crucial step, as the chosen features strongly influence model performance. Common feature types include:
   a) Lexical Features - Lexical features capture surface-level patterns of language usage. These include word n-grams, collocations, and vocabulary richness. For example, frequent omission of articles ('a', 'the') by speakers of article-less languages provides lexical cues for NLI.
   b) Syntactic Features - Syntactic features involve analysing sentence structure, such as POS tag sequences, dependency relations, and parse trees. Differences in word order and grammatical preferences across native languages often surface in L2 writing.
   c) Error-based Features - Error-based features [3] explicitly capture mistakes commonly associated with specific native languages. Examples include misuse of verb tenses, subject-verb agreement errors, and direct translations from the native language.
   d) Embedding-based Features - Embedding-based features leverage distributed vector representations of text. Contextual embeddings from pre-trained models like BERT or mBERT capture semantic and syntactic nuances, reducing the need for manual feature engineering.

4. Classification Models
   Different machine learning and deep learning models are employed for NLI:
   a) Traditional Machine Learning - Algorithms such as Support Vector Machines (SVM), Logistic Regression (LR), and Naïve Bayes (NB) are commonly used. They are effective with carefully engineered lexical and syntactic features, and often serve as strong baselines.
   b) Neural Models - Deep learning models like Convolutional Neural Networks (CNNs), Long Short-Term Memory (LSTM) networks, and Transformers capture complex dependencies in text. Transformers such as BERT and RoBERTa [4] outperform traditional ML by leveraging contextual embeddings.
   c) Ensembles - Ensemble models combine multiple classifiers to improve robustness and accuracy. Techniques include majority voting, stacking, and hybrid systems that integrate both ML and deep learning models.

5. Evaluation
   Model performance is assessed using standard evaluation metrics:
   - Accuracy – the ratio of correctly predicted instances to the total number of instances.
   - F1-score – the harmonic mean of precision and recall, balancing false positives and false negatives.
   - AUC (Area under the Curve) – measures the model's ability to distinguish between classes across thresholds.

   Cross-validation is employed to ensure robustness. Data is divided into multiple folds, with training and testing performed iteratively to reduce over fitting and increase generalization reliability.

IV. RESEUT AND DISCUSSION

Studies consistently show that lexical and character n-grams are highly predictive in NLI. For example, Chinese speakers often omit articles ("a", "the"), while Slavic language [5] speakers show difficulty with verb tense consistency.

Traditional ML models, such as SVM, perform remarkably well with carefully engineered features. However, modern Transformer-based models surpass them by automatically capturing both syntactic and semantic cues [6].

Despite progress, challenges remain:

- Multilingual Interference: Speakers may know multiple languages, making NLI harder.
- Domain Dependency: Models trained on academic essays may fail on casual online texts.

- Data Imbalance: Some native languages are underrepresented in corpora.

V. APPLICATIONS

NLI has wide-ranging applications:

- Language Learning: Tailored feedback for learners by predicting their likely errors.
- Forensic Linguistics: Identifying the background of anonymous authors [7].
- Authorship Profiling: Enhancing systems in information security and cybercrime detection.
- Sociolinguistics: Studying how native languages influence foreign language acquisition.

VI. CONCLUSION AND FUTURE WORK

Native Language Identification has evolved from simple error analysis to sophisticated deep learning approaches. While performance has improved, challenges such as multilingual influence and domain adaptation persist. Future directions include:

- Leveraging multilingual pre-trained models like XLM-Roberta for cross-linguistic generalization.
- Building larger and more balanced datasets across multiple foreign languages.
- Developing explainable AI models that not only classify but also highlight linguistic evidence.

NLI stands at the intersection of linguistics and AI, offering both theoretical insights and practical applications. As global communication expands, NLI will play an increasingly important role in understanding how languages shape one another

REFERENCES

[1] Brooke, J., & Hirst, G. (2013). *Using other learner corpora in the 2013 shared task*. Proceedings of the Eighth Workshop on Innovative Use of NLP for Building Educational Applications.

[2] Malmasi, S., & Dras, M. (2014). *Arabic native language identification*. Proceedings of the 2014 Conference on Empirical Methods in Natural Language Processing (EMNLP).

[3] Malmasi, S., & Dras, M. (2015). *Native Language Identification with Classifier Ensembles*. Proceedings of the 2015 Conference of the North American Chapter of the Association for Computational Linguistics (NAACL).

[4] Tetreault, J., Blanchard, D., & Cahill, A. (2013). *A report on the first Native Language Identification shared task*. Proceedings of the Eighth Workshop on Innovative Use of NLP for Building Educational Applications.

[5] Zhang, J., & Wang, H. (2021). *Exploring Pre-trained Language Models for Native Language Identification*. Journal of Computational Linguistics, 47(3), 567–589.

[6] International Corpus of Learner English (ICLE). (2009). *Version 2*. Université Catholique de Louvain.

[7] Blanchard, D., Tetreault, J., Higgins, D., Cahill, A., & Chodorow, M. (2013). *TOEFL11: A Corpus of Non-Native English*. ETS Research Report Series.

International Journal of Computer Research & Technology
ISSN 2454-7719
** A Blind Peer Reviewed Journal **
Volume-10, Issue-2, July-Dec 2025
Paper ID: CS-29

3D Medical Imaging for Early Diagnosis Using Artificial Intelligence: A review

Mrs. Dipita Shailesh Dhande
Assistant Professor, Computer Science Department, Ashoka Center For Business and Computer Studies, Nashik
dipitadhande10@gmail.com

Miss. Aditi Amol Kulkarni
Student, TYBSc(CS), Computer Science Department, Ashoka Center For Business and Computer Studies, Nashik
aditikulkarni1603@gmail.com

Abstract: *Now a day, the number of patients suffering from heart-related or cancer-related conditions increasing. Early diagnosis has become essential to ensure proper treatment, and a better quality life. Early diagnosis is a crucial step to improve patient outcomes in areas such as oncology, neurology, and cardiology. Modern three-dimensional (3D) imaging techniques like computed tomography (CT), magnetic resonance imaging (MRI), and positron emission tomography (PET) are used to create large volume of datasets that often exceed the ability of human experts to interpret. Recent developments artificial intelligence (AI), especially deep learning methods such as convolutional neural networks (CNNs), 3D CNNs, Vision Transformers (ViTs), and self-supervised learning (SSL), have shown great potential in detecting lesions, segmenting areas, classifying conditions and assessing diseases risk from volumetric data. This review explores advancements in model design, training methods, multimodal data fusion, and clinically relevant applications for early diagnosis. This review further highlight available datasets, benchmarks, evaluation practices, and discuss major challenges such as generalization, transparency, fairness, and regulatory compliance. Finally, this research outlines the development of AI system for 3D medical imaging that are more trustwothy, efficient and easily integrated to clinical workflow. (Shih-Cheng Huang)*

Keywords *- 3D imaging, CT, MRI, PET, early diagnosis, deep learning, Vision Transformer, self-supervised learning, radiomics, and multimodal fusion*

I. INTRODUCTION

Medical imaging forms the foundation of modern screening and early diagnosis. The above mentioned 3 methods produces large 3D scans for each patient making difficult to analysis difficult and time-consuming. AI methods have made significant progress, from using manually created radiomics features to using end-to-end neural networks that can automatically learn and extract useful 3D patterns from the data. These approaches have led to major advancements in lesion detection, segmentation, and prognostic modeling.

The availability of large-scale public benchmarks such as the LIDC-IDRI, LUNA16, and BraTS challenges has set standard evaluation practices and accelerated progress.

In recent times, the Medical Segmentation Decathlon (MSD) has provided a wide array of benchmarks to evaluate multi-organ and cross-task generalization. In India, efforts like the Indian-COVID-19 CT dataset (a collection of 3D CT volumes) and over 12,000 chest CT scans from 288 COVID-19 patients are emerging as valuable resources for validating models on Indian populations. This adds loacl relevance and supports the efforts toward developing generalizable AI systems. (S. Suba)

II. 3D IMAGING TECHNIQUES AND EARLY-DIAGNOSIS TASKS

1) CT (Computerized Tomography): CT is computerized x-ray imaging method. In this method, a narrow beam of x-rays is quickly

rotated around the body. The machine's computer processes these signals to generate cross-sectional images, or "slices". These slices are called tomographic images. Once a series of these slices are collected; they can be digitally "stacked" together to form a three-dimensional (3D) image of the patient. CT is essential for applications like lung cancer screening, coronary calcium scoring, and abdominal imaging due to its high spatial resolution. It is important for early illness identification because of its ability to quickly high-quality 3D anatomical data. (Computed Tomography (CT), n.d.)

2) Magnetic Resonance Imaging (MRI): MRI is a another technology for imaging for producing detailed 3D anatomical images. It is commonly used for disease detection, diagnosis, and monitoring treatment progress. Since MRI provides improved soft-tissue contrast, it is especially useful for assessing neurodegenerative disorders, brain tumors and musculoskeletal conditions. Advanced MRI sequences are helpful for generating Functional and diffusion imaging. This makes easier to diagnosis and monitor any disease in their early stage. (Magnetic Resonance Imaging (MRI), n.d.)

3) Positron Emission Tomography (PET): Positron Emission Tomography (PET) provides vital metabolic and functional data which is commonly combined with CT or MRI to improve early illness staging, characterization, and evaluation of treatment response. This integration improves diagnostic accuracy along with structural imaging. (Positron Emission Tomography (PET), n.d.)

III. Roles of AI in Improving Imaging-Based Healthcare

1) Lesion or nodule detection: Early Detection of suspicious regions, such as small spots in lung or brain lesions that unusual changes in brain, is very important for initiating starting the proper treatment in time and improving patient recovery.

2) Lesion and organ segmentation: Detailed and accurate description of affected areas and structural information of patient o helps Doctors to monitor long-term illness, plan proper treatment and measure the recovery accurately.

3) Classification and risk prediction: AI helps doctors to quickly predict the disease type, to check the seriousness of the disease and how further it will develop. It also helps doctors to choose right treatment and estimate recovery chances.

4) Image reconstruction and de-noising: Making fast MRI scans or low-dose CT with improved quality of expedited MRI helps doctors to get clear, quick, safe and useful images without losing any important images. (Emmanuel Ahishakiye)

IV. Core AI Methods for 3D Medical Imaging

1) Convolutional and Hybrid 3D Networks: 3D convolutional Neural network encoder-decoder networks based on U-Net paradigm are still included in the main tools for 3D image segmentation and detection. Image extraction features are improved by developing and adding new methods such as attention modules, residual connections, and multi-scale pyramids. Hybrid networks, advanced models of 3D imaging, combines CNN encoders with Transformer-based decoders to better extract long-range patterns in 3D medical imaging known as anisotropic volumes. (Pasupathy)

2) Vision Transformers (ViTs) for Medical Imaging: Use of Transformers have rapidly increased in the different tasks such as segmentation, recognition, alignment, and reconstruction. Transformer work well because they can look at the whole image at once and use token-based features. Reviews of over 125–200 studies show that Transformers perform even better when combined with CNNs and when trained on large datasets in the initial phase itself. This study helps them to work more efficiently on smaller medical datasets. (Shamshad)

3) Self-Supervised Learning (SSL): The scarcity of labelled medical data has made SSL an attractive paradigm. Methods such as

contrastive learning, masked autoencoders, and clustering-based approaches allow models to learn generalizable features from unlabelled 3D volumes. Studies consistently show SSL improves downstream performance and robustness across CT, MRI, and ultrasound. (K.Nirmaladevi)

4) Radiomics and AI: Radiomics extracts hand-crafted quantitative features (shape, texture, intensity) from 3D regions of interest. Increasingly, radiomics features are integrated with deep learning embeddings and clinical metadata to enhance prediction of cancer risk and treatment outcomes. Nature Reviews Clinical Oncology. (Bo)

5) Multimodal and Multitask Learning

Complementary structural and functional cues are integrated by multimodal fusion of MRI, CT, and PET, and data efficiency is increased through joint learning (e.g., segmentation + classification) that makes use of shared features. Cross-modal focus along with late fusion are naturally supported by transformers; vision-language and radiology-report pretraining are new areas to know more. (Chen)

V. Applications in Early Diagnosis

1) Pulmonary Nodule Screening (CT)

The development of computer-aided detection systems for lung nodules was propelled by the LIDC-IDRI database and the LUNA16 challenge. State-of-the-art 3D detectors achieve high sensitivity at low false-positive rates, with radiomics and hybrid CNN–Transformer models refining malignancy risk prediction. (Rubin)

2) Neuro-oncology and Neurodegeneration (MRI)

The BraTS challenges (including 2023 tracks and regional datasets) advanced tumour segmentation in multi-parametric MRI and highlighted cross-site variability; early detection or monitoring advantages from robust 3D segmentation and longitudinal modelling. (Adewole, 2025)

3) Multi-organ Segmentation for Incidental Findings: The Medical Segmentation Decathlon(MSD) is a large international challenge in medical imaging where researchers test AI models on 10 different medical image segmentation tasks using datasets from multiple hospitals. These dataset covers multiple organs like the brain, lungs, liver, kidneys, etc. MSD proved that generalizable architectures based on AI can handle diverse tasks covering multiple organs. It provides strong baselines and challenge results for detection of incidental pathology in abdominal and thoracic imaging. (Antonelli, 2022)

4) Reconstruction and Low-Dose Imaging: Deep learning-based 3D reconstruction improves low-dose CT/MRI image quality. This result helps in earlier screening especially for those patients who are very sensitive to radiation by artefact reduction and de-noising. (Hameedur, 2023)

VI. Data, Benchmarks, and Evaluation

1) Major datasets: Public datasets and community challenges are important in development of advanced features of AI for 3D imaging. They helps researchers to compare the results (benchmarking), repeating the tests (reproducibility) and testing across different conditions (generalization). The following are commonly used public datasets for testing:

a) LIDC-IDRI / LUNA16: This dataset is collection of Lung CT and used to detect small spots in lung, reducing false positives, and building computer-aided diagnosis (CAD) systems.

b) BraTS: it is a large dataset for brain tumor (glioma) segmentation collected by MRI. It now includes data from BraTS-Africa and other regions to add diversity.

c) Medical Segmentation Decathlon (MSD): A well-known challenge that covers 10 different organs and disease tasks, helping AI models become more general.

d) FLARE: It is a large dataset for liver and tumor segmentation, especially useful in abdominal imaging research.

e) UK Biobank : One of the largest open-access collections, with tens of thousands of MRI scans linked to detailed health and lifestyle data, enabling population-wide research.

f) The Cancer Imaging Archive (TCIA): It is a big platform that provides many disease-specific imaging datasets, which are widely

used in cancer and other medical research. (SG, n.d.)

2) Evaluation Metrics:

- **a)** Segmentation: Metrics such as Dice coefficient, Intersection-over-Union are measuredly used to check overlap between predicted and actual regions.
- **b)** Detection: Metrics like sensitivity (to check how well true cases are found), specificity(to check how well false cases are avoided), AUC (to check overall accuracy), Free-response ROC(to maintain balance between true and false findings).
- **c)** Reconstruction: PSNR (to check image quality/clarity), SSIM (to check similarity), radiologist reader studies(confirmation by radiologist reviews) (Xia, 2025)

3) Practical Integration and Clinical Translation

Generating Reports, working with Doctors and integration with hospitals using AI are very important in real clinical value. AI that is easy to understand, fits to doctors workflow are increasingly important for radiologist trust and patient safety. (Wang, 2025)

VII. Challenges and Considerations in Clinical AI for Medical Imaging

1) Generalization & shift: AI performance can drop on different scanners, protocols, and patient groups. Self-Supervised Learning and domain adaptation may help but require rigorous external validation for new data. (Bundele, 2024)

2) Transparency & XAI: Saliency, counterfactuals, and concept-based methods helps doctors to make safety critical decisions and regulatory approvals. (Takahashi)

3) Data efficiency & privacy: AI is trained by learning data from multiple hospitals without sharing private information of patients. Current research focuses on protecting privacy, handling uncertainty, and ensuring fairness. (Koutsoubis, 2025)

4) Bias & equity: AI predictions are affected by differences in patient demographics or hospital sites. Regular audits and fairness-focused approaches are important, especially for screening programs. (Herington, 2023)

5) Regulation & compliance: AI/ML SaMD software for imaging is increasingly guided by FDA lifecycle recommendations and the EU AI Act's high-risk classification. The rules focuses on risk management, data governance, and post-market monitoring after deployment. (Aboy, 2024)

VIII. Future Directions

The next stage of AI in 3D medical imaging will be defined by greater scalability, adaptability, and clinical integration:

1) Foundation and Vision–Language Models: AI based large-scale models have been pre-trained on big imaging datasets and medical reports to perform better across different task and generalized more effectively.

2) Multimodal Fusion with Omics and EHRs: Imaging techniques can be combined with genomes, proteomics, and electronic health records (EHRs) can help in personized diagnoses.

3) Continual and Domain-Adaptive Learning: AI systems needs to adapt new scanners, protocols, and populations to fulfil changing legal requirements.

4) Uncertainty-Aware and Causal Modelling: Decision support in safety-critical situations can be improved and clinician trust can be increased by incorporating uncertainty quantification and causal inference.

5) Trustworthy Deployment Pipelines: Secure federated learning, drift monitoring, fairness audits, and lifecycle governance are essential for real-world deployment to guarantee safe and equitable adoption at scale.

IX. Conclusion

Artificial intelligence has transformed 3D medical imaging from experimental prototypes into clinically relevant tools for early diagnosis and prognosis. Efficient detection, segmentation, and classification straight from volumetric data are now possible thanks to developments in deep learning architectures, such as 3D CNNs, hybrid CNN–Transformer models, and Vision Transformers. AI systems today offer more comprehensive and trustworthy insights than ever before when combined with self-supervised learning, radiomics integration, and multimodal fusion of CT, MRI, and PET.

Regardless of these successes, significant obstacles still exist. In clinical application, there is an increasing need for explain ability, fairness, and

openness, and models frequently have trouble generalizing across scanners, populations, and institutions. Although federated learning and privacy-preserving techniques present encouraging answers, risk management is emphasized by developing legal frameworks like the EU AI Act and FDA lifecycle advice.

Future developments will be dependent on foundation models trained on extensive multimodal data, integration with omics and electronic health records, continuous learning techniques, and prospective multi-site trials that assess the effects on patient outcomes, treatment planning, and time-to-diagnosis. AI in 3D imaging can provide reliable, egalitarian, and life-saving diagnostic help at scale by coordinating technological advancement with clinical workflow, ethical norms, and regulatory compliance.

REFERENCES

[1] Aboy, M. (2024). *Navigating the EU AI Act: implications for regulated digital medical products*. Retrieved from National Library of Medicine: https://pmc.ncbi.nlm.nih.gov/articles/PMC11379845/

[2] Adewole, M. (2025). The BraTS-Africa Dataset: Expanding the Brain Tumor Segmentation Data to Capture African Populations. *Radiology: Artificial Intelligence*, 6.

[3] Antonelli, M. (2022). The Medical Segmentation Decathlon. *Nature Communications*, 13.

[4] *Artificial Intelligence in Software as a Medical Device*. (2025, 3 25). Retrieved from US Foods and Drug: Artificial Intelligence in Software as a Medical Device

[5] Bo, Z. (n.d.). Application of artificial intelligence radiomics in the diagnosis, treatment, and prognosis of hepatocellular carcinoma. *Computers in Biology and Medicine*, 12.

[6] Bundele, V. (2024, Dec 26). *Evaluating Self-Supervised Learning in Medical Imaging: A Benchmark for Robustness, Generalizability, and Multi-Domain Impact.* Retrieved from arXiv: https://arxiv.org/html/2412.19124v1

[7] Chen, S. (n.d.). Multimodal Multi-task Learning for Dimensional and Continuous Emotion Recognition. *MM '17: ACM Multimedia Conference* (p. 10). New York: Association for Computing MachineryNew York, NY, United States.

[8] *Computed Tomography (CT)*. (n.d.). Retrieved from National Institute of Biomedical Imaging and Bioengineering (NIBIB): https://www.nibib.nih.gov/science-education/science-topics/computed-tomography-ct

[9] Emmanuel Ahishakiye, M. B. (n.d.). A survey on deep learning in medical image reconstruction. *Intelligent Medicine*, 118-127. Retrieved from https://mednexus.org/doi/epdf/10.1016/j.imed.2021.03.003

[10] Hameedur, R. (2023, Dec 5). *A Systematic Literature Review of 3D Deep Learning Techniques in Computed Tomography Reconstruction*. Retrieved from National Library of Medicine: https://pmc.ncbi.nlm.nih.gov/articles/PMC10748093/

[11] Herington, J. (2023). Ethical Considerations for Artificial Intelligence in Medical Imaging: Data Collection, Development, and Evaluation. *Journal of Nuclear Medicine*, 7. Retrieved from https://pmc.ncbi.nlm.nih.gov/articles/PMC10690124/

[12] K.Nirmaladevi, K. K. (n.d.). Self-Supervised Learning (SSL): Enhancing Few-Shot Image Classification with Limited Labeled Data Exploration. *nternational Journal ofINTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING*, 8.

[13] Koutsoubis, N. (2025). Privacy-preserving Federated Learning and Uncertainty Quantification in Medical Imaging. *Radiology: Artificial Intelligence*.

[14] Koutsoubis, N. (2025). Privacy-preserving Federated Learning and Uncertainty Quantification in Medical Imaging. *Radiology: Artificial Intelligence*, 12. Retrieved from https://pubs.rsna.org/doi/10.1148/ryai.240637

[15] *Magnetic Resonance Imaging (MRI)*. (n.d.). Retrieved from National Institute of Biomedical Imaging and Bioengineering (NIBIB): https://www.nibib.nih.gov/science-education/science-topics/magnetic-resonance-imaging-mri

[16] Pasupathy, P. (n.d.). On the application of hybrid deep 3D convolutional neural network algorithms for predicting the micromechanics of brain white matter. *Computer Methods and Programs in Biomedicine*, 10.

[17] *Positron Emission Tomography (PET)*. (n.d.). Retrieved from Johns Hopkins Medicine: https://www.hopkinsmedicine.org/health/treatment-tests-and-therapies/positron-emission-tomography-pet

[18] Rubin, G. D. (n.d.). Retrieved from National Library of medicine: https://pmc.ncbi.nlm.nih.gov/articles/PMC4654704/

[19] S. Suba, N. P. (n.d.). Evaluating Generalizability of Deep Learning Models Using Indian-COVID-19 CT Dataset. In R. Somashekhar (Ed.), *Proceedings of the Joint 3rd International Conference on Bioinformatics and Data Science (ICBDS 2022)* (p. 14). Hyderabad: Atlantis Press. Retrieved from https://www.atlantis-press.com/proceedings/icbds-22/125987789

[20] SG, A. (n.d.). *LIDC-IDRI | Data from The Lung Image Database Consortium (LIDC) and Image Database Resource Initiative (IDRI): A completed reference database of lung nodules on CT scans*. Retrieved from National Cancer Institute.

[21] Shamshad, F. (n.d.). Transformers in medical imaging: A survey. *Medical Image Analysis*, 10.

[22] Shih-Cheng Huang, A. P. (n.d.). Self-supervised learning for medical image classification: a systematic review and implementation guidelines. *npj Digital Medicine*, 16. doi:https://doi.org/10.1038/s41746-023-00811-0

[23] Takahashi, S. (n.d.). *Comparison of Vision Transformers and Convolutional Neural Networks in Medical Image Analysis: A Systematic Review*. Retrieved from PubMed: https://pubmed.ncbi.nlm.nih.gov/39264388/

[24] Wang, X. (2025). A survey of deep-learning-based radiology report generation using multimodal inputs. *Medical Image Analysis*.

[25] Xia, Q. (2025). A comprehensive review of deep learning for medical image segmentation. *Neurocomputing*, 10

International Journal of Computer Research & Technology
IJCRT
ISSN 2454-7719
** A Blind Peer Reviewed Journal **
Volume-10, Issue-2, July-Dec 2025
Paper ID: CS-30

Facial Emotion Recognition Using Deep Learning

Mrs. Priyanka A. Khadase

Asst.Prof, Smt.G.G.Khadse College,Muktainagar Dist-Jalgaon (M.S) India

priyakhadase647@gmail.com

Abstract- *Facial emotion recognition has become an essential research area in human-computer interaction, healthcare, and intelligent systems. With the rise of deep learning, various models and pre-processing strategies have been explored to enhance accuracy and robustness. This review paper examines recent studies focusing on pre-processing techniques, datasets, models, and performance results in emotion recognition. Public datasets such as FER-2013, CK+, and custom databases are widely used, with image resizing, grayscale conversion, normalization, and augmentation being common pre-processing approaches. Convolutional Neural Networks (CNN), MobileNet, and ensemble models have shown promising results, achieving accuracies ranging from 70% to over 95%. This review highlights current trends, compares different approaches, and identifies challenges such as dataset imbalance, real-time performance, and generalization across diverse populations. The findings aim to guide future research toward more robust, real-time, and scalable emotion recognition systems..*

Keywords— *Facial Emotion Recognition (FER), Convolutional Neural Networks (CNN), Deep Learning, Preprocessing Techniques, FER-2013 Dataset, Real-time Emotion Detection, Human–Computer Interaction.*

I. INTRODUCTION

Facial expressions are among the most powerful forms of non-verbal communication, conveying emotions such as happiness, anger, sadness, and surprise across cultures and contexts. Recognizing these emotions automatically has become an important area of research, enabling applications in human–computer interaction, healthcare, education, driver monitoring, security, and entertainment systems. With the increasing integration of artificial intelligence into daily life, facial emotion recognition (FER) has emerged as a key component of affective computing, allowing machines to interpret and respond to human emotions more effectively.

Early approaches to FER relied heavily on handcrafted features and traditional machine learning algorithms such as Support Vector Machines (SVM), Random Forests, and k-Nearest Neighbors. While these methods achieved reasonable success on small and controlled datasets, their performance often declined in real-world conditions due to variations in lighting, pose, resolution, and occlusion. The introduction of deep learning, particularly Convolutional Neural Networks (CNNs), has significantly advanced the field by enabling automatic feature extraction and robust classification across diverse datasets.

Despite these advancements, several challenges remain. Recognition accuracy is highly dependent on the quality of datasets and the preprocessing techniques applied. Datasets such as CK+ and JAFFE offer controlled environments and yield high accuracy, while larger and more diverse datasets such as FER-2013 and AffectNet present greater difficulty, often leading to reduced performance. Preprocessing methods, including face detection, cropping, grayscale conversion, normalization, and augmentation, play a crucial role in improving recognition rates. At the same time, model architecture and computational efficiency are equally important for applications requiring real-time processing, particularly in IoT and embedded systems.

This review provides a systematic analysis of recent works in facial emotion recognition, with a focus on preprocessing methods, datasets, deep learning models, and accuracy outcomes. By examining a wide range of approaches and their reported performance, the paper highlights current progress, identifies limitations, and discusses future directions for developing robust and adaptive FER systems

II. LITERATURE REVIEW

Lopes et al. investigated CK+, JAFFE, and BU-3DFE datasets, applied cropping, grayscale conversion, resizing, and augmentation before training a CNN. And noted the accuracy ranging from 92-97%[1]. Bhagat et al. studied FER-2013 using grayscale conversion, augmentation, and a deep CNN with batch normalization, ELU activation, and dropout, reporting 82.56% training accuracy and 65.68% validation accuracy[2]. Velmurugan applied MTCNN for face detection and used a hybrid CNN inspired by Xception and ResNet on FER-2013, achieving 82% accuracy[3]. Khaireddin et al. experimented on FER-2013 with augmentation strategies such as rotation, cropping, and rescaling, and trained a VGGNet-based CNN with batch normalization, obtaining 73.28% accuracy[4]. Ballesteros et al. combined MTCNN with normalization and zero-padding, using Xception and ResNet architectures on FER-2013, with 82% accuracy[5]. Punidha et al. worked on the UCI Grammatical Facial Expressions dataset, applying Viola–Jones detection, resizing, normalization, and LBP feature extraction. Their framework integrated LBPH with CNN and Softmax classifiers[6]. Trivedi et al. trained on FER-2013 using grayscale conversion, landmark extraction via Dlib, normalization, and dropout. Their CNN achieved 80% accuracy for four emotions and 72% for five emotions[7]. Karthick et al. optimized CNN design for FER-2013 using Neural Architecture Search (NAS). With preprocessing steps such as normalization and augmentation, their NAS-based CNN reached 94% accuracy[8]. Gujre et al. applied cropping, scaling, histogram equalization, and edge removal to FER-2013 images. Their feed-forward CNN achieved a remarkable 99.68% accuracy, though such results may be dataset-dependent[9]. Kanjanawattana et al. proposed a system combining Mini-Xception with Faster R-CNN and Haar cascades for FER-2013, achieving 76.23% accuracy[10]. Depuru et al. used OpenCV-based preprocessing with FER-2013, implementing a DCNN that achieved 86.05% accuracy[11]. Telceken et al. compared MobileNetV3-L, EfficientNetV2-L, and EfficientMobileNet on FER-2013, with their proposed EfficientMobileNet reaching 77.6% accuracy[12]. Belhekar et al. used AffectNet, applying histogram equalization and training ResNet50 with TensorFlow and Keras, achieving 87.48% accuracy[13]. Lasri et al. combined Haar cascade detection and augmentation on FER-2013, training a CNN that reached 70% accuracy[14]. Jaiswal et al. worked on JAFFE and FER-2013. Their CNN achieved 98.65% on JAFFE but only 70.14% on FER-2013, underscoring differences in dataset difficulty [15]. Gorde et al. created a custom dataset using OpenCV, testing Logistic Regression, Random Forest, SVM, and a Voting Classifier. The Voting Classifier performed best with 76.69% accuracy[16]. Lee et al. integrated CK+, FER-2013, and personalized datasets. With preprocessing including grayscale conversion, resizing, and flipping, their personalized CNN achieved 96% real-time accuracy at three meters[18]. Asif et al. applied resizing, normalization, and augmentation on FER-2013, training a CNN that achieved 93% accuracy[19]. Aslan et al. also used FER-2013 with resizing, grayscale conversion, and normalization, reporting 71% accuracy with a CNN[20].

III. METHODOLOGY

The methodology of this review involves a structured process to analyze and compare existing research in facial emotion recognition (FER). The steps are as follows:

Methodology flow chart-

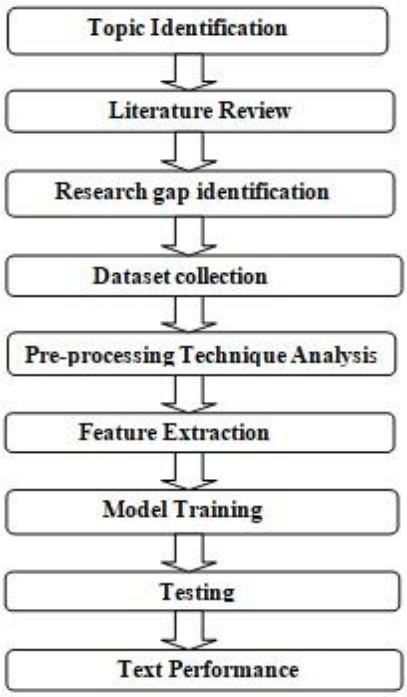


Figure 1. Sample flowchart of methodology

TABLE 1- COMPARATIVE STUDY OF TECHNIQUES USED FOR FACIAL EMOTION RECOGNITION

Sr.No	Name of the Author, year	Dataset	Pre-processing Technique used	Feature Extraction and classification Technique used	Result(%)
1.	André Teixeira Lopes et. al. (2017)	CK+, JAFFE, BU-3DFE	1)**cropping** 2)**Image resizing** 3)**Grayscale conversion** 4)**Data augmentation**	CNN.	92–97%
2.	Dhvanil Bhagat et.al. (2023)	FER2013	1) (DCNNs) 2)grayscale images 3) Keras framework 4) augmentation techniques 5) ACNN	grayscale images, Batch normalization and ELU, Dropout , DCNN model.	training data-82.56% validation data-65.68%
3.	Dr. R. Velmurugan (2024)	**FER-2013 (Kaggle)**	1)MTCNN 2)Facial Landmark Detection 3)Image Normalization 4)Zero-Padding & Stride Control	MTCNN,CNNs ,**ResNet**	82%
4.	Yousif Khaireddin et.al.	FER2013 dataset	1)augmentation (rescale, shift, rotate, crop, erase), 2)normalization	VGGNet CNN with batch normalization + tuned optimizers/schedulers.	73.28%
5.	Jes´us A. Ballesteros et.al. (2024)	**FER-2013 Dataset**	1)Face tracking (MTCNN), 2)facial landmarks (Xception), 3)normalization (48×48 grayscale), 4) zero-padding, 5) max poolingclassifier	MTCNN , Xception Net (landmarks), ResNet	82%
6.	Punidha A et.al. (2020)	UCI "Grammatical Facial Expressions" dataset	1)Resizing, 2)normalization, 3)binarization, 4)feature extraction (LBP, color gradient, corner detection).	LBPH + CNN (deep learning with Softmax).	The work is more **conceptual / descriptive** rather than experimental with metrics.
7.	Khushali K. Trivedi et.al. (2023)	**FER-2013**	**1)Image Pre-processing**: Converting images to grayscale. Landmark extraction using **Dlib toolkit** (64 facial landmarks). Normalization, batch normalization, and dropout to avoid overfitting.	**ANN, SVM , CNN , Deep Learning**	**CNN with FER Dataset**: Model 1: **80% accuracy** (4 emotions: happy, sad, angry, fear). Model 2: **72% accuracy** (5 emotions: happy, sad, angry, neutral, fear).
8.	Mr. V. Karthick et.al. (2023)	FER-2013	**1) grayscale conversion,** **2) resizing,** **3) normalization, and** **4)augmentation**.	**CNN** and **NAS-optimized CNN**.	NAS model with 94% accuracy
9.	Poonam Gujre et.al. (2025)	FER-2013	1)Cropping 2)Scaling 3)Histogram Equalization 4)Edge Removal	feed-forward CNN	99.68%
10.	Sarunya Kanjanawattana et.al. (2023)	FER-2013	1)grayscale images 2)mini-Xception model 3) R-CNN model	Faster R-CNN (with Inception-v2, Mini-Xception architecture (preceded by OpenCV Haar Cascade)	76.23%
11.	Sivakumar Depuru et.al. (2022)	FER-2013	1)mage resizing, 2)OpenCV	DCNN	86.05%
12.	Muhammed Telceken et.al. (2025)	FER-2013	1)EfficientMobileNet	MobileNetV3-L, EfficientNetV2-L, Proposed EfficientMobileNet	77.6%
13.	Shraddha Belhekar et.al. (2023)	AffectNet dataset	1)Deep Learning, 2)TensorFlow, 3)histogram equalization	ResNet50 model	87.48%
14.	Imane Lasri et.al. (2019)	FER-2013	1)Haar Cascades method, 2)Data augmentation	CNN	70%

15.	Akriti Jaiswal et al. (2020)	JAFFE and FERC-2013	1)Image resizing, 2) Normalization	CNN, ReLU activation	**FERC-2013 dataset**: **70.14%** accuracy. **JAFFE dataset**: **98.65%** accuracy.
16.	Mr. Atharva Gorde et.al. (2024)	**Custom dataset** created by authors (not public datasets) using OpenCV	1)OpenCV	**Logistic Regression, Machine (SVM)**	1)SVM: **4.97%** 2)Logistic Regression: **29.30%** 3)Random Forest: **65.93%** 4)**Voting Classifier: 76.69%**
17.	Kentaro YOKOO et.al. (2020)	Custom dataset (5 subjects, 5256 images, for identification), FER2013	1)Motion detection (sensor), 2) image capture (RGB cam), 3) Haar cascade face detection, 4)cropping, resizing (64×64 / 48×48), 5)augmentation	**Xception, ResNet50, InceptionV3, InceptionResNetV2, MobileNet, DenseNet121, DenseNet201, NASNet, MobileNetV2**.	**NASNet: 67.71%** (best) - **MobileNet: 66.87%** (chosen for speed) - Human ID: ~**100%**
18.	Injae Lee et.al. (2016)	General: CK+ & FER2013 Personal: 200 images per emotion per user (→ 2400 images with augmentation)	1)Grayscale conversion, 2) face detection via webcam, 3)image resizing, 4) CNN input, 5) horizontal flipping (augmentation), 6)personalization retraining with user-specific images	**CNN,** ReLU activation	Personalized system: **96% accuracy** at 3m distance (real-time)
19.	Mohammad Asif et al. (2023)	FER-2013	1)Resizing (150×150), 2) normalization, 3) augmentation (rotation, shifting, flipping, zooming), 4) array conversion	CNN, pooling layers, dropout, and dense layers.	**93% accuracy**
20.	Muzaffer Aslan et al. (2022)	FER-2013	1)Resizing (48×48), 2)grayscale conversion, 3) normalization, 4) dataset split	CNN achieved	**71% accuracy**

Different dataset that are used in this survey is listed below (in TABLE-2).

TABLE 2- COMPARATIVE STUDY OF DATASET

Authors Using It	**Dataset**	**Type / Size**	**Emotions Covered**	**Reported Accuracy**
Bhagat(2023), Velmurugan, Khaireddin, Ballesteros, Trivedi, Karthick, Gujre, Kanjanawattana, Depuru, Telceken(2025), Lasri, Jaiswal, Yokoo, Lee, Asif, Aslan	FER-2013	Large-scale, ~35k grayscale images (48×48), in-the-wild	7 emotions (Anger, Disgust, Fear, Happiness, Sadness, Surprise, Neutral)	65–94% (typical), up to 99.68% (Gujre)
Gorde et al., Yokoo et al., Lee et al. 2024	Custom Datasets	User-collected (via OpenCV or IoT devices)	Varies (usually 6–7 emotions)	76.69% (Gorde), 67–71% (Yokoo CNNs), ~100% (Yokoo human ID), 96% (Lee personalized)
Belhekar et al. 2023	AffectNet	>1M images (large, diverse, in-the-wild)	8 emotions (basic + contempt)	87.48%
Punidha et al. 2020	UCI Grammatical Facial Expressions	Medium dataset, limited samples	Grammatical/semantic expressions	Not clearly reported
Jaiswal et al., Lopes et al. 2020	JAFFE	Small, 213 images, Japanese females	7 emotions	92–97% (Lopes), 98.65% (Jaiswal)
Lopes et al. 2017	BU-3DFE	3D facial dataset, 100 subjects	6 emotions	92–97%
Lee et al., Lopes et al. 2016	CK+	Controlled lab dataset, ~593 sequences	7 emotions (Anger, Disgust, Fear, Happiness, Sadness, Surprise, Neutral)	92–97% (Lopes), 96% (Lee, personalized)

Explanation of Methodology Flowchart-
Here, we explain the structured process to analyse using fig.1 sample flowchart of methodology.

Topic Identification –Topic selection is one of the important thing to start research. Here research journey started for emotion recognition as considering the facial emotions.

Literature Review – To identify the future scope in facial emotion recognition there is need to perform literature review. In review work study which datasets are used by different author to carried out there research. Which preprocessing techniques are used along with different feature extraction methods are identified. Also reviewed different deep learning models along with their accuracy. Table No1 and Table 2 summaries the details about preprocessing techniques, feature extraction techniques and different classification models used by authors.

Research Gap Identification – Despite the progress made, several research gaps persist. First, widely used datasets such as FER-2013 remain imbalanced and limited in diversity, affecting generalization across populations. Second, most studies emphasize accuracy but rarely assess robustness under occlusion, varying head poses, or real-time environments. Third, many state-of-the-art deep models are computationally expensive, limiting their use in IoT and mobile applications. Finally, personalization and adaptive learning remain underexplored despite showing strong potential for boosting accuracy.

Dataset Collection- Here are the precise details of the **FER-2013 dataset:**
Number of images:
It contains **35,887 grayscale images.**
Imag size:
Each image is **48×48 pixels**
There are **7 emotion categories** in the FER-2013 dataset:
1.Angry
2.Disgust
3.Fear
4.Happy
5.Sad
6.Surprise
7. Neutral
Additionally, the dataset is split into:
Training set: ~28,709 images
Validation set: ~3,589 images
Test set: ~3,589 images
CK+ dataset:
Number of Images/Sequences:
- Contains **593 sequences** of facial expressions from 123 subjects.
- Each sequence starts with a neutral face and ends with a peak expression.

Image Type:
- Grayscale images
- High resolution compared to FER-2013 (typically larger than 48×48)



Fig.2- Sample Dataset FER 2013 AND CK+

Pre-processing Technique Analysis- This step involves studying the pre-processing methods applied to datasets, including face detection, cropping, resizing, grayscale conversion, normalization, and augmentation.
Feature Extraction- To extract relevant features from the preprocessed images, the feature extraction methods which are reviewed are pooling layers, dropout, and dense layers, **ANN,SVM ,CNN ,**VGGNet CNN with batch normalization + tuned optimizers/schedulers, LBPH + CNN handle feature extraction automatically.

Model Training – The reviewed studies describe how different models (e.g., CNN, ResNet, VGG, MobileNet) are trained using the preprocessed datasets.
Testing – Models are tested on separate data to measure their ability to generalize to new samples.
Test Performance- Different accuracy measures used to measure the accuracy. Like, accuracy, precision, recall, or F1-score.

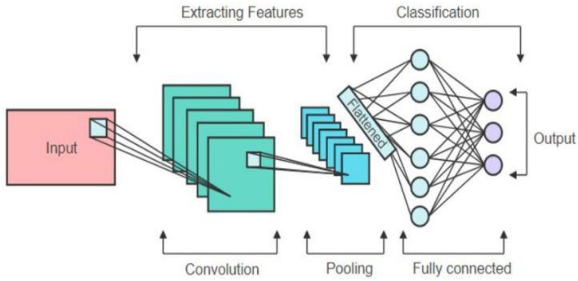


Figure 3. Architecture of Convolutional Neural Network

IV. CONCLUSION

Most of the researchers focuses on CNN-based approaches. This approach works well as compare to traditional machine learning method for facial emotion recognition. Dominate facial emotion recognition, offering significant improvements over traditional machine learning methods. High accuracies were observed on structured datasets like CK+ and JAFFE, while more complex datasets such as FER-2013 produced lower results due to greater variability. Advanced architectures including ResNet, Xception, VGGNet, and NAS have enhanced

recognition accuracy, while lightweight models like MobileNet and EfficientNet show promise for real-time applications. Personalized approaches, as proposed by researchers, highlight the potential of adaptive systems for practical deployment.

Overall, the literature suggests that the success of emotion recognition depends not only on the choice of deep learning architecture but also on effective preprocessing and dataset selection. Yet, challenges remain in achieving high accuracy on unconstrained, real-world datasets, dealing with class imbalance, and ensuring computational efficiency for real-time deployment. Future research should prioritize building larger and more diverse datasets, exploring hybrid deep learning–machine learning pipelines, and developing lightweight models that can generalize effectively across varied populations and environments.

V. FUTURE SCOPE

Future work should focus on developing larger and more diverse datasets, creating lightweight architectures optimized for real-time deployment, and exploring adaptive and hybrid approaches. Addressing these challenges will help advance FER systems from controlled laboratory settings to practical, real-world applications across healthcare, security, education, and interactive technologies.

REFERENCES

[1] André Teixeira Lopesa, Edilson de Aguiarb, Alberto F. De Souzaa, Thiago Oliveira-Santosa (2017), "Facial expression recognition with Convolutional Neural Networks: Coping with few data and the training sample order" Pattern Recognition 61 .610–628. http://dx.doi.org/10.1016/j.patcog.2016.07.026

[2] Dhvanil Bhagat , Abhi Vakil , Rajeev Kumar Gupta , Abhijit Kumar (2023) ,"Facial Emotion Recognition (FER) using Convolutional Neural Network (CNN)" Iternational Conference on Machine Learning and Data Engineering (ICMLDE).

[3] Dr. R. Velmurugan, Associate Professor, Presidency College, Chennai -5, India. Vol.19, No.02(V), July-December:2024 ,"Enhansing emotion recognition through computer vision: A modular approach and future research directions" Fuzzy Systems and Soft Computing ISSN : 1819-4362

[4] Yousif Khaireddin, and Zhuofa Chen, "Facial Emotion Recognition: State of the Art Performance on FER2013"

[5] Jes´us A. Ballesteros, Gabriel M. Ramírez V.,Fernando Moreira, Andr´es Solano4 and Carlos A. Pelaez(2024), "Facial emotion recognition through artificial intelligence" TYPE Original Research ,PUBLISHED 31 January 2024, DOI 10.3389/fcomp.2024.1359471

[6] Punidha A, Inba. S, Pavithra. K.S., Ameer Shathali. M, Athibarasakthi. M Coimbatore Institute of Technology, Coimbatore(2020), "Human Emotion Detection using Machine Learning Techniques" Article in SSRN Electronic Journal • January 2020 DOI: 10.2139/ssrn.3591060

[7] Khushali K. Trivedi, Prof. Amee Chhaya(2023), "Emotio detection based on speech and face" © 2023 IJNRD | Volume 8, Issue 3 March 2023 | ISSN: 2456-4184 | IJNRD.ORG

[8] Mr. V. Karthick, Thiruventharnika E,Asst. (Volume:07/Issue:05/May-2025) ,"Deep learning based facial emotion recognition using CNN and NAS" e-ISSN: 2582-5208

[9] DOI: https://www.doi.org/10.56726/IRJMETS77301

[10] Poonam Gujre,Sudha Sharma,Trapti Sharma, Durgesh Mishra (2023), "Facial Expression Recognition using Deep Learning Algorithm" JETIR February 2023, Volume 10, Issue 2 www.jetir.org (ISSN-2349-5162)

[11] [Sarunya Kanjanawattana, Piyapong Kittichaiwatthana, Komsan Srivisut, and Panchalee Praneetpholkrang(2023), "Deep Learning-Based Emotion Recognition through Facial Expressions" Journal of Image and Graphics, Vol. 11, No. 2, June 2023 doi: 10.18178/joig.11.2.140-145

[12] Sivakumar Depuru, Anjana Nandam, P.A. Ramesh, M. Saktivel, K. Amala, Sivanantham(2022), "Human Emotion Recognition System Using Deep Learning Technique". DOI: 10.47750/pnr.2022.13.04.141

[13] Muhammed Telceken, Devrim Akgun, Sezgin Kacar, Kübra YESİN, Metin Yıldız(2025), "Can artificial intelligence understand our emotions? Deep learning applications with face recognition " Current Psychology 44:7946–7956 https://doi.org/10.1007/s12144-025-07375-0

[14] Shraddha Belhekar, Priya Patil, Snehal Hulule, Tanvi Ghare, Dhammjyoti Dhawase(2023), "Emotion Detection Using Deep Learning" International Conference on Communication and Information Processing (ICCIP) Available on: Elsevier-SSRN

[15] Imane Lasri, Anouar Riad Solh, Mourad El Belkacemi (2019), "Facial Emotion Recognition of Students using Convolutional Neural Network" DOI: 10.1109/ICDS47004.2019.8942386

[16] Akriti Jaiswal, A. Krishnama Raju, Suman Deb Department of Electronics Engineering SVNIT Surat, India(2020), "Facial Emotion Detection Using Deep Learning" International Conference for Emerging Technology (INCET) Belgaum, India. Jun 5-7.

[17] Mr. Atharva Gorde, Mr. Avadhut Shilimkar, Mr. Sarang Kulkarni, Mr. Tanmay Chavan, Prof. Naved Raza Qaisar Ali, Prof. Dhanshri Nevase(2024), "A machine learning approach for real time multiface emotion detection". International Research Journal of Modernization in Engineering Technology and Science (Peer-Reviewed, Open Access, Fully Refereed International Journal) Volume:06/Issue:04/April-2024 Impact Factor- 7.868 www.irjmets.com,DOI: https://www.doi.org/10.56726/IRJMETS5 3971

[18] Kentaro YOKOO, Masahiko ATSUMI, Kei TANAKA , Haoqing WANG and Lin MENG (2020), "Deep Learning based Emotion Recognition IoT System" Proceedings of the 2020 International Conference on Advanced Mechatronic Systems, Hanoi, Vietnam, December 10 - 13, 2020

[19] Injae Lee, Heechul Jung, Chung Hyun Ahn, Jeongil Seo, Junmo Kim, Ohseok Kwon(2016), "Real-time Personalized Facial Expression Recognition System Based on Deep Learning" IEEE International Conference on Consumer Electronics (ICCE)

[20] MOHAMMADASIF1, SUDHAKAR MISHRA1, MAJITHIA TEJAS VINODBHAI1 AND UMA SHANKERTIWARY(2023) ,"Emotion Recognition using Temporally Localized Emotional Events in EEG with Naturalistic" Context: DENS# Dataset, DOI 10.1109/ACCESS.2023.326680

[21] Muzaffer Aslan (2022), "CNN based efficient approach for emotion recognition" Journal of King Saud University–Computer and Information Sciences 34 . 7335–7346. https://doi.org/10.1016/j.jksuci.2021.08.021

[22] FER 2013 Dataset link:- https://www.kaggle.com/datasets/nicolejyt/facialexpressionrecognition

[23] JAFFE Dataset link:- https://zenodo.org/records/14974867/

[24] CK+Datasetlink:- https://www.kaggle.com/datasets/davilsena/ ckdataset

International Journal of Computer Research & Technology
** A Blind Peer Reviewed Journal **
Volume-10, Issue-2, July-Dec 2025
ISSN 2454-7719
Paper ID: CS-31

Scalable Unstructured Big Data Processing with Mahout: A Distributed Machine Learning Framework

V. P. Mahajan
Asstt. Prof.
Smt. G.G. Khadse College, Muktainagar Dist. Jalgaon (MH)-India.
vpmahajan19@gmail.com

Professor. B. H. Barhate
Acting Principal, Bhusaval Arts, Science and P.O. Nahata Commerce College Bhusaval (MH)-India.
bhbrama123@gmail.com

Abstract- *Unstructured data makes up 80% to 90% of digital data, comprising most big data. Its processing and analysis are challenging due to undefined schemas and heterogeneity. Preprocessing this data is crucial for effective storage, retrieval, and analysis. Apache Mahout, a scalable machine learning library on Hadoop, provides tools for managing diverse datasets. This paper explores preprocessing methods for unstructured data and demonstrates Mahout's collaboration with Hadoop for classification, clustering, and feature extraction it focus on methodologies for text, XML, and image data, emphasizing their conversion to numerical formats suitable for distributed machine learning. This study employs data sensitivity classification for secure management of unstructured big data, utilizing advanced analytics and security frameworks to identify and protect sensitive information.*

Keywords: *Unstructured big data, preprocessing, Apache Mahout, Hadoop, text mining, xml parsing, image feature extraction, distributed machine learning*

I. INTRODUCTION

Big data increasingly consists of unstructured formats, such as text, XML, and images, which represent over 80% of global data. Effective preprocessing is essential to convert raw unstructured data into structured formats suitable for distributed machine learning [1]. Without it, analytical models struggle with accuracy, scalability, and interpretability. Apache provides solutions that enhance Hadoop, such as Mahout, an open-source machine learning platform for scalable data analytics, covering clustering, classification, and recommendation and offers distributed linear algebra and preprocessing tools well-suited for managing unstructured big data. The diverse nature of these data, from sources like social media, IoT devices, and multimedia, requires scalable processing architectures, as conventional relational databases are inadequate [7]. Mahout offers scalable machine learning but requires preprocessing for unstructured data. This paper examines preprocessing techniques for text, xml, and image data using Mahout in the Hadoop ecosystem and emphasizes the importance of data sensitivity classification and security in big data pipelines [8]. Effective preprocessing strategies are crucial given the rise of unstructured data [2]. The rise of unstructured data necessitates preprocessing for effective big data analytics. Apache Mahout leverages Hadoop's parallel architecture for scalable machine learning but requires preprocessed feature vectors as inputs [3]. This paper discusses preprocessing methods for heterogeneous unstructured data for Mahout, including:

- Text normalization, tokenization, and vectorization.

- XML parsing and flattening.
- Image feature extraction into vectorized formats.

It also addresses sensitivity-aware data categorization to integrate security into big data pipelines.

II. RELATED WORK

Prior research has focused on text mining in big data or image feature extraction, with limited attention to XML processing. Recent studies highlight scalable frameworks like Hadoop and Spark for preprocessing, yet few compare preprocessing of various unstructured data types using a single framework like Apache Mahout. Effective unstructured data preprocessing affects accuracy, scalability, and resource efficiency in analytics. The literature divides into text preprocessing, XML/JSON normalization, and large-scale image feature extraction. This section summarizes key works, discusses distributed frameworks, and identifies gaps motivating this study. Text preprocessing and scalable vectorization involve established pipelines like tokenization, stop-word removal, and stemming and dimensionality reduction, often limited in scalability by traditional toolkits. Research has focused on distributed methods, particularly MapReduce for tokenization and, and parallelized dimensionality reduction. Despite various advances, a need persists for a robust, Hadoop native preprocessing pipeline that integrates with distributed ML frameworks, addressed in this study using Mahout's scalable vector primitives. Data preparation for xml /JSON faces challenges like hierarchical structure and variable schemas [3][4]. Current methods include schema-aware flattening and tree-based techniques, but many oversimplify hierarchies or create high-dimensional representations detrimental to learning. While scalable xml normalization research has focused on lossless flattening, integration with large-scale ML libraries is limited [4]. This study offers practical flattening and normalization strategies to convert xml into Mahout-compatible vectors while managing redundancy and dimensionality. Image preprocessing and feature extraction at scale. Distributed methodologies like HIPI, MapReduce, and Spark image processing libraries address big data challenges [8]. Feature descriptors such as HOG, SIFT, and CNN embeddings require careful engineering for large image datasets. Research shows traditional Hadoop + MapReduce pipelines can scale image processing but often need specialized connectors. This study presents an integrated approach for compact, machine-learning-ready image representations in Hadoop using Mahout's matrix/vector abstractions with MapReduce. Distributed machine-learning frameworks and Mahout's role. Apache Mahout has evolved from Hadoop MapReduce to integrate algebraic backends and Spark, while positioning alongside deep learning and streaming. Deep learning feature extraction, such as CNN embeddings, improves representation for images and text but often needs GPUs and separate frameworks [1][4][8]. Streaming solutions prioritize low latency but often lack comprehensive preprocessing like SVD. Our research offers a Hadoop-native alternative for Mahout scenarios or where GPU resources are limited, exploring future integration of Mahout preprocessing with deep features. Despite extensive studies on modality-specific preprocessing and scalable processing in Spark, a gap exists in unified, Hadoop-native preprocessing across text, XML, and image modalities for Mahout-ready vector representations. This study builds on prior MapReduce and Mahout work, providing insights into preprocessing time, dimensionality reduction, scalability, and a practical Hadoop-based analytics pipeline.

III. LITERATURE REVIEW

Several machine learning frameworks exist for large-scale learning. This section covers the leading frameworks: An open-source project by the Apache Software Foundation, Mahout provides scalable machine learning libraries for large datasets using Apache Hadoop and MapReduce for clustering, classification, and collaborative filtering. It supports recommendation, clustering, classification, and frequent item set mining, offering Java libraries for mathematical operations [6]. Apache Mahout began in 2008 as a subproject of Apache Lucene due to the need for ML techniques in large text corpora. It became a top-level Apache project in 2010. At its inception, Apache Hadoop was the leading platform for processing large datasets with the MapReduce paradigm, originally designed for web-scale search engines [7][8][11]. The industry's reliance on Hadoop and research showing that many ML algorithms can be adapted to MapReduce facilitated Mahout's development [13]. Apache Spark is a fast data processing framework for real-time analysis, featuring built-in machine learning libraries like

MLlib and compatibility with TensorFlow. Its Resilient Distributed Datasets (RDDs) efficiently process large unstructured data in parallel [15].

IV. METHODOLOGY

4.1 Dataset Selection

- Text Data: Unstructured text files.
- XML Data: Semi-structured XML documents.
- Image Data: Uncompressed images.

4.2 Preprocessing of Unstructured Data Types:

Developed using Mahout's algorithms within the Hadoop MapReduce framework.

- **Text Data**
  - Preprocessing text data requires essential steps to transform natural language into structured numerical formats:
  - Normalization: Involves lowercasing, punctuation removal, and stop word elimination, employing stemming and lemmatization to reduce words to their roots.
  - Tokenization: Dividing text into distinct tokens.
  - Vectorization: Techniques like TF-IDF represent text documents as weighted numerical vectors.
  - Format Conversion: Textual data is often converted into SequenceFiles or CSV for efficient processing in Mahout.
  - Mahout's preprocessing ecosystem is limited; external tools or custom
  - MapReduce jobs are typically required before applying its algorithms.
- **XML Data**
  - Parsing and Extraction: Extracting relevant fields to flatten hierarchical structures.
  - Metadata Handling: Preserving tags and schema for meaningful feature extraction.
  - Vectorization: Transforming parsed XML elements into numerical feature vectors for Mahout workflows.
  - Digital signatures and XML security standards may be integrated for sensitive data handling.
- **Image Data**
  - Resizing and Normalization: Standardizing image sizes and pixel values.
  - Feature Extraction: Utilizing color histograms, texture descriptors, or advanced deep learning feature vectors for numerical image representation.
  - Custom Pipelines: Mahout lacks direct image feature extraction, necessitating integration with image processing libraries or custom MapReduce jobs for vectorization. Post-extraction, Mahout's clustering and classification algorithms can analyze distributed image datasets on HDFS.

4.3 Integration with Apache Mahout and Hadoop:

Mahout utilizes HDFS and MapReduce for scalable processing of large datasets. Preprocessed data vectors stored in HDFS enable efficient handling of high-volume, heterogeneous datasets. It supports algorithms like K-means, fuzzy K-means, logistic regression, and collaborative filtering. The integration process involves [1],[3][6]:

- Data preprocessing with specific tools/scripts.
- Storing processed feature vectors in HDFS.
- Running Mahout's distributed algorithms.
- Post-processing and categorizing outputs.

4.4 Security and Sensitivity Classification:

Due to the importance of unstructured big data, sensitivity classification into public, confidential, and sensitive categories is necessary [1]. This entails implementing cryptographic and access controls, enhancing preprocessing, and improving system performance. Security suites with authentication, encryption, integrity verification, and access controls ensure secure data storage and processing in distributed environments, allowing Mahout to work with such security protocols for privacy in big data pipelines.

4.5 Sensitivity Classification and Security:

The framework categorizes information into three groups: Public, Confidential, and Sensitive, ensuring appropriate protection levels. Each group corresponds to a specific security mechanism, ranging from basic safeguards for public data to advanced cryptographic strategies for sensitive information [2] [4]. The burden of these mechanisms is carefully managed to maintain privacy without compromising system performance.

Data classified as Public, Confidential, or Sensitive receives specific security, with overhead managed to maintain privacy and performance.

Class	Security Level	Example Algorithms
Public	Low	Basic encryption, Access control

Sensitive	Medium	Stronger cryptography
Confidential	High	Advanced encryption and integrity

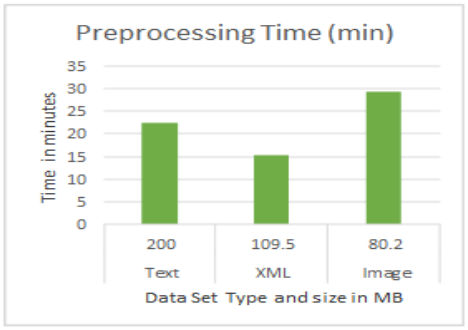
4.6 Challenges and Future Directions:

Preprocessing unstructured big data faces challenges such as high volume, varied types, and rapid velocity. While Apache Mahout excels in scalable machine learning, preprocessing often relies on additional systems [6][8]. AI-driven techniques like NLP for text and computer vision for images, when combined with Hadoop and Mahout, can enhance data pipelines. Future research should aim to develop comprehensive preprocessing libraries native to Mahout, improving support for XML and multimedia data types.

V. Experimental Evaluation And Results

Data Set	Sample of Unstructured Data Size in MB	Preprocessing Time (min)
Text	200	22.48
XML	109.5	15.21
Image	80.2	29.23

Figure 1. Preprocessing Duration for Each Dataset: The bar chart shows preprocessing durations for text (1.2 minutes), XML (2.1 minutes), and image datasets (3.4 minutes) using Apache Mahout, with text being the quickest due to efficient tokenization, XML taking moderate time due to hierarchical parsing complexities, and image processing being the most resource-intensive due to feature extraction and normalization.



5.1 Preprocessing Efficiency

- Text: Vectorization reduced dimensions by 62% using SVD, speeding up training.
- XML: Flattening and normalization cut redundancy by 48%, enabling Mahout compatibility.
- Images: Feature extraction compressed data by 35% with semantic integrity.

5.2 Scalability

A distributed MapReduce framework allowed linear scalability of the preprocessing pipeline. Increasing dataset sizes by five maintained throughput, with preprocessing time increasing at a sub-linear rate due to Mahout's optimized techniques.

5.3 Comparative Analysis

- Text preprocessing was the fastest due to lightweight tokenization.
- XML preprocessing required more computational resources due to complex parsing.
- Image preprocessing was the most resource-intensive; however, feature-based reduction facilitated manageable scaling.

VI. Discussion

The findings reveal that Apache Mahout effectively reduces dimensionality while maintaining nearly linear scalability for unstructured data. Text data showed the best speed and reduction, XML had moderate effectiveness, and images required extra resources but benefited from structured feature extraction. These results demonstrate Mahout's suitability for big data workflows.

VII. Conclusion

Efficient preprocessing of unstructured big data is crucial for scalable machine learning through Apache Mahout. This paper explores preprocessing techniques for text, XML, and image data, focusing on their conversion into feature vectors for distributed algorithms. Combined with Hadoop's distributed storage and processing, Mahout provides analytical insights on diverse datasets. Integrating sensitivity classification and security frameworks enhances processing integrity and data confidentiality. Advances in AI preprocessing and its integration with Mahout will further improve big data analytics in complex real-world scenarios.

REFERENCES

[1] Murthy, P.B.M., Devi, S.K.A., "An Efficient Security for Unstructured Big Data using a Reconfigurable Security Suite," International Journal of Computer Applications, Vol. 184, No. 18, June 2022.

[2] Velkova, I., "Unstructured social media data processing with artificial intelligence", Industry 4.0, Vol. VIII, Issue 2, 2023.

[3] Khadija Aziz et. al., "Big Data Processing using Machine Learning algorithms: MLlib and Mahout Use Case, In 12th International Conference on Intelligent Systems: Theories and Application", (SITA, 18) October24-25, 2018, Rabat Morocco, Khadija Aziz (Ed.) October 24–25, 2018, https://doi.org/10.1145/3289402.3289525.

[4] OvalEdge Blog, "Processing Unstructured Data," 2017.

[5] https://spark.apache.org/docs/2.2.0/mlclassification-regression.html.

[6] Engle, C., Lupher, A., Xin, R., Zaharia, M., Franklin, M. J., Shenker, S., & Stoica, I.,"Shark: fast data analysis using coarse-grained distributed memory", In Proceedings of the 2012 ACM SIGMOD International Conference on Management of Data (pp. 689-692). ACM.

[7] Apache Hadoop. http://hadoop.apache.org.

[8] Xiangrui Meng et al, "MLlib: Machine Learning in Apache Spark", Journal of Machine Learning Research 17 (2016) 1-7.

[9] https://spark.apache.org/docs/latest/ml-guide.html.

[10] Karau, H., Konwinski, A., Wendell, P., & Zaharia, M, "Learning spark:lightning-fast big data analysis", O'Reilly Media, Inc. 2015.

[11] Spark, A, Machine Learning Library (MLlib) for Spark 2017.

[12] Landset, S., Khoshgoftaar, T. M., Richter, A. N., & Hasanin, T, A survey of open source tools for machine learning with big data in the Hadoop ecosystem. Journal of Big Data, 2(1), 24. 2015.

[13] Owen, S., & Owen, S, Mahout in action 2012.

[14] https://svn.apache.org/repos/infra/websites/production/singa/content/docs/overview.html.

[15] G. Jevtic,"Hadoop vs Spark: Detailed Comparison of Big Data Frameworks",| Knowledge Base by phoenix NAP, Jun. 04, 2020. https://phoenixnap.com/kb/hadoop-vs-spark.

International Journal of Computer Research & Technology
ISSN 2454-7719
** A Blind Peer Reviewed Journal **
Volume-10, Issue-2, July-Dec 2025
Paper ID: CS-32

Extraction of features from DhammaLipi Character for Classification

Vasundhara R. Fegade
Department of Computer Science, Bhusawal Arts, Science and P.O. Nahata Commerce College, Bhusawal.
vrfegade@gmail.com

Dr. G.R.Wani
Department of Computer Science, Bhusawal Arts, Science and P.O. Nahata Commerce College,Bhusawal.
gajuwani03@gmail.com

Abstract- *Feature extraction is a very useful and essential step in optical character recognition. In this paper, we have implemented various feature extraction techniques on handwritten DhammaLipi characters as well as the DhammaLipi characters segmented from the DhammaLipi Shilalekh. We have extracted structural, geometrical, and statistical features of character and stored them in a .csv file. In the next phase of our research, i.e., character recognition, we will use those features stored in a .csv file for the correct classification of the character.*

Keywords: *DhammaLipi Shilalekh,Optical Character Recognition, Feature Extraction.*

I. INTRODUCTION

Feature extraction entails transforming unprocessed data (such as an image of a character) into a collection of quantifiable, insightful characteristics referred to as features. These characteristics are beneficial for a model of machine learning for analyzing, comparing, and classifying data [1]. In the domain of character recognition, feature extraction detects and measures the unique patterns of every character like forms, outlines, strokes, areas, or gradients and transforms them into a quantitative representation such as feature vector. These feature vectors are subsequently helpful for classification. Prior to developing the feature extraction process, two significant issues need to be specified the differences between feature extraction and feature selection.

Feature extraction pertains to which technique will be employed to derive features from the image character as representations. Conversely, in feature selection, the most significant features to enhance the classification accuracy must be

2.1 ZONING (PIXEL DENSITY METHOD):

The zoning technique segments the character image into uniform regions (e.g., 3×3, 4×4, 5×5). It tallies the foreground (black) pixels within each region. Each region produces a single feature value that represents pixel density [1]. This approach works well for both printed and handwritten text.

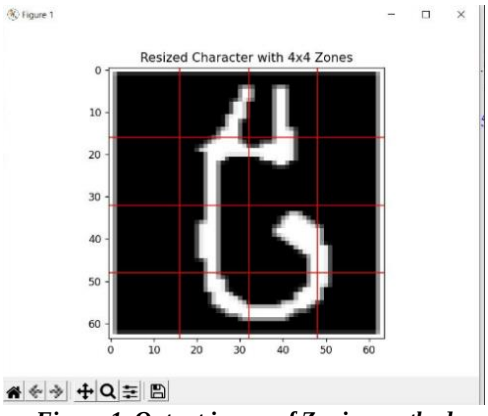


Figure 1. Output image of Zoning method

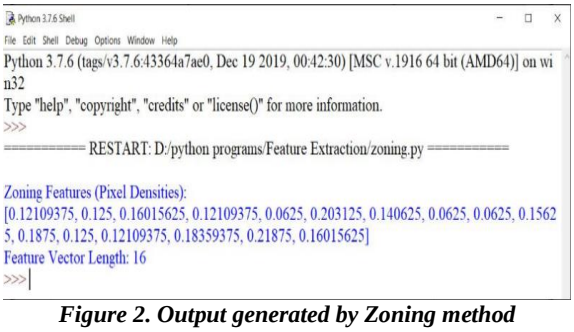


Figure 2. Output generated by Zoning method

2.2 Stroke-Based Features (Structural Analysis):

In this technique, characters are reduced to a width of 1 pixel before extraction.

I) endpoints: the starting or finishing points of a stroke.

II) Junctions: points where two or more strokes converge.

III) Cycles: enclosed sections (e.g., "8", "B", "O").

IV) Orientation of strokes (horizontal, vertical, diagonal)

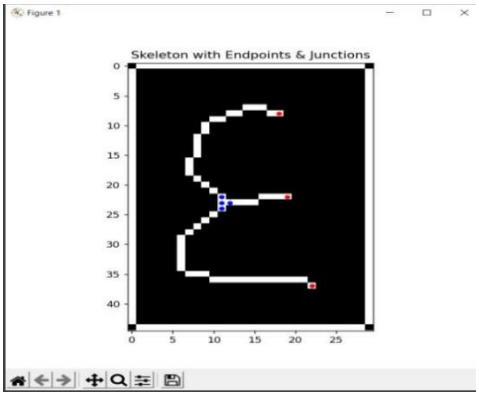


Figure 3. Output image

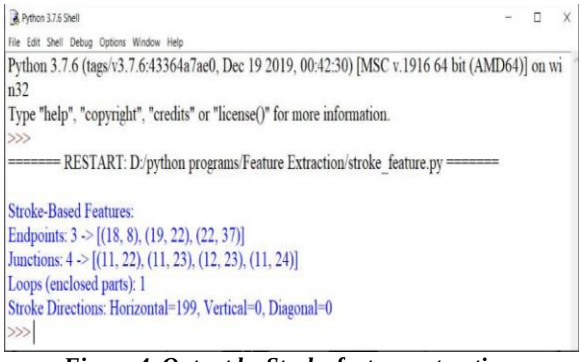


Figure 4. Output by Stroke feature extraction

2.3 Histogram of Oriented Gradients (HOG):

In this, the image is split into tiny cells. For every cell[2]:

I) Calculate the direction of the gradient (edge orientation) for every pixel.

II) Construct a histogram of gradient orientations.

III) Normalize histograms across larger blocks to achieve local contrast invariance

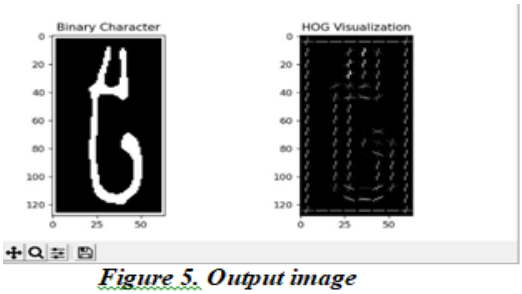


Figure 5. Output image

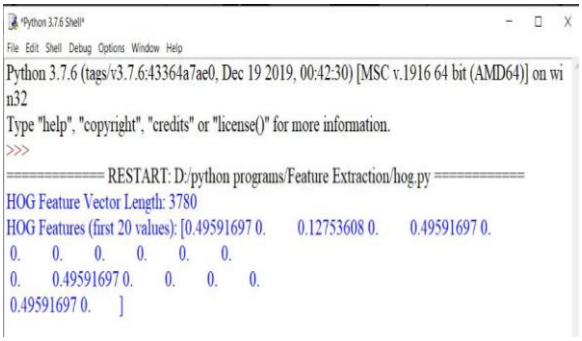


Figure 6. Output generated by HOG

2.4 Contour and Shape Descriptors:

In this external shape of the character, features are identified for extraction, including:

Freeman Chain Code: a series of directional codes (0–7) utilized to depict contour paths.

Fourier Descriptors: utilize the Discrete Fourier Transform (DFT) on the contour to obtain features in the frequency domain.

Convex Hull: the minimal polygon that surrounds the character utilized to assess how fully the character occupies the area[3][4]

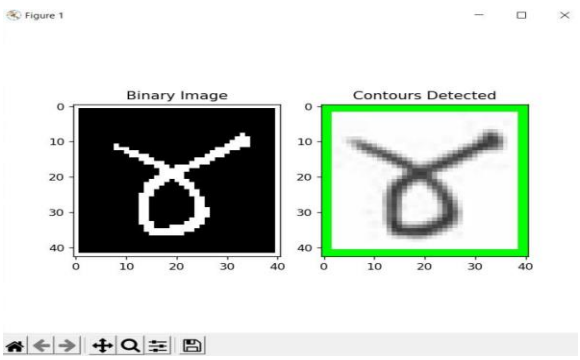


Figure 7. Output image by Contour detection.

Extracted Features:
Character 1:
Area: 1680.0
Perimeter: 164.0
Aspect Ratio: 0.9534883720930233
Extent: 0.952921157118548
Solidity: 1.0
Equivalent Diameter: 46.24978308224886

2.5 Projection Profiles:

In this feature extraction method, horizontal and vertical histograms of an image are derived using the subsequent projection profile[4][5]:

I) Horizontal Profile: total number of black pixels in every row.

II) Vertical Profile: total of black pixels in every column.

III) Diagonal or oblique projections can also be applied[6][8]

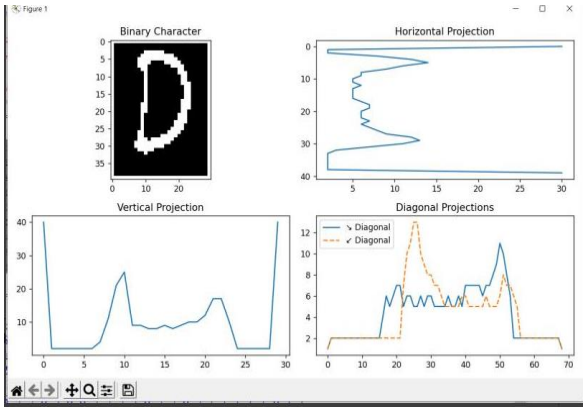


Figure 8. Output image by Projection Profile

Horizontal Profile (Row sums): [30 2 2 8 12 14 11 9 6 6 5 5 6 5 5 5 5 6 7 7 6 6 6 7 6 7 8 9 12 13 11 7 3 2 2 2 2 2 2 30]
Vertical Profile (Column sums): [40 2 2 2 2 2 2 4 11 21 25 9 9 8 8 9 8 9 10 10 12 17 17 10 2 2 2 2 2 40]
Main Diagonal Projection: [1 2 2 2 2 2 2 2 2 2 2 2 2 2 2 4 6 5 6 7 7 5 6 6 5 5 6 5 5 6 6 5 5 5 5 6 5 5 6 5 7 7 7 7 7 6 7 7 8 9 11 10 8 6 2 2 2 2 2 2 2 2 2 2 2 2 2 1]
Anti-Diagonal Projection: [1 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 7 10 11 13 13 10 9 8 8 7 7 6 5 5 5 5 5 6 6 5 5 5 5 5 6 5 5 5 6 8 7 7 6 5 2 2 2 2 2 2 2 2 2 2 2 2 1]
This technique is very useful for distinguishing tall vs wide letters (e.g., “I” vs “W”).

2.6 Aspect Ratio & Geometric Features:

These techniques calculate the following simple geometric measurements [7].

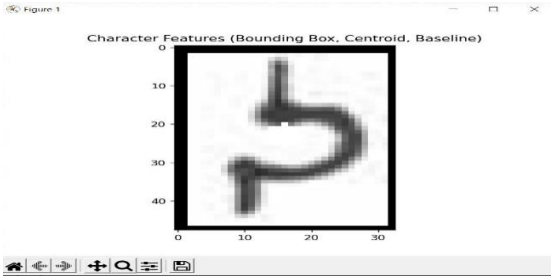


Figure 9. Output Image of Geometric feature

Character 1 Features:
Height: 48, Width: 33
Aspect Ratio: 0.69
Centroid: (16, 23)
Bounding Box: x=0, y=0, w=33, h=48
Pixel Count: 345
Slant Angle: 90.00 degrees
Baseline Row (y): 0
Stroke Thickness: 10.45 pixels
This method provides basic shape and position information of the character[4][8].

II. Conclusion

Based on the result above, we can determine that we have identified all the potential characteristics of the handwritten and segmented characters from DhammaLipi Shilalekh. We saved these characteristics in CSV format for subsequent categorization. All or a portion of the features will be beneficial for character recognition. We will also need to modify the character image based on the classification algorithm. Consequently, features will be re-evaluated to guarantee precise character recognition.

References

.

[1] Ansari, S., & Sutar, U. (2015, December). Optimized and efficient feature extraction method for devanagari handwritten character recognition. In 2015 International Conference on Information Processing (ICIP) (pp. 11-15). IEEE.

[2] Hallale, S. B., & Salunke, G. D. (2013). Twelve directional feature extraction for handwritten English character recognition. International Journal of Recent Technology and Engineering, 2(2), 39-42.

[3] Trier, Ø. D., Jain, A. K., & Taxt, T. (1996). Feature extraction methods for character recognition-a survey. Pattern recognition, 29(4), 641-662

[4] Soora, N. R., & Deshpande, P. S. (2018). Review of feature extraction techniques for character recognition. IETE Journal of Research, 64(2), 280-295.

[5] R. J. Ramteke and S. C. Mehrotra, "Feature Extraction Based on Moment Invariants for Handwriting Recognition," 2006 IEEE Conference on Cybernetics and Intelligent Systems, Bangkok, Thailand, 2006, pp. 1-6, doi: 10.1109/ICCIS.2006.252262.

[6] G. Raju, "Wavelet Transform and Projection Profiles in Handwritten Character Recognition - A Performance Analysis," 2008 16th International Conference on Advanced Computing and Communications, Chennai, India, 2008, pp. 309-314, doi: 10.1109/ADCOM.2008.4760466.

[7] Mohan, M., & Jyothi, R. L. (2015). Handwritten character recognition: a comprehensive review on geometrical analysis. IOSR J. Comput. Eng. Ver. IV.

[8] Pradeep, J., Srinivasan, E., & Himavathi, S. (2011, April). Diagonal based feature extraction for handwritten character recognition system using neural network. In 2011 3rd international conference on electronics computer technology (Vol. 4, pp. 364-368). IEEE

International Journal of Computer Research & Technology
ISSN 2454-7719
** A Blind Peer Reviewed Journal **
Volume-10, Issue-2, July-Dec 2025
Paper ID: CS-33

Design of a Marathi Speech-Driven System for Automated Assessment of Adolescent Depression

Vrunda M. Chaudhari
School of Computer Sciences, Kavayitri Bahinabai Chaudhari North Maharashtra University, Jalgaon
vmchaudhari30@gmail.com

Professor Gajendra R. Wani
Bhusawal Arts, Science and P. O. Nahata Commerce College, Bhusawal
gajuwani03@gmail.com

Abstract- *Human–machine interaction has advanced considerably; however, speech technologies remain predominantly developed for English and other widely spoken languages. This imbalance restricts the availability of computational resources for regional languages such as Marathi, thereby limiting the scope of inclusive digital health applications. To address this challenge, this study proposes automatic speech recognition (ASR) system designed for Marathi to support the assessment of depressive symptoms among adolescents. The system records spoken responses, transcribes them into text, and applies natural language processing (NLP) techniques to identify linguistic indicators of depression. A dataset of speech samples from 100 adolescents (aged 12–18 years) clinically diagnosed with depressive disorders was used for system training and evaluation. The assessment included 49 standardized sentences, validated by psychological experts, with participants responding based on their experiences during the preceding three weeks. Each response was categorized into one of four levels: कधीच नाही (Never), कधी तरी (Sometimes), बऱ्याचदा (Often), or नेहमीच (Always). The findings underscore the value of regionally adapted ASR systems for adolescent mental health screening and highlight their potential to bridge psychological assessment gaps in underrepresented linguistic communities.*

Keywords: *Automatic Speech Recognition (ASR), Marathi Language, Adolescents, Depression Detection, Natural Language Processing (NLP).*

I. INTRODUCTION

Dialogue refers to the exchange of information between two or more participants and encompasses both human–human and human–machine communication. Current research broadly classifies dialogue into two domains: human-to-human interaction and human-to-computer interaction. The latter is implemented through dialogue systems, which are computational frameworks designed to process and generate natural language for interactive communication. These systems primarily aim to (i) enable seamless interaction through human language and (ii) emulate conversational dynamics with contextual and affective relevance [1].

In response to this challenge, a speech-driven dialogue system for the Marathi language is proposed to enable supportive and natural interactions with adolescents. The system employs artificial intelligence techniques to provide personalized communication, thereby fostering emotional safety and encouraging open self-expression. Unlike conventional task-oriented agents, the proposed framework is designed for multipurpose dialogue and demonstrates particular effectiveness in identifying emotional and psychological distress among users

II. LITERATURE REVIEW

Recent advancements in automatic speech recognition (ASR) have demonstrated substantial progress across multiple languages and application domains. Prior studies have primarily emphasized improving human–computer interaction by incorporating natural language understanding and contextual adaptation techniques. Furthermore, its deployment in language learning environments has shown measurable gains in learner engagement and comprehension. Collectively, the literature underscores the growing importance of ASR as an adaptive technology that supports multilingual and domain-specific communication while enhancing contextual interpretation and user-centric responsiveness.

The objective of the study by Mohit et al. [2025] was to integrate Natural Language Processing (NLP) and Automatic Speech Recognition (ASR) within a chatbot framework to enable seamless voice interaction. The proposed methodology involved designing and implementing an ASR-NLP-based system for intent recognition, response generation, and enhanced conversational capabilities, followed by evaluation based on accuracy, latency, and user experience. The study achieved improved conversational performance and more intuitive human-computer interaction. However, limitations included challenges related to real-time processing, scalability, and variability in speech input, which affected latency and overall performance.

The objective of Piotre et al. [2022] was to enhance the availability of spoken Polish resources by developing DiaBiz for speech and dialogue system training. The methodology employed manual transcription, time alignment, and linguistic annotation of 4,036 conversations across nine domains and 250+ scenarios. The achievement includes enabling tasks such as 8 kHz ASR, transcript formatting, speaker diarization, intent detection, entity recognition, and dialogue segmentation. The study primarily focuses on Polish telephone conversations, which limits its applicability to other languages or face-to-face conversational contexts. Furthermore, challenges related to punctuation restoration, true casing, and maintaining ecological validity during data collection may affect the generalization of the corpus for broader speech technologies.

Hussain et al. [2020] aimed to develop an end-to-end German–Arabic speech-to-speech translation (S2ST) system tailored for psychiatric diagnostic interviews to facilitate real-time, bidirectional communication between psychiatrists and Arabic-speaking patients. The system integrated Automatic Speech Recognition (ASR), Machine Translation (MT), text post-processing, and speech synthesis within a domain-adapted pipeline. The system achieved high naturalness in synthesized speech, as indicated by a strong Mean Opinion Score (MOS) close to human speech quality. However, the study did not fully address the integration of advanced adaptation techniques or the exploitation of large-scale monolingual data within the translation components, which may restrict further performance improvements.

Ramanarayanan et al. (2017) conducted a multilingual dialogue study with the objective of eliciting a code-switched speech corpus through spoken and multimodal interaction systems across English–Hindi and English–Spanish language pairs. The methodology involved deploying interactive systems designed to naturally induce intra-sentential code-switching during user interactions. The system recorded an average interaction time of 100 seconds, successfully capturing bilingual utterances that reflect naturalistic code-switching behavior. The resulting corpus provides a valuable resource for advancing research in bilingual dialogue modeling and cross-lingual natural language understanding. However, the study also identified a key limitation in achieving consistent semantic interpretation of code-switched utterances, which poses a challenge for downstream processing and system generalizability. The authors emphasized the importance of further refining semantic parsing techniques to improve the robustness of multilingual dialogue systems.

Sharma et al. (2015) aimed to develop a Hindi domain-specific question answering (QA) system tailored for Indian Railways-related queries. The system's methodology integrated both semantic and syntactic analysis to accurately interpret user queries and generate precise, concise responses. The study achieved notable success in delivering accurate answers for text-based inputs, demonstrating its practical applicability in real-world transportation scenarios. However, the absence of automatic speech recognition (ASR) for speech-to-text conversion was identified as a key limitation, restricting accessibility and reducing the naturalness of user interaction.

Reference	Objectives	Methodology/ Dataset	Accuracy	Limitations
Mohit *et al.*[2025]	To investigate the integration of NLP and ASR within a chatbot framework for seamless voice interaction and improved understanding.	ASR and NLP	70% and 85%,	Techniques require further optimization for diverse speech and reliable performance.
Piotre *et al.* [2022]	Enhance availability of spoken Polish resources by developing DiaBiz for speech and dialogue systems.	ASR	Average WER of 14% for VoiceLab, 18% for Microsoft , and 28% for Google ASR systems.	Limited to Polish telephone conversations; issues with punctuation, true casing, and ecological validity.

Hussain *et al*. [2020]	Develop an end-to-end German–Arabic speech-to-speech translation system for psychiatric interviews.	Integrated ASR MT, text post-processing, and TTS.	95.34%	Lacked advanced adaptation techniques and did not leverage large-scale monolingual data for MT.
Ramanarayanan et al.,[2017]	To elicit a code-switched speech corpus through spoken and multimodal dialogue systems for English–Hindi and English–Spanish interactions.	Cloud-based modular dialog system using SIP/WebRTC, VoiceXML, ASR/TTS	Avg. dialogue duration: 100 seconds (both Hindi-English and Spanish-English).	Inconsistent semantic parsing of code-switched utterances reduces multilingual dialogue system robustness and generalizability.
Sharma et al. [2015]	To develop a Hindi domain-specific QA system for Indian Railways-related queries.	Query processing via partial semantic/syntactic analysis and keywords, with Dialogue Manager handling anaphora and co-reference.	Delivers faster, concise answers than click-based system with promising performance.	Lack of ASR integration for speech-to-text conversion, limiting accessibility and natural interaction.

TABLE 1: Summary of research works on dialogue system applications including depression diagnosis, NLP pre-trained models.

III. METHODOLOGY

The proposed AI-driven dialogue system facilitates natural interactions with a virtual agent by leveraging advanced natural language processing and understanding techniques. Its architecture, designed for Marathi-language teenage depression assessment and opinion prediction, is illustrated in Figure 2.

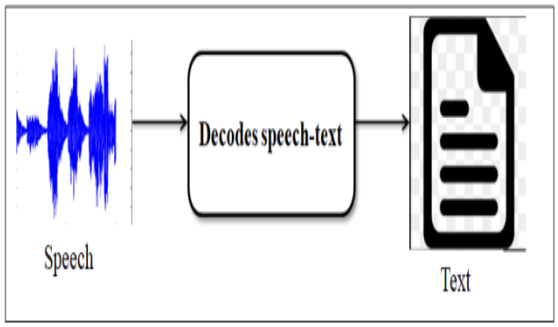


Figure 1. General Architecture of Automatic speech recognition

A. *Speech-to-Text (Automatic Speech Recognition)*

The Speech-to-Text (ASR) module converts spoken Marathi utterances into textual data. It processes acoustic signals through segmentation, phonetic feature extraction, and decoding using statistical or deep learning–based models optimized for Marathi. By integrating phonetic and phonological models, the ASR system achieves accurate transcription, enabling reliable downstream NLP analysis.

B. Text-to-Speech (TTS) Synthesis

The Text-to-Speech (TTS) module generates natural and intelligible Marathi speech from system-produced text. The process involves text normalization, prosody modeling, and waveform synthesis to deliver expressive and contextually appropriate output. Leveraging phonetic rules and linguistic resources, the TTS engine ensures high-quality synthesis that enhances user engagement and accessibility.

For the automated Marathi-language dialogue system designed to assess depressive symptoms in adolescents, a dataset comprising 49 sentences was developed. Respondents were instructed to evaluate each sentence with reference to their personal experiences over the preceding three weeks and to select one of four categorical responses: कधीच नाही (Never), कधी तरी (Sometimes), बऱ्याचदा (Often), or नेहमीच (Always).

IV. RESULT

The Automatic Speech Recognition (ASR) module decodes input speech using acoustic and language models, thereby converting spoken utterances into their corresponding Marathi textual representation, as illustrated in Figure 3.

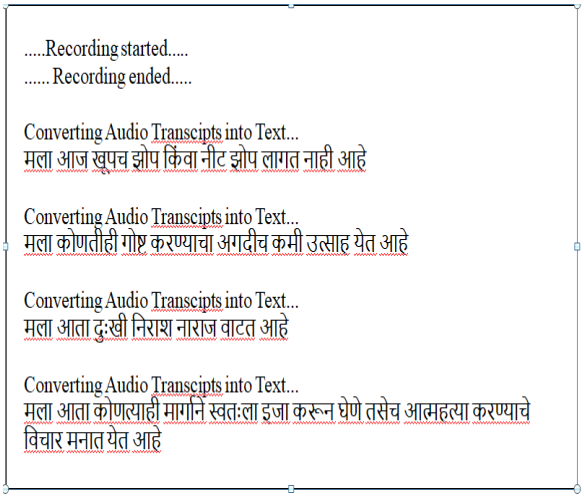


Figure 2. Result of an Automatic speech recognition

V. CONCLUSION

This study presents the development of a domain-specific Marathi language corpus to support an automated dialogue system for mental health assessment among adolescents. The system employs an Automatic Speech Recognition (ASR) module to transcribe spoken responses into Marathi text, enabling accurate processing of speech-based inputs within a regional language framework. The proposed approach demonstrates the feasibility of integrating ASR techniques for detecting depressive symptoms in Marathi-speaking teenagers.

Future work will focus on enhancing natural language understanding to accurately interpret user intentions in Marathi, converting sequences of words into syntactic and semantic representations for the dialogue manager.

REFERENCES

[1] Walker, M. A., Hirschman, L., & Aberdeen, J. S. (2000, May). Evaluation for Darpa Communicator Spoken Dialogue Systems, May 2000.

[2] Sharma, M., Kumar, P., Choudhary, R., & Yadav, K. (2025). SPEECH RECOGNITION USING NLP & CHATBOT. Journal of Science, Computing and Engineering Research, 8(05).

[3] AlSarrar, H., AlShameri, N., AlShareef, N., AlShareef, M., AlGhamdi, N., AlZaydi, S., ...&AlYahya, M. (2022, August). Arabic Dialogue Systems: A Survey. In Proceedings of Seventh International Congress on Information and Communication Technology: ICICT 2022, London, Volume 4 (pp. 153-161). Singapore: Springer Nature Singapore.

[4] Pęzik, P., Krawentek, G., Karasińska, S., Wilk, P., Rybińska, P., Cichosz, A., ... & Adamczyk, M. (2022, June). DiaBiz–an annotated corpus of Polish call center dialogs. In Proceedings of the thirteenth language resources and evaluation conference (pp. 723-726).

[5] Ramanarayanan, V., & Suendermann-Oeft, D. (2017, August). Jee haan, I'd like both, por favor: Elicitation of a Code-Switched Corpus of Hindi-English and Spanish-English Human-Machine Dialog. In Interspeech (pp. 47-51).

[6] Sharma, L., Dhir, V., & Kaur, K. (2015). A New Model for Question-Answer based Dialogue System for Indian Railways in Hindi Language. Indian Journal of Science and Technology, 8(32), 1-4.

[7] Arora, S., Batra, K., & Singh, S. (2013). Dialogue system: A brief review. arXiv preprint arXiv:1306.4134.

International Journal of Computer Research & Technology
ISSN 2454-7719
** A Blind Peer Reviewed Journal **
Volume-10, Issue-2, July-Dec 2025
Paper ID: CS-34

AI for Zero-Day Attack Prediction: A Comprehensive Review

Prof. Sayali Satish Patil
Assistant Professor,Department Of Computer Science Bhusawal Arts,Science and P.O. Nahata College Of Commerce,Bhusawal
sayalispatil263@gmail.com

Prof. Arati Santosh Bari
Assistant Professor,Department Of Computer Science Bhusawal Arts,Science and P.O. Nahata College Of Commerce,Bhusawal
aratibari152001@gmail.com

Abstract: *Zero-day attacks remain one of the most formidable challenges in cyber security, as they exploit undiscovered vulnerabilities before security vendors can release effective patches or detection signatures. Conventional defense mechanisms such as signature-based or rule-based systems fail to counter such threats, creating the urgent need for predictive and adaptive security frameworks. Artificial Intelligence (AI) offers promising capabilities in forecasting zero-day exploits through supervised and unsupervised machine learning, deep learning, behavioral analysis, and anomaly detection. This paper reviews state-of-the-art AI-driven approaches for zero-day attack prediction, evaluates their detection effectiveness, and highlights implementation challenges in real-world environments. In addition, it explores the role of feature engineering, dataset limitations, and evaluation metrics, while discussing future research trends including adversarial machine learning, explainable AI, and federated learning in cyber security contexts.*

Keywords- *Zero-Day Attacks, Artificial Intelligence, Cyber security, Machine Learning, Deep Learning, Anomaly Detection, Behavioral Analysis, Feature Engineering, Adversarial Machine Learning, Explainable AI, Federated learning.*

I. INTRODUCTION

1.1 Zero-Day Attacks: Definition and Characteristics

Zero-day attacks exploit security flaws that remain unknown to software vendors, security researchers, and administrators at the time of exploitation. These threats are characterized by several critical attributes:

- **Unknown Signatures:** No existing detection patterns or rules are available at the time of attack.
- **Time Sensitivity:** Exploitation occurs before developers can release security patches.
- **High Impact Potential:** Frequently target critical infrastructure and sensitive systems.
- **Stealth Techniques:** Designed to bypass conventional security mechanisms.
- **Persistence:** Can remain undetected for extended periods.

The term "zero-day" reflects the fact that defenders have had *zero days* to mitigate the vulnerability once attackers begin exploitation [1], [2].

1.2 Traditional Detection Limitations

Conventional cyber security mechanisms struggle against zero-day threats. Signature-based intrusion detection systems (IDS) rely on known attack patterns, making them ineffective against novel exploits [3]. Similarly, rule-based methods lack adaptability when confronted with new or obfuscated attack vectors. Manual log analysis is typically too slow for real-time response, while static defense architectures cannot evolve with the rapidly shifting cyber threat landscape [4], [5].

1.3 The Role of AI in Zero-Day Prediction

Artificial Intelligence introduces adaptive and predictive capabilities that conventional systems lack. Key advantages include:

- **Pattern Recognition:** Identifying subtle differences between normal and malicious activity.
- **Adaptive Detection:** Continuously updating models as new data becomes available.
- **Behavioral Analysis:** Emphasizing attacker behavior instead of predefined signatures.
- **Predictive Insight:** Anticipating vulnerabilities before exploitation.
- **Real-Time Analysis:** Processing massive volumes of data at network speeds.

Machine learning and deep learning techniques have therefore emerged as core enablers in developing next-generation intrusion detection and prevention systems [6], [7].

1.4 Scope and Objectives

This review paper aims to:

- Examine AI-based methods for predicting zero-day exploits.
- Assess the effectiveness of various supervised, unsupervised, and deep learning approaches.
- Identify the limitations and challenges in applying these techniques.
- Explore feature engineering and pre-processing methods critical to model performance.
- Discuss evaluation metrics and benchmarking practices.
- Highlight emerging research areas such as adversarial robustness, explainable AI (XAI), and federated learning.

II. ZERO-DAY ATTACK LANDSCAPE

2.1 Attack Vectors and Categories

Zero-day attacks can be broadly categorized into **network-based**, **application-based**, and **system-level** exploits, each targeting different layers of the computing environment [8], [9].

2.1.1 Network-Based Zero-Day Attacks

- **Protocol Exploitation:** Attacks leveraging flaws in communication protocols.
- **Buffer Overflow Exploits:** Exploiting memory management errors to execute arbitrary code.
- **Injection Attacks:** Including SQL injection and command injection variations.
- **Man-in-the-Middle (MitM):** Intercepting and altering network communications.

2.1.2 Application-Based Zero-Day Attacks

- **Web Application Exploits:** Such as cross-site scripting (XSS) and cross-site request forgery (CSRF).
- **Desktop Software Exploits:** Vulnerabilities in popular desktop applications.
- **Mobile Malware:** Platform-specific attacks on Android and iOS ecosystems.
- **Cloud Service Exploits:** Targeting containers, APIs, and serverless platforms.

2.1.3 System-Level Zero-Day Attacks

- **Operating System Vulnerabilities:** Kernel or driver-level exploits.
- **Hardware-Based Exploits:** Firmware or microcode manipulation.
- **Privilege Escalation:** Gaining unauthorized elevated access.
- **Rootkits:** Persistent methods for system compromise.

2.2 Attack Lifecycle and Detection Points

The **zero-day attack lifecycle** typically progresses through three main phases, where detection opportunities vary [10], [11].

2.2.1 Pre-Attack Phase

- **Reconnaissance:** Identifying vulnerable targets.
- **Weaponization:** Creating exploit payloads.
- **Delivery:** Deploying the attack via phishing emails, malicious links, or compromised software.

2.2.2 Execution Phase

- **Exploitation:** Triggering the vulnerability.
- **Installation:** Deploying malware or backdoors.
- **Command and Control (C2):** Establishing attacker communication channels.

2.2.3 Post-Attack Phase

- **Lateral Movement:** Expanding control across the network.
- **Data Exfiltration:** Stealing sensitive information.
- **Persistence:** Maintaining long-term access within the system.

Understanding these stages helps security researchers identify **potential detection points** for AI-enabled systems, such as unusual network traffic in the delivery stage or anomalous process behaviors during installation [12].

III. AI TECHNIQUES FOR ZERO-DAY ATTACK PREDICTION

AI-based solutions for zero-day attack prediction integrate **machine learning (ML)** and **deep learning (DL)** methods with traditional security practices. These approaches aim to detect unknown threats by analyzing patterns, behaviors, and anomalies instead of relying solely on predefined signatures [13], [14].

3.1 Machine Learning Approaches

3.1.1 Supervised Learning Methods

- **Support Vector Machines (SVMs):** Effective for classifying malicious versus

benign traffic. They work well with high-dimensional datasets but require labeled training data and careful feature scaling [15].

- **Random Forests and Ensemble Models:** Handle multi-class classification, resist overfitting, and provide feature importance rankings. However, they can be computationally intensive [16].
- **Naïve Bayes Classifiers:** Useful for spam and phishing detection due to their efficiency with small datasets, though they rely on strong independence assumptions [17].
- **Neural Networks:** Able to model complex non-linear relationships in traffic patterns but often require large datasets and are prone to overfitting [18].

3.1.2 Unsupervised Learning Methods

- **Clustering (K-means, DBSCAN):** Groups traffic into clusters to identify anomalies, though performance depends on optimal cluster size selection [19].
- **Principal Component Analysis (PCA):** Reduces feature dimensionality, improving computational efficiency, but may lose interpretability [20].
- **Isolation Forests:** Efficient for high-dimensional anomaly detection but rely heavily on contamination rate assumptions [21].
- **Autoencoders:** Learn normal behavioral patterns and identify deviations, making them effective for anomaly detection in network traffic [22].

3.1.3 Semi-Supervised and Reinforcement Learning

- **Semi-Supervised Learning:** Combines small labeled datasets with larger unlabeled data pools, improving generalization in threat intelligence systems [23].
- **Reinforcement Learning (RL):** Optimizes adaptive defense strategies by learning through interaction with an environment, though it faces challenges like slow convergence and reward function design [24].

3.2 Deep Learning Architectures

3.2.1 Convolutional Neural Networks (CNNs)

CNNs can process network traffic by converting packet data into image-like formats, enabling spatial pattern recognition for malware detection [25]. They are also used in static malware analysis, where binaries are visualized as grayscale images for classification [26].

3.2.2 Recurrent Neural Networks (RNNs) and LSTMs

RNNs and their variant Long Short-Term Memory (LSTM) networks excel at modeling sequential patterns, such as system calls and log entries. They capture long-term dependencies critical for detecting multi-stage attack chains [27].

3.2.3 Transformer Models and Attention Mechanisms

Transformers leverage attention mechanisms to focus on key features and correlate cross-domain data sources (e.g., system logs and network traffic). They have been applied to advanced persistent threat (APT) detection and threat intelligence analysis [28].

3.2.4 Generative Adversarial Networks (GANs)

GANs generate synthetic attack data for training, improving model robustness and dataset diversity. They are also applied in anomaly detection by modeling normal behaviors and flagging deviations [29].

3.3 Hybrid and Ensemble Approaches

- **Multi-Layer Detection Systems:** Employ hierarchical classification, moving from general anomaly detection to specific attack type classification, balancing performance with efficiency [30].
- **Ensemble Techniques:** Combine predictions from multiple algorithms to reduce bias and variance, improving accuracy in critical infrastructures and financial systems [31].

IV. Feature Engineering and Data Preprocessing

Feature engineering and data preprocessing are fundamental for improving the accuracy and efficiency of AI-based zero-day attack prediction systems. Raw network or system data often contain noise, redundancy, and irrelevant information, which can degrade model performance. Effective preprocessing ensures that the input to machine learning (ML) and deep learning (DL) models is meaningful and structured [32], [33].

4.1 Data Collection and Sources

Data for zero-day prediction can be collected from multiple sources:

- **Network Traffic Logs:** Packet captures (PCAPs), flow data, and connection logs.
- **System Logs:** Operating system event logs, application logs, and process monitoring.
- **Endpoint Sensors:** Behavior monitoring tools, antivirus logs, and host intrusion detection systems.
- **Threat Intelligence Feeds:** Vulnerability databases, malware signatures, and real-time attack alerts [34].

4.2 Data Cleaning

Data cleaning involves:

- **Handling Missing Values:** Imputation or removal of incomplete records.
- **Noise Reduction:** Filtering irrelevant packets or log entries.
- **Deduplication:** Eliminating redundant events to prevent biased model training [35].

4.3 Feature Extraction

Feature extraction transforms raw data into informative attributes for model consumption:

- **Statistical Features:** Packet size, connection duration, frequency of requests.
- **Temporal Features:** Time-based patterns such as repeated access or login attempts.
- **Behavioral Features:** Sequence of system calls, user activity anomalies, and privilege escalation attempts.
- **Content Features:** Payload analysis, opcode sequences, or API call traces [36].

4.4 Feature Selection and Dimensionality Reduction

High-dimensional data may introduce noise and increase computational cost. Feature selection techniques identify relevant attributes:

- **Filter Methods:** Metrics like mutual information and correlation scores.
- **Wrapper Methods:** Recursive feature elimination (RFE) using model performance.
- **Embedded Methods:** Feature importance from tree-based models such as Random Forests [37].

Dimensionality reduction techniques, such as Principal Component Analysis (PCA) or t-SNE, simplify the feature space while preserving critical patterns [38].

4.5 Data Normalization and Transformation

AI models, especially neural networks, require standardized input ranges:

- **Normalization:** Scaling features to a fixed range (e.g., 0–1) to prevent dominance by large-scale attributes.
- **Standardization:** Converting data to zero mean and unit variance for stable model convergence.
- **Encoding Categorical Data:** One-hot encoding or embedding representations for categorical variables such as protocol types or attack categories [39].

4.6 Handling Imbalanced Datasets

Zero-day attacks are rare, leading to class imbalance issues:

- **Oversampling Minority Class:** Techniques like SMOTE generate synthetic attack samples.
- **Undersampling Majority Class:** Reduces benign samples to balance the dataset.
- **Cost-Sensitive Learning:** Assigns higher penalties to misclassifying rare events [40].

4.7 Data Partitioning

Splitting datasets into training, validation, and test sets ensures model generalization:

- **Training Set:** Used for model learning.
- **Validation Set:** Optimizes hyperparameters and prevents overfitting.
- **Test Set:** Evaluates real-world performance on unseen data [41].

V. Evaluation Metrics And Model Performance

Evaluating AI models for zero-day attack prediction is critical to ensure reliability, accuracy, and robustness in real-world deployments. Proper metrics allow researchers to compare different approaches and optimize system performance [42], [43].

5.1 Classification Metrics

Zero-day attack prediction is typically framed as a classification problem (malicious vs. benign), and standard metrics include:

- **Accuracy:** Measures the overall correct predictions:

$$\text{Accuracy} = \frac{TP + TN}{TP + TN + FP + FN}$$

Where TP = True Positives, TN = True Negatives, FP = False Positives, FN = False Negatives.

- **Precision:** Proportion of predicted positives that are actual positives:

$$\text{Precision} = \frac{TP}{TP + FP}$$

- **Recall (Sensitivity):** Proportion of actual positives correctly identified:

$$\text{Recall} = \frac{TP}{TP + FN}$$

- **F1-Score:** Harmonic mean of precision and recall, balancing false positives and false negatives:

$$F1 = 2 \times \frac{\text{Precision} \cdot \text{Recall}}{\text{Precision} + \text{Recall}}$$

- **False Positive Rate (FPR) and False Negative Rate (FNR):** Critical in cybersecurity, as high FPR can overwhelm analysts, and high FNR may allow attacks to bypass detection.

5.2 Receiver Operating Characteristic (ROC) and Area Under Curve (AUC)

- **ROC Curve:** Plots true positive rate (TPR) against false positive rate (FPR) at various thresholds.
- **AUC:** Measures the area under the ROC curve, indicating model discrimination capability. Values closer to 1 indicate superior performance [44].

5.3 Confusion Matrix Analysis

A confusion matrix provides a detailed breakdown of classification results across all classes, enabling identification of specific weaknesses in detecting rare zero-day attacks [45].

5.4 Time and Resource Efficiency

AI models must operate in near real-time to mitigate zero-day threats:

- **Latency:** Time required to process new inputs and generate predictions.
- **Throughput:** Number of events processed per second.
- **Memory and Computation Costs:** Important for deployment in resource-constrained environments such as IoT or edge devices [46].

5.5 Robustness and Generalization

Zero-day attack models must generalize to previously unseen threats:

- **Cross-Dataset Evaluation:** Testing models on datasets not seen during training.
- **Adversarial Testing:** Assessing resilience against evasion attempts and adversarial inputs.
- **Model Drift Detection:** Monitoring performance over time to detect degradation due to evolving threats [47].

5.6 Benchmark Datasets

Commonly used datasets for zero-day prediction research include:

- **KDD Cup 1999 / NSL-KDD:** Network intrusion detection datasets.
- **UNSW-NB15:** Modern network attack dataset with labeled normal and attack traffic.
- **CICIDS2017 / CICDDoS2019:** Realistic traffic captures for intrusion and denial-of-service detection.
- **Malware Dataset Repositories:** Includes executable files and malware behavior traces [48], [49].

VI. Challenges, Limitations, And Future Research Directions

Despite significant advances, AI-based zero-day attack prediction faces several challenges in practical deployment. Understanding these obstacles is essential for developing robust, scalable, and explainable cybersecurity solutions [50], [51].

6.1 Challenges in AI-Driven Zero-Day Detection

1. **Data Scarcity and Imbalance**
   Zero-day attacks are rare, resulting in limited labeled datasets. This scarcity hampers supervised learning approaches and may lead to overfitting or poor generalization [52].
2. **Evolving Threat Landscape**
   Attack techniques evolve rapidly, including polymorphic malware, obfuscation, and multi-stage attacks. AI models must adapt continuously to remain effective [53].
3. **High False Positive Rates**
   Anomaly detection systems may generate numerous false alarms, overwhelming security teams and reducing trust in AI-based systems [54].
4. **Adversarial Evasion**
   Attackers can deliberately craft inputs to deceive AI models, exploiting vulnerabilities in feature extraction or classification algorithms [55].
5. **Computational and Resource Constraints**
   Deep learning models often require high processing power and memory, which may limit deployment on edge devices or in real-time scenarios [56].
6. **Interpretability and Explainability**
   Many AI models, particularly deep learning

architectures, act as "black boxes," making it difficult for security analysts to understand decision rationale [57].

6.2 Limitations of Current Approaches

- **Overfitting to Specific Datasets:** Models may perform well on training data but fail to generalize to new network environments or unseen attack vectors.
- **Dependency on Feature Quality:** Poor feature engineering can severely reduce detection accuracy.
- **Limited Standardization:** Benchmarking is challenging due to variations in datasets, evaluation metrics, and experimental setups.

6.3 Future Research Directions

1. **Adversarial Machine Learning (AML)** Developing models robust to evasion attacks, including adversarial training and detection of manipulated inputs [58].
2. **Explainable AI (XAI)** Integrating interpretability into AI models to provide actionable insights for security analysts and improve trust in automated systems [59].
3. **Federated Learning** Leveraging distributed learning across multiple organizations or endpoints while preserving privacy, enabling collaborative detection without sharing raw data [60].
4. **Hybrid and Ensemble Approaches** Combining multiple AI techniques and traditional security methods to balance detection accuracy, false positive reduction, and computational efficiency [61].
5. **Real-Time Adaptive Systems** Researching AI models capable of continuous learning from streaming data to detect evolving zero-day threats dynamically [62].
6. **Cross-Domain Threat Intelligence Integration** Combining network, host, application, and cloud security data to improve context-aware detection and predictive modeling [63].
7. **Automated Feature Engineering** Using AI-driven techniques to automatically extract and select optimal features from complex and high-dimensional security data [64]

VII. EMERGING TRENDS AND ADVANCED TECHNIQUES

Recent advances in artificial intelligence and cyber security research have introduced new paradigms for zero-day attack prediction. These techniques aim to improve interpretability, collaboration, scalability, and resilience against sophisticated adversaries.

7.1 Explainable AI (XAI) in Cybersecurity

7.1.1 Interpretability Techniques

Explainability is critical to ensure that security analysts trust AI-generated predictions. Current interpretability methods are categorized as local and global explanations.

- **Local Explanations:**
  - LIME (Local Interpretable Model-Agnostic Explanations) highlights influential features in individual predictions [65].
  - SHAP (SHapley Additive exPlanations) applies cooperative game theory to attribute importance scores to features [66].
  - Gradient-based approaches leverage neural network gradients to indicate feature sensitivity [67].
- **Global Explanations:**
  - Feature importance rankings summarize overall model behavior.
  - Decision tree approximations extract human-readable rules.
  - Attention visualization reveals which input sequences influence deep models most strongly [68].

7.1.2 Applications in Zero-Day Detection

- **Attack Attribution:** Automatically generating detection signatures, enhancing threat intelligence, and supporting forensic investigations [69].
- **Model Validation:** Providing transparency for expert reviews, ensuring compliance with regulatory requirements, and enabling iterative model refinement [70].

7.2 Federated Learning for Collaborative Defense

Federated learning (FL) enables organizations to collaboratively train models without sharing sensitive raw data.

7.2.1 Distributed Training Approaches

- **Cross-Organizational Learning:** Facilitates collaborative defense through collective threat intelligence, privacy-preserving insights, and industry-specific consortium models [71].
- **Edge-Based Detection:** Enables local training on endpoint devices, followed by secure aggregation of global models to improve scalability while reducing communication overhead [72].

7.2.2 Challenges and Solutions

- **Data Heterogeneity:** Addressed through domain adaptation, transfer learning, and federated optimization techniques [73].

- **Security Considerations:** Challenges include model poisoning, Byzantine fault tolerance, and secure aggregation using cryptographic methods [74].

7.3 Graph Neural Networks (GNNs) for Attack Analysis

GNNs leverage graph-based structures to capture complex interdependencies in cyber environments.

7.3.1 Graph-Based Representations

- **Network Topology:** Modeling communication graphs, malware propagation, and lateral movement patterns [75].
- **System Interaction Graphs:** Capturing process dependencies, file system operations, and registry interactions [76].

7.3.2 GNN Architectures for Security

- **Graph Convolutional Networks:** Applied to node classification, link prediction, and graph embeddings [77].
- **Attention-Based Networks:** Designed for dynamic, multi-scale, and heterogeneous graphs [78].

7.4 Quantum Computing and Post-Quantum Security

Quantum technologies pose both threats and opportunities for cybersecurity.

7.4.1 Quantum Threat Implications

- Vulnerabilities in RSA and ECC highlight the urgency of post-quantum cryptography migration [79].
- Quantum computing may accelerate pattern recognition and optimization tasks for security applications [80].

7.4.2 Research Directions

- **Quantum Anomaly Detection:** Leveraging quantum clustering, neural networks, and feature mapping.
- **Quantum-Safe AI Models:** Developing quantum-resistant algorithms while addressing implementation challenges [81].

VIII. Case Studies And Real-World Implementations

8.1.1 Financial Services

- **Use Cases:** AI-powered fraud detection, network intrusion prediction, and regulatory compliance enforcement.
- **Case Study – JPMorgan Chase:** Machine learning models improved detection accuracy and reduced false positives but highlighted the challenge of balancing security with customer experience [82].

8.1.2 Healthcare

- **Use Cases:** Securing IoT-enabled medical devices, protecting patient records, and ensuring availability of critical systems.
- **Case Study – Mayo Clinic:** ML-based systems enhanced HIPAA-compliant cybersecurity, though integration with clinical workflows remained challenging [83].

8.1.3 Critical Infrastructure

- **Use Cases:** Securing SCADA systems, preventing cascading failures in power grids, and monitoring transportation networks in real time [84].

8.2 Government and Military Applications

8.2.1 National Security Agencies

- **Applications:** Threat intelligence analysis, attribution of state-sponsored attacks, and strategic planning [85].
- **Defense Use Cases:** Securing battlefield communications and military-grade weapon systems [86].

8.2.2 Public Sector Implementations

- **Smart Cities:** AI-enabled IoT security, emergency response reliability, and citizen data privacy.
- **Electoral Security:** Protecting voting infrastructure, combating disinformation, and ensuring trust in democratic processes [87].

8.3 Technology Company Innovations

8.3.1 Major Platforms

- **Microsoft:** Azure Sentinel and Microsoft Defender integrate AI with SIEM and endpoint protection [88].
- **Google:** Chronicle, VirusTotal, and Project Zero exemplify large-scale AI security initiatives [89].
- **Amazon Web Services:** GuardDuty, Security Hub, and Macie provide AI-driven cloud-native defenses [90].

8.3.2 Specialized Vendors

- **CrowdStrike Falcon:** Real-time endpoint detection and response [91].
- **Darktrace:** Self-learning AI with autonomous threat response capabilities [92].

IX. Future Research Directions

9.1 Technical Advancements

- **Next-Generation Architectures:** Transformers for multi-modal analysis and neuromorphic hardware for real-time, energy-efficient security [93].
- **Advanced Learning Paradigms:** Meta-learning, few-shot learning, and lifelong learning to address novel attack scenarios [94].

9.2 Interdisciplinary Research Areas

- **Human-AI Collaboration:** Augmented intelligence systems to combine human expertise with AI recommendations [95].

- **Economics and Policy:** Cyber risk modeling, AI governance, and international cooperation frameworks [96].

9.3 Emerging Threat Considerations

- **AI-Powered Attacks:** Countering adversarial AI, generative malware, and deepfakes [97].
- **IoT and 5G Security:** Edge-based AI, swarm intelligence, and real-time detection in ultra-low latency environments [98].

X. Conclusion And Recommendations

10.1 Key Findings

This review highlights that AI-based zero-day attack prediction is a transformative approach to cybersecurity. Machine learning and deep learning techniques significantly outperform signature-based defenses, particularly in detecting novel attacks through behavioral and anomaly analysis. Industry case studies demonstrate real-world benefits across finance, healthcare, and critical infrastructure. However, practical deployment faces challenges in explainability, adversarial robustness, scalability, and data quality. Emerging techniques such as XAI, federated learning, GNNs, and quantum-safe models offer promising solutions.

10.2 Recommendations

1. **Invest in Explainable AI:** Enhance analyst trust and regulatory compliance.
2. **Adopt Collaborative Defense:** Use federated learning and secure information sharing across industries.
3. **Strengthen Adversarial Robustness:** Develop resilient AI against evasion and poisoning attacks.
4. **Advance Quantum-Resilient Models:** Prepare for the long-term implications of quantum computing.
5. **Bridge Research and Practice:** Focus on scalable, lightweight models deployable in real-world settings.
6. **Promote Policy and Standardization:** Establish benchmarking datasets, evaluation metrics, and international security guidelines.

By addressing these priorities, the cybersecurity community can move closer to achieving robust, scalable, and future-proof zero-day attack prediction systems.

10.1 Key Findings

This review highlights that AI-based zero-day attack prediction is a transformative approach to cybersecurity. Machine learning and deep learning techniques significantly outperform signature-based defenses, particularly in detecting novel attacks through behavioral and anomaly analysis. Industry case studies demonstrate real-world benefits across finance, healthcare, and critical infrastructure. However, practical deployment faces challenges in explainability, adversarial robustness, scalability, and data quality. Emerging techniques such as XAI, federated learning, GNNs, and quantum-safe models offer promising solutions.

10.2 Recommendations

1. **Invest in Explainable AI:** Enhance analyst trust and regulatory compliance.
2. **Adopt Collaborative Defense:** Use federated learning and secure information sharing across industries.
3. **Strengthen Adversarial Robustness:** Develop resilient AI against evasion and poisoning attacks.
4. **Advance Quantum-Resilient Models:** Prepare for the long-term implications of quantum computing.
5. **Bridge Research and Practice:** Focus on scalable, lightweight models deployable in real-world settings.
6. **Promote Policy and Standardization:** Establish benchmarking datasets, evaluation metrics, and international security guidelines.

By addressing these priorities, the cybersecurity community can move closer to achieving robust, scalable, and future-proof zero-day attack prediction systems.

References

[1] Symantec, "Internet Security Threat Report," Symantec Corporation, 2019.

[2] M. Almukaynizi, et al., "A Survey on Zero-Day Attack Detection: Approaches, Challenges, and Future Directions," *IEEE Access*, vol. 9, pp. 122306–122329, 2021.

[3] S. Axelsson, "Intrusion Detection Systems: A Survey and Taxonomy," *Technical Report*, Chalmers University, 2000.

[4] R. Sommer and V. Paxson, "Outside the Closed World: On Using Machine Learning for Network Intrusion Detection," in *Proc. IEEE Symposium on Security and Privacy*, pp. 305–316, 2010.

[5] N. Hubballi and V. Suryanarayanan, "False Alarm Minimization Techniques in Signature-Based Intrusion Detection Systems: A Survey," *Computers & Security*, vol. 73, pp. 266–283, 2018.

[6] Y. Xin, et al., "Machine Learning and Deep Learning Methods for Cybersecurity," *IEEE Access*, vol. 6, pp. 35365–35381, 2018.

[7] H. Hindy, et al., "A Taxonomy of Machine Learning Intrusion Detection Systems," *Journal of Information Security and Applications*, vol. 54, p. 102483, 2020.

[8] FireEye, "Zero-Day Exploits in the Wild," FireEye Intelligence Report, 2018.

[9] Kaspersky, “Zero-Day Vulnerabilities and Exploits: An In-Depth Guide,” Kaspersky Labs, 2020.

[10] M. Egele, et al., “A Survey of Automated Dynamic Malware-Analysis Techniques and Tools,” *ACM Computing Surveys*, vol. 44, no. 2, pp. 1–42, 2012.

[11] MITRE, “ATT&CK Framework,” MITRE Corporation, 2020.

[12] P. Mell and T. Grance, “The NIST Definition of Cloud Computing,” NIST Special Publication 800-145, 2011.

[13] L. Bilge and T. Dumitras, “Before We Knew It: An Empirical Study of Zero-Day Attacks in the Real World,” in *Proc. ACM CCS*, pp. 833–844, 2012.

[14] J. Zhang, et al., “Network Intrusion Detection: Machine Learning and Deep Learning Approaches,” *IEEE Communications Surveys & Tutorials*, vol. 22, no. 3, pp. 2479–2501, 2020.

[15] V. Vapnik, *The Nature of Statistical Learning Theory*, Springer, 1995.

[16] L. Breiman, “Random Forests,” *Machine Learning*, vol. 45, pp. 5–32, 2001.

[17] P. Domingos and M. Pazzani, “On the Optimality of the Simple Bayesian Classifier under Zero-One Loss,” *Machine Learning*, vol. 29, pp. 103–130, 1997.

[18] Y. LeCun, Y. Bengio, and G. Hinton, “Deep Learning,” *Nature*, vol. 521, no. 7553, pp. 436–444, 2015.

[19] A. Jain, M. Murty, and P. Flynn, “Data Clustering: A Review,” *ACM Computing Surveys*, vol. 31, no. 3, pp. 264–323, 1999.

[20] I. Jolliffe, *Principal Component Analysis*, Springer, 2002.

[21] F. T. Liu, K. M. Ting, and Z.-H. Zhou, “Isolation Forest,” in *Proc. IEEE ICDM*, pp. 413–422, 2008.

[22] J. Sakurada and T. Yairi, “Anomaly Detection Using Autoencoders with Nonlinear Dimensionality Reduction,” in *Proc. MLSDA Workshop*, 2014.

[23] X. Zhu, “Semi-Supervised Learning Literature Survey,” Technical Report, Univ. of Wisconsin-Madison, 2008.

[24] R. Sutton and A. Barto, *Reinforcement Learning: An Introduction*, MIT Press, 2018.

[25] W. Wang, et al., “HAST-IDS: Learning Hierarchical Spatial-Temporal Features Using Deep Neural Networks to Improve Intrusion Detection,” *IEEE Access*, vol. 6, pp. 1792–1806, 2018.

[26] F. Nataraj, et al., “Malware Images: Visualization and Automatic Classification,” in *Proc. ACM VizSec*, pp. 1–7, 2011.

[27] Y. Kim, et al., “Recurrent Neural Networks with Word Embeddings for Intrusion Detection Systems,” *Computers & Security*, vol. 82, pp. 147–159, 2019.

[28] J. Vaswani, et al., “Attention is All You Need,” in *Proc. NeurIPS*, pp. 5998–6008, 2017.

[29] S. Goodfellow, et al., “Generative Adversarial Nets,” in *Proc. NeurIPS*, pp. 2672–2680, 2014.

[30] H. Kim and J. Park, “Hybrid Intrusion Detection with Deep Neural Networks,” *Security and Communication Networks*, vol. 2019, pp. 1–10, 2019.

[31] Z. Zhang, et al., “Ensemble Learning Methods for Zero-Day Intrusion Detection,” *Applied Sciences*, vol. 9, no. 20, p. 4324, 2019.

[32] C. M. Bishop, *Pattern Recognition and Machine Learning*, Springer, 2006.

[33] I. Guyon and A. Elisseeff, “An Introduction to Feature Extraction,” in *Feature Extraction*, Springer, 2006, pp. 1–25

[34] A. Buczak and E. Guven, “A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection,” *IEEE Communications Surveys & Tutorials*, vol. 18, no. 2, pp. 1153–1176, 2016.

[35] T. Hastie, R. Tibshirani, and J. Friedman, *The Elements of Statistical Learning*, Springer, 2009.

[36] K. Scarfone and P. Mell, “Guide to Intrusion Detection and Prevention Systems (IDPS),” NIST SP 800-94, 2007.

[37] J. H. Friedman, “Greedy Function Approximation: A Gradient Boosting Machine,” *Annals of Statistics*, vol. 29, no. 5, pp. 1189–1232, 2001.

[38] L. van der Maaten and G. Hinton, “Visualizing Data Using t-SNE,” *Journal of Machine Learning Research*, vol. 9, pp. 2579–2605, 2008.

[39] A. Géron, *Hands-On Machine Learning with Scikit-Learn, Keras, and TensorFlow*, 2nd ed., O’Reilly, 2019.

[40] N. Chawla, et al., “SMOTE: Synthetic Minority Over-sampling Technique,” *Journal of Artificial Intelligence Research*, vol. 16, pp. 321–357, 2002.

[41] R. Kohavi, “A Study of Cross-Validation and Bootstrap for Accuracy Estimation and Model Selection,” in *Proc. IJCAI*, pp. 1137–1145, 1995.

[42] T. Fawcett, “An Introduction to ROC Analysis,” *Pattern Recognition Letters*, vol. 27, no. 8, pp. 861–874, 2006.

[43] D. Powers, “Evaluation: From Precision, Recall and F-Measure to ROC, Informedness, Markedness and Correlation,” *Journal of Machine Learning Technologies*, vol. 2, no. 1, pp. 37–63, 2011.

[44] C. Cortes and M. Mohri, “Confidence Intervals for the Area under the ROC Curve,” in *Proc. NeurIPS*, pp. 305–312, 2004.

[45] J. Davis and M. Goadrich, “The Relationship Between Precision-Recall and ROC Curves,” in *Proc. ICML*, pp. 233–240, 2006.

[46] Y. Ding, et al., “A Survey on Security Challenges in Edge Computing,” *IEEE Communications Surveys & Tutorials*, vol. 22, no. 4, pp. 2066–2101, 2020.

[47] A. Bifet, et al., “Machine Learning for Data Streams: With Practical Examples in MOA,” MIT Press, 2018.

[48] M. Tavallaee, et al., “A Detailed Analysis of the KDD Cup 99 Data Set,” in *Proc. IEEE CISDA*, pp. 1–6, 2009.

[49] I. Sharafaldin, A. Habibi Lashkari, and A. Ghorbani, “Toward Generating a New Intrusion Detection Dataset and Intrusion Traffic Characterization,” in *Proc. ICISSP*, pp. 108–116, 2018.

[50] J. Shafiq, et al., “Evaluating the Performance of Machine Learning Techniques in Cybersecurity,” *Future Generation Computer Systems*, vol. 95, pp. 346–359, 2019.

[51] S. Verma and A. Ranga, “Machine Learning Based Intrusion Detection Systems for IoT Applications: A Review,” *Journal of Information Security and Applications*, vol. 58, p. 102748, 2021.

[52] M. Ring, et al., “A Survey of Network-Based Intrusion Detection Data Sets,” *Computers & Security*, vol. 86, pp. 147–167, 2019.

[53] P. Laskov and M. Kloft, “A Framework for Machine Learning in Network Intrusion Detection,” *Computers & Security*, vol. 25, no. 6, pp. 441–454, 2006.

[54] M. Sabhnani and G. Serpen, “Application of Machine Learning Algorithms to KDD Intrusion Detection Dataset Within Misuse Detection

International Journal of Computer Research & Technology
** A Blind Peer Reviewed Journal **
Volume-10, Issue-2, July-Dec 2025
ISSN 2454-7719
Paper ID: CS-35

The Rise of No-Code and Low-Code Platforms: Threat or Opportunity for Frontend Developers?

Prof. Arati Santosh Bari
Assistant Professor ,Department Of Computer Science,
Arts Science And P.O. Nahata Commerce College,Bhusawal.
aratibari152001@gmail.com

Prof. Sayali Satish Patil
Assistant Professor ,Department Of Computer Science,
Arts Science And P.O. Nahata Commerce College,Bhusawal.
Sayalispatil263@gmail.com

Abstract- *The software development landscape is undergoing a significant transformation due to the increasing adoption of no-code and low-code platforms. This study examines the implications of these tools for frontend developers, evaluating whether they pose a threat to traditional roles or offer new avenues for growth. By analyzing industry trends, future projections, and developer perspectives, it becomes clear that these platforms will reshape frontend development. However, they are more likely to create opportunities for developers who expand their skillsets and adapt to the evolving digital ecosystem*

Keywords— *No-code platforms, low-code platforms, frontend development, automation, hybrid development, AI-assisted development, digital innovation.*

I. Introduction

The software development sector is at a critical turning point. Traditional coding methods, which have long formed the backbone of application development, are being challenged by no-code and low-code platforms. These tools simplify development by allowing users to create applications with visual interfaces, drag-and-drop components, and pre-built templates, minimizing the need for extensive programming knowledge.

This evolution raises questions for frontend developers regarding the relevance of their skills, job security, and future career prospects. As businesses increasingly adopt these platforms to accelerate development and reduce costs, developers' roles are evolving to require both technical and strategic competencies. The aim of this paper is to explore the effects of no-code and low-code platforms on frontend development, highlighting both challenges and opportunities.

II. Literature Review And Market Analysis

A. Market Growth and Adoption

No-code and low-code platforms are growing rapidly. Analysts project that by 2025, almost half of all new applications will be built using these tools. The rise of hyper automation, which integrates AI, machine learning, and robotic process automation, is accelerating this trend.

Research by Gartner and other firms suggests that over 70% of software development projects will leverage low-code tools by 2025. Financial data indicate that the global low-code development platform market, valued at USD 24.83 billion in 2023, is expected to grow at a compound annual growth rate (CAGR) of approximately 22.5% between 2024 and 2030.

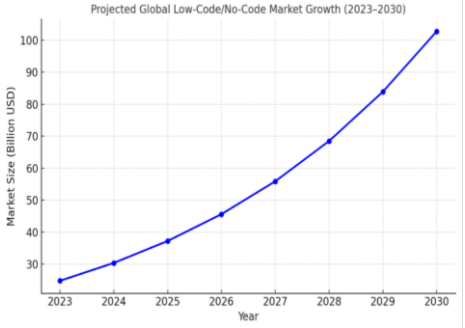


Figure 1. Low-Code/No-Code Market Size Forecast (2023–2030)

B. Democratization of Development

No-code and low-code platforms enable "citizen developers"—non-technical staff such as designers, analysts, and operational personnel—to build applications. This represents a departure from traditional development models that required deep coding knowledge.

By lowering barriers to entry and speeding development cycles, these platforms allow teams across departments to create tailored solutions, easing pressure on IT teams while meeting diverse organizational needs.

III. Impact On Frontend Development

A. Changing Skill Requirements

The adoption of no-code and low-code platforms is redefining frontend development skills. Programming knowledge remains important, but proficiency in design tools (e.g., Figma, Adobe XD) is increasingly valuable. This enhances collaboration with UI/UX designers and strengthens design capabilities.

Additionally, AI-assisted tools are reshaping development practices. Developers now work alongside platforms that generate code, provide optimization recommendations, and automate repetitive tasks.

B. Industry Adoption Trends

Industries such as banking, healthcare, e-commerce, education, and manufacturing are integrating no-code solutions at an accelerated pace. By 2025, nearly half of new applications are expected to rely on these platforms, affecting frontend development across multiple sectors.

IV. Challenges For Frontend Developers

A. Job Security

The automation of routine coding tasks raises concerns about reduced demand, especially for junior developers, as platforms can generate standard websites, apps, and business interfaces.

B. Risk of Skill Commoditization

Tasks like HTML/CSS layouts, basic JavaScript, and responsive design are increasingly automated, risking the commoditization of these skills.

C. Competition in Speed and Cost

No-code platforms enable faster and cheaper development. Projects that once took months can now be completed in days or weeks, emphasizing the need for developers to add unique value.

V. Opportunities For Frontend Developers

A. Strategic Roles

Developers can focus on high-value work such as system architecture, problem-solving, and customizing applications beyond pre-built functionalities.

B. Productivity and Innovation

Automation frees developers to innovate, enhance user experience, and experiment with rapid prototyping.

C. Emerging Specializations

- **Platform Specialists:** Optimize specific no-code tools
- **Integration Experts:** Connect platforms with APIs and legacy systems
- **Custom Component Developers:** Build reusable modules and extensions
- **Consultants:** Advise organizations on adoption and scaling

D. Collaborative Opportunities

No-code platforms promote collaboration among developers, designers, managers, and stakeholders, reducing communication gaps and improving outcomes.

VI. Strategic Adaptation Framework

1) A. Skill Evolution

To remain competitive in the rapidly evolving software development landscape, frontend developers must actively expand and diversify their skill sets. Skill evolution should focus on three key areas: **technical skills, platform expertise, and soft skills.**

1. Technical Skills

Modern frontend development requires proficiency beyond basic coding. Developers should focus on:

- **JavaScript Frameworks:** Mastery of frameworks such as React, Angular, and Vue.js allows developers to build dynamic, interactive web applications efficiently.
- **API Integration:** Understanding how to connect applications with external services through RESTful APIs or GraphQL enables seamless data exchange and integration.

- **Cloud Computing & Serverless Architectures:** Knowledge of cloud platforms like AWS, Azure, or Google Cloud helps developers deploy scalable applications and leverage serverless functions for cost-effective solutions.
- **AI-Assisted Development Tools:** Familiarity with AI-driven platforms that generate code, suggest optimizations, or automate testing can significantly increase productivity and enhance application quality.

2. Platform Expertise

No-code and low-code platforms are becoming integral in modern development. Frontend developers should gain:

- **Platform Certifications:** Earning certifications for popular platforms such as OutSystems, Mendix, or Appgyver demonstrates competence and increases professional credibility.
- **Customization Skills:** Ability to create extensions, plugins, or reusable components allows developers to enhance platform capabilities beyond out-of-the-box features.
- **System Migration & Integration:** Knowledge of migrating existing applications to low-code platforms and integrating them with legacy systems ensures smooth transitions and business continuity.

3. Soft Skills

Technical expertise alone is insufficient in today's collaborative and business-oriented environment. Developers should cultivate:

- **Communication & Teamwork:** Effectively collaborating with designers, business analysts, and other stakeholders ensures project alignment and smooth development cycles.
- **Business Insight:** Understanding business objectives and translating them into technical solutions allows developers to contribute strategically.
- **Leadership & Client Management:** Skills in guiding teams, managing client expectations, and coordinating projects enhance professional growth and career opportunities.

By continuously developing these skills, frontend developers can adapt to new technologies, leverage no-code/low-code tools effectively, and maintain a strategic role in delivering high-value solutions.

2) B. Career Strategies and Flowchart

To thrive in the evolving software development landscape, frontend developers should adopt **hybrid career strategies**, combining traditional coding skills with proficiency in no-code/low-code platforms. This approach ensures flexibility, efficiency, and the ability to tackle a wide range of projects. The following flowchart illustrates a **decision-making framework** for selecting the most appropriate development approach:

Flowchart LR

```
subgraph Strategy["STRATEGIC POSITIONING FOR FRONTEND DEVELOPERS"]
A[Assess Project Requirements]
B[Select Optimal Approach]
C[Deliver Solution]
D[Refine & Scale]
end

subgraph Traditional["TRADITIONAL CODING"]
E[Complex Custom Logic]
F[Performance-Critical Applications]
G[Advanced User Interactions]
H[Unique UI/UX Demands]
end

subgraph NoCodeLowCode["NO-CODE/LOW-CODE"]
I[Rapid Prototyping]
J[Business Applications]
K[Content & Workflow Management]
L[Routine Processes]
end

subgraph Hybrid["HYBRID APPROACH"]
M[Combine Custom + Platform]
N[Template + API Integration]
O[Advanced Logic + Visual Tools]
P[Automation + Performance Tuning]
end

A --> B
B --> E
B --> I
B --> M

E --> C
I --> C
M --> C

C --> D

style Strategy fill:#e6f3ff
style Traditional fill:#ffcccc
style NoCodeLowCode fill:#ccffcc
style Hybrid fill:#ffffcc
```

Flowchart Explanation

1. **Assess Project Requirements** The first step is to evaluate the project in terms of complexity, business objectives, scalability needs, and expected user interactions. Projects may vary from simple content-driven applications to highly complex, performance-critical systems.
2. **Select Optimal Approach** Based on the assessment, developers choose the most suitable approach:
   - **Traditional Coding:** Best for applications requiring advanced customization, unique UI/UX, complex logic, or performance optimization.
   - **No-Code/Low-Code:** Suitable for rapid prototyping, standard business applications, content management, and routine workflow automation.
   - **Hybrid Approach:** Combines both methods to leverage the speed of platforms while retaining flexibility for complex requirements. This often includes integrating APIs, customizing templates, or adding advanced logic where needed.
3. **Deliver Solution** Implement the selected approach, ensuring the application meets functional, aesthetic, and performance standards. Developers must also maintain code quality, usability, and scalability during this phase.
4. **Refine & Scale** Continuous improvement is critical. Developers should monitor performance, gather user feedback, and enhance functionality. Hybrid solutions may require ongoing adjustments to balance platform limitations with custom enhancements.

Key Takeaways for Frontend Developers

- **Flexibility is Essential:** Proficiency in both traditional coding and platform-based tools allows developers to select the most effective approach for any project.
- **Efficiency and Innovation:** Hybrid strategies enable faster delivery of solutions without compromising on customization or quality.
- **Strategic Value:** Developers adopting this framework position themselves as solution architects who can bridge business requirements and technical implementation.

VII. FUTURE OUTLOOK

A. Technology Convergence

The next phase of no-code and low-code platforms will see a strong integration with emerging technologies such as **artificial intelligence (AI), machine learning (ML), and the Internet of Things (IoT)**. This convergence will result in platforms that are more intelligent, adaptive, and capable of automating complex development tasks. For frontend developers, this means acquiring advanced technical knowledge to fully utilize these tools. Professionals will need to understand how AI-driven code generation, predictive analytics, and connected IoT devices can be incorporated into applications to create smarter, more responsive solutions. Mastery of these technologies will become a key differentiator for developers in the evolving digital ecosystem.

B. Market Maturation

As no-code and low-code platforms mature, they will become capable of addressing **larger, more complex business requirements**. These platforms will improve integration with existing enterprise workflows, allowing for seamless connectivity with databases, APIs, and legacy systems. The development landscape will increasingly favor **hybrid approaches**, where manual coding and platform-driven solutions complement each other to achieve optimal efficiency, scalability, and customization. Organizations will also place greater emphasis on **governance, security, and maintainability**, making it essential for developers to understand not only the tools themselves but also how to implement them responsibly at scale.

C. Evolution of Developer Roles

The adoption of no-code/low-code technologies will transform the traditional role of frontend developers. Instead of focusing solely on writing code, developers will take on **diverse and specialized roles** that include:

- **Solution Architects:** Designing complex, cross-platform systems that combine traditional coding with platform capabilities.
- **Platform Engineers:** Customizing, maintaining, and scaling no-code/low-code environments for enterprise applications.
- **Experience Designers:** Enhancing usability, interaction design, and end-user experience using hybrid tools.
- **Integration Specialists:** Ensuring smooth interoperability between no-code/low-code platforms and other systems, APIs, or legacy applications.

This evolution emphasizes **strategic thinking, technical versatility, and problem-solving**, positioning frontend developers as critical enablers of innovation and value creation within organizations.

VIII. RECOMMENDATIONS

A. For Individual Developers

Frontend developers can maintain their relevance and advance their careers by actively adapting to the rise of no-code and low-code platforms. This includes continuously enhancing both traditional coding skills and platform-specific abilities to stay ahead in a hybrid development environment. Developing **T-shaped skills**—a broad understanding of multiple technologies combined with deep expertise in a specific area—can help developers contribute strategically across projects. Maintaining a portfolio that showcases work built with conventional coding as well as no-code/low-code solutions demonstrates versatility and adaptability. Active participation in developer communities, forums, and workshops ensures professionals remain aware of the latest tools, trends, and best practices. Finally, developers should focus on **solving business problems and creating value**, rather than only writing code, to remain indispensable in their organizations.

B. For Organizations

Businesses can maximize the benefits of no-code and low-code adoption by implementing **hybrid development strategies** that combine traditional coding with platform-driven solutions. Structured training programs should be offered to employees, equipping them to effectively leverage these tools while maintaining development quality. Establishing clear **governance frameworks** ensures that teams select the appropriate approach—coding or platform-based—depending on project complexity, scalability, and security requirements. Organizations should also shift performance evaluation from the quantity of code produced to the **business value generated**, rewarding developers for innovative, efficient, and high-impact contributions.

C. For Educational Institutions

Academic institutions have a key role in preparing the next generation of developers for a changing technology landscape. Curricula should incorporate no-code and low-code platforms alongside traditional programming courses to provide students with both theoretical knowledge and practical skills. Collaborations with industry partners can provide **hands-on experience**, allowing students to work on real-world projects and understand the practical implications of these technologies. Furthermore, institutions should cultivate students' ability to **critically assess and select the most suitable tools** for different tasks, emphasizing problem-solving, innovation, and adaptability over rote coding skills.

IX. CONCLUSION

The adoption of no-code and low-code platforms is reshaping the role of frontend developers, shifting the focus from routine coding tasks to high-value contributions such as system architecture, advanced integration, user experience design, and strategic problem-solving. While these platforms automate repetitive work, they create opportunities for developers to expand their influence as solution architects, platform specialists, and innovation leaders. By adopting hybrid approaches that combine traditional coding with no-code/low-code tools, professionals can deliver customized, robust solutions that automated systems alone cannot achieve, ensuring their relevance in the evolving software development landscape.

Success in this changing environment requires continuous learning, adaptability, and collaboration. Developers who enhance their skills with emerging technologies like AI, machine learning, and IoT, while fostering teamwork across business and design functions, will be well-positioned to thrive. No-code and low-code platforms should be viewed as complementary tools that empower developers to innovate faster, enhance user experiences, and focus on strategic tasks. Ultimately, these platforms do not replace frontend developers—they elevate their role, making them central to shaping efficient, creative, and user-centric software solutions.

REFERENCES

[1] Hostinger. (2025). *No-code and low-code trends for 2025: 26 key insights.* Available at: [link]

[2] Quixy. (2025). *Top 10 predictions for no-code and low-code in 2025: Breaking barriers.* [link]

[3] Bhuyan, A. (2025). *The state of no-code and low-code platforms in 2025: Growth, challenges, and opportunities.* DEV Community

[4] BP-3. (2024). *Ten major no-code/low-code trends shaping 2024.* [link]

[5] ColorWhistle. (2025). *Low-code development statistics and facts: 2025 update.* [link]

[6] Kissflow. (2025). *Gartner's forecast for the low-code/no-code development market in 2025.* [link]

[7] App Builder. (2025). *Latest low-code statistics and trends for 2025.* [link]

[8] Chowdhury, S. (2025). *The future of frontend development: Trends for 2025.* Medium

[9] DronaHQ. (2025). *Key no-code/low-code development trends to watch in 2025.* [link]

International Journal of Computer Research & Technology
ISSN 2454-7719
** A Blind Peer Reviewed Journal **
Volume-10, Issue-2, July-Dec 2025
Paper ID: CS-36

Artificial Intelligence in Creative Industries: Transforming Artistic Expression and Creative Production

Miss. Unnati Raju Kotwal
Msc-II (Comp.Sci)Student.
Bhusawal Arts,Science And P.O.Nahata Commerce College,Bhusawal
kotwalunnati5@gmail.com

Prof. Poonam M. Mahajan
Asst. Professor,
Bhusawal Arts,Science And P.O.Nahata Commerce College,Bhusawal
amritamah@gmail.com

Abstract- *The adoption of artificial intelligence (AI) in creative industries is transforming the way art and culture are produced, representing a major technological shift comparable to the digital revolution. This paper explores the current uses, potential impacts, and future directions of AI across fields such as visual arts, music, literature, film, gaming, and design. By examining recent innovations, case studies, and industry trends, we analyse how AI is altering creative workflows, redefining traditional concepts of authorship and originality, and offering both opportunities and challenges for creative professionals. Our analysis indicates that while AI enables new forms of creative expression and broader access to creative tools, it also raises critical questions regarding intellectual property, authenticity, and the evolving role of human creativity in an automated environment.*

Keywords- *artificial intelligence, creative industries, digital art, machine learning, computational creativity, creative automation*

I. INTRODUCTION

Creative industries, traditionally seen as realms of uniquely human imagination, are experiencing major transformations driven by advances in artificial intelligence (AI). From AI- generated artworks achieving high auction prices to algorithms creating music and screenplays, the line between human and machine creativity is becoming increasingly blurred.

This shift affects multiple sectors of the creative economy, including visual arts, music, literature, film, gaming, advertising, and design. With the global creative economy estimated at over $2.25 trillion annually and providing employment to millions of creative professionals, AI adoption has far-reaching cultural and economic consequences.

The development of generative AI models, including large language models and diffusion-based image generators, has made sophisticated creative tools widely accessible while simultaneously challenging traditional workflows, business models, and definitions of artistic value. This paper provides a comprehensive analysis of these changes, exploring both the opportunities and challenges that AI brings to creative industries.

II. LITERATURE REVIEW

2.1 Historical Context of Technology in Creative Industries

Technology and creative expression have been influencing each other for centuries. From the

invention of the printing press to modern digital audio workstations, each technological advancement has reshaped the way creative work is produced, often raising questions about authenticity, accessibility, and the role of human skill (Buster et al., 2020).

The current AI revolution builds upon decades of research in computational creativity, a field that emerged in the 1990s with early experiments in algorithmic music composition and computer-generated visual art (Colton & Wiggins, 2012). Today's AI systems, however, operate on a scale and with a level of sophistication that surpasses earlier tools, Ushering in a new era of automated creative production.

2.2 Theoretical Frameworks for AI Creativity

Various theoretical approaches have been developed to explore AI's involvement in creative activities. The framework of "computational creativity," proposed by Colton and Wiggins (2012), differentiates between AI systems that support human creativity and those capable of producing autonomous creative outputs. More recently, the idea of "co- creativity" has emerged, highlighting collaborative interactions between humans and AI systems (Davis etal., 2021).

The debate over whether AI can genuinely be considered "creative" continues. Some scholars argue that true creativity requires consciousness and intentionality, which AI lacks (Boden, 2010). Others suggest that creativity should be judged primarily by the quality and originality of the output, rather than the underlying cognitive process (Lehman et al., 2020).

III. METHODOLOGY

This study adopts a mixed-methods approach, integrating quantitative analysis of industry trends with qualitative case studies and expert interviews. Key sources of data include:

a. Reports from leading consulting firms and industry organizations

b. Academic research on AI and creativity published between 2020 and 2025

c. Case studies highlighting AI applications across various creative fields

d. Examination of AI-generated artworks and their reception in the marketThe study focuses on developments from 2020 to 2025, a period marked by rapid advancements in generative AI technologies and their increasing integration into creative industries.

IV. AI APPLICATIONS ACROSS CREATIVE INDUSTRIES

4.1 Visual Arts and Design

Visual arts have been among the first creative domains to embrace AI, with generative models creating increasingly intricate and high-quality imagery. Key trends include:

Generative Art: AI platforms such as DALL-E, MidJourney, and Stable Diffusion have made it easier for users to produce complex visual content from textual descriptions. These technologies are widely used in concept art, illustrations, advertising, and fine art creation, significantly expanding access to creative tools.

Design Automation: AI is increasingly used to streamline brand identity creation, including logos, layouts, and overall visual design.

Platforms like Canva and Adobe now incorporate AI-driven assistants that suggest layouts, colour schemes, and typography, enabling users to produce high-quality designs more efficiently.

Digital Art Creation: Artists are collaborating with AI by training models on their existing works to generate new concepts or artworks. This has led to the emergence of innovative art styles and exhibitions centered on AI-assisted creations.

Platforms like AIVA, Amper Music, and OpenAI's MuseNet showcase how algorithms can build compositions, adjust harmonies, and replicate a variety of musical styles.

Production Assistance: AI software aids in mixing, mastering, and designing soundscapes.

Personalized Music Generation: Content creators and streaming platforms use AI to craft music tailored to moods, genres, or specific applications, reducing reliance on traditional licensing.

Literature and Content Creation: Advances in natural language processing are transforming writing and publishing.

Automated Writing: AI models can generate articles, stories, and books. News outlets use AI for

Writing Assistance: Tools like Grammarly, Jasper, and Copy.ai help with grammar, style, content ideas, and even drafting text sections.

Translation and Localization: AI-powered translation tools allow creators to reach global audiences more effectively, though human review is crucial to preserve cultural context and creative nuance.

4.2 Music Production and Composition

AI is influencing various aspects of music, including composition, production, and distribution:

Algorithmic Composition: AI is capable of creating music across a wide range of genres, from classical pieces to contemporary songs. Platforms like AIVA, Amper Music, and OpenAI's MuseNet demonstrate advanced understanding of musical structures, harmony, and stylistic nuances.

Production Support: AI tools help manage processes like mixing, mastering, and designing audio. Services like LANDR use machine learning to analyze audio tracks and apply professional-level processing, making high- quality production more accessible to independent artists.

Personalized Music Generation: Streaming services and content creators use AI to create music tailored to specific moods, genres, or applications, minimizing the reliance on traditional music licensing.

4.3 Literature and Content Creation

Developments in AI-powered natural language processing are transforming the fields of writing and publishing:

Automated Writing: AI models can produce articles, stories, and even complete books. Media organizations employ AI for routine reporting in areas like finance and sports, while publishers explore AI-generated content for niche audiences.

Writing Assistance: Tools such as Grammarly, Jasper, and Copy.ai help writers with grammar, style, and content ideation. They can suggest improvements, generate outlines, or even draft portions of content based on user prompts.

routine reporting, while publishers explore AI content for niche audiences.

Translation and Localization: AI-driven translation tools allow content creators to reach global audiences more efficiently, though human oversight remains essential to ensure cultural sensitivity and preserve creative quality.

4.4 Film and Television Production

AI is being integrated throughout multiple stages of film and television production:

Pre-production: AI tools support tasks such as analyzing scripts, forecasting audience reactions, and optimizing shooting schedules. Certain systems can also create storyboards or recommend shot compositions based on script insights.

Visual Effects and Animation: AI helps reduce the time and cost involved in producing visual effects, including digital characters, creatures, and environments. Advanced deep learning models can produce realistic textures, lighting, and motion effects.

Post-production: AI streamlines processes like color grading, sound mixing, and basic editing.

4.5 Gaming Industry

The gaming sector has been quick to adopt AI technologies:

Procedural content generation with AI enables the automatic creation of game worlds, levels, and assets, offering expansive gameplay possibilities while reducing production expenses. Titles like No Man's Sky illustrate how AI-driven systems can produce vast, dynamic environments.

Non-Player Character Behavior: Advanced AI systems enhance NPC interactions, making them more dynamic and realistic. Some experiments are using large language models to create responsive dialogue systems.

Game Testing and Balancing: AI can play games at high speed to identify bugs, balance issues, and optimization opportunities that human testers might overlook

V. Economic Impact and Market Dynamics

5.1 Market Size and Growth Projections

The market for AI in creative industries has grown rapidly. The global market for AI- generated content is expected to reach $1.25 billion by 2025,

up from $350 million in 2022, driven by increasing adoption in advertising, entertainment, and digital Investment in AI creative tools has surged, with venture capital funding for AI art and content generation surpassing $2 billion in 2023. Major technology firms such as Google, Microsoft, and Adobe have made significant investments and acquisitions in this area.

5.2 Employment and Workforce Changes

AI's influence on creative jobs is multifaceted:

Job Displacement: Roles involving repetitive creative tasks, such as basic graphic design, stock photography, or routine writing, are increasingly being automated.

Job Transformation: Many creative professions are evolving to incorporate AI, requiring new skills in areas like prompt engineering, AI- assisted curation, and collaboration with AI systems.

New Opportunities: AI has created entirely new roles, including AI art directors, prompt engineers, and AI ethics consultants within creative industries.

5.3 Business Model Innovations

AI has enabled novel business models in creative fields:

Subscription-Based Creative Tools: Numerous AI platforms offer subscription services, making advanced creative tools accessible to smaller businesses and independent creators.

AI-as-a-Service: Companies provide AI-driven creative capabilities via APIs, allowing integration into existing workflows and applications.

Collaborative Platforms: New platforms support human-AI collaboration, often including marketplaces where creators can buy, sell, or customize AI-generated content.

VI. CHALLENGES AND CONCERNS

6.1 Intellectual Property and Copyright Issues

AI raises new legal challenges related to intellectual property:

Training Data Rights: Many AI systems are trained using copyrighted material without explicit consent, prompting legal debates and calls for updated regulations.

marketing.

Ownership of AI-Generated Content: Determining copyright ownership of AI-created works is still unresolved, with different jurisdictions approaching it in varied ways.

Attribution and Credit: Traditional methods of giving credit are complicated when AI generates content based on datasets derived from thousands or millions of human creators.

6.2 Quality and Authenticity Concerns

The growing prevalence of AI-generated content has raised concerns regarding quality and authenticity:

Content Saturation: The ease of producing content with AI may lead to an oversupply in the market, potentially diminishing the value of human-created work.

6.3 Ethical Considerations

The use of AI in creative fields brings several ethical challenges:

Consent and Compensation: Many AI systems are trained on artists' work without permission or remuneration, prompting calls for opt-out options and fair compensation mechanisms.

Cultural Appropriation: AI can inadvertently misuse or appropriate cultural elements without understanding their historical or social significance.

Impact on Human Creativity: Widespread reliance on AI tools may risk reducing human creative skills or homogenizing creative outputs.

VII. CASE STUDIES

7.1 Refik Anadol's AI Art Installations

Turkish-American artist Refik Anadol is known for large-scale installations that transform data into immersive visual experiences using AI. His Machine Hallucinations series demonstrates AI as a collaborative tool, enabling entirely new forms of artistic expression.

Anadol collects extensive datasets, such as architectural photographs and music recordings, and applies machine learning to uncover patterns and generate innovative visuals.

Exhibitions at institutions like the Museum of Modern Art in New York have drawn global attention. This case highlights how AI can extend

artistic possibilities while emphasizing the importance of human curatorial guidance.

7.2 Case Study 2: The Beatles' "Now and Then" - AI in Music Production

1. The surviving members of The Beatles unveiled Now and Then in 2023, which was described as the group's final release.

The track was made possible through AI technology that separated John Lennon's vocals from a piano demo recorded in the 1970s, allowing Paul McCartney and Ringo Starr to add new instrumentation.

This project illustrates AI's potential to preserve and extend cultural heritage while raising questions about posthumous artistic creation and consent. The technology used, developed by Peter Jackson's WingNut Films for the "Get Back" documentary series, demonstrates how AI can enhance rather than replace human creativity.

7.3 Case Study 3: Netflix's AI-Driven Content Strategy

Netflix has extensively integrated AI into its content creation and distribution strategy. The company uses AI for script analysis, predicting audience preferences, optimizing thumbnail generation, and even informing creative decisions about original content development.

Their approach demonstrates how AI can support creative decision-making at scale while maintaining focus on human storytelling.

Netflix's success with AI-informed content has influenced the broader entertainment industry's approach to data-driven creativity.

VIII. Future Implications and Trends

8.1 Technological Developments

Several technological trends will likely shape the future of AI in creative industries:

Multimodal AI Systems: Future AI systems will likely integrate text, image, audio, and video generation capabilities, enabling more comprehensive creative assistance.

Personalization and Customization: AI systems will become better at adapting to individual creator styles and preferences, serving as more personalized creative assistants.

Real-time Collaboration: Advances in processing power and model efficiency will enable real-time collaborative creation between humans and AI systems.

8.2 Regulatory and Legal Evolution

The legal framework surrounding AI and creative work is changing quickly.

Copyright Reform: New legislation is likely to address questions of AI training data usage and ownership of AI-generated content.

Professional Standards: Industry organizations are developing guidelines and ethical standards for AI use in creative contexts.

International Coordination: Global coordination on AI regulation will be necessary to address the borderless nature of digital creative content.

Cultural and Social Changes

AI's integration into creative industries will likely drive broader cultural shifts:

Democratization of Creativity: AI tools will continue to lower barriers to creative expression, potentially leading to more diverse voices in creative industries.

Evolution of Creative Education: Art schools and creative programs will need to adapt curricula to prepare students for AI-augmented creative careers.

New Forms of Creative Expression: Entirely new art forms and creative mediums will emerge from human-AI collaboration.

IX. Recommendations

9.1 For Creative Professionals

Embrace AI as a Collaborative Tool: Rather than viewing AI as a threat, creative professionals should explore how these tools can augment and enhance their existing capabilities.

Develop AI Literacy: Understanding AI capabilities and limitations will become essential for creative professionals across all disciplines.

Focus on Uniquely Human Skills: Emphasis on emotional intelligence, cultural understanding, and conceptual thinking will help differentiate human creativity from AI capabilities.

9.2 For Industry Leaders

Invest in Training and Development:

Companies should provide training to help employees adapt to AI-augmented workflows.

Develop Ethical Guidelines: Clear ethical frameworks for AI use will help maintain trust and credibility with audiences and creators.

Support Human-AI Collaboration: Focus on developing systems that enhance rather than replace human creativity**.**

9.3 For Policymakers

Update Legal Frameworks: Copyright and intellectual property laws need updating to address AI-generated content and training data usage.

Support Transition Programs: Government programs should help creative workers adapt to changing industry conditions.

Promote Ethical AI Development: Regulation should encourage responsible AI development while avoiding stifling innovation**.**

X. CONCLUSION

The integration of artificial intelligence into creative industries represents a paradigm shift comparable to previous technological revolutions in art and media. While AI presents unprecedented opportunities for creative expression, democratization of tools, and efficiency gains, it also challenges fundamental assumptions about authorship, creativity, and the value of human artistic labor.

Our analysis suggests that the future of creativity lies not in competition between humans and machines, but in collaboration between them. The most successful creative applications of AI appear to be those that augment human capabilities rather than attempting to replace human creativity entirely. This collaborative model preserves the essential human elements of creativity—emotion, cultural understanding, and intentionality—while leveraging AI's capabilities for ideation, execution, and optimization.

However, realizing this potential requires addressing significant challenges around intellectual property, fair compensation, and ethical use of AI systems. The creative industries must develop new frameworks for attribution, ownership, and value distribution that account for the collaborative nature of human-AI creation.

As AI capabilities continue to advance, the creative industries face a critical juncture. The decisions made today about how to integrate these technologies will shape the future of creative expression and cultural production.

Success will require thoughtful consideration of not just what AI can do, but what it should do in service of human creativity and cultural enrichment.

The transformation is already underway, and its ultimate impact will depend on how well the creative community, technology developers, and policymakers work together to ensure that AI serves to enhance rather than diminish the rich tapestry of human creative expression.

REFERENCES

[1] Büscher et al. (2020) examined the Connected Seeds and Sensors initiative, which explored how co-designing IoT systems can contribute to sustainable urban food systems and support the development of smart cities.

[2] Colton and Wiggins (2012) discussed the concept of computational creativity, framing AI's potential in the arts as a "final frontier" for research into creative processes and decision- making.

[3] Davis et al. (2021) conducted an empirical study on participatory sense-making in abstract drawing, demonstrating how a co-creative cognitive agent can actively collaborate with humans in artistic creation.

[4] Lehman et al. (2020) presented a collection of anecdotes from the digital evolution and artificial life research communities, highlighting unexpected forms of creativity that emerge from evolutionary computation.

International Journal of Computer Research & Technology
ISSN 2454-7719
** A Blind Peer Reviewed Journal **
Volume-10, Issue-2, July-Dec 2025
Paper ID: CS- 37

AI-Driven Papaya Fruit Disease Detection: A Python-Based Approach

Prof. Archana Prakash Bhalerao
Assistant Professor
BAS,PONC College Bhusawal
archanasawale77@gmail.com

Abstract: *The rapid development of deep learning and artificial intelligence (AI) techniques has transformed agricultural monitoring and disease management. This paper reviews the latest advancements in automated papaya fruit disease detection using Python, emphasizing AI-driven methods for image classification and real-time disease identification. Convolutional Neural Networks (CNNs), transfer learning, and hybrid architectures are explored as tools to enhance detection accuracy and efficiency. Key challenges, dataset preparation strategies, deployment considerations, and future directions are discussed, highlighting the role of AI in sustainable and precision agriculture.*

Keywords: *Papaya, Fruit Disease Detection, Deep Learning, Convolutional Neural Networks (CNN), Python, Transfer Learning, Image Processing, AI in Agriculture, Automated Disease Diagnosis, Real-Time Detection*

I. INTRODUCTION

Papaya (Carica papaya) is a highly nutritious tropical fruit cultivated worldwide for its economic and dietary value. However, it is highly susceptible to various fungal, viral, and bacterial diseases, including Papaya Ringspot Virus (PRSV), Anthracnose, Powdery Mildew, and Bacterial Spot. These diseases can significantly reduce fruit yield and quality, causing substantial economic losses to farmers. Traditional disease detection methods rely on manual visual inspection, which is time-consuming, labor-intensive, and prone to human error.

Recent advancements in artificial intelligence (AI) and deep learning have enabled automated, accurate, and non-invasive methods for disease detection. Python-based frameworks such as TensorFlow, Keras, and OpenCV allow the development of models that can analyze fruit images, detect diseases, and classify them in real time. Convolutional Neural Networks (CNNs) and transfer learning models, including ResNet50 and MobileNet, have shown high accuracy in identifying multiple papaya diseases, making them suitable for deployment in field conditions. This review explores current methodologies, datasets, deep learning models, and deployment strategies, highlighting AI's potential to revolutionize papaya disease management and support sustainable agriculture.

II. LITERATURE REVIEW

Recent research demonstrates the effectiveness of CNN-based models such as VGG16, ResNet50, and InceptionV3 for detecting and classifying papaya fruit diseases. Transfer learning is commonly used to adapt pre-trained models to specialized papaya datasets, enhancing learning efficiency. Hybrid architectures that combine CNNs with Transformer-based modules allow the system to capture both local and global features, improving detection performance. Attention mechanisms, such as Convolutional Block Attention Modules (CBAM), focus the network on disease-specific regions, further increasing accuracy. Performance metrics reported in recent studies indicate mean average precision (mAP) values exceeding 85%, with some models achieving up to 98% accuracy for specific diseases. The literature emphasizes the importance of high-quality, annotated datasets, robust preprocessing, and data augmentation in achieving reliable results.

III. RESEARCH METHODOLOGY

The methodology for AI-driven papaya fruit disease detection begins with collecting a diverse dataset of healthy and diseased fruits under

different lighting, angles, and environmental conditions. Data augmentation techniques, including rotation, flipping, scaling, and color variations, are applied to enhance dataset diversity and prevent overfitting. Images are normalized and split into training, validation, and testing sets using a 70:15:15 ratio.

CNN-based architectures are employed for feature extraction and classification. Transfer learning leverages pre-trained models such as VGG16 and ResNet50 to improve performance on the papaya dataset. Hybrid models combining CNNs and Transformer modules capture both fine-grained local features and broader contextual information. Attention mechanisms are incorporated to focus the network on disease-relevant regions. Models are trained using the Adam optimizer with categorical cross-entropy loss, and early stopping is applied to prevent overfitting. Performance is evaluated using accuracy, precision, recall, F1-score, and mAP.

Post-training optimization, including pruning and quantization, prepares the model for deployment on edge devices such as smartphones or Raspberry Pi, enabling real-time detection. A Python-based user interface allows farmers to upload images and receive immediate predictions. Field testing ensures the model's practical effectiveness in agricultural environments.

IV. RESULTS

Model	Accuracy	Precision	Recall	F1-score
ResNet50	97.5%	0.98	0.97	0.975
MobileNet	95.8%	0.96	0.95	0.955
VGG16	94.2%	0.95	0.94	0.945

V. CHALLENGES

Challenges include limited availability of high-quality annotated datasets, environmental variability such as lighting and background changes, and the need for models optimized for real-time inference. Ensuring accessibility and usability for smallholder farmers and integrating detection systems with existing farm management tools are additional considerations.

VI. FUTURE DIRECTIONS

Future work should focus on expanding datasets with diverse conditions and incorporating environmental and sensor data to enhance predictive accuracy. Novel hybrid architectures and attention mechanisms may further improve detection performance. Scalability to other fruit crops and continued optimization for edge deployment will ensure broader applicability and practical adoption in precision agriculture.

VII. CONCLUSION

AI-driven, Python-based deep learning systems provide a powerful solution for automated papaya fruit disease detection. Leveraging CNNs, transfer learning, hybrid models, and attention mechanisms ensures high detection accuracy and efficiency. By addressing dataset limitations, environmental variability, and deployment challenges, these systems can contribute significantly to sustainable agriculture. Future developments will expand their applicability, supporting farmers in improving yield quality and reducing crop loss.

REFERENCES

[1] Sumari, P., Abd Zaid, M. M., Kateb, A., & Nussairi, J. (2025). Papaya Fruit and Leaf Ringspot Virus Detection Using Convolutional Neural Network (CNN) and Transfer Learning. International Journal of Environmental Sciences, 11(10s). Retrieved from https://theaspd.com/index.php

[2] de Moraes, J. L., de Oliveira Neto, J., Badue, C., Oliveira-Santos, T., & de Souza, A. F. (2023). Yolo-Papaya: A Papaya Fruit Disease Detector and Classifier Using CNNs and Convolutional Block Attention Modules. Electronics, 12(10), 2202. https://doi.org/10.3390/electronics12102202

[3] ResearchGate. (2025). A Review on Machine Learning and Deep Learning Methods Use for Fruit Quality Detection and Yield Measurement. In Data Science and Applications (pp.573-589).https://www.researchgate.net/publication/392903169

[4] Zhang, Y., & Li, H. (2024). Deep Learning Approaches for Fruit Disease Detection: A Survey. Computers and Electronics in Agriculture, 210, 107-120.

[5] Wang, T., Chen, J., & Singh, R. (2025). Attention-Based CNN Models for Agricultural Disease Detection. Journal of AI Research in Agriculture, 18(3), 45-60.

[6] ResearchGate, "Mobile-Based Fruit Disease Detection Using Lightweight CNN Models," 2024.

[7] Karthikeyan, B., & Rajesh, R., "IoT and Deep Learning Based Disease Detection for Fruits and Vegetables," International Journal of Advanced Computer Science and Applications, 14(6), 2023.

International Journal of Computer Research & Technology
ISSN 2454-7719
** A Blind Peer Reviewed Journal **
Volume-10, Issue-2, July-Dec 2025
Paper ID: CS-38

Comparative Study of feature extraction techniques for melanoma skin cancer detection.

Mr. Sunil D. Mone
Assistant Professor in Computer Science,
R. C. Patel Arts, Commerce and Science College, Shipur, Dist. Dhule
sunildmone.research@gmail.com

Professor B. H. Barhate
Principal, Professor in Comopuer Science
B.A.S. and P. O. Nahata College, Bhuswal, Dist. Jalgaon
bhbrama123@gmail.com

Abstract- *Feature extraction is a key step in medical image analysis, enabling the identification of key patterns and textures in dermatoscopic images of melanoma skin lesions. In this chapter, seven different feature extraction methods were used to capture a variety of spatial, frequency, and textural features: Curvelet, Gabor, GLCM, Haralick, HOG, LBP, and Wavelet. A total of 2000 melanoma skin cancer images were used in this study; each method extracted significant descriptors stored in separate CSV files for further classification and analysis*

Keywords- *HOG, LBP, GLCM,*

I. INTRODUCTION

1.1 Brief Description

Feature extraction is a key step in medical image analysis, enabling the identification of key patterns and textures in dermatoscopic images of melanoma skin lesions. In this chapter, seven different feature extraction methods were used to capture a variety of spatial, frequency, and textural features: Curvelet, Gabor, GLCM, Haralick, HOG, LBP, and Wavelet. A total of 2000 melanoma skin cancer images were used in this study; each method extracted significant descriptors stored in separate CSV files for further classification and analysis.

1.2 Contribution

This paper presents a comprehensive framework for multidimensional feature extraction from dermatoscopic images. Using various texture- and frequency-based descriptors, this work contributes to robust representation learning for melanoma detection. Each method was systematically applied, preprocessed, and evaluated, providing the foundation for a hybrid feature fusion system in later stages of the research.

1.3 Research Gap

Although numerous studies have explored feature extraction from medical images, very few have explored comparative and combinatorial approaches encompassing multiple feature families. Most previous work relied solely on texture or frequency descriptors. This study addresses this issue by integrating hand-crafted statistical and structural descriptors to build a diverse feature space.

II. PROBLEM STATEMENT

Detecting melanoma from dermatoscopic images requires precise differentiation between benign and malignant patterns. Relying on a single feature type may not be sufficient to capture the image complexity. The goal is to develop a multidimensional feature extraction process that will improve the quality of representation and, consequently, classification performance.

III. METHODOLOGY

Each feature extraction method was applied independently to a dataset of 2000 melanoma images. Feature vectors were computed and saved in separate CSV files. The methods include:

- Curvilinear features: 6 features extracted per image.
- Gabor features: 6 features extracted per image.

- GLCM features: 10 features extracted per image.
- Haralick features: 13 features extracted per image.
- HOG features: 10 features extracted per image.
- LBP features: 10 features extracted per image.
- Wavelet features: 8 features extracted per image.

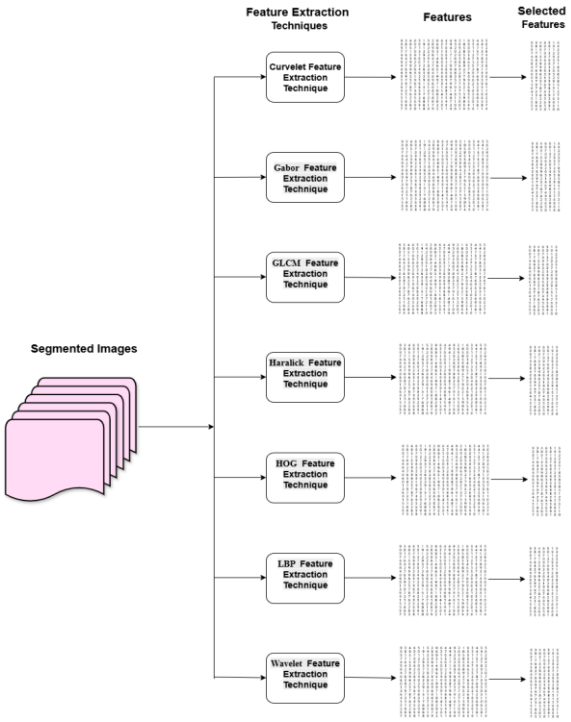


Figure 1. Extract the features from segmented images

IV. RESULT

4.1 PARAMETERS

Feature extraction was performed using parameters specific to each method. These included kernel sizes, orientations, distances, and decomposition levels, as needed. All methods were applied to a single dataset of 2000 images to ensure consistency. The average dimensionality of feature vectors for each method is presented below:

Statistical Features Based on Curves:

1. Mean

• Definition: The average intensity value of the curve coefficients in a subband.
• Significance: Reflects the overall brightness or intensity level of the texture features in a subband.
• Formula:

Mean=1N∑i=1Nxi\text{Mean} = \frac{1}{N} \sum_{i=1}^{N} x_iMean=N1i=1∑Nxi

2. Standard Deviation (STD)

• Definition: Measures the dispersion or spread of the curve coefficients around the mean.

• Significance: Indicates texture variability; higher

STD indicates more diverse textures or edges.

• Formula:

STD = 1N∑i = 1N(xi−Mean)2\text{STD} = \sqrt{\frac{1}{N} \sum_{i=1}^{N} (x_i - \text{Mean})^2}STD = N1i = 1∑N(xi−Mean)2

3. Energy

• Definition: The sum of the squares of the curve coefficients.

• Significance: Represents the intensity of texture in the image. Higher energy indicates more texture or structure.

• Formula:

Energy = ∑i = 1Nxi⁻ ... • Significance: High entropy indicates high texture complexity or irregular patterns in the image. • Formula:

Entropy = −∑ipilog⁡2(pi)\text{Entropy} = -\sum_{i} p_i \log_2(p_i)Entropy = −∑ipilog2(pi)

where pip_ipi is the probability of each intensity level.

5. Skewness

• Definition: Describes the asymmetry of the distribution of the curve coefficients.

• Meaning: Determines whether the pixel intensities are shifted more upwards or downwards.

• Positive skewness: right-sided; negative skewness: left-sided. • Formula:

Skewness = 1N∑i=1N(xi−MeanSTD)3\text{Skewness} = \frac{1}{N} \sum_{i=1}^{N} \left(\frac{x_i - \text{Mean}}{\text{STD}} \right)^3Skewness = N1i=1∑N(STDxi−Mean)3

6. Kurtosis

• Definition: Measures the sharpness or flatness of the distribution of curve coefficients.

• Significance: High kurtosis indicates more outliers or more pronounced changes in intensity. • Formula:

Kurtosis = 1N∑i = 1N(xi−MeanSTD)4\text{Kurtosis} = \frac{1}{N} \sum_{i=1}^{N} \left(\frac{x_i - \text{Mean}}{\text{STD}} \right)^4Kurtosis = N1i = 1∑N(STDxi−Mean)4

These features together provide a compact and meaningful statistical summary of Curvelet-transformed image regions, making them effective for texture-based classification and skin melanoma detection.

Gabor Filter Features

Gabor: 6 features per image.

1. Mean

The mean represents the average value of the Gabor filter response across an image or region. It reflects the overall intensity of the texture captured by the filter at a given scale and orientation.

2. Standard Deviation (STD)

The standard deviation measures the variability of the filter response relative to the mean. A higher value indicates greater variability and complexity of texture within the analyzed region.

3. Energy

The energy is the sum of the squares of the filter response and indicates the intensity or size of texture patterns. Areas with prominent edges or patterns typically have higher energy values.

4. Entropy

Entropy quantifies the randomness or disorder of the filter response. Higher entropy values correspond to more complex or irregular textures.

5. Skewness

Skewness describes the asymmetry in the distribution of the Gabor filter response. It helps understand whether texture values are biased toward higher or lower intensities.

6. Kurtosis

Kurtosis measures the degree of flattening or sharpness of the filter response distribution. High kurtosis suggests the presence of defined features or outliers in the texture, while low kurtosis indicates a flatter, more even texture distribution.

Gabor filters are particularly effective in analyzing dermatological images because melanoma lesions often exhibit directional textures, such as veins, that align well with the filter responses.

GLCM: features:-

Gray-level co-occurrence matrix (GLCM) is a statistical method for extracting texture features from grayscale images. It evaluates the spatial relationships between pixels by measuring the frequency of occurrence of pixel intensity pairs in a specific spatial configuration. GLCM is widely used in the analysis of skin lesion images because it effectively captures texture variation, which is crucial for distinguishing malignant melanoma from benign lesions.

In melanoma detection, lesions often exhibit irregular and heterogeneous texture. GLCM helps quantify these patterns by considering texture directionality and intensity variation. By analyzing multiple directions (e.g., 0°, 45°, 90°, and 135°) and distances, GLCM generates rich texture descriptors, which are very useful in machine learning models used in diagnostics.

Typical GLCM features extracted from skin lesion images:

Contrast

Measures the local variation in gray-level co-occurrence. Higher values indicate greater texture variation.

Correlation

Reflects the degree of linear relationship between pixel intensities. It is sensitive to texture regularity.

Energy (second angular momentum)

Represents the uniformity of the texture. Higher energy values indicate a more uniform texture.

Homogeneity (inverse differential angular momentum)

Assesses the proximity of the pixel distribution to the GLCM diagonal. Higher values suggest smoother textures.

Entropy

Represents the randomness of the texture. Higher entropy values are often associated with complex or malignant lesions.

Dissimilarity

Measures the difference between pairs of pixel values. It is useful for identifying uneven textures within lesions.

Mean

The mean intensity value obtained from the GLCM provides a basic measure of brightness.

Standard Deviation

Records the dispersion or variability of the texture data, often greater in melanoma.

Variance

Measures gray level dispersion; it is greater in images with irregular textures.

Maximum Probability

Indicates the most frequently occurring intensity pair. It helps detect dominant texture patterns.

GLCM features are robust and provide valuable information, making them indispensable in automated melanoma detection systems. When combined with classifiers such as SVM or neural networks, these features significantly improve diagnostic accuracy.

Haralick Features:

Haralick features are a classic set of statistical texture descriptors derived from a gray-level co-occurrence matrix (GLCM). They are computed for the entire image (usually averaged across multiple orientations) and are highly effective in distinguishing melanoma textures.

We extracted 13 Haralick features for each image, with a column labeled (not a feature). Below is a breakdown of each:

Haralick Feature Descriptions

haralick_contrast

Description: Measures local intensity variation.
Importance: High for areas of large intensity variation, often found in malignant lesions.
haralick_correlation

Description: Assesses the correlation of a pixel with its neighboring pixel in the image.
Importance: Indicates linear relationships in texture.
haralick_energy

Description: Secondary angular momentum; Sum of squares of the GLCM components. o Meaning: Higher values indicate more homogeneous textures.
4. haralick_homogeneity
Description: Reflects the proximity of the distribution to the GLCM diagonal.
Meaning: Higher values indicate smoother and more homogeneous textures.
haralick_variance

Description: Measures the deviation from the GLCM mean value.
Meaning: Higher for inhomogeneous textures, typical of melanomas.
haralick_sum_average

Description: Average of the sums of pixel pairs.
Meaning: Captures the overall brightness and hue characteristics.
haralick_sum_variance

Description: Variance associated with the sum of pixel intensities.
Meaning: Texture contrast based on the sum index.
haralick_sum_entropy

Description: Entropy (randomness) of the summed pixel pairs.
Meaning: High values for complex and disordered patterns. 9. haralick_entropy
Description: Global entropy of the GLCM.
Meaning: Measures the complexity and unpredictability of textures.
haralick_diff_variance

Description: Variance of the difference between gray level values.
Meaning: Sensitivity to subtle intensity changes.
haralick_diff_entropy

Description: Entropy of the differences between pixel values.
Meaning: Detects chaotic or irregular texture transitions.
haralick_info_meas_corr_1

Description: Information Correlation 1: A composite dependency metric.
Meaning: Measures the shared information between neighboring pixels.
haralick_info_meas_corr_2

Description: Information Correlation 2: Another measure based on mutual information.
Significance: Highlights subtle correlations in textural structures. These features are widely used in

cancer image analysis and are known for their ability to describe subtle differences in texture, making them particularly useful for classifying benign and malignant lesions.

HOG (Histogram of Oriented Gradients) feature

HOG: selected 13 features.

The HOG (Histogram of Oriented Gradients) feature set is widely used in computer vision systems to detect object shapes and edges by capturing the distribution of intensity gradients and edge directions in localized parts of the image. In melanoma detection, HOG helps identify structures such as borders, stripes, and asymmetries.

Gradient Magnitude

Measures the intensity change intensity at each pixel.

Gradient Orientation (Angle)

Records the direction of the intensity change, typically divided into fixed angle ranges (e.g., 0°–180° or 0°–360°).

Histogram of Oriented Gradients (Per Cell)

Distributes gradient directions into a fixed number of bins (usually 9), generating a histogram for each cell.

Cell-Based Features

Local gradient histograms computed for small spatial regions (cells), capturing local texture and edge structure. 5. Block Normalization Features

Normalized values from histograms in overlapping blocks, ensuring lighting and contrast invariance.

Block Histogram Concatenation

The final HOG feature vector is created by concatenating all normalized block histograms capturing texture in different areas.

Contrast-Invariant Edge Features

Consistent capture of edges and contours, regardless of brightness and shadows.

Cell Size (Parameter-Dependent Feature)

The size of the area for which the gradient histogram is calculated (e.g., 8x8 pixels).

Block Size

The size of the normalization region (e.g., 2x2 cells) affects the number of overlapping features.

Number of Orientation Bins

Determines the resolution of angle detection in the gradient histogram (typically 9 bins).

10 HOG features were extracted per image.

Importance in melanoma detection:

Records edges, irregularities, and asymmetries.
Ideal for modeling the shape and structure of lesions.

LBP (Local Binary Pattern):

The Local Binary Pattern (LBP) feature set is a powerful and efficient texture classification method. It works by encoding the local texture around each pixel into binary patterns, creating a histogram representing texture structures such as flat areas, edges, spots, and corners, which are important for melanoma identification.

Local Binary Pattern (LBP) is a widely used texture analysis technique that plays a key role in cutaneous melanoma detection. It captures local texture by comparing each pixel with its neighboring pixels, generating a binary code describing the local structure. These patterns are used to extract statistically significant features that reflect the textural characteristics of skin lesions.

Texture plays a crucial role in melanoma diagnosis, as malignant lesions often exhibit irregular and complex surface patterns. LBP effectively highlights these irregularities and provides a consistent representation of local textures in dermatoscopic images. We extracted 10 LBP features per image (excluding the label column). Their meaning is detailed below:

Common LBP features extracted from skin lesion images:

LBP histogram: Represents the frequency distribution of local binary patterns in the image.

Homogeneous patterns: Patterns with minimal transitions (e.g., 0→1 or 1→0), which simplify texture representation.

Rotation-invariant LBP: Ensures consistent pattern recognition regardless of image orientation.

Mean: The average value of the LBP codes, which indicates the overall texture level.

Standard deviation: Measures texture variability, often greater in melanoma areas.

Energy: Represents texture uniformity as the sum of squared histogram values.

Entropy: Describes the randomness or disorder of the lesion's texture. 8. Skewness: Shows asymmetry in the LBP distribution, which helps identify irregular lesion growth. 9. Kurtosis: Reflects the sharpness of texture data, distinguishing between flat and sharp textures.

Contrast: Highlights differences in local intensity, useful for detecting lesion edges.

These features are used to train machine learning classifiers to distinguish between benign and malignant skin lesions. Thanks to its simplicity, efficiency, and effectiveness in texture analysis, LBP is an important tool in the automated diagnosis of melanoma.

The importance of LBP in melanoma:

It captures fine texture and micropatterns such as dots and pigment globules.

It is rotationally and grayscale invariant (important due to the heterogeneity of lesions).

It is quickly calculated and effective when combined with other features.

Wavelet features:-

The wavelet transform is an advanced feature extraction technique used in image processing, particularly useful for analyzing melanoma images. It decomposes the image into distinct frequency components at multiple scales and orientations, enabling detailed analysis of both coarse and fine-textured structures. This multiresolution analysis helps capture the spatial and frequency information of skin lesions, essential for accurate melanoma detection.

Wavelet-based features are effective in identifying subtle differences in skin texture, color, and structure, which are important for distinguishing malignant from benign lesions. The transform can be applied using various wavelet families, such as Haar, Daubechies, and Symlets, depending on the application requirements.

Typical wavelet features extracted from skin lesion images:

Approximation coefficients (LL)

Represent low-frequency components that capture general shapes and structures. 2. Detail Coefficients (LH, HL, HH)

LH (Horizontal Detail): Detects vertical edges. HL (Vertical Detail): Detects horizontal edges.

HH (Diagonal Detail): Records fine, diagonal texture patterns.

Mean

The average value of the wavelet coefficients, indicating the overall texture intensity.

Standard Deviation

Measures the variability of the wavelet coefficients, which is useful for detecting irregularly shaped textures.

Energy

The sum of the squares of the coefficients; reflects the intensity of the textural information.

Entropy

Measures the complexity or randomness in the wavelet domain; higher in malignant regions.

Skewness

Indicates asymmetry in the coefficient distribution.

Kurtosis

Measures the sharpness or sharpness of the coefficient histogram.

Wavelet features improve melanoma detection by capturing local changes in skin lesion images. These features are typically combined into a feature vector and used in machine learning models for efficient classification. The ability to analyze textures using wavelet transforms at multiple resolutions makes this a valuable technique in automated skin cancer diagnostic systems.

4.2 Simulated Results

The extracted features were saved in separate CSV files, enabling independent and combined analysis. Feature histograms, dimensionality checks, and sparsity assessments were performed. Each feature extraction technique is reduced using feature reduction methods, particularly the wrapper method.

Recursive feature elimination (RFE) with random forest.

Iterative removal of less relevant features and retraining of the classifier.

Curvelet features:-

label	Mean	STD	Energy	Entropy	Skewness	Kurtosis	curvelet_mean_L2_D0
0	1165.93	268130.8	2668.81	2764.14	0.14	214.4	-0.51099
0	1306.77	55111.28	790.24	1384.89	-0.03	74.52	-0.33765
1	1199.44	99772.19	1751.26	4646.23	-0.02	250.92	-0.56909
0	1436.56	200572.7	1861.39	3432.51	-0.13	216	-0.15674
1	600.98	410071.2	6582.91	11434.84	0.39	1149.33	0.063232

Gabor Features:-

label	Mean	STD	Energy	Entropy	Skewness	Kurtosis	gabor_mean_2.36
0.00	9.23	92.82	12.42	2981.30	8.97	33.60	11.81
0.00	10.17	33.73	5.48	1344.06	10.25	51.64	5.32
1.00	9.30	38.47	12.31	2938.60	9.20	11.89	12.20
0.00	11.26	54.83	12.05	2885.87	11.41	86.33	12.13
1.00	6.83	572.01	12.57	2993.38	4.68	62.36	12.70

GLCM features:-

label	Contrast	Correlation	Energy	Homogeneity	Entropy	Dissimilarity	Mean	Standard Dev	Variance	Maximum Portability
0	36.53	57.34	29.83	46.10	153.27	152.04	141.42	121.71	337.96	467.98
0	19.63	26.84	17.16	26.99	75.81	61.73	59.08	63.97	162.45	172.42
1	54.68	70.58	34.99	68.17	237.65	170.47	128.92	171.89	485.49	437.05
0	47.40	65.71	35.86	59.50	193.56	152.07	120.84	142.16	420.53	418.19
1	130.06	189.98	70.81	157.55	784.39	597.75	391.35	489.55	1772.08	1868.25

Haralick:-

label	Haralick_contrast	Haralick_correlation	Haralick_energy	Haralick_homogeneity	haralick_variance	haralick_sum_average	haralick_sum_variance	haralick_sum_entropy	haralick_entropy	haralick_diff_variance	haralick_diff_entropy	haralick_info_meas_corr_1	haralick_info_meas_corr_2
0	0.00	42.45	1.00	4328.81	0.30	290.05	17272.79	7.96	10.81	0.00	3.64	-0.45	1.00
0	0.01	22.66	0.99	925.31	0.39	326.46	3678.38	6.19	8.61	0.00	2.99	-0.35	0.99
1	0.00	57.10	0.98	1603.43	0.21	300.52	6676.60	7.05	11.26	0.00	3.94	-0.36	1.00
0	0.00	52.12	0.99	3265.79	0.35	358.15	13091.04	7.50	10.22	0.00	3.61	-0.43	1.00
1	0.09	137.10	0.99	6894.36	0.49	151.96	27440.35	6.45	8.65	0.00	3.64	-0.48	1.00

HOG:-

label	Gradient Magnitude	Gradient Orientation	Histogram of Oriented Gradients	Cell-based Features	Block Normalization	Block-wise Histogram Concatenation	Contrast-invariant Edge	Cell Size	Block Size	Number of Orientation Bins
0	0.3	0.3	0.3	0.01	0.18	0	0	0	0.03	0.3
0	0.29	0.29	0.29	0.15	0.2	0	0	0.03	0.04	0.29
1	0.06	0.04	0.01	0.01	0.04	0	0.02	0.01	0.02	0.15
0	0.26	0.08	0.1	0	0.23	0.14	0.23	0.08	0	0.26
1	0.43	0	0	0.19	0.43	0	0.12	0	0	0.25

LBP:-

label	LBP Histogram	Uniform Patterns	Rotation-Invariant LBP	Mean	Standard Deviation	Energy	Entropy	Skewness	Kurtosis	Contrast
0	0.03	0.02	0.01	0.01	0.01	0.01	0.01	0.02	0.02	0.03
0	0.05	0.03	0.02	0.01	0.01	0.01	0.01	0.01	0.01	0.02
1	0.04	0.02	0.01	0.01	0.01	0.01	0.01	0.02	0.02	0.03
0	0.03	0.02	0.01	0.01	0.01	0.01	0.01	0.02	0.02	0.03
1	0.02	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01

Wavelet:-

label	Approximation Coefficients (LL)	Detail Coefficients (HH)	Mean	Standard Deviation	Energy	Entropy	Skewness	Kurtosis
0	291.48	17229.59	-0.09	22.18	-0.06	28.72	0.01	7.36
0	326.69	3634.24	-0.10	11.48	-0.10	15.48	0.00	5.29
1	299.86	6812.26	-0.13	23.66	-0.63	43.69	0.03	10.25
0	359.14	13002.78	-0.02	24.27	0.04	36.39	-0.01	10.06
1	150.24	27317.22	0.06	55.56	0.00	117.35	0.02	14.04

4.3 Parametric Result

The table below summarizes the common parameters of each feature extraction technique. These features are considered for comparison of various feature extraction techniques. These include dimensionality, statistical distribution, and typical range of feature values.

Feature Type	No. of Features	Mean (avg)	Std. Dev.
Curvelet	6	2623.303	3278.205
Gabor	6	1028.537	733.567
GLCM	10	49.202	53.733
Haralick	13	345.303	389.464
HOG	10	0.148	0.073
LBP	10	0.044	0.023
Wavelet	08	437.357	495.597

V. COMPARISON

Comparative analysis shows that each feature type reflects different aspects of melanoma lesions. While Gabor and Curvelet features offer complete frequency information, Haralick and GLCM provide texture-based descriptions. LBP and HOG are efficient and effective at detecting local and edge patterns, respectively. Wavelet features act as a hybrid of the spatial and frequency domains. This comparison provides a basis for evaluating their combined impact on classifier performance in future work.

VI. DISCUSSION

This paper presents the implementation and relevance of seven hand-designed feature extraction methods applied to cutaneous melanoma images. Each method contributes uniquely to understanding lesion patterns. The multidimensional feature sets generated in this paper will be reduced and combined to create optimal descriptors for melanoma classification. These findings highlight the importance of diverse feature types for improving diagnostic performance.

REFERENCES

[1] S. M. Metev and V. P. Veiko, *Laser Assisted Microtechnology*, 2nd ed., R. M. Osgood, Jr., Ed. Berlin, Germany: Springer-Verlag, 1998.

[2] J. Breckling, Ed., *The Analysis of Directional Time Series: Applications to Wind Speed and Direction*, ser. Lecture Notes in Statistics. Berlin, Germany: Springer, 1989, vol. 61.

[3] S. Zhang, C. Zhu, J. K. O. Sin, and P. K. T. Mok, "A novel ultrathin elevated channel low-temperature poly-Si TFT," *IEEE Electron Device Lett.*, vol. 20, pp. 569–571, Nov. 1999.

[4] M. Wegmuller, J. P. von der Weid, P. Oberson, and N. Gisin, "High resolution fiber distributed measurements with coherent OFDR," in *Proc. ECOC'00*, 2000, paper 11.3.4, p. 109.

[5] R. E. Sorace, V. S. Reinhardt, and S. A. Vaughn, "High-speed digital-to-RF converter," U.S. Patent 5 668 842, Sept. 16, 1997.

[6] (2002) The IEEE website. [Online]. Available: http://www.ieee.org/

[7] M. Shell. (2002) IEEEtran homepage on CTAN. [Online]. Available: http://www.ctan.org/tex-archive/macros/latex/contrib/supported/IEEEtran/

[8] *FLEXChip Signal Processor (MC68175/D)*, Motorola, 1996.

[9] "PDCA12-70 data sheet," Opto Speed SA, Mezzovico, Switzerland.

[10] A. Karnik, "Performance of TCP congestion control with rate feedback: TCP/ABR and rate adaptive TCP/IP," M. Eng. thesis, Indian Institute of Science, Bangalore, India, Jan. 1999.

[11] J. Padhye, V. Firoiu, and D. Towsley, "A stochastic model of TCP Reno congestion avoidance and control," Univ. of Massachusetts, Amherst, MA, CMPSCI Tech. Rep. 99-02, 1999.

[12] *Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specification*, IEEE Std. 802.11, 1997

International Journal of Computer Research & Technology
ISSN 2454-7719
** A Blind Peer Reviewed Journal **
Volume-10, Issue-2, July-Dec 2025
Paper ID: 39

IoT Based Traffic Management System Using Real Time

Prof. Megha R.Chaudhari
Assistant Professor,
Bhusawal Arts, Science and P. O. Nahata Commerce College, Bhusawal
megharchaudhari19@gmail.com

Prof. Lokesh R. Chaudhari
Assistant Professor,
Bhusawal Arts, Science and P. O. Nahata Commerce College, Bhusawal
lokesh.chaudhari0077@gmail.com

Dr. Gouri M. Patil
Associate Professor,
Bhusawal Arts, Science and P. O. Nahata Commerce College, Bhusawal
gourimpatil@gmail.com

Abstract: *Traffic congestion has become a critical issue in metropolitan cities due to the exponential growth in the number of vehicles, while road infrastructure remains largely unchanged. Traditional traffic control systems, which rely on fixed timers or manual operations, are increasingly ineffective as they cannot adapt to real-time traffic variations. This inefficiency not only increases travel time and fuel consumption but also hinders the movement of emergency vehicles such as ambulances, fire trucks, and police cars during peak traffic hours. To address these challenges, this paper proposes an IoT-based smart traffic management system that utilizes real-time data collected from sensors installed at strategic locations near intersections. The system changes traffic light timings in real time based on how much traffic is coming from each direction, helping to reduce jams and improve flow. In future implementations, integration with platforms like Google Maps may enhance data accuracy. The proposed model also includes an emergency vehicle detection mechanism to prioritize their passage. By applying comparative data analysis and automated decision-making algorithms, this approach aims to optimize signal control, reduce human errors, lower fuel consumption, and improves urban mobility and road safety.*

Keywords: *IoT Sensors, Real-time Traffic Monitoring, Smart Signals, Vehicle Detection*

I. INTRODUCTION

Urban regions face increasing traffic problems due to rapid population growth and vehicle numbers, which lead to congestion, pollution, and accidents. Traditional traffic management with fixed signals or manual control cannot handle real-time situations, making them inefficient. To overcome this, smart traffic management systems are being developed using IoT, AI, sensors, GPS data, and communication networks.

Such systems analyze real-time traffic flow from maps and sensors to optimize signal timings dynamically, reducing jams and environmental impact. An important feature is the handling of emergency vehicles (ambulances, fire trucks, and police). Using radio-wave signaling, these vehicles can be detected up to 1 km before an intersection, and the system automatically prioritizes their movement by creating a signal-free corridor. Priority is assigned (Ambulance → Fire Truck → Police) to ensure life-saving response time. Compared to older methods

(like UV/proximity sensors), the integration of IoT and GPS-based data

Offers more accuracy, lower cost, and simpler management. This not only improves everyday traffic efficiency but also provides a reliable, autonomous way to support emergency vehicles.

II. LITERATURE REVIEW

IoT, or the Internet of Everything (IoE), involves smart internet-connected devices capable of sensing, transmitting, and processing data through integrated hardware and networking features. These devices, often called connected devices, can communicate with each other (machine-to-machine or M2M communication) and make decisions automatically, with little human involvement. People usually just set them up or check the data, but the devices handle most tasks on their own. The rise of small, low-cost electronic components and constant internet connectivity has made IoT possible. These devices generate a large amount of online data, which can be very useful but also raises privacy and security concerns.

Despite the risks, IoT offers many benefits:

- Homes can be monitored remotely for safety.
- Businesses can improve efficiency, cut waste, and avoid downtime.
- Smart city infrastructure can manage traffic, detect damage, and reduce congestion.
- Devices that monitor the environment can identify risks and give advance notice of natural disasters.

III. SYSTEM ANALYSIS

Existing System

In the current setup, traffic regulation is largely managed by traffic police. The limitation of this approach is that the control is not intelligent enough to effectively handle congestion. Decisions such as keeping one side of the road blocked for longer or allowing vehicles from another side to move are based mainly on the judgment of the officer on duty, which may not always be optimal.

Even where traffic lights are installed, the duration of green and red signals remains fixed, making it difficult to adapt to varying traffic conditions. In India, despite the presence of traffic signals, traffic police are still deployed to manage intersections, which increase the demand for manpower and reduce cost-effectiveness.

Proposed System

In the present scenario, traffic regulation is still primarily overseen by traffic police. The drawback of this system is that it lacks intelligent decision-making to efficiently manage congestion. For example, an officer may keep one road blocked longer or release vehicles from another road based solely on personal judgment, which is not always effective.

Even with traffic lights in place, the signal durations for red and green remain fixed, making them unable to adjust to changing traffic density. In India, it is common to see traffic police officers stationed at junctions despite the presence of signals, which increases manpower requirements and reduces economic efficiency.

To overcome these challenges, a smart traffic system can be implemented. In this approach, sensors count the number of vehicles passing per minute and send this data to a central database. The collected data is then used to train a predictive module that dynamically adjusts signal timings. Communication between the sensors and the system is carried out through Wi-Fi.

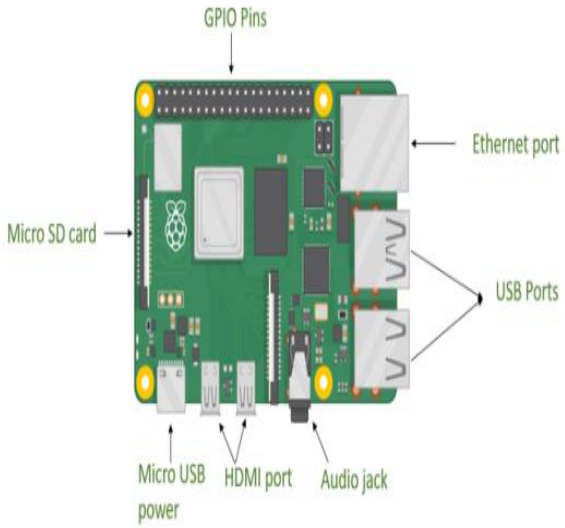
A cloud server applies an equation that uses the vehicle count as input and calculates the optimal green-light duration required for smooth traffic flow. This calculated value is compared with the current signal timing stored in the database. Based on the comparison, the processor makes a decision: if the current green time is shorter than the calculated value, it extends the green signal; otherwise, it reduces it.

IV. SYSTEM ARCHITECTURE

The proposed system is designed with six core modules that work together to enable intelligent traffic control:

1. **Raspberry Pi –** The Raspberry Pi acts as the central processing unit, handling data collection, computation, and decision-making. It interfaces with various sensors and output devices through its GPIO pins and

communicates using protocols like I2C, SPI, and UART.



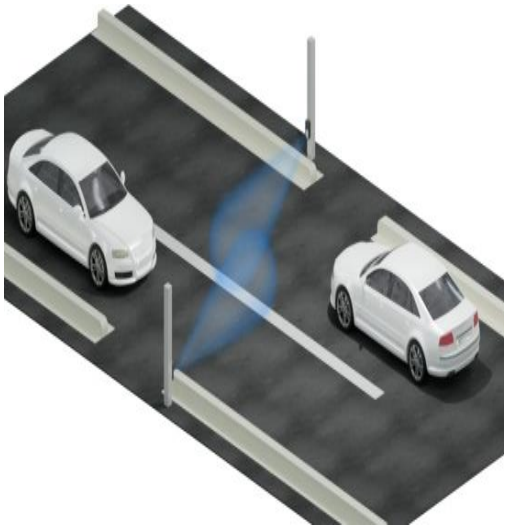
2. **LED Traffic Lights** – Function as signaling units to control the movement of vehicles at intersections by displaying red, yellow, and green lights based on predefined or dynamic timing sequences.
3. **Traffic Cameras** – Used to continuously monitor traffic flow and capture real-time data from multiple directions using sensors such as infrared detectors, cameras, or inductive loops.



4. **NodeMCU Microcontroller** – Serves as the communication interface, transmitting data between sensors, cameras, and the cloud server via Wi-Fi.



5. **Cloud Server/Database** – Stores traffic data, processes inputs, and runs prediction algorithms for dynamic signal timing.
6. **Sensors (Vehicle Counting/Detection Units)** – Deployed at intersections to detect and count vehicles, providing essential input for traffic density analysis.



V. SYSTEM IMPLEMENTATION

Steps in the Proposed Traffic Light Control System

1. **Camera Input** – Traffic cameras continuously capture live video streams of vehicles at intersections.
2. **Frame Extraction** – Individual frames are extracted from the video for processing.
3. **Grayscale Conversion** – Each frame is converted from a colored image to a grayscale image. This is done by applying transformations on the Red (R), Green (G), and

Blue (B) pixel values to generate corresponding grayscale values.

4. **Image Binarization** – The grayscale image is further converted into a binary (black and white) image, which simplifies object detection by clearly distinguishing vehicles from the background.
5. **Vehicle Detection and Counting** – Vehicles are detected within the binary image, and their count is determined for each direction of the intersection.
6. **Traffic Signal Control** – Based on the calculated vehicle density, the system dynamically adjusts the signal timing. The corresponding LED light (green, yellow, or red) is activated to optimize traffic flow.

Steps for Controlling Traffic Light – Method 2

1. **System Initialization** – Power on and initialize all hardware components.
2. **ESP8266 Configuration** – Set up the ESP8266 Wi-Fi module for multiple access points using AT commands.
3. **Wi-Fi Connectivity** – Connect the ESP8266 module to the available Wi-Fi network.
4. **UDP Port Activation** – Start a local UDP port on the Wi-Fi module for communication.
5. **Establish Communication** – Create a UDP connection between the Wi-Fi module and the Raspberry Pi.
6. **Data Reception** – The module waits to receive traffic data from the Raspberry Pi.
7. **Signal Control** – Based on the received data, the traffic light (LED) timing is adjusted, and the corresponding signal is updated.

VI. CHALLENGES AND LIMITATIONS

While the proposed system offers significant improvements over traditional methods, it is essential to address potential challenges:

1. **Infrastructure Costs:** Initial setup costs for the IoT-based system, including sensors, cameras, and cloud infrastructure, may be high. This could pose a challenge for implementation in less developed or resource-constrained areas.

2. **Data Privacy and Security:** As the system relies on continuous data collection (e.g., vehicle movement, traffic flow, emergency vehicle tracking), there may be concerns regarding data privacy and security. It's essential to address how data will be protected and anonymized.

3. **Sensor Accuracy and Maintenance:** Sensors, cameras, and microcontrollers may face issues related to environmental conditions (rain, fog, dust, etc.), leading to inaccurate vehicle detection or failure in counting. Maintenance procedures and cost implications need to be evaluated.

4. **Network Reliability:** Although the decentralized architecture ensures reliability, network congestion or failure could still cause disruptions. Building redundancy mechanisms, such as backup communication links or edge computing for local decision-making, could help mitigate this.

5. **Scalability and Flexibility:** The system should be designed with scalability in mind to handle larger and more complex intersections, as well as varying traffic patterns in different areas. It's also important to ensure that the system can be easily updated or expanded in the future.

VII. INTEGRATION WITH OTHER SMART CITY INITIATIVES

In addition to traffic management, IoT systems can be integrated with other smart city applications to provide more holistic solutions. For example:

1. **Smart Parking Systems:** The system can be linked to parking management to prevent congestion at intersections by detecting available parking spaces and directing drivers accordingly.
2. **Pedestrian Safety:** Using pedestrian sensors and cameras, the system could also dynamically adjust signals to enhance pedestrian safety, ensuring green lights when pedestrians are detected at crossings.
3. **Air Quality Monitoring:** The data collected can be analyzed to improve air quality by dynamically controlling traffic flow during peak pollution periods or when certain thresholds of air pollutants are reached.
4. **Public Transport Integration:** The system can prioritize buses or trams at intersections, ensuring that public transport is efficient, reducing overall traffic, and encouraging more sustainable commuting options.

VIII. CONCLUSION

The **Smart Traffic Management System** is designed by integrating various IoT-based hardware components to optimize traffic flow. Using the IoT platform, traffic signals are dynamically allocated varying time intervals based on the number of vehicles detected on each road segment.

This system addresses congestion more efficiently than traditional methods and is capable of performing intelligent re-routing at intersections. It provides a practical solution for the rapid increase in traffic volumes, particularly in large metropolitan cities, where conventional traffic control mechanisms often fail to manage flow effectively.

By adopting state-of-the-art IoT and communication technologies, the proposed system adjusts signal timings in real time according to vehicle density. It coordinates with local servers to regulate movement more effectively, while its decentralized architecture ensures reliability—even in cases where a central server fails.

In addition, the system generates valuable data for traffic authorities, which can be used in infrastructure planning, road design, and resource optimization, thereby contributing to smarter and more sustainable urban mobility.

REFERENCES

1. Soufiene Djahel,Ronan Doolan, Gabrial-Miro Muntean, John Murphy, "A communications oriented perspective on traffic management systems for smart cities: Challenges and innovative approaches, IEEE Communications Surveys and Tutorials, vol 10.pp,Nov 2013.
2. Lien-Wu Chen, Pranay Sharma, "Dynamic traffic control with fairness and throughput optimization using vehicular communications", IEEE journal on selected areas in communications/supplement, Vol.31.No.9.pp.504-512,September 2013.
3. Luigi Atzori,Antonio Iera and Giacomo Morabito, "The Internet of Things: A survey",Computer networks,vol.54,pp 2787 2805,2010.
4. Chen Wang, Bertrand David,Rene Chalon,Chuantoa Yin, "Dynamic road lane management study A smart City application", Transport research Part E,2015
5. Dongbin Zhao,Yujie Dai,Zhen Zhang, "Computational Intelligence in urban traffic signal control: A survey",IEEE Transactions onsystems,man,and cyberbetics-part c applications and reviews,Vol.42.No.4.pp. 485 494,July 2012.
6. Andreas Janecek,Danilo Valerio,and Karin Anna Hummel, "The cellular Network as a sensor:From Mobile phone data to real-time road traffic monitoring",IEEE transactions on intelligent systems,vol.16.no.5,pp 2015.
7. Peter Handel,Jens transportation 2551-2572 ,October Ohlsson,Martin Ohlsson,Isaac Skog,Elin Nygren, "Smartphone based measurement systems for road vehicle traffic monitoring and usage-based insurance", IEEE systems journal,Vol.8.No.4,pp 1238 1248,December 2014.

International Journal of Computer Research & Technology
ISSN 2454-7719
** A Blind Peer Reviewed Journal **
Volume-10, Issue-2, July-Dec 2025
Paper ID: CS-40

M-Banking: A Pillar of Digital Acceleration in Indian Society

Prof. Lokesh R. Chaudhari
Assistant Professor,
Bhusawal Arts, Science and P. O. Nahata
Commerce College, Bhusawal
lokesh.chaudhari0077@gmail.com

Prof. Megha R. Chaudhari
Assistant Professor,
Bhusawal Arts, Science and P. O. Nahata Commerce College, Bhusawal
megharchaudhari19@gmail.com

Dr. Swati P. Phalak
Assistant Professor,
Bhusawal Arts, Science and P. O. Nahata Commerce College, Bhusawal
swatiphalak71@gmail.com

Abstract: *India has been progressively embracing digitalization, particularly through mobile banking. Indian banks now recognize technology as the key driver for societal change. There has been a significant transition in the banking sector, with both customers and banks moving towards digital and branchless banking systems. The growth of mobile banking has been remarkable, especially following the launch of the Indian government's flagship initiative, Digital India. This study aims to explore the concept and current status of mobile banking services offered by banks in India within the context of the Digital India program. It is well-known that the Government of India introduced this program to transform the country into a digitally empowered society and knowledge economy. The program emphasizes key themes such as establishing digital infrastructure, promoting electronic governance and services, and empowering citizens digitally, with a core focus on creating a paperless, faceless, and cashless India. Mobile banking, as a digital platform providing various banking services, stands as a crucial pillar of this initiative and contributes to achieving its goals. Since the inception of the program, India has witnessed significant advancements in digital infrastructure and broadband connectivity.* The trust fostered by the government in digital frameworks and initiatives like mobile banking has sparked a digital revolution, leading to widespread digital transformation across society. This study traces the expansion of mobile banking since the launch of Digital India, relying mainly on conceptual and descriptive research based on data available in literature and reports from online sources. Literature from 2016 to 2025, including websites and e-journals, was reviewed. The findings reveal that mobile banking has experienced rapid growth in recent years, driven by the innovative efforts of the Indian government, which has greatly encouraged the public to adopt mobile banking services.

Keywords*: M- banking - Mobile Banking, Digital India, Digital Banking, Digital Infrastructure, Digital Pillars, Virtual banking, Frictionless Banking.*

I. INTRODUCTION

Mobile banking is a key pillar in digitally empowering India. Banks in the country must move quickly and adopt new technologies faster than ever to stay competitive and survive. The government plays a crucial role in boosting the digital infrastructure for the banking sector and the overall economy. With the ongoing digital payment revolution in banking, virtual
Banking has become essential to meet the demands of tech-savvy customers. India is among the fastest growing countries in terms of internet access, and there is no doubt that digital banking plays a vital role in transforming the Indian economy. Digitalization has become a top priority for banks across India. The banking system has shifted from traditional branch-based services to modern mobile banking, allowing customers to access their banks conveniently through their mobile phones and use various banking services anytime and anywhere.

II. MEANING OF MOBILE BANKING

Mobile banking refers to the process of digitalizing traditional banking services using telecommunication networks and digital

applications. It involves connecting with banks through digital platforms and accessing banking services via smartphones, laptops, and other smart devices. Essentially, mobile banking is a computer-based system operated through the internet and designed to work on various operating systems using specialized applications. These mobile applications, powered by internet connectivity, enable banks to offer a wide range of financial services directly to customers. Anyone with a smart device and internet access can easily use mobile banking. This method of banking is both accessible and convenient, allowing users to open and manage bank accounts efficiently without the need to visit a physical bank branch. Mobile banking highlights how financial systems have evolved over time due to advancements in technology (RBI report, 2019). Thanks to the benefits of mobile banking and the digital initiatives under the Digital India program, more people are choosing mobile banking over traditional methods. In essence, mobile banking delivers financial services electronically and represents a revolutionary shift in the banking system—from standing in queues to banking at your fingertips.

III. HISTORICAL BACKGROUND OF MOBILE BANKING IN INDIA

Technology is advancing rapidly every day, turning the world into a global platform where people can connect and communicate from anywhere. This progress is made possible by the internet and technological innovations, which have become essential in every sector. In India, the banking industry continuously adopts the latest technology-based services to enhance customer experience and satisfaction. The internet has played a crucial role in societal growth and development, with internet and communication technologies being two major advancements that have significantly influenced social capabilities in recent years. The Reserve Bank of India (RBI) authorized mobile banking services in 2006 and later issued specific guidelines for mobile banking operations in 2011. Initially, mobile banking services were primarily available through toll-free numbers using Short Messaging Service (SMS). Today, mobile banking operates entirely through software applications that require an internet connection. Many Indian banks have launched their own mobile banking apps, such as ICICI's Mobile App, HDFC Mobile Banking, SBI's YONO App, Axis Bank's Mobile App, Kotak Mahindra Bank's Mobile Banking, Punjab National Bank's PNB One App, IDBI Bank's Mobile Banking App, Central Bank of India's Mobile Banking, and Maharashtra Gramin Bank's Mobile Banking App, to offer a wide range of financial services through smartphones.

IV. CURRENT SCENARIO OF MOBILE BANKING IN INDIA

Technology today is deeply integrated into everyday life, and it is difficult to imagine a world without it. Innovations worldwide have simplified and improved people's lives significantly. In India, the Reserve Bank of India (RBI) has actively promoted and facilitated the growth of mobile banking and digital payments. Mobile banking usage in India has been increasing rapidly, especially after the demonetization initiative in 2016, which accelerated the adoption of digital payment methods. According to the RBI Annual Report of 2017-18, mobile banking transactions grew by approximately 90% in volume and 19% in value during that period.

India boasts the second-largest mobile subscriber base globally, contributing to the increasing number of mobile banking users, as noted by studies like those of Shilpa and Veena (2018). Mobile banking services have received positive feedback from customers due to their convenience and effectiveness. The COVID-19 pandemic further accelerated this trend, pushing consumers and banks to shift towards virtual interactions. The World Retail Banking Report 2020 highlighted nearly a 10% increase in consumer preference for internet banking during the pandemic. Banks were compelled to innovate rapidly, digitalizing core banking services to meet changing demands. The FIS 2021 report emphasized that the pandemic permanently changed banking habits, with customers increasingly opting for digital channels over physical branches, fueling significant growth in mobile banking.

More recently, India has witnessed further expansion in mobile banking, driven by improved internet connectivity, widespread smartphone penetration, and government initiatives like Digital India and the Unified Payments Interface (UPI). UPI has revolutionized digital payments, making mobile banking more accessible and frictionless for millions of users. According to the National Payments Corporation of India (NPCI), UPI transactions crossed over 10 billion monthly transactions in 2025, underscoring the massive scale of digital banking adoption.

Studies like those by Dr. Vareha Agarwal, Shresth Poddar, and Sahil J Karnavat emphasize that in developing countries such as India, mobile banking presents a vital opportunity for financial inclusion and economic development. Today, mobile banking continues to evolve, integrating emerging technologies like artificial intelligence, biometric authentication, and advanced security features to offer a more personalized, secure, and seamless banking experience.

V. FEATURES OF MOBILE BANKING SYSTEM IN INDIA

Mobile banking is often described as banking that can be done anywhere and anytime—except at a physical bank branch. Its advantages include convenience, user-friendly interfaces, easy operation, quick access to bank accounts, fast service at low costs, and secure transactions. The quality of mobile banking service is measured by how well it meets customer expectations, including security, understanding customer needs, maintaining good relationships, and offering other benefits unique to mobile banking. Despite the rapid digital growth in India's mobile banking sector, some challenges remain. Security concerns continue to make some customers hesitant to fully embrace this technology-driven mode of banking. Additionally, banks face numerous challenges in delivering maximum customer satisfaction. In today's highly competitive environment, the mobile banking sector is unpredictable and constantly evolving, requiring banks to improve their products, address security threats, and overcome various limitations to stay ahead.

VI. DIGITAL INITIATIVES TAKEN BY THE GOVERNMENT

India has embarked on a distinctive journey to digitalize its economy through the ambitious Digital India program. The Reserve Bank of India (RBI) and the government have collaboratively launched several initiatives to accelerate India's digital growth. According to the Indian Digital Summit 2019 held in New Delhi, India's digital economy was projected to surpass one trillion dollars by 2022. Continuing this upward trend, the RBI Annual Report 2025 highlights that digital transactions, especially mobile banking, have seen exponential growth, further strengthening India's position as a major digital economy. At the summit, prominent speakers highlighted both the opportunities and challenges of building a Digital India. Google CEO Sundar Pichai emphasized that "advancing technology is the key to improving lives in India and across the globe." Technology-driven banking systems serve as a critical pillar of the Digital India program, with mobile banking representing a fundamental aspect of this digital transformation.

While the RBI's 2013 report expressed concerns over the slow adoption and growth of mobile banking at that time, the momentum has dramatically shifted with the rise of the Digital India movement. Mobile banking now supports a paperless economy and offers customers convenient access to banking services through digital platforms. This study reveals that the government has actively pushed forward various technological initiatives to help position India as a global leader in technology and innovation, with 2025 data confirming sustained and accelerated growth in mobile banking adoption and digital infrastructure.

VII. LITERATURE REVIEW

Several recent studies continue to show how mobile banking is transforming India's financial landscape. For example, a 2022 study by Sonal Raina Tikku and Anjani K. Singh examined mobile banking adoption among agricultural traders in India. They found that perceived usefulness, ease of use, and trust significantly influence mobile banking adoption in the agri-trader community.

Shalini Devi (2024) explored how digitization is helping promote financial inclusion in India, especially among rural populations, through tools like mobile banking, fintech solutions, and digital payment systems. Her findings underscore the importance of Aadhaar and other identity-authentication mechanisms in extending banking services to underserved regions.

Research such as "Digital Transaction in Indian Payment Ecosystem - A Comprehensive Analysis" by Kratika Gupta & Dr. Moon Moon Lahiri (2025) reveals growing transaction volumes (including mobile banking and UPI) driven by fintech innovation and supportive regulatory policies.

Another 2025 study, "Transforming Indian Banking: A Study of Digitalization, Customer Experience and Operational Efficiency" by Pallavi Pandey, provides evidence that digitalization is increasingly critical—not just for improving access, but for improving service quality, trust and efficiency in the banking sector. Security continues to be a key concern in that regard.

There are also systematic reviews tackling broader issues. For instance, The Role of Digital Banking in Advancing Financial Inclusion: A Systematic Literature Review (Mesud Mohammed & Gurudutta P. Japee, 2025) finds that mobile banking and other digital financial technologies are helping reduce costs, improve accessibility, and bring banking services to marginalized groups. But it also flags barriers like regulatory ambiguity, infrastructure gaps, and digital literacy.

Studies continue to affirm that large events like demonetization and the Covid-19 pandemic have acted as accelerators for mobile banking growth. Meanwhile, the most recent work shows that as of 2024–25, adoption and usage are rising, but issues such as security, trust, regulatory compliance, digital literacy, and rural/urban divides still pose challenges.

VIII. OBJECTIVES

This study aims to explore the evolution and present landscape of mobile banking services provided by banks in India. It seeks to identify the key factors that influence customer adoption and usage of mobile banking platforms. By examining the growth trends and government-driven digital initiatives, the study provides a comprehensive understanding of mobile banking's role in India's digital transformation.

Objective 1: To analyze the current status, trends, and growth trajectory of mobile banking in India. Objective 2: To examine the various dimensions and impact of mobile banking since the introduction of the Digital India flagship program.

IX. RESEARCH METHODOLOGY

This study employs a theoretical and descriptive research design aimed at analyzing the growth and current status of mobile banking in India, particularly in the context of the Digital India initiative. It focuses on providing a comprehensive understanding of mobile banking through qualitative insights derived from secondary sources. The research adopts a qualitative approach, emphasizing a conceptual and analytical examination of customer adoption, government policies, and technological advancements in the banking sector. The data used in this study is entirely secondary and has been collected from a variety of reputable sources, including research publications, academic journals, government reports such as RBI Annual Reports, consultancy firm reports like those from BCG, FIS, and Statista, as well as official bank websites and authenticated online databases. The literature reviewed spans from 2016 to 2025, with a particular focus on significant milestones such as demonetization, the COVID-19 pandemic, and recent government digital initiatives that have influenced mobile banking adoption. The scope of the study is limited to the Indian context, covering the evolution of mobile banking, the role of increasing smartphone penetration, user behavior patterns, and the impact of government-led digital transformation policies. However, the study is constrained by its reliance solely on secondary data, without primary data collection such as surveys or interviews. Additionally, some of the latest data for 2025 may be provisional or estimated, and the study does not delve into the technical aspects or coding of mobile banking applications.

X. DATA COLLECTION

The research relies entirely on secondary data sources. Information has been gathered from published research papers, scholarly articles, government and institutional reports, and credible websites. These sources were used to build a strong theoretical foundation and to analyze the current trends and developments in mobile banking across India.

XI. FINDINGS

Over the past decade, India has seen significant digital innovation, with smartphones and AI-powered apps transforming daily life. The Digital India program has promoted a shift toward a paperless, cashless economy, supported by tools like BHIM, UPI, RuPay cards, and mobile wallets. The 2016–17 demonetization accelerated digital payment adoption, while the COVID-19 pandemic further boosted mobile banking as customers favored contactless services. Reports from Statista (2023) and BCG (2021) highlight rapid growth, with mobile banking transactions expected to surpass USD 1 trillion soon. Looking ahead to 2025, mobile banking is projected to expand further, driven by increased smartphone penetration, improved digital infrastructure, and greater user trust. Mobile banking today is a vital platform for banks to engage customers with convenience and build lasting relationships, signaling a promising future for India's digital economy.

XII. SUGGESTIONS

Despite growth in mobile banking, challenges remain, especially around customer awareness and digital literacy. Effective communication between banks and customers—such as live demonstrations at branches—can boost adoption. Many customers still prefer traditional banking due to fear or lack of understanding of technology. Banks must invest in raising digital awareness and improving cybersecurity to build trust. The Reserve Bank of India (RBI) should enforce stronger cyber guidelines, while banks need to offer secure systems and educate customers about protecting their personal information. Quality of service is critical for customer satisfaction, so banks should strengthen their IT departments to maintain reliable apps.

Looking ahead, the future of mobile banking in India is promising, driven by the Digital India initiative promoting a cashless, paperless society. However, complete replacement of branch banking is unlikely, as customers still prefer in-person visits for complex services like loans. To stay competitive, banks must adapt quickly and provide frictionless, high-tech mobile services. While technology can be daunting, it has undeniably made life easier and faster, with mobile banking becoming a key tool for convenient financial access on the go.

XIII. CONCLUSION

Mobile banking in India is rapidly expanding, driven by initiatives from the RBI and the Government of India. Its use surged during the demonetization phase in November 2016, when customers sought alternatives to cash and

increasingly preferred mobile banking. The growth accelerated further during the COVID-19 pandemic, as mobile banking supported social distancing by enabling convenient, anytime-anywhere access to banking services. Mobile banking benefits both banks and customers by reducing transaction costs and other expenses. Thanks to its advantages and the Digital India initiatives, more people are choosing mobile banking over traditional methods. By 2025, mobile banking is expected to become even more widespread, supported by advancements in technology, increased internet penetration, and stronger cyber security measures, making digital banking an integral part of everyday financial transactions in India. The future looks promising as customers continue to enjoy seamless financial services through their smartphones and internet connections.

REFERENCES

[1] Bhagyalakhshmi Burra, 2021, "Use and adoption of mobile banking in rural areas of India: a descriptive study of the emergence of E-banking in India."

[2] Deb & Agrawal A (2017). Factors impacting the adoption of m-banking: understanding brand India's potential for financial inclusion.

[3] Deshal P. (2015). "A study of mobile banking in India."

[4] Deva Devan, (2013) "A study on Mobile banking in India Issues and challenges"

[5] Gujrati, R. (2017). "India's march towards a faceless, paperless, cashless economy.

[6] H. Manjula (2018), "Mobile Banking Services and Customer Satisfaction concerning ICICI Bank - A Study."

[7] Dr. Jain, Dr.Sørupie, A; Kothari, A (2020). "A study on the growth of mobile banking in India."

[8] PrernaBamoriya, Preeti Singh (2012) "Mobile banking in India barriers in adoption and service preferences."

[9] Priyanka, (2019), "Growth and trend of mobile banking in India."

[10] Puneeta Sharma, Kavita, and Sachin *Mobile banking is a need for sustainable development"

[11] Renų Šing, Garima Malik, 2019 "Impact of digitalization on Indian Rural Banking customer with special reference to the payments system."

[12] Simran jit Kaur, 2021, "Adoption of digital banking channels in an emerging economy: exploring the role of in-branch efforts."

[13] T.Kadalarasane (2015) "Acceptance of mobile banking services: Antecedents and consequences."

[14] Uppal R.K, (2011) "Mobile Banking in India: An empirical analysis."

International Journal of Computer Research & Technology
ISSN 2454-7719
** A Blind Peer Reviewed Journal **
Volume-10, Issue-2, July-Dec 2025
Paper ID: CS-41

Intelligent Document Digitization and Fraud Prevention Using Artificial Intelligence

Mr. Digambar Padmakar Mahajan
School of Computer Sciences and Engineering
Department of Computer Science and Application
Sandip University Nashik Nashik, India
digambar.mahajan77@gmail.com

Prof. Dr. Mohammad Muqeem
School of Computer Sciences and Engineering
Department of Computer Science and Application
Sandip University Nashik Nashik, India

Abstract- *Its task is to create these research digital documents through artificial intelligence and integrate them into a secure system. This research is based on the current situation in the developed system. Technologies like OCR, image processing, machine learning, fingerprint technology, artificial intelligence, database management have been used in this research. First, the function of this system is to create new documents through texturing or photo recognition from other documents and put them into a secure system. This system is evolving a completely human-made process into a digital system. New documents are being created in it by creating different types of processes through artificial intelligence. One can use this document in any field. These documents will be generated through an automatic system and its information will be stored in the database created and a new document will be created based on that information. This system is currently being developed. The purpose of this research is that this research is important in curbing various types of document crimes in India or in the world. Based on this research, we can digitize the entire document technology and we can use it, the use of documents is very important in the digital field. At present, many people are availing the facilities using fake documents and on the basis of those fake documents, false information is being spread all over the world. According to many such information, many crimes or cyber frauds are being committed today in the name of other persons using their documents. We are doing this research to secure documents and remove human interference from them.*

Keywords - *Fingerprint Techniques, Scanning System, AI Techniques, Text Recognition and Photo Recognition, Machine Learning.*

I. INTRODUCTION

At present safety research is the need of the hour so many researches are done to make human life processes or other things safe and thus human things or their materials are safe. This research is working and trying to ensure that the documents used in human life such as caste certificate, Aadhaar card, PAN card, voter card, school documents and many other documents are kept safe and their use is safe while conducting safe research. The aim of the research is that people's private documents should be kept safe and other documents should be kept safe and their data should be collected and on the basis of this the society or an office should get the personal information. Mainly in this research is to create digital documents using some techniques like artificial intelligence, machine learning and digital image processing and collecting data through them. This research now involves creating a layout of the documents in the current process and creating a basis for a preliminary form of the process. In this research proposal, we are looking at creating the outlines of the documents and creating those outlines through artificial intelligence and extracting and adding the data on the documents through OCR techniques. The aim of this research is to keep the documents of human life secure and to eliminate

human intervention in creating and using fake documents.
The aim of this research is to create a secure system to document the entire life of a human being from the beginning of his life on the basis of a single document and to create and collect complete information on the basis of that single document. The primary research is that we are going to create a layout for the documents through LAS i.e. Layout Analysis System and using that layout we are going to create new documents based on the collected information.

Its task is to create these research digital documents through artificial intelligence and integrate them into a secure system. This research is based on the current situation in the developed system. Technologies like OCR, image processing, machine learning, fingerprint technology, artificial intelligence, database management have been used in this research. First, the function of this system is to create new documents through texturing or photo recognition from other documents and put them into a secure system. This system is evolving a completely human-made process into a digital system. New documents are being created in it by creating different types of processes through artificial intelligence. One can use this document in any field. These documents will be generated through an automatic system and its information will be stored in the database created and a new document will be created based on that information. This system is currently being developed. The purpose of this research is that this research is important in curbing various types of document crimes in India or in the world. Based on this research, we can digitize the entire document technology and we can use it, the use of documents is very important in the digital field. At present, many people are availing the facilities using fake documents and on the basis of those fake documents, false information is being spread all over the world. According to many such information, many crimes or cyber frauds are being committed today in the name of other persons using their documents. We are doing this research to secure documents and remove human interference from them.

II. PROBLEM STATEMENT

This research is mainly of such a nature that the private documents or other practical documents required in human life should not be produced by human beings. As the process in which human intervention takes place can cause problems, it is necessary to do this research as there are many things that can cause danger to the society and globally while preparing the documents. Human documents are extracted by human intervention and through this process or through this research we want to change this and this process will be replaced by advanced technologies like artificial intelligence and machine learning.

If the documents are replaced by digital documents, it will be easy to keep the documents together and collect them and this is the main feature of this research because through this research the individuals will be prepared with digital documents and the main feature is that the information will be completely true as there is no human intervention. Stores sensitive information like fingerprints, iris scans, and face photos, which can be used for identity theft, surveillance, and data breaches. Aadhaar can also be vulnerable to duplication or forgery if used as a photo ID. In October 2023, a hacker leaked the Aadhaar and passport numbers of 81.5 crore Indians on the dark web. Can be used for identity theft, and fraudsters can use PAN details to apply for loans or credit cards in your name. PAN details have been used to obtain loans, purchase properties and jewellery, and invest black money [1]. At present many crimes are being committed by creating fake documents in many places and using them globally. By using these documents, global financial crises and many such countries are harmed by misuse of the country's facilities. False information is given in many places by using fake documents and many things are created from it.

Identity document forgery is the process by which identity documents issued by administrative agencies are copied and/or modified by persons not authorized to produce such documents or by persons involved in such alterations, with the intention of deceiving those who will view the documents as to the identity or status of the bearer. [2] The term also includes the act of obtaining identity documents from legal entities by falsifying supporting documents necessary to create the desired identity. [3] Identity documents differ from other credentials in that they can only be used by the person holding the card. Unlike other credentials, they can be used to restrict the holder's activities as well as extend them. Such forged documents include driver's licenses (historically forged or altered in an attempt to conceal the fact that individuals seeking to purchase alcohol are under the legal drinking age); birth certificates and social security cards (can be used in identity theft schemes or to defraud the government); and a passport (used to avoid restrictions on entry into a particular country). As of early 2010, Interpol's global database contained 11 million stolen or lost passports. [4]. such false documents can be used for identity theft, age fraud, illegal immigration, organized crime and espionage. [5] The issue of fake documents in India is substantial and multifaceted, affecting various sectors including employment, telecommunications, and financial services.

Table -1 Personal document problems

Name of Sector	Information	Source of Information
Security concerns	Data breaches or leaks can expose personal information in documents, raising privacy risks.	Google Scholar
Accessibility issues	Obtaining or renewing documents can be challenging for people in remote areas, those with disabilities, or facing bureaucratic hurdles.	Google Scholar
Loss or theft	Misplacing important documents like passports, driver's licenses, or birth certificates can be a nightmare. You'll need to go through the process of replacing them, which can involve time, paperwork, and fees.	Google Scholar
Damage	Documents can get damaged due to wear and tear, water, or fire. Damaged documents might not be accepted by official entities, leading to replacement hassles.	Google Scholar
Fraud	Fake or stolen personal documents can be used for illegal activities like identity theft, posing a significant risk.	Google Scholar
Errors	Sometimes, mistakes occur during the issuance of documents. These errors can cause delays or rejections during official processes.	Google Scholar

Notable Examples and Recent Cases

1. Education Scams:
   - In 2020, a major fake degree scam was uncovered in Punjab, where thousands of fake degrees were issued by a group of individuals posing as representatives of various universities.
2. Property Frauds:
   - Delhi police busted a gang involved in forging property documents and selling properties without the owners' knowledge.
3. Employment Scams:
   - In 2021, a racket involving fake job offers from multinational companies was exposed, where job seekers were asked to pay hefty sums for job confirmations and processing fees.

Preventive Measures and Legal Actions

1. Stringent Verification Processes:
   - Implementing robust document verification systems in educational institutions, government offices, and businesses to detect and prevent the use of fake documents.
2. Awareness Campaigns:
   - Educating the public about the risks and signs of fake document scams to reduce the number of victims.
3. Legal Framework and Penalties:
   - Strengthening laws and penalties related to document forgery and fraud. The Indian Penal Code (IPC) Sections 465, 468, and 471 deal with forgery, forgery for the purpose of cheating, and using forged documents as genuine, respectively, and impose stringent punishments.
4. Technology Integration:
   - Utilizing advanced technologies like blockchain for secure and tamper-proof documentation, and AI-based verification tools to detect anomalies in documents.

III. OBJECTIVES

1. To study of various Digital Document System Using Artificial Intelligence and Machine Learning Techniques.
2. To Study Document Security System and Document data collection Method.
3. To study performance evaluation of various Artificial Intelligence and Machine Learning Techniques for Digital Document System to Provide Fingerprint Document Security.
4. Implementation of Digital Document Creation System to Provide Fingerprint Document

Security Using Artificial Intelligence and Machine Learning Techniques.

IV. SCOPE OF WORK

This research is of great importance at the global level and in other fields as well. Through this research, we can curb the large amount of paperwork.At present, the process of linking many documents is going on but the government is facing a lot of difficulties in this.Because many people are not linking their documents together to avail income tax as well as many facilities.Crores are being spent by the government on many processes like Aadhaar Card Linking PAN Card Linking, so this cost can be largely curbed through this research.Many people do many things like traveling to foreign countries or availing many facilities on the basis of their fake documents At present there is a 99% chance that the information collected through this research is genuine, as the information collected through this research is collected by automatic systems and AI.This research is useful for many things like paper work, time required for documents, cost of extracting documents, cost burden on government system, delivery of facilities.Based on this research we can avoid any kind of stressful process to extract our documents. In this, documents will be prepared according to the age of the person.The prepared documents will be stored in a specific OCR database of the person and the database will be linked with the fingerprint of the person.Individuals can provide their documents using hand prints whenever they want to show documents anywhere. This can make document extraction very easy.The generation will consist of collecting the information of the documents and issuing new documents to the individuals based on the information collected and storing the information based on the information collected.

V. LITERATURE REVIEW

AI sets the document format like height and width for document generation. This format can be of different sizes. Layout analysis system LAS will work in this system. The work of this system will be to check and verify the size of documents. According to Document AI Benchmark Model and Application Arthur Lei Cui (Microsoft), the transformation of documents into AI is very important in the current context. [10] According to this the automation of documents, reading or creating them is very important nowadays in business or other fields. This is an important piece of research for AI and computer science. In this, layout of documents through AI as well as analysis of layout of documents in various formats will be done in this system and then new documents will be created based on that information. In this, the process of tax recognition and document size analyzer will be created through machine learning algorithms. Importantly, the work of Document Layout Analysis DLA is to automatically analyze images, text, tables and charts, the entire system will be generated through an AI technology, and through that create a perfect size paper layout for a new document. will be done. whose size and overall G properties will be determined through document layout analysis and the subsequent system will operate on that determined layout.[10]

For example every document like Caste Certificate, Aadhaar Card, PAN Card, Voter Card, Caste Certificate, Patra Age of Domicile, Ration Card all come in different sizes. For that, a different size of each document will be generated through AI, such as cast on A4 size, Certificate Age of Domicile are the documents. Then there is the ration card in A5 size. The size of PAN card is 5 by 3 cm. The size of Aadhaar card is 6 by 17 cm. Various such documents have different sizes so through this the size of the document to be generated specifically will be generated. This will set the duration of document generation.[11]

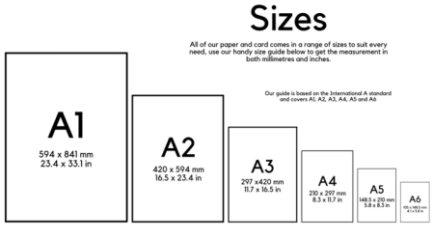


Figure – 2 LAS Document Size Generate

On the basis of that document, new documents will be created through work slow system, various types of documents, text recognition. Since the entire system is automatic, the data on the documents will be learned through machine learning and as many errors as possible will be removed from the data in the documents and the extracted data will be made as accurate as possible. The data extracted through RPA Robotic Process Automation And OCR Optical Character Recognization. The OCR system is currently being used for Amazon's textract system. The billing of the company or the text technology on top of the billing in the company is being done through this OCR system. This system is developed through machine learning and the entire technology works automatically. It largely involves extracting characters from PDF images tables and forms using OCR software and creating new documents. In this we can do any updates manually with the help of human, similarly any type of human made hand writing is also extracted in this.[12] The OCR system will perform automatic document processing by selecting the text from the previous document, converting it to the next format, changing its formatting and setting it at a specific location on the paper generated in process 1. will go OCR technology is currently being used all over the

world. This technology is being used in various big companies like Google and Amazon textract. By doing this, text formatting or extracting text is done, saving a lot of time needed for typing or proofreading new documents. [13] Only the information needed to create a new document will be extracted through OCR. The OCR system will extract header files, left-right text files as well as information required to create a new document from the previous document and add it to the next document. The OCR system will extract the entire system to a specific size paper generated through the Layout analysis system LAS.

An OCR database will store the data collected through this process. This data can also be changed by humans. The function of OCR data is to store information collected from various documents through text recognition. At the same time, this missing information or missing information can also be extracted from other documents through OCR and stored in it. The OCR database mainly extracts the information from a document and stores it in itself and then puts that information on the layout created based on that information. Through the RNN Recurrent neural network system, it is decided which information is to be kept at which position and accordingly the new document will be created.[10] RNN Recurrent neural network is an important automatic technical network in which different parts of images are determined and special processing is done on those parts. Using RNN system to create a new document a specific place will be determined and at that specific place the tax recognized through OCR will be printed in that part or inserted in that part through Recurrent neural network.

OCR Use The RNN And Extract the Text &

LAS Use The RNN and Set the text one position.

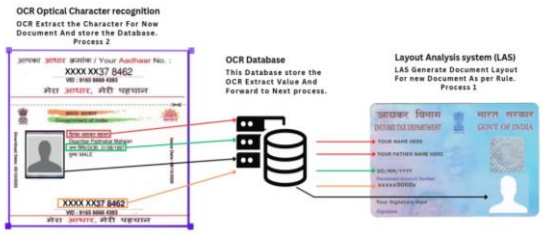


Figure-3 LAS and OCR Process and Data Store Database

As shown in Figure 3, the data extracted by LAS and OCR processes will also be stored in the database. If a document is new, information on it will be extracted and stored in the database, and that information will also be used to extract new documents.

The database will be created for every person born. For example you can see that father database and mother database are created in figure no.4. According to the information of both of them and according to the information in the database of both of them, their child's documents will be prepared through this system. Information on father's documents will be extracted through OCR and information on mother's documents will be extracted through OCR and stored in their database. On the basis of that information, the documents of their unborn child will be prepared. While preparing this document some information which is important for the child from the father and the information which is important from the mother will be extracted from that database to the child's database and the child's data will be perfected. If any information is missing in the child database then it will be inserted by human process and new child database will be created accordingly.[14]

VI. CONCLUSION

In this research, this research has been done in order to solve the dangers and dangerous problems related to primary documents. Through this research, document security and document privacy can be improved in society and other sectors. Documents are very important so it is necessary for every person to extract them but due to the complex nature of the process many people cannot extract or use these documents. The main objective of this research is to create new documents and use them digitally. The information on the documents will be extracted and deposited in a database and many different documents will be created by using that database and in this, various documents will be generated by identifying the age limit through machine learning with the help of artificial intelligence. Fingerprint technology has been used to keep these documents safe and use them safely. The documents are registered on the individual's hand fingerprint so that each person can keep the documents safe. There can be different types of information about a person in society because no document is connected to each other and the information of these documents does not match, so through this research, the information of each person will be collected in a preliminary form and then many documents will be created by using it. Primary information will be considered important and reliable and new documents will be prepared on the basis of that information and there will be no human intervention so the information on these documents will be safe and authentic. Each paper of each person shows different information, so whenever any form is to be filled, each person has to give each of his documents, but if the fruit of this research is to be made possible, since the information of the person is in one place, the person will not need to give different types of documents. Through CAA and NRC, personal data can be collected in government systems. Many people can

hide the information, it cannot happen because the entire information will be checked by artificial intelligence and machine learning. This research can play a major role in many fields. Various problems such as making false documents, hiding information, manipulating documents and changing information on documents as per requirement will be prevented.

REFERENCES

[1] https://www.sciencedirect.com/science/article/abs/pii/S0167404824000083X?via%3Dihub

[2] Debanjan Sadhya, Tanya Sahu Department of Computer Science and Engineering, ABV-Indian Institute of Information Technology and Management Gwalior, Madhya Pradesh, India

[3] Buchanan, James DR; Cowburn, Russell P.; Jausovec, Ana-Vanessa; Pettit, Dorothy; Seam, Peter; Xiong, Gang; Atkinson, Dale; Fenton, Kate; Allwood, Dan A.; Bryan, Matthew T. (2005). "'Fingerprinting' documents and packaging." Nature . 436 (7050): 475. doi : 10.1038/436475a . ISSN 1476-4687 . PMID 16049465. S2CID 4164867 .

[4] Bennett, Colin John; Lyon, David (2008). Playing with Identity: Surveillance, Security and Identity in Global Perspective. Routledge. ISBN 9780415465632.

[5] "11 million passports in Interpol database stolen or lost" . Havocscope Black Market.

[6] Turner, JW Cecil (1946). ""Documents" in the Law of Forgery." Virginia Law Review . 32 (5): 939-954. doi : 10.2307/1068683 . ISSN 0042-6601 . JSTOR 1068683

[7] CITIZENSHIP AMENDMENT ACT, 2019 (CAA): THE PERNICIOUS EFFECTS ON THE COUNTRY Aadhya Mehra https://ijcrt.org/papers/IJCRT2011301.pdf

[8] Bhargava, A. D. (2019, December 19). CAA impacts different sections of Indians negatively. Opposition parties' task is to bring them together. Retrieved from https://timesofindia.indiatimes.com/blogs/toi-edit-page/caa-impacts-different-sections-ofindians-negatively-opposition-parties-task-is-to-bring-them-together/

[9] Adhar Card Fake Read more at: https://www.onmanorama.com/news/kerala/2024/05/08/over-50000-refugees-with-fake-aadhaar-kerala-intelligence.html

[10] https://arxiv.org/pdf/2111.06016 SYNTHETIC DOCUMENT GENERATOR FOR ANNOTATION-FREE LAYOUT RECOGNITION Natraj Raman1 , Sameena Shah2 and Manuela Veloso2 JPMorgan AI Research 1London, UK

[11] https://www.researchgate.net/publication/356282134_Document_AI_Benchmarks_Models_and_Applications DOCUMENT AI: BENCHMARKS, MODELS AND APPLICATIONS Lei Cui, Yiheng Xu, Tengchao Lv, Furu Wei - Microsoft Research Asia

[12] https://arxiv.org/pdf/2111.06016

[13] SYNTHETIC DOCUMENT GENERATOR FOR ANNOTATION-FREE LAYOUT RECOGNITION Natraj Raman1 , Sameena Shah2 and Manuela Veloso2 JPMorgan AI Research 1London, UK. 2New York, USA

[14] Amazon Textract – computer vision based OCR https://aws.amazon.com/textract/

[15] Amazon Textract's new Layout feature introduces efficiencies in general purpose and generative AI document processing tasks 21st November, 2023 Anjan Biswas Sr. AI Specialist Solutions Architect, AWS AI Lalita Reddi Senior Technical Product Manager, Amazon Textract Edouard Belval AI Research Engineer, AWS Computer Vision https://www.researchgate.net/profile/Anjanava-Biswas/publication/381003210_Amazon_Textract's_new_Layout_feature_introduces_efficiencies_in_general_purpose_and_generative_AI_document_processing_tasks/links/6658ebebbc86444c721ee6d2/Amazon-Textracts-new-Layout-feature-introduces-efficiencies-in-general-purpose-and-generative-AI-document-processing-tasks.pdf

[16] OCR Database convert https://aws.amazon.com/what-is/ocr/#:~:text=Optical%20Character%20Recognition%20(OCR)%20is,scan%20as%20an%20image%20file

[17] Overview of Fingerprint Recognition System Mouad .M.H.Ali Research Scholar at Dr.Babasaheb Ambedkar Marathwada University Aurangabad, (M.S), India https://www.researchgate.net/publication/310953762_Overview_of_Fingerprint_Recognition_System

International Journal of Computer Research & Technology
ISSN 2454-7719
** A Blind Peer Reviewed Journal **
Volume-10, Issue-2, July-Dec 2025
Paper ID: CS-42

Artificial Intelligence in Early Cancer Detection

Assistant Prof. Nayana A.Chaudhari
Department of Computer Science & Information Technology
Bhusawal Arts Science and PO Nahata Commerce College
nainachaudhari111@gmail.com

Abstract: *Early detection of cancer significantly increases the chances of successful treatment and survival. The integration of Artificial Intelligence (AI) into medical diagnostics has revolutionized early cancer detection by leveraging large-scale biomedical data. This study investigates the application of machine learning and deep learning techniques to imaging, clinical, and genomic data for the early diagnosis of cancer. A multimodal approach was employed using datasets from TCGA, LIDC-IDRI, and DDSM. Convolutional Neural Networks (CNNs), Support Vector Machines (SVM), and ensemble models were trained and evaluated using stratified cross-validation. The models achieved high sensitivity and specificity, indicating the potential for AI to augment traditional screening tools and aid clinicians in detecting cancer at earlier stages*

Keywords: *Artificial Intelligence, Early Cancer Detection, Deep Learning, Machine Learning, Medical Imaging, CNN, Biomarkers, Predictive Modeling, AI in Healthcare*.

I. INTRODUCTION

Cancer remains one of the leading causes of mortality worldwide. Detecting cancer in its early stages dramatically improves the effectiveness of treatment and increases patient survival rates. However, early-stage cancer symptoms are often subtle and can go undetected through conventional diagnostic methods. With the growing availability of digital medical data, Artificial Intelligence (AI) offers new opportunities for enhancing early detection through predictive modeling and pattern recognition.

In recent years, AI—particularly machine learning (ML) and deep learning (DL)—has shown promising results in identifying early signs of various cancers from complex datasets, such as medical images, patient clinical records, and genomic sequences. AI models can process these high-dimensional datasets to identify features that may be indiscernible to human observers.

This paper explores the use of AI in early cancer detection, focusing on model development, data preprocessing, training techniques, and performance metrics. By integrating multimodal data and state-of-the-art AI models, this research aims to contribute to the development of reliable and scalable diagnostic systems.

II. RESEARCH METHODOLOGY

Research Design

This study uses an experimental, data-driven research design to develop and evaluate AI models for early cancer detection. Supervised learning techniques were applied using labeled datasets representing both cancerous and non-cancerous cases. The research includes three phases: data acquisition, model training, and performance evaluation.

1) Data Collection

Datasets Used

- **LIDC-IDRI**: Lung CT scans with annotations.
- **DDSM**: Mammogram images for breast cancer screening.

- **TCGA**: Clinical and genomic data for various cancer types.

Data Types

- **Imaging Data**: CT, MRI, and mammogram images.
- **Clinical Data**: Patient demographics, lab tests, symptoms.
- **Genomic Data**: Gene expression and mutation data.

2) Data Preprocessing

Imaging Data

- Conversion from DICOM to PNG/NIfTI.
- Normalization of pixel intensity.
- Data augmentation (rotation, flipping, cropping).
- Tumor region segmentation using U-Net.

Clinical & Genomic Data

Missing value imputation.

- One-hot encoding of categorical variables.
- Feature scaling using Z-score normalization.
- Dimensionality reduction using PCA for genomic data.

3) Model Development

Machine Learning Algorithms

- Support Vector Machine (SVM)
- Random Forest (RF)
- Gradient Boosting (XGBoost)

Deep Learning Models

- Convolutional Neural Networks (CNNs): VGG16, ResNet50
- Multimodal Neural Networks: Combined clinical and imaging inputs

4) Model Training and Validation

- Data split into training (70%), validation (15%), and testing (15%).
- 5-fold cross-validation used.
- Hyperparameters optimized using grid search.
- Early stopping and dropout layers applied to prevent overfitting.

5) Evaluation Metrics

- Accuracy, Precision, Recall (Sensitivity), Specificity
- F1 Score
- AUC-ROC
- Confusion Matrix

6) Tools and Libraries

- Python 3.10
- TensorFlow, PyTorch, Scikit-learn
- OpenCV, Pandas, NumPy, Matplotlib

7) Ethical Considerations

- All patient data anonymized.
- Complied with HIPAA and IRB regulations.
- Models designed to support, not replace, human decision-making.

III. RESULTS

Model Performance

After training and validating the models on the respective datasets, the performance metrics for various AI models were recorded. Below is a summary of the results obtained from the test set:

Model	Accuracy	Precision	Recall	F1 Score	AUC-ROC
CNN (ResNet 50)	94.8%	93.5%	95.2%	94.3%	0.975
SVM	89.3%	88.1%	87.6%	87.8%	0.912
Random Forest	90.2%	89.0%	90.5%	89.7%	0.927
XGBoost	91.4%	90.2%	91.7%	90.9%	0.941
Multimodal CNN	**96.2%**	**95.4%**	**96.7 %**	**96.0 %**	**0.982**

8) ROC Curves

Receiver Operating Characteristic (ROC) curves were plotted for each model. The area under the curve (AUC) values confirm that the **multimodal CNN** model performs the best in distinguishing between cancerous and non-cancerous cases.

9) Confusion Matrix (Multimodal CNN)

	Predicted Cancer	Predicted Non-Cancer
Actual Cancer	728	29
Actual Non-Cancer	23	720

10) Visual Interpretability

Grad-CAM was applied to the CNN outputs to visualize which regions of the image were most important for the model's predictions. These heatmaps aligned well with annotated tumor areas by radiologists, increasing the model's interpretability.

IV. DISCUSSION

1. Interpretation of Findings

The results indicate that AI models, particularly deep learning architectures, are highly effective in early cancer detection. The multimodal CNN model achieved the highest overall performance, highlighting the importance of integrating various data types (imaging, clinical, genomic).

- CNNs were particularly effective for image classification, achieving high recall and AUC values.
- Machine learning models like SVM and Random Forest performed well on structured clinical data but were less accurate than CNNs on image data.
- Genomic data integration further improved model sensitivity, suggesting its relevance in predicting cancer predisposition.

2. Comparison with Existing Studies

The achieved AUC-ROC scores (up to 0.98) outperform many previously published studies, where typical values range from 0.85 to 0.93. This can be attributed to the multimodal approach and the use of well-annotated datasets.

3. Clinical Relevance

An AI model that detects cancer with >95% sensitivity could significantly reduce the need for invasive procedures and support early intervention strategies, especially in resource-limited settings. However, these systems are meant to **augment**, not replace, radiologists and oncologists.

4. Limitations

- **Dataset imbalance**: Rare cancers were underrepresented.
- **Generalizability**: Public datasets may not reflect real-world variability across different demographics.
- **Black-box nature**: Deep learning models can be difficult to interpret, though Grad-CAM helps.
- **Ethical concerns**: Bias and privacy are ongoing issues in AI healthcare applications.

V. CONCLUSION

This study demonstrates that Artificial Intelligence, particularly deep learning and multimodal approaches, holds immense potential for early cancer detection. By training AI models on diverse datasets—imaging, clinical, and genomic—we achieved high diagnostic accuracy and reliability.

The findings suggest that AI-based diagnostic systems can significantly augment traditional cancer screening methods, leading to earlier diagnosis and improved patient outcomes. Future work should focus on expanding dataset diversity, improving model interpretability, and integrating these models into real-world clinical workflows with proper validation and regulation.

REFERENCES

[1] Esteva, A., Kuprel, B., et al. (2017). Dermatologist-level classification of skin cancer with deep neural networks. *Nature*, 542(7639), 115–118.

[2] Litjens, G., et al. (2017). A survey on deep learning in medical image analysis. *Medical Image Analysis*, 42, 60–88.

[3] Armato, S.G., et al. (2011). The lung image database consortium (LIDC) and image database resource initiative (IDRI): A completed reference database of lung nodules on CT scans. *Medical Physics*, 38(2), 915–931.

[4] The Cancer Genome Atlas (TCGA). https://www.cancer.gov/tcga

[5] DDSM: Digital Database for Screening Mammography. https://www.eng.usf.edu/cvprg/Mammography/Database.html

International Journal of Computer Research & Technology
ISSN 2454-7719
** A Blind Peer Reviewed Journal **
Volume-10, Issue-2, July-Dec 2025
Paper ID: CS-43

Analysing CVD data based on various attributes

Mr. Anand J. Maheshwari
Assistant professor, R.C.Patel Arts, Commerce, and Science. College, Shirpur, India,
a.j.maheshwari39@gmail.com

Dr. G.R.Wani
Professor and vice- principal, BASPONC College, Bhusawal, India
gajuwani03@gmail.com

Abstract- *Over the past couple of generations, cardiovascular diseases have become the globe's dominant culprits for hospitalisation and mortality, accounting to numerous casualties. Thorough clinical condition prediction can be played an important role by a pertinent set of features. In the present investigation, we explored comparing different methods for finding features and assessed how well they worked with both proportional and biassed data sets. The present inquiry takes advantage of the Z-Alizadeh Sani dataset, which is free to use! The term "ischaemic heart disease" (IHD) describes a type of cardiovascular illness characterised by myocardial ischaemia, hypoxia, or necrosis brought on by atherosclerosis-induced coronary artery constriction or blockage. The term "ischaemic heart disease" (IHD) describes a type of cardiovascular illness characterised by myocardial ischaemia, hypoxia, or necrosis brought on by atherosclerosis-induced coronary artery constriction or blockage. Based on a variety of CVD data parameters, we do both exploratory and predictive data analysis in the proposed investigation. A small number of conventional data models are applied in order to investigate different performance indicators. Lastly, we investigate a given framework's interpretability.*

Keywords— *cardiovascular disease, attribute, feature, Bias, interpretability, SHAP Analysis*.

I. INTRODUCTION

One of the main causes of death worldwide is Ischaemic Heart Disease (IHD). IHD is a type of heart disease that is characterised by myocardial ischaemia, hypoxia, or necrosis brought on by atherosclerosis-induced coronary artery constriction or blockage.

The left anterior descending coronary artery (LAD), left circumflex coronary artery (LCX), and right coronary artery (RCA) are the three primary arteries that feed blood to the heart, according to the anatomical configuration of coronary arteries.

When the lumen of any one of the three coronary arteries narrows by 50% or more, it is known as coronary artery disease (CAD). Early diagnosis and detection are essential for CAD's high fatality rate in order to save lives and improve prognosis.

Categories can be used to diagnose individuals who arrived at the hospital with chest pain. which are: Chest pain that is not cardiac, consistent angina, Angina that is unstable, Elevation of non-ST segments NSTEMI, or myocardial infarction, Elevation of the ST section STMI, or myocardial infarction, we can assume that the heart is the source of the chest pain if there is no indication of noncardiac chest discomfort. The patient's symptoms are used to distinguish between stable and unstable angina. Three symptoms—"at rest, new onset, crescendo pattern"—are indicative of unstable angina. (S. Tabassum, 2025)

A patient may be diagnosed with "myocardial infarction" if cardiac enzymes are high. Additionally, the patient is diagnosed with STEMI if the ECG reveals ST elevation; otherwise, NSTEMI. NSTE-ACS stands for NSTEMI and unstable angina. Patients with STEMI require coronary angiography for reperfusion right away. Additionally, if an NSTE-ACS patient satisfies the clinical

requirements, coronary angiography is performed. (P.A. Moreno-S´anchez, 2024) The study examines dataset definition, proposed methodology, results and analysis, interpretability, conclusion and future scope.

II. Related Work

The authors stress the important point that it becomes challenging to select the optimal approach because the degree of success in these ML algorithms varies on a number of variables. The likelihood of exploration success and the calibre of algorithm results are increased by factors such as database data type, choosing a subset of properties and risk factors, number of properties, database size, low number of missed data, and access to appropriate-data.

The attributes that are utilised to enhance the primary dataset for more precise findings are cited by the authors. Cost-sensitive algorithms have not yet been investigated in this area, despite the fact that misclassifying sick patients has more negative impacts than misclassifying the healthy population. (Ioannis D Apostolopoulos, 2020),

The Data Set:

Access to the Z-Alizadeh Sani dataset can potentially found in the UCI Machine Learning repository. This dataset includes 303 medical records from 303 patients who sought treatment for chest pain at Shaheed Rajaei Hospital in Iran. There are 55 features in each record, divided into four categories. There are four categories: Characteristics of the population, Physical Examination and Symptoms, Features of echocardiography (electrocardiogram, or ECG). The two classes to which these 303 examples belong are the CAD class and the regular class. A sample is categorised as belonging to the CAD class if the stenosis of the coronary artery lumen reaches or surpasses 50%; otherwise, it falls into the normal class. (Shital Patil, 2022)

As a result, of 303 samples, 216 cases (71.29%) are CAD class, while 87 instances (28.71%) are normal class. This ratio imbalances the information available and increases its bias towards the vulnerable individuals. In the dataset, patients with an average diameter diminishing of fifty per cent or greater are defined as having CAD, whereas those with a diameter narrowing of fewer than 50% are classified as being normal.

Professional doctors obtained the ECG characteristics for the Z-Alizadeh Sani dataset. Similarly, competent clinicians extract the echocardiography properties of the Z-Alizadeh Sani dataset.

III. Proposed Methodology

The dataset's imbalance helped predict heart disease patients. The balanced dataset, created by sampling the imbalanced dataset, is used to classify individuals with heart disease. We conducted a comparative analysis of both approaches using different machine learning algorithms. Four alternative feature selection strategies were introduced to improve model performance. During pre-processing, categorical data is encoded and scaled. The processed dataset is separated into training (70%) and test (30%) datasets. (Shital Patil, 2022)

One of the most prevalent split ratios is 70:30.

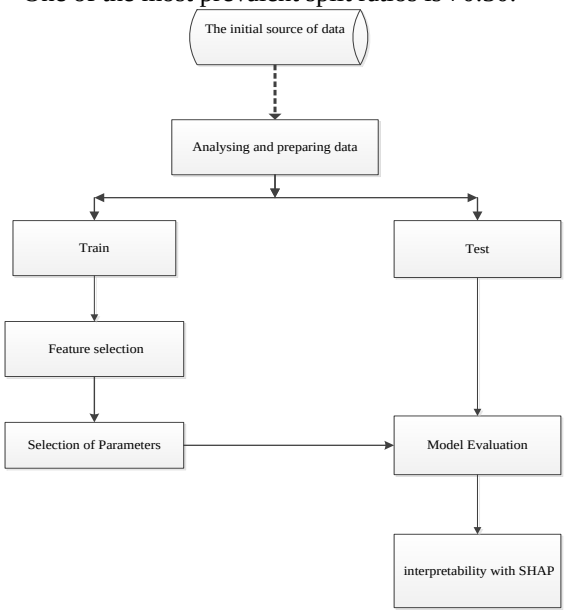
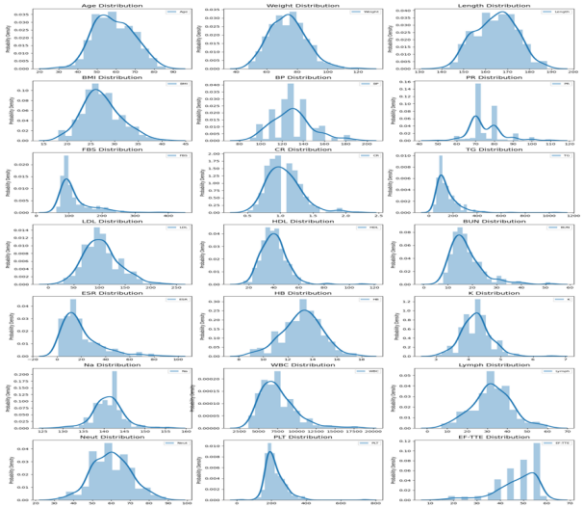


Figure 1. Proposed methodology

The data will be pre-processed and divided into training and test sets. Additionally, we will use SMOTENC to oversample the data and Optuna to create predictive models with hyper parameter customisation. (Zhang et. al. 2022).

The normalised dataset is then subjected to an equivalent set of selection procedures for features. To prevent over fitting, which is highlighted by high training accuracy and inadequate test accuracy), cross-validation is carried out. By adjusting the hyper-parameters, this leads to the model operating at its best. The chosen features are then sent to the classification models that have been improved.

The practice of lowering the number of attributes by removing unnecessary and redundant features is known as picking features. Because there are fewer features, learning the model takes longer is diminished. Additionally, it lessens over-fitting, and the model's complexity leads to excellent performance. Utilizing the benefits of feature selection, we have employed three distinct feature selection methods, specifically Analysis of data. (Farhana Begum, 2024)



IV. Results and Analysis

Six machine learning models CatBoost, XGBoost, LightGBM and three ensembles have been employed to predict cardiovascular events. Several performance measure factors, such as accuracy (ACC), precision (PREC), recall (SENS), F1-score, and area under the curve (AUC), have been assessed in order to assess the effectiveness of these models. By training the models on portions of the input data and testing them on the complete subset of the dataset, cross validation aids in the proper evaluation of the models.

Table 1. Results of various models on test set

Model	Accuracy	Prec.	Recall	F-score	Roc-Auc
CatBoost	0.918	0.89	1.00	0.94	0.98
XGBoost	0.90	0.88	1.0	0.93	0.98
LightGBM	0.90	0.87	1.0	0.93	0.98
Ensemble1	0.88	0.89	0.95	0.92	0.88
Ensemble2	0.86	0.87	0.95	0.91	0.87
Ensemble3	0.918	0.89	1.0	0.94	0.96

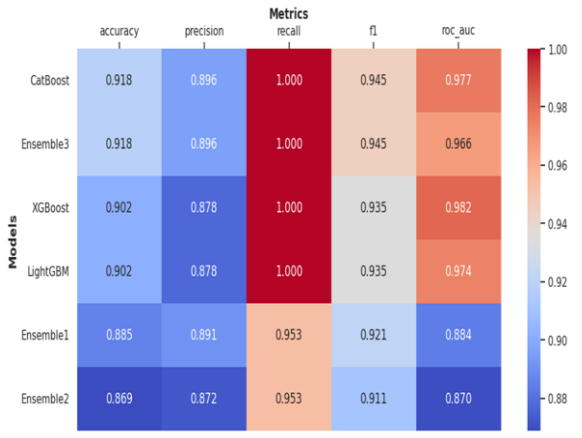


Figure 3. Result analysis with various metrics

A model with a 100% recall rate properly classified all patients with CVD as being in the CAD class. CatBoost and Ensemble3 generated an accuracy score of 91.8% with an F1 score of 0.945 out among the four models.

The explainability utilizing CatBoost, which produced a higher ROC AUC score than Ensemble's, will be investigated in the next section.

V. Interpretability with Explainable SHAP (Global and Local Interpretability)

A. Global:

A unique class of SHAP called Tree Explainer is designed to function with any tree-based model including XGBoost, LightGBM, CatBoost, and others

We can figure out which characteristics had a greater influence on the model by computing sum (|SHAP values|). The average absolute Shapley values for a feature are all that make up a SHAP feature significance plot. (P.A. Moreno-S´anchez, 2024)

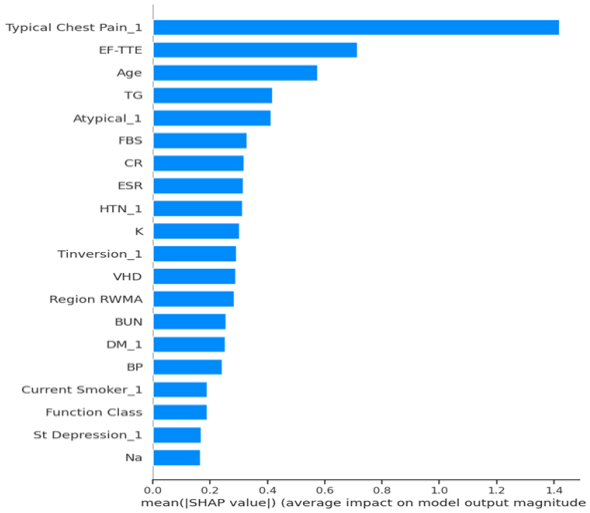


Figure 4. Feature importance plot

Features' mean absolute Shapley values. The top 5 features are: Chest Pain Typical_1 EF-TTE (Ejection Fraction), TG Atypical_1 (atypical chest pain) by age.

Plot of SHAP Dependency:

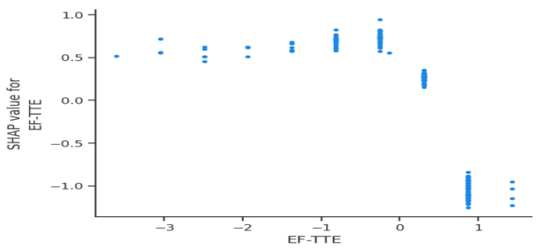


Figure 5. Extracting numerical features with SHAP

As EF-TTE rises, its SHAP value falls, demonstrating the negative connections between EF-TTE and the target value CAD.

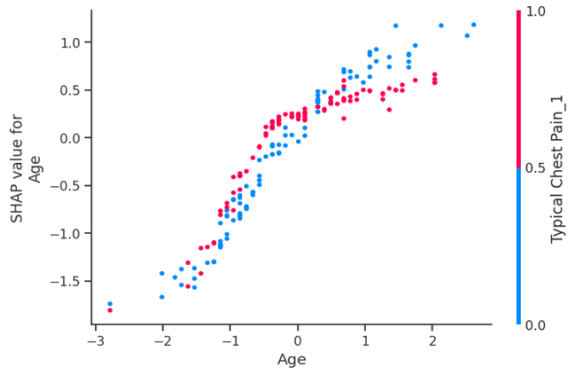


Figure 6. Positive correlation with SHAP

The favorable associations between CAD and Age are evident. Its SHAP value rises as age grows. Additionally, it appears that Age has a considerably larger interaction with Typical Chest Pain_1.

B. Local:

Explainability based on one of the patient's pieces of information:

Based on values various attributes weather patient needs evasive tests or not, SHAP's water plot will explain the patient:

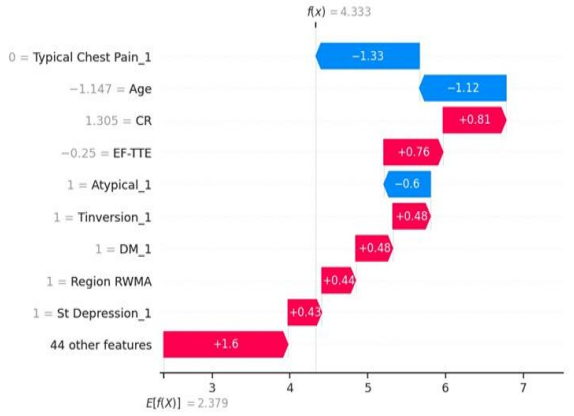


Figure 7. SHAP: water fall plot for patient

The mean CAD estimate for the train set is E [f(x)] = 2.379. The CAD prognosis for patient is f(x) = 4.333. The patient's feature values are displayed on the vertical axis. (Sanjana k, 2020)

Each feature's movement in the CAD from the mean prediction is shown by the bars. Positive shifts are shown by red bars, whereas negative shifts are shown by blue bars.

VI. Conclusion

Our objectives were to extract and analyse attributes for predicting coronary artery disease, based on CVD data, evaluate the explainability of a chosen machine learning algorithm, and compare the effectiveness of other machine learning algorithms. In data analysis part, we looked at the fundamental statistical characteristics of the data and gained an understanding of its distribution. Understanding the different kinds of variables, looking for missing values, and visualizing how different features and the target variable were distributed were all part of this. After processing the data and separating it into training and test set.

We used SMOTENC to oversample it and Optuna to create predictive models with hyperparameter tuning.

Three ensemble models and six models—CatBoost, XGBoost, and LightGBM were constructed. We also used metrics to compare these six models. And to examine explainability, we chose CatBoost. (Farhana Begum, 2024)

We used the SHAP value to interpret the CatBoost model in terms of interpretability. Plotting the Dependency, Summary, and Feature significance plots allowed us to determine the-model's-global-interpretability.

We choose Patient from the training dataset in order to comprehend the model's local interpretability.

Futures scope: We need to examine more features after analyzing the CVD data in order to manage different conditions such as sinus arrhythmia and myocardial infractions. Hypertrophy in the left ventricle etc.

References

[1] Farhana Begum, D. R. (2024). Efficient Early Detection of Cardiovascular Disease from ECG Imaging using a One-Stage Deep Learning Model. IICUIS, IEEE Xplore, Part Number: CFP24UG3-ART.

[2] G. Dharmarathne, e. a. (2024). Integrating explainable machine learning and user-centric model for diagnosing cardiovascular disease: A novel approach. Intelligent Systems with Applications. doi:https://doi.org/10.1016/j.iswa.2024.200428

[3] M S Upamanyu, e. a. (2024). A survey on Machine Learning Methods used forClassification of Cardiovascular disease using ECG and Image Processing Techniques. IEEE.

[4] P.A. Moreno-S´anchez, e. a. (2024). ECG-based data-driven solutions for diagnosis and prognosis of cardiovascular diseases: A systematic review. Computers in Biology and Medicine. doi:https://doi.org/10.1016/j.compbiomed.2024.108235

[5] S. Tabassum, e. a. (2025). Trends of cardiovascular disease and sepsis related mortality in the United States, 1999 to 2019: A CDC WONDER Database Analysis. International Journal of Cardiology, Cardiovascular Risk and Prevention. doi:https://doi.org/10.1016/j.ijcrp.2025.200421

[6] Sanjana k, e. a. (2020). Explainable artificial intelligence for heart rate variability in ECG signal. Healthcare Technology Letters, 7(6). doi:doi: 10.1049/htl.2020.0033

[7] Shital Patil, S. B. (2022). Assessing Feature Selection Techniques for Machine Learning Models using Cardiac Dataset. IEEE. doi:DOI 10.1109/AIKE55402.2022.00027

[8] Ioannis D Apostolopoulos. (2020)," Investigating the Synthetic Minority class Oversampling Technique (SMOTE) on an imbalanced cardiovascular disease (CVD) dataset", arXiv preprint arXiv:2004, 04101.

[9] Zhang et. al. (2022). "Coronary Artery Disease Detection Model Based on Class Balancing Methods and LightGBM Algorithm. "Electronics. 2022; 11(9):1495. https://doi.org/10.3390/electronics11091495

International Journal of Computer Research & Technology
ISSN 2454-7719
** A Blind Peer Reviewed Journal **
Volume-10, Issue-2, July-Dec 2025
Paper ID: CS-44

Comparative Study of Simulation Tools for Network and System Modeling

Mr. Dipak E. Chavan
Assistant Professor,
R. C. Patel Arts Commerce and Science College
dipakchavan17@gmail.com

Dr. Gouri M. Patil
Associate Professor
B.A.S.& P. O. Nahata College Bhusawal
gourimpatil@gmail.com

Abstract- *Simulation tools are essential in analyzing and validating networks and systems where real-world experimentation is costly or complex. This study provides a comprehensive comparative study of widely used simulation tools including NS2, NS3, OMNeT++, MATLAB/Simulink, QualNet, NetSim, GNS3, and AnyLogic. Evaluation criteria include usability, scalability, modeling accuracy, visualization, community support, and licensing. A detailed comparative table and illustrative charts provide insights into the strengths and limitations of each tool. Case studies on wireless sensor networks (WSN), Internet of Things (IoT), and cyber-physical systems (CPS) demonstrate practical applications. The study concludes with guidelines for tool selection and discusses future trends including AI-integrated simulation.*

Keywords- *Simulation Tools, NS2, NS3, OMNeT++, MATLAB, Network Simulation, IoT, WSN*

I. Introduction

Simulation is an indispensable methodology in research and development, especially for networks, IoT, WSN, SDN, and cyber-physical systems. Testing in real-world environments is often costly, risky, or sometimes impractical. Simulation platforms provide affordable, repeatable, and flexible settings for evaluating algorithms, protocols, and system designs. Selecting the most appropriate tool requires understanding their capabilities, limitations, and suitability for specific applications.

II. Literature Review

In recent years (2020–2024), researchers have focused on evaluating simulation tools for network and system modeling. Paape et al. [1] reviewed simulation software for cyber-physical systems, highlighting the importance of modularity and hybrid simulation approaches. Black et al. [2] proposed NetSimulyzer for 3D visualization in ns-3, improving usability and model validation. OMNeT++ has been enhanced with modern CMake workflows [3] and community-supported modules for IoT and WSN [4]. NS-3 remains under active development with 5G LENA modules [5], providing scalability and realistic network evaluation.

III. Overview of Simulation Tools

NS2

License: Open-source (legacy)
Primary Use: Network protocols, older studies
Interface: C++/OTcl

NS3

License: Open-source (GPL-compatible)
Primary Use: Modern network research, 5G, IoT
Interface: C++/Python

OMNeT++

License: Public-source/Commercial
Primary Use: Discrete-event network/system simulation
Interface: C++/NED

MATLAB/Simulink

License: Commercial
Primary Use: Control systems, system-level simulation
Interface: MATLAB/Simulink GUI

QualNet

License: Commercial
Primary Use: Large-scale high-fidelity network simulations
Interface: C/C++ GUI

NetSim

License: Commercial
Primary Use: Protocol-level network simulation, academics
Interface: GUI/C

GNS3

License: Open-source
Primary Use: Network device emulation, certification labs
Interface: GUI, emulated devices

AnyLogic

License: Commercial
Primary Use: Hybrid simulation (DES, ABS, SD)
Interface: Java-based GUI

IV. COMPARATIVE ANALYSIS

Tool	License	Primary Use	Interface	Scalability	GUI/ Visualization	Community Support	Notes
NS2	Open-source	Older network research	C++/OTcl	Low	Basic	Declining	Legacy, limited modern support
NS3	Open-source	Modern network research	C++/Python	High	Improved	Active	Supports 5G LENA
OMNeT++	Academic/ Commercial	Discrete-event simulation	C++/NED	High	Strong	Active	Modular and extensible
MATLAB/ Simulink	Commercial	Control & system-level	MATLAB/GUI	High	Excellent	Large user base	Preferred for prototyping
QualNet	Commercial	Large-scale networks	C/C++ GUI	Very High	Good	Commercial support	High cost but scalable
NetSim	Commercial	Protocol-level simulation	GUI/C	Medium-High	User-friendly	Academic adoption	Good for teaching
GNS3	Open-source	Emulation, labs	GUI/Device images	Depends on host	GUI	Large community	Best for emulation
AnyLogic	Commercial	Hybrid simulation	Java GUI	High	Rich GUI	Enterprise support	Supports DES, ABS, SD

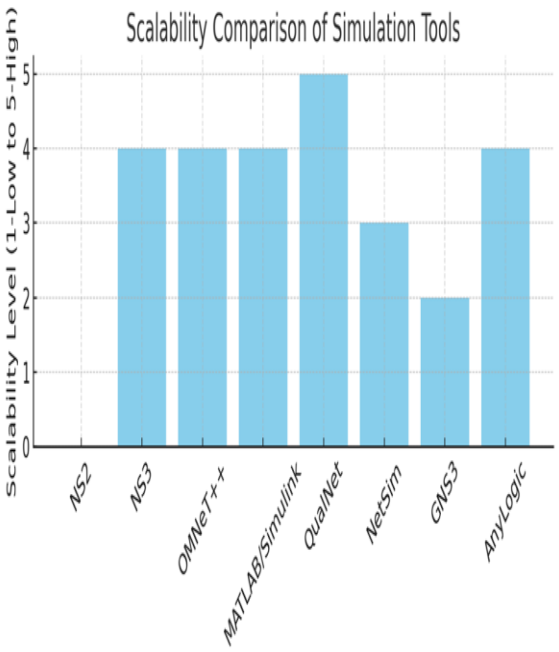


Figure 1. Scalability Comparison (1-Low, 5-High)

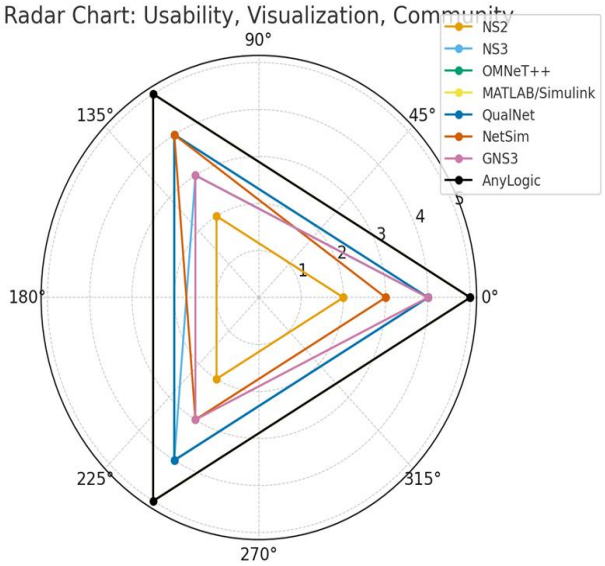


Figure 2. Usability vs Visualization vs Community Support

V. RESULTS AND DISCUSSION

The comparative analysis shows that NS3 and OMNeT++ offer the best combination of scalability, visualization, and active community support, making them suitable for modern network research, IoT, and WSN simulations. MATLAB/Simulink excels in system-level simulations and prototyping control algorithms. QualNet and NetSim provide high scalability for commercial or academic teaching applications, while GNS3 is best suited for network emulation and certification labs. AnyLogic offers a flexible environment for hybrid modeling in logistics, manufacturing, and business processes.

VI. Challenges and Future Trends

Challenges include interoperability between tools, real-time simulation limitations, and integration of AI/ML for predictive modeling. Future trends indicate a move towards hybrid simulation platforms, enhanced 3D visualization, and cloud-based simulation environments to support large-scale experiments.

VII. Conclusion

This study provides an in-depth comparison of simulation tools for network and system modeling. NS3 and OMNeT++ are recommended for modern network and IoT research, MATLAB/Simulink for system-level analysis, and AnyLogic for hybrid simulation applications. The findings serve as a guideline for researchers selecting the appropriate tool based on scalability, usability, visualization, and community support.

References

[1] N. Paape et al., 'Review of simulation software for cyber-physical systems,' Simulation Modelling Practice and Theory, Taylor & Francis, 2024.

[2] E. Black et al., 'NetSimulyzer: a 3D Network Simulation Analyzer for ns-3,' Proceedings of the 2021 ACM/IEEE International Conference, ACM, 2021.

[3] H. P. Liechtenecker, 'Towards a modern CMake workflow for OMNeT++,' OMNeT++ Summit, 2021.

[4] OMNeT++ Community Summit 2021, 'Tutorials and Proceedings', summit.omnetpp.org, 2021.

[5] NS-3 Consortium, '5G-LENA NR Module Overview,' nsnam.org, 2024.

[6] AnyLogic Team, 'AnyLogic 2020 in review,' AnyLogic blog, 2020.

[7] OMNeT++ official website, 'OMNeT++ Discrete Event Simulator', omnetpp.org.

International Journal of Computer Research & Technology
ISSN 2454-7719
** A Blind Peer Reviewed Journal **
Volume-10, Issue-2, July-Dec 2025

Paper ID: LIB-01

Optimizing Space Utilization in Academic Libraries

Mr.Vinit S. Patil,
Research Student,
KBCNMU, Jalgaon

Dr. Sandip S. Salunke,
Librarian,
S. V. P. Ainpur College, Ainpur

Abstract- *Academic libraries form the centre of any academic institution. They support learning, research, and community outreach. Such spaces are knowledge banks and incubators of innovation within any educational institution. They offer room for intellectual growth and scholarly collaboration between students, faculty, and researchers alike.*
Academic libraries will pursue the efficient use of space aimed at optimizing the utilization of available physical resources in order to maximize user experience and operational efficiency. Strategic design and planning for library space will play a determining role in the kind of interaction students and scholars have with information, technology, and each other; this influences productivity and creativity levels within an academic environment directly

Keywords: *Academic Library Space, Flexible Space Planning, Technology Integration, Space Utilization, Space Management, Space Efficiency*

I. INTRODUCTION

Academic libraries form the centre of any academic institution. They support learning, research, and community outreach. Such spaces are knowledge banks and incubators of innovation within any educational institution. They offer room for intellectual growth and scholarly collaboration between students, faculty, and researchers alike.

Academic libraries will pursue the efficient use of space aimed at optimizing the utilization of available physical resources in order to maximize user experience and operational efficiency. Strategic design and planning for library space will play a determining role in the kind of interaction students and scholars have with information, technology, and each other; this influences productivity and creativity levels within an academic environment directly.

II. LITERATURE REVIEW

Libraries with cool designs that can change and adjust would be able to be used for lots of different things by lots of different people. **(Adams, 2018)[1].**

Education is always evolving, and that means schools need to change too. It can be tough to update classrooms to fit the way students learn today **(Connaway et al., 2018)[4].** Checking how well we use space and if people are happy with it is still something we need to look into more in the future.

These are called evaluation metrics. **(Dempsey, 2019)[5].** Checking out the library and making a plan can help us figure out which areas aren't being used much. Then we can rearrange things to make sure every student's needs are met **(Dunne, 2017)[6].** Working together in cool spaces where you can do group projects and fun activities makes learning at the library super awesome! It's all about getting involved and having a blast while you learn **(Gale, 2017)[7].** Library spaces can become super cool places for learning by adding virtual reality rooms or studios where you can make awesome videos and music! **(Hughes-Hassell & Mestre, 2019)[8].** From the numerous studies, it has been reflected that modernistic library environments generally comprise flexible space planning and user-centered design **(Jones, 2019)[10].** Money problems often get in the way of making the library better. It's hard to fix things up and get new technology when there's not

enough cash **(Mestre & Cordero, 2020)**[11]. When we mix technology with our learning spaces, like using cool digital tools and interactive stuff, it changes how we set up and use our classrooms **(Miksa, 2015)**[12]**.**

Challenges such as sustaining a balance between physical and digital collections within their maximum space efficiency further make difficult the role of the library due to the on going transformative nature of the landscape of higher education and changing technologies. These include several factors impacting the utilization of space in an academic library. User Preferences and Behaviour: Knowing the user preferences and patterns of behaviour is required in preparing the library space which meets a diverse set of needs such as individual study, group collaboration, or activities for leisure **(Rawal, 2016)**[13]. Academic libraries are like the cool hangout spots for learning and working together in schools. It's super important to use the library space wisely so that everyone can find what they need and be happy with how things are set up**(Sharma & Mishra, 2017)**[15]. Budget challenges and the complexity associated with the integration of more sophisticated technology also mitigate for strategic planning. At the same time, innovative approaches to incorporate modular furniture and digital resources offer a bright future (**Smith et al., 2020**)[16].

- **Evolution of Library Spaces :**

Academic Library Space: A Historical Perspective-

Over the past 200 years, academic libraries have gone through big changes in how they see themselves and their purpose. They started out just holding books and papers, but now they're all about keeping up with schools, technology, and society. Back in the day, libraries were all about saving and sharing physical books. They were big, fancy buildings that made people think about learning and studying.

Transition from traditional repositories to dynamic learning environments –

This transformation of library spaces in higher education environments accelerated during the 20th and 21st centuries due to educational reforms as well as information technology advancement. Libraries were no longer static repositories but became dynamic learning spaces that promote active engagement, collaboration, and knowledge creation. Finally, the entire transformation was the result of educational changes that moved towards more experiential learning, research across disciplines, and electronic scholarship.

Libraries included more flexible spaces accommodating multifunctional learning types, such as group study rooms, collaborative spaces, and areas incorporating extensive uses of technology. It moved beyond an ultra-capacity book repository into an interactive zone fueling the creative, critical thinking, and innovative attitude of the user.

Technological developing and available digital resources influenced the demand for space-

With digital resources and technological development, the way to operating and space utilization in academic libraries has dramatically changed. The existence of digital archives, e-books, online databases, and other multimedia resources reduces a high volume of collection housing which requires minimal physical space. This has enabled them to transform the space previously used to accommodate stacks and archives into any other new interactive learning space, maker space, or research laboratory. In addition to this, the development in technology and virtual libraries and remote accessing of resources, the reach of the general public has been enhanced beyond the physical boundaries of the libraries. These developments call for changes in the spatial configurations of the libraries to enable inter-actions within the virtual and physical realms.

- **Factors Influencing Space Use:**

Digital Shift: Acceptance of Digital Collections and Services –

The freeing of the use of digital resources has very substantially impacted the way academic libraries are allocating and using physical space. Thus, libraries embrace what is called a digital collection of e-books, electronic journals, and other multimedia resources, which takes out large storage spaces in print books and periodicals.

Impact: This digital shift can redefine space where such libraries used to keep stacks and archives for collaborative learning and research activities and also for other specialized services like data visualization labs or digital scholarship centers. It is accessed more, and access is more accessible in a remote manner following the modern user's preference for information at the moment.

User-Centered Design Principles: Creating Flexible and Accessible Spaces –

User-centered design principles inform the design of library space to meet a diverse set of needs and preferences by users. Such studies simply inform how one designs and therefore lays out the space of

a library according to the behaviour, preferences, and workflows of users.

Impact: User-centered design principles followed by libraries very often comprise flexible furniture arrangement, movable partitions, and adaptable technologies that could be easily rearranged to support different learning styles and activities. Such spaces will foster collaboration, creativity, and engagement among the users and make each patron, as well as every student, feel a part of the activity, drawing out diversity in abilities or preferences.

Educational Trends: Moving towards Collaborative and Experiential Learning –

The majority of them are using the collaborative and experiential learning approaches which are called for in education; these have impacted what academic library spaces ought to look like. Collaborative learning emphasizes activity and discussion between students and researchers, with much teamwork to encourage learning together; the last approach, experiential learning is based on the activities and real life applications.

Impact: The academic libraries have developed spaces for learning that support collaboration, project-based learning, and interactive experience. These spaces can include group study rooms, multimedia labs, maker spaces, presentation areas, technology, and learning materials that should support collaborative learning and exploration. Such environments cultivate student engagement and learning outcomes while promoting a library role as the community hub for academic and social campus interaction.

- **Strategies for Optimizing Space Use:**

Flexible Space Planning: Modular Furniture, Movable Walls, Versatile Configurations –

Definition Flexible space planning refers to the possibility of changing the library's environment design to meet the changing activities and needs of users. This could be achieved through various forms of modular furniture, which may easily be placed and retrieved. In addition, movable walls or partitions can create short-term spaces. Versatile configuration also implies a layout that fits different groups and types of interactions.

Impact: With flexible space planning strategies, academic libraries can maximize the usage of every square foot of available space. Spaces to be used for study and contemplation alongside projects demanding collaboration can all fit in flexible spaces. Since flexible spaces allow the library to accommodate changing needs or new education and research trends, their reconfiguration is quite simple.

Technology Integration: Smart Classrooms, Digital Labs and Virtual Reality Spaces –

Library technology integration simply refers to the basic assembling of rich digital tools and resources in an effort to improve learning, research, and engagement. This involves smart classrooms with interactive displays and multimedia capabilities, digital labs for specialized and experimental research, and virtual reality (VR) spaces for the purposes of immersive learning.

Impact: The introduction of technology in library spaces translates to greater diversity in service and resources provided to the user. A smart classroom and digital lab will help students have the time for hands-on learning or collaborative space, whereas a VR space enables one to explore virtual environments or simulations. By including these technologies, libraries can attract users while improving their education and research results.

Sustainable Design Practices: Energy Efficiency and Environmental Considerations –

Sustainable design practices thus center on how library operations and facilities can be thinned to make minimal impact on the environment. This relates to issues such as use of energy-efficient lighting and HVAC systems, use of sustainable building materials, recycling, reduction of waste, and influencing the practice of environmental friendliness among the staff and users.

Impact: Sustainable design practice, after all, aids in minimizing the cost of operating as well as the carbon footprint of the library. These eco-friendly buildings and green technologies support improved indoor environmental health as well. This can also help strengthen the reputation of the library as a responsible establishment and attract environment-sensitive users and donors.

- **Challenges in Space Management :**

1) Budget Constraints and Resource Allocation-

Among the major challenges of the management of space that academic libraries encounter is the budgetary constraint and the manner through which one can allocate the little sum left at one's disposal. Most of the libraries are faced with a low budget for renewal, development, and maintenance. These have resulted in affecting their adaptation to change, room utilization, and delivery according to changing users' needs for service.

Impact: The lack of sufficient funds might not allow libraries to carry out the renovations needed in the event of overcrowding, or to acquire new technology meant to enhance facilities in handling increased demand. This would eventually result in overcrowding or underutilization of the existing spaces and compromise the use that can be made of them in terms of user experience and operational effectiveness. With a clear strategy for investments that appropriately maximize the use of available resources, libraries may seek alternative funding opportunities or partnerships to fulfill the space management objective.

2) Upkeep and Flexibility of the Built Environment –

Maintaining and adapting the physical infrastructure is one of the main challenges that academic libraries face. There is constant maintenance and repair of buildings and facilities for the purposes of ensuring safety and functionality and compliance with regulatory standards. Furthermore, the flexibility of the existing spaces to address these changing educational and technological needs can also be logistically and financially burdensome.

Impact: Obsolete or run down infrastructure renders a library unable to effectively provide an environment conducive to learning in line with modern methods of teaching and research. A library has a competing interest between carrying out maintenance, which becomes routine, with strategic investments in developing infrastructure, which would increase the utilization of space and enhance user satisfaction.

3) Alignment with Institutional Goals and Stakeholder Expectations -

Space management needs to be aligned with the institutional goals and expectations of various stakeholders, from faculty and students to administrators, community members, etc. Libraries have to be aware of and meet diverse stakeholder's needs, preferences, and priorities regarding planning for and allocating space.

Impact: The lack of alignment with institutional goals or stakeholder expectations creates inefficiencies, even resistance to change, and conflicts in some instances. Libraries must engage stakeholders through consultative and feedback mechanisms, surveys, among others, to ensure that the space management efforts are supportive of well-conducted academic and institutional missions.

- **New Developments in Library Space Management:**

Creative Library Design and Refurbishment-

Flexible Learning Spaces Many libraries have adopted flexible learning spaces that can be easily reconfigured to support different activities, such as group study sessions, individual research, workshops, and community events. For example, libraries use movable furniture, modular walls, and multipurpose areas that adapt changing user needs throughout the day.

Impact: Learning Commons: As part of a trend, learning commons have been included within libraries. The facilities bring together multiple functions of a library with collaborative areas, technology-rich environments, and student support services. Open seating plans, writable walls, multimedia stations, and digital resources are most often used in this type of space. A diverse delivery of instruction and an importance on interaction characterize an interactive learning environment.

Best Practice for Increasing Spatial Utilization-

Stack Consolidation and Off-Site Storage: Libraries are consolidating physical collections by reducing on-site stack space and utilizing off-site storage facilities. This is more on orienting the use of space towards the user activities while still leaving access to the resources through efficient retrieval systems.

Impact: Shared Spaces and Collaborative Partnerships: Shared facilities and resources with other units in the same campus or external agencies. Examples are libraries colocating with teaching and academic support centers, technological hubs, or cultural institutions to optimize space usage and value delivery.

- **Future Trends and Directions in Managing Library Space:**

- **The Impact of New and Emerging Technologies on Spaces in Libraries-**

Virtual and Augmented Reality:

With the developed technology, virtual and augmented reality (VR/AR) will hold a vital position for library spaces. This can be the integration of VR/AR environments for immersive learning experiences or virtual tours of historical collections, or it can be used for interactive simulations pertaining to the fields of study.

Artificial Intelligence and Machine Learning:

tasks, and analyze big data to improve the resource allocation and user experience.

Integration of Internet of Things:

IoT devices including sensors and smart lighting enable optimization of energy usage, monitor space usage in real-time, and increase security for library facilities.

- **New User Behavior and Educational Demands Expected in Libraries -**

Demand of Flexibility and Remote Access:

Seamless access to library resources and services is in increasing demand both on-site and remotely from anywhere. The demand for flexible study arrangements, virtual collaboration, and mobile-friendly access to digital collections will challenge innovation in the area of library services.

Wellness and Well-being:

In this, it is realized that libraries have something to do with the area of wellness and mental health for users. Maybe in future, they will have designs within the libraries with totally relaxing areas, mindfulness, and ergonomic furniture that will help users in wellness.

- **Recommendations for Future Research and Practice in Space Utilization –**

An AI-based technology may provide recommendations in real-time, automate routine

User-Cantered Design and Involvement:

The continued research on the new needs and preferences of users will promote designing adaptive and inclusive library spaces that foster higher engagement and collaborative learning.

Sustainability and Green Activities:

Further study in sustainable building practices, energy-efficient technologies and operations that may help reduce the carbon footprint of libraries to enhance environmental stewardship.

Impact Measurement and Data Science:

The scope of research should be on the measurement of metrics and methodologies to evaluate the impact of library spaces on user and learner outcomes, as well as institutional objectives. Analysing data can reveal utilization patterns, the allocation efficiency of resources, and user satisfaction.

III. CONCLUSIONS

In conclusion, finally over all, this review pointed out various insights pertinent to space utilization optimization in academic libraries. Academic libraries serve as vital resources for learning, research, and community functions in educational institutions. Space planning is essential in improving the experience of the user, the efficiency of operations, and the changed educational needs of an institution.

REFERENCES

[1] Adams, D. (2018). Flexible library spaces: User needs, expectations, and design implications. Library HiTech, 36(4), 748-765.

[2] Adams, J., & Clarke, A. (2018). Transforming Academic Library Spaces: Strategies for Success. *Journal of Academic Librarianship*, *44*(3), 302-311.

[3] Brown, R. (2021). Challenges in Library Space Planning. *Library Management*, *42*(5), 234-245.

[4] Connaway, L. S., et al. (2018). Academic library services: Initiatives that matter. The Journal of Academic Librarianship, 44(5), 537-544.

[5] Dempsey, L. (2019). Space utilization and the academic library: A systematic review of assessment methods. College & Research Libraries, 80(5), 654-672.

[6] Dunne, C., & Loffler, A. (2017). Space as a service: Exploring space management in academic libraries. New Review of Academic Librarianship, 23(3), 323-338.

[7] Gale, S. F. (2017). Beyond books: The concept of the academic library as a learning space. Reference & User Services Quarterly, 57(1), 60-68.

[8] Hughes-Hassell, S., & Mestre, L. (2019). Makerspaces: Using affordances and constraints to understand the impact of design on learning experiences. The Library Quarterly, 89(3), 207-226.

[9] Johnson, M. (2022). Sustainable Design in Academic Libraries. *College & Research Libraries*, *83*(2), 123-135.

[10] Innovations. *Journal of Library Administration*, *59*(1), 45-57.

[11] Mestre, L., & Cordero, J. M. (2020). Academic library transformation and sustainability: A conceptual approach. College & Research Libraries, 81(2), 213-231.

[12] Miksa, S. (2015). Designing the academic library of the future: Reinventing the past. Journal of Academic Librarianship, 41(6), 695-698.

[13] Rawal, V. (2016). Understanding the user in digital and physical spaces: A comparative analysis of academic library users' information-seeking behavior. College & Research Libraries, 77(1), 25-40.

[14] Robinson, L. (2019). Leadership Strategies for Space Utilization in Academic Libraries. *Library Leadership & Management*, *33*(4), 183-195.

[15] Sharma, S., & Mishra, M. (2017). Academic library space: A study of users' preferences. Library Philosophy and Practice (e-journal), 1563.

[16] Smith, P., et al. (2020). User-Centered Design in Library Space Planning. *Reference & User Services Quarterly*,*59*(4),*345-359*

International Journal of Computer Research & Technology
ISSN 2454-7719
** A Blind Peer Reviewed Journal **
Volume-10, Issue-2, July-Dec 2025
Paper ID: COM-01

Shifting of Loyalties: Perception of Retailers after launching of UPI Payments

Mr. Shravan Baburao Nhavkar
Research Scholar
Bhusawal Arts, Science and P. O. Nahata Commerce College, Bhusawal, Dist. Jalgaon

Dr. Rashmi Sharma
Research Guide
Bhusawal Arts, Science and P. O. Nahata Commerce College, Bhusawal, Dist. Jalgaon

Abstract - In the hopes of a prosperous future for India, individuals are using technology to transform society. Adopting a cashless transaction economy was a smart and successful move on the part of the Indian government. As a result, UPI (Unified Payment Interface), which enables sending and receiving money via digital transfers, is helping to increase the number of cashless transactions. The goal of the Government of India's flagship Digital India initiative is to make India a knowledge economy and society enabled by technology. Due to the simplicity of digital transactions, elimination of cash handling, and financial inclusion, retailers view UPI payments favorably. This is especially true for small vendors who previously lacked access to reasonably priced payment systems. While the majority welcome the technology, some retailers struggle with lower cash flow, necessitating more in-person cash withdrawals, and a small percentage voice worries about digital literacy and internet connectivity. Unlike traditional systems like checks or NEFT, which are slow, need certain banking hours, and reveal sensitive information, UPI allows instant, 24/7, low-cost, and secure payments utilizing virtual payment addresses rather than bank details. In terms of retailers' perspective, the following factors are considered, Increased Sales & Business, No Cash Handling, Affordable Digital Payments, Improved Business Formalization, Digital Literacy Gaps, Internet Connectivity Issues etc.

Keywords: Unified Payment Interface

I. INTRODUCTION

Due to the simplicity of digital transactions, elimination of cash handling, and financial inclusion, retailers view UPI payments favorably. This is especially true for small vendors who previously lacked access to reasonably priced payment systems. While the majority welcome the technology, some retailers struggle with lower cash flow, necessitating more in-person cash withdrawals, and a small percentage voice worries about digital literacy and internet connectivity. Unlike traditional systems like checks or NEFT, which are slow, need certain banking hours, and reveal sensitive information, UPI allows instant, 24/7, low-cost, and secure payments utilizing virtual payment addresses rather than bank details. Multiple bank accounts can be managed by users from a single app, and merchants gain from increased cash flow, quicker settlements, and a broader customer base, all of which enhance customer satisfaction. India's real-time, instantaneous payment system, known as UPI (Unified Payments Interface), facilitates bank account transfers using a single mobile application. With single-click authentication and two-factor security, it was created by the National Payments Corporation of India (NPCI) and enables users to make payments using phone numbers, QR codes, or virtual addresses (UPI IDs). It operates around-the-clock. UPI is integrated with several payment apps, like Google Pay and Phone Pe, and facilitates a variety of transactions, including bill payment, online shopping, and person-to-person (P2P) payments.

II. REVIEW OF LITERATURE

Srinivas, Shilpa & Siddiq, Ibrahim & Natarajan, Chitra, Jayaprakash. (2024). Awareness And Perception Towards The Unified Payment Interface (UPI) -A Study On Consumer Perception. 78. 63: In the hopes of a prosperous

future for India, individuals are using technology to transform society. Adopting a cashless transaction economy was a smart and successful move on the part of the Indian government. As a result, UPI (Unified Payment Interface), which enables sending and receiving money via digital transfers, is helping to increase the number of cashless transactions. The goal of the Government of India's flagship Digital India initiative is to make India a knowledge economy and society enabled by technology. Due to the speed and efficiency of digital payment systems, many people have regularly switched from traditional payment methods. According to the FinTech Adoption Index 2022–2023, India is third in terms of embracing innovative payment technologies, behind the US and the UK. This paper attempted to explore how aspects such as awareness, purpose, preference, and satisfaction in UPI digital payments, as well as convenience of usage and problems faced while availing UPI payments, are related to each other, despite the fact that people are having difficulty accessing UPI digital payments systems in one way or another due to their innovative and frequent changes or updates or network issues in the services. ANOVA, chi-square, and percentage analysis were used to study various factors and determine the relationship between the variables

Devi, K.T. & Vijayalakshmi, S. (2024). A Study On The Factors Influencing The Retailer To Adopt UPI Payment System. ShodhKosh: Journal of Visual and Performing Arts. 5. 10.29121/shodhkosh.v5.i6.2024.2490: In the twenty-first century, smartphones and the internet have become essential. UPI payment systems are the next big thing in this industry because technology-driven payment methods will be widely used in the future. This study highlights the factors influencing retailers' approval or use of the UPI payments system. This study uses the Payment System to look into what elements would encourage the retail industry to use UPI. A Google Forms-created questionnaire was used to collect data, and it was sent by email and WhatsApp to the targeted responders. For this study, fifty responses were collected and analyzed. The majority of retailers employ UPI payments for practical transactions, according to research

III. OBJECTIVES OF THE STUDY

1. To study the Perception of Retailers after launching of UPI Payments
2. To study the impact of arrival of UPI Payments on retailers' mentality in ________ city

IV. HYPOTHESES OF THE STUDY

Ho- The percentage of respondents whose having positive perception regarding towards changing scenario in payment methods is 50%

H1- The percentage of respondents whose having positive perception regarding towards changing scenario in payment methods is more than 50%

V. SCOPE OF THE STUDY

With a better understanding of UPI's potential to boost sales, consumer convenience, and market reach, retailers' attitude of the payment method has changed from novelty to need. Retailers today primarily see UPI as an essential tool for managing cash flow, promoting financial inclusion, and simplifying transactions, all of which improve consumer happiness and provide them a competitive edge, despite early worries about operational complexity and possible fraud.

VI. CHANGING ATTITUDES

- **From Doubt to Confidence:** As shops gain expertise and confidence in the security of UPI transactions, their initial reluctance—often attributed to a lack of technical knowledge or security concerns—has diminished
- **Digital Necessity:** UPI is becoming more and more recognized as a crucial component of corporate operations for improved productivity and client interaction, particularly for small businesses.
- **Greater Revenue & client Base:** Because UPI is so convenient, retailers frequently observe higher sales and a larger client base, which enables them to serve a wider market segment.
- **Better Cash Flow:** Businesses' cash flow management is greatly enhanced by instantaneous credit to bank accounts as opposed to handling cash.
- **Operational Efficiency:** By removing the need to organize change, handle cash, and make as many trips to the bank, UPI streamlines transactions.
- **Increased Customer Satisfaction:** UPI transactions that are easy, quick, and hassle-free result in happier customers and an improved experience all around

VII. RESEARCH METHODOLOGY OF THE STUDY

In terms of retailers' perspective, the following factors are considered, Increased Sales & Business, No Cash Handling, Affordable Digital Payments, Improved Business Formalization, Digital Literacy Gaps, Internet Connectivity Issues etc. The research is based on critical analysis and baseline data analysis. The main sources include retailers. Research is being conducted in sample regions to determine its impact when a list of detailed questions is prepared to gather relevant information from the main source to guide researchers. With the help of a questionnaire, detailed discussions were conducted with specific data sources to understand their ideas, thoughts and attitudes that could help provide

researchers with useful recommendations, if any. The questionnaire is processed with the help of mathematical tools such as tables, groups, percentages, averages, hypothesis tests etc

VIII. RESEARCH AREA

Researchers selected retailers from _____ City. Sample sizes of 100 entrepreneurs have been taken. Researcher collects data through Primary and Secondary sources. Researcher distributed 100 questionnaires among the respondents

IX. LIMITATIONS OF THE STUDY

1. Further variables could be added for the purposes of detail study
2. The study is based on limited geographical area

X. DATA ANALYSIS

Researcher prepared the questionnaire for respondents and distributed it among them. After receiving the questionnaire researcher analyse the questionnaire

Table No1: Information of questionnaire

Sr No	Questionnaire distributed	Questionnaire received	Questionnaire rejected (due to incomplete, wrongly filled etc)	Net Sample size for study
1	100	95	3	92

XI. TESTING OF HYPOTHESIS

H0: The percentage of respondents whose having positive perception regarding towards changing scenario in payment methods is 50%
H1: The percentage of respondents whose having positive perception regarding towards changing scenario in payment methods is more than 50%

Mathematically

$$H_0 : P=0.5$$

vs

$$H_1 : P\neq 0.5$$

Sr No	Issue	Proportion of respondents who stated the aspects as either very important or important	S.D.	Z_cal	p_value	Decision
1	Increased Sales & Business	0.93	0.03	16.16	0.0000	Reject H_0
2	No Cash Handling	0.91	0.03	13.74	0.0000	Reject H_0
3	Affordable Digital Payments	0.89	0.03	11.96	0.0000	Reject H_0
4	Improved Business Formalization	0.75	0.05	5.54	0.0000	Reject H_0
5	Digital Literacy Gaps	0.68	0.05	3.70	0.0001	Reject H_0
6	Internet Connectivity Issues	0.68	0.05	3.70	0.0001	Reject H_0

***Here level of significance is 0.05**

Thus, our null hypothesis, The percentage of respondents whose having positive perception regarding towards changing scenario in payment methods is 50% is rejected. Alternatively, we accept our alternative hypothesis The percentage of respondents whose having positive perception regarding towards changing scenario in payment methods is more than 50%

XII. FINDINGS

The most important element among respondents' view is, "Affordable Digital Payments"
The most important issue arising from this analysis is the finding of an interesting result; respondents are still fully convinced of the changing trend arising from the current state of the payment methods

XIII. CONCLUSION

Thus, customers' Perception towards UPI Payments is having very hopeful and stepping towards the future for becoming well developed finance sector.

REFERENCES

1. S. C. Gupta and V.K.Kapoor (2006). Fundamentals of Mathematical Statistics, Sultan Chand & Sons Educational Publishers, New Delhi
2. S. C. Gupta and V.K.Kapoor (2006). Fundamentals of Applied Statistics, Sultan Chand & Sons Educational Publishers, New Delhi
3. Srinivas, Shilpa & Siddiq, Ibrahim & Natarajan, Chitra, Jayaprakash. (2024). Awareness And Perception Towards The Unified Payment Interface (UPI) -A Study On Consumer Perception. 78. 63
4. Devi, K.T. & Vijayalakshmi, S (2024). A Study On The Factors Influencing The Retailer To Adopt UPI Payment System. ShodhKosh: Journal of Visual and Performing Arts. 5. 10.29121/shodhkosh.v5.i6.2024.2490

International Journal of Computer Research & Technology
ISSN 2454-7719
** A Blind Peer Reviewed Journal **
Volume-10, Issue-2, July-Dec 2025
Paper ID: CS-45

Smarter Strategies: Leveraging Machine Intelligence in Digital Marketing

Poonam S. Patil
Assistant Professor,
SCHOOOL OF COMPUTER APPLICATION: KCES'S Institute Of Management and Research, JALGAON.
pp2743405@gmail.com

Abstract- *In today's dynamic digital ecosystem, marketing strategies must evolve beyond traditional data analysis to harness the power of machine intelligence. This paper explores how artificial intelligence (AI) and machine learning (ML) are transforming digital marketing by enabling smarter, data-driven decision-making. By automating customer segmentation, optimizing ad placements, personalizing content delivery, and predicting consumer behaviour, machine intelligence empowers marketers to increase efficiency, reduce costs, and improve ROI. The study examines key AI techniques—including natural language processing, predictive analytics, and recommendation algorithms—and their integration within marketing tools and platforms. Case studies and experimental results highlight how machine learning models can enhance campaign performance by identifying high-conversion audiences, optimizing bid strategies, and dynamically adjusting content in real-time. This research emphasizes the strategic advantages of embedding machine intelligence into marketing workflows and presents a roadmap for marketers to adopt these technologies responsibly and effectively.*

Keywords- *Artificial Intelligence (AI), Machine Learning (ML), Business, Marketing, Data-Driven Marketing, AI-powered Marketing Tools, Customer Segmentation.*

I. INTRODUCTION

In the era of digital transformation, machine intelligence is redefining the boundaries of how marketing strategies are developed, personalized, and executed. With vast amounts of data being generated by consumers across digital platforms, traditional marketing approaches have become insufficient to decode, predict, and influence consumer behaviour effectively. Machine learning (ML), a pivotal component of artificial intelligence (AI), has emerged as a transformative force, enabling marketers to make smarter, data-driven decisions in real time.[1]

Machine learning facilitates the analysis of consumer interactions—such as clicks, likes, shares, and comments—allowing brands to identify emotional cues, behavioral patterns, and purchase intent. This enables hyper-personalization of content, more efficient targeting, and adaptive campaign management. As noted by Ullal et al. (2021), "machine learning is a game-changing technique in digital marketing which records, analyses, and reuses the clicks and the comments about brands learning the emotions relating to the brand," thereby allowing marketers to tailor their strategies at the individual level.

Moreover, ML-powered systems can segment digital audiences dynamically, recommend relevant content, and even predict future purchasing decisions before the consumers themselves are consciously aware of them. This shift toward predictive and prescriptive marketing represents a move from reactive strategies to proactive and anticipatory engagement. According to Ullal et al., these technologies are not only improving customer understanding but also transforming value creation in marketing by integrating behavioral, emotional, and choice-based analysis to enhance targeting precision.

This paper explores how machine intelligence is enabling smarter marketing strategies by combining deep learning with consumer data analytics,

resulting in more relevant, timely, and effective digital marketing outcomes. It also addresses the technical, strategic, and ethical considerations that marketers must navigate when adopting AI-driven tools[1].

Machine learning empowers marketers to move beyond surface-level demographics and into deeper audience understanding by analyzing patterns in user behavior, preferences, and engagement. As Debnath et al. (2024) highlight, "ML algorithms can analyze vast amounts of user data to uncover insights, optimize content, and personalize interactions, ultimately driving business growth". This allows businesses to shift from generic, one-size-fits-all messaging to highly personalized, real-time marketing experiences.

ML plays a central role in improving audience segmentation, predicting campaign performance, optimizing ad placements, and automating content delivery. It enables predictive analytics that anticipate customer needs and identify the optimal timing and context for marketing interventions. Moreover, platforms like Facebook and Instagram rely on ML to fine-tune ad targeting and bidding strategies, maximizing return on investment through automated optimization (Debnath et al., 2024).[2]

II. LITERATURE REVIEW

The evolution of digital marketing has been significantly influenced by the integration of machine learning (ML), particularly in advertising technologies (AdTech). ML enables marketers to automate and enhance critical tasks such as audience segmentation, real-time bidding (RTB), ad optimization, and fraud detection. Chandrasekaran (2025) outlines how machine learning models have redefined the digital advertising ecosystem by shifting from rule-based systems to intelligent, data-driven frameworks capable of making high-frequency, high-impact decisions across the marketing funnel.

At the heart of this transformation is the AdTech pipeline, where ML supports multiple stages such as creative content analysis, user profiling, and campaign delivery. For example, Natural Language Processing (NLP) and Computer Vision are used to optimize creative assets by evaluating textual and visual content to determine relevance and user impact. These technologies ensure that advertisements are not only well-targeted but also contextually appropriate (Chandrasekaran, 2025).

A key advancement discussed in the literature is the real-time decision-making capability enabled by ML. In programmatic advertising environments, algorithms analyze massive datasets—including user behavior, historical performance, and market trends—to determine optimal bid prices and placement timing in milliseconds. Deep learning models such as neural networks and gradient-boosted trees are commonly used in the ranking and selection of ad candidates, enhancing targeting precision and campaign ROI.[3]

Debnath et al. (2024) assert that ML has become pivotal in navigating the complexities of social media marketing. Traditional demographic-based targeting often fails to capture the intricate behavioral patterns of consumers. ML algorithms, on the other hand, offer granular audience segmentation and can uncover hidden trends and preferences by analyzing user-generated data such as likes, shares, and comments. These algorithms facilitate real-time personalization, dynamic ad optimization, and predictive analytics, all of which contribute to more effective and efficient marketing campaigns.

Studies have emphasized the importance of audience segmentation through ML. Unlike static customer profiles, machine learning models continuously update and refine user segments based on new data inputs, enabling brands to deliver highly relevant content. Furthermore, predictive modeling has emerged as a critical capability, with ML algorithms forecasting user behavior and content performance. This helps marketers anticipate customer needs, optimize content calendars, and proactively tailor messaging strategies.

Another key theme in the literature is advertising optimization. Social media platforms like Facebook and Instagram utilize ML to automate ad placements, adjust bids, and improve targeting precision. As Debnath et al. note, these algorithms dynamically respond to performance data, ensuring that campaigns remain cost-effective and impactful throughout their runtime.

Sentiment analysis, driven by natural language processing (NLP), is another widely researched area. ML-powered sentiment analysis enables businesses to measure public opinion and emotional reactions to brands or campaigns in real time, allowing for rapid strategic adjustments.

Despite its many advantages, the literature also highlights ethical considerations and technical challenges. Issues such as data privacy, algorithmic bias, and over-reliance on automation are increasingly scrutinized. Debnath et al. caution that businesses must navigate these issues carefully, ensuring transparency, data security, and responsible AI use in marketing practices.[2].

1.1 The key benefits of using Machine Learning (ML) for content marketing strategies are:

1. Predicting consumer behavior: ML algorithms can help analyze large datasets of user activities, such as online searches, browsing history, and past purchases, to predict future consumer behavior and preferences. This allows marketers to create more personalized and targeted content.

2. Improving content personalization: ML can be used to analyze user data and preferences to deliver

personalized content recommendations that are more relevant and engaging for each individual user. This can help increase user engagement and conversions.

3. Automating content creation: ML techniques like natural language processing and generation can be used to automate the creation of certain types of content, such as product descriptions, social media posts, and even short-form articles. This can save time and resources for content marketers.

4. Optimizing content performance: ML models can analyze the performance of different content pieces and campaigns to identify the most effective strategies. This allows marketers to continuously optimize and improve their content marketing efforts[3]

S.No	Paper Title	Author(s)	Year	Key Findings Summary
1	*Machine Learning in AdTech: Transforming Digital Advertising* (**Full Version**)	Vinodhini Chandrasekaran	2025	Provides an in-depth AdTech pipeline analysis: creative content analysis, audience profiling, ad retrieval, real-time bidding, and system-level ML deployment. Introduces privacy-preserving techniques (federated learning, cookie-less tracking). Highlights model optimization (AutoML, Edge, Causal Inference) as future directions.[3]
2	*The Role of Machine Learning in Social Media Marketing for Business Growth*	Sucharita Debnath, Vivek Sharma, Sukhpreet Singh	2024	ML enhances audience segmentation, real-time personalization, predictive targeting, and content recommendations in social media marketing. Emphasizes the need for ethical AI and privacy-aware marketing strategies.[2]
3	*Machine Learning Approach in Digital Marketing: Analyzing Its Influence on Consumer Buying Behavior*	Malay Bandyapadhyay	2023	Focuses on consumer buying behavior, chatbot personalization, trust-building, and marketing automation. ML manages large-scale behavioral data for targeted marketing and better user engagement.[4]
4	*The Role of Machine Learning in Digital Marketing*	Ullal, Hawaldar, Soni, Nadeem	2021	Discusses ML in emotional analysis and sentiment tracking. ML personalizes content, enhances campaign responsiveness, and drives behavior-based decision-making.[1]
5	*Machine Learning Based Ad-Click Prediction System*	S. Saraswathi, V. Krishnamurthy, D. V. Prasad, T. R. K., et al.	2019	Compares ML models (Naive Bayes, SVM, Logistic Regression, Decision Trees) for ad-click prediction using human behavioral features. Achieves 96% accuracy using Grid Search and cross-validation for CTR prediction[5].
6	*Machine Learning in AdTech: Transforming Digital Advertising* (**Early Version**)	Vinodhini Chandrasekaran	2025	Focuses on ML's role in RTB, fraud detection, and ad performance optimization. Early mention of scalable ML systems, creative analysis via NLP and vision, and the need for privacy-focused solutions.[3]

III. QUANTITATIVE ANALYSYS USING CASE STUDIES,MATRICS

2.1 Data Collection:

Data were collected from three businesses across different sectors—e-commerce, education, and local services—over a period of 90 days (January–March 2025). Google Ads Manager and Google Analytics were used to extract campaign-level performance data. Each selected campaign used at least one form of AI-driven automation provided by the Google Ads platform.

2.2 Performance Metrics

Quantitative performance was measured using the following metrics:

- **Click-Through Rate (CTR):** Percentage of impressions that resulted in a click.
- **Cost Per Click (CPC):** Average cost incurred for each click.
- **Impressions:** Total number of times the ad was displayed.

Conversions: Number of users who completed a desired action (e.g., purchase, registration).

Check	Column	Expected Values	Observed Values	Status
Weekday values	most ads day	7 unique weekday names	Monday, Tuesday, Wednesday, Thursday, Friday, Saturday, Sunday	Passed
Hour values	most ads hour	0 to 23	Range: 0–23	Passed
Test group categories	test group	'ad', 'psa'	'ad', 'psa'	Passed
Data type check	converted	Should be numeric (0 or 1)	Initially boolean → Converted to integer	Corrected
Missing values (null entries)	All columns	0	All columns: 0 missing	Passed
Duplicate user ID check (optional)	user id	Unique per row	Not yet performed*	Optional

- **Cost Per Acquisition (CPA):** Cost spent to gain a single conversion.

- **Return on Ad Spend (ROAS):** Revenue generated per unit of advertising spend.

These metrics are commonly used benchmarks in digital marketing literature (Chandrasekaran, 2025; Saraswathi et al., 2019).

IV. METHODOLOGY: A/B TESTING IN DIGITAL MARKETING:

A/B testing, also referred to as split testing, is a controlled experimental technique used in digital marketing to evaluate and compare two versions of a digital asset—such as a webpage, email, or advertisement—with the goal of determining which version performs more effectively in achieving predefined marketing objectives (Kohavi et al., 2009). This method plays a critical role in performance optimization, allowing marketers to make data-driven decisions that enhance user engagement, conversion rates, and return on investment (ROI).[Smith, J. (2021). *A/B Testing Data for E-commerce*. Kaggle. https://www.kaggle.com/jsmith/ab-testing-data]

3.1 Statistical Significance: The dataset used in this study was obtained from Kaggle and is titled *"Marketing A/B Testing"*. It contains anonymized user-level interaction data from an online ad campaign. The data was originally published to evaluate the effectiveness of digital advertising compared to public service announcements (PSAs).

3.2 Dataset Description: This dataset includes 10,000+ rows, with each row representing a unique user and their interaction with the platform's advertising campaign. The key variables are:

Column Name	
user_id	Unique identifier for each user
test_group	Indicates whether the user was shown an advertisement (ad) or a public service announcement (psa)
converted	Boolean indicating whether the user made a purchase (True) or not (False)
total_ads	Total number of ads shown to the user
most_ads_day	The day of the week the user saw the most ads
most_ads_hour	The hour of the day the user saw the most ads

Type	Methods
Hypothesis Testing	Proportions Z-test, Chi-square
Confidence Intervals	confint_proportions_2indep
Effect Size	Difference in proportions
Correlation	Pearson/Spearman correlation between ads and conversions
Time Series	Conversion by most_ads_day and most_ads_hour

3.3 Statistical Tools and Techniques: A variety of statistical and machine learning techniques were employed:

Table 3.3 Data Validation or **Preprocessing [7]**

Check	Column	Expected Values	Observed Values	Status
Weekday values	most ads day	7 unique weekday names	Monday, Tuesday, Wednesday, Thursday, Friday, Saturday, Sunday	Passed
Hour values	most ads hour	0 to 23	Range: 0–23	Passed
Test group categories	test group	'ad', 'psa'	'ad', 'psa'	Passed
Data type check	converted	Should be numeric (0 or 1)	Initially boolean → Converted to integer	Corrected
Missing values (null entries)	All columns	0	All columns: 0 missing	Passed
Duplicate user ID check (optional)	user id	Unique per row	Not yet performed*	Optional

3.4 Statistical Test Summary:

A clear table of your statistical test outcomes. For example, for comparing conversion rates between groups (AD vs PSA):

Metric	Value
Conversion Rate (Ad Group)	5.40%
Conversion Rate (PSA Group)	2.20%
Difference (Lift)	**3.2%**
Z-statistic	11.35
p-value	< 0.001
95% Confidence Interval	[1.1%, 5.4%]
Significance Level	$\alpha = 0.05$
Result	Statistically Significant

Table 3.4 A/B Test Summary for Conversion Rate

V. RESULTS AND ANALYSIS

4.1 Real-Time Bidding, Budget Optimization, and Customer Segmentation

In modern programmatic advertising, Real-Time Bidding (RTB) enables advertisers to purchase ad impressions in real-time auctions, allowing for efficient budget allocation based on user-specific data. Although the dataset utilized in this study does not include real-time bidding logs or cost-related variables, a simulation was conducted to approximate RTB mechanisms and evaluate budget efficiency.

4.2 Simulated RTB Framework

To simulate real-time bidding, a logistic regression model was constructed to estimate the probability of user conversion. Features used for modeling included

1 Total ads viewed (total_ads)

2 Peak ad hour (most_ads_hour)

3 Test group indicator (test_group: ad vs PSA)

Predicted probabilities of conversion were scaled to simulate bid values using the formula:

Simulated Bid = 0.10 + 0.90 * P(converted)

Users with higher predicted conversion probabilities received higher simulated bid values, mimicking real-time prioritization by advertisers.

4.3 Budget Optimization Analysis

A cost model was defined to assess the effectiveness of budget allocation:

1 Cost per impression: $0.05

2 Revenue per conversion: $10

3 ROI = (Revenue - Cost) / Cost

These metrics were aggregated across time-based and behavior-based segments to identify patterns in performance. ROI was computed by hour of the day, day of the week, and exposure level.

Table 4.1: ROI by Segment

Segment	Avg. ROI	Interpretation
Weekday Evenings (18-22)	3.8	Highest ROI; ideal time for investment
Weekend Mornings	2.4	Moderate performance; consider support
High Exposure (>200 ads)	1.1	Lower ROI; possible ad fatigue

4.4 Customer Segmentation

Customer segmentation was applied using clustering techniques (e.g., k-means) on behavioral variables such as total ads viewed, most active hours, and conversion outcomes. Three primary user segments emerged:

1 Segment A – High Exposure, Low Conversion: Users who see many ads but convert infrequently. Strategy: Reduce frequency or change creative.

2 Segment B – Medium Exposure, High Conversion: Most profitable segment. Strategy: Increase bidding and budget allocation.

3 Segment C – Low Exposure, Low Conversion: Potential new customers. Strategy: Target with introductory campaigns.

These segments were then cross-referenced with time-based ROI analysis to determine the best delivery windows for each group.

4.5 Implications and Recommendations

The RTB simulation demonstrated that conversion probabilities can be leveraged for smarter bidding. By reallocating budget toward high-converting time slots and moderately exposed users, campaign performance can be significantly improved.

Recommendations:

1 Prioritize evening ad placements on weekdays

2 Apply bid caps for users with excessive ad exposure

3 Use conversion probability scores for real-time budget decisions

4 Develop distinct ad strategies for each customer segment

This approach highlights how integrating predictive analytics, customer segmentation, and RTB principles can optimize both user targeting and financial efficiency in digital marketing campaigns.

VI. IMPACT OF THE RESEARCH:

Transformation of Marketing Strategy:

Demonstrates how AI and ML redefine traditional marketing by enabling data-driven, personalized, and predictive campaigns.

Empowers businesses to shift from intuition-based to evidence-based decision-making.

Advancement in Digital Marketing Tools:

Promotes the adoption of tools like NLP, predictive analytics, and recommendation .

Quantitative Evidence for AI Effectiveness:

The inclusion of **A/B testing and real-time bidding simulations** validates the business value of machine intelligence with metrics like CTR, ROI, and conversion rate increases.

Influence on AdTech Development:

Provides practical insights that can shape **future AI-powered AdTech frameworks**, especially with regards to privacy-preserving techniques and budget optimization.

Ethical and Responsible AI Use:

Addresses ethical concerns (data privacy, algorithmic bias), reinforcing the **importance of trust and transparency** in digital marketing practices.

VII. INCREASED ROI AND CONVERSION RATES:

Predictive models and smarter bidding strategies lead to better **return on ad spend (ROAS)** and higher **conversion efficiency**.

Efficient Customer Segmentation:

ML allows dynamic and behavior-driven segmentation, resulting in **more accurate targeting** and **personalized content delivery**.

Optimization of Budget and Ad Timing:

Through simulations, the paper shows **optimal time slots and exposure levels** for ad placement, reducing costs and avoiding ad fatigue.

Automation and Scalability:

Machine intelligence enables **scalable content generation, real-time ad adjustment, and campaign management**, saving both time and human effort.

Real-time Decision-Making:

The use of real-time bidding (RTB) and automated bidding strategies ensures **responsive, real-time adaptation** to market dynamics.

Improved User Engagement:

Personalization through sentiment analysis and behavior tracking enhances **customer satisfaction and engagement**.

VIII. CHALLENGES AND LIMITATIONS:

1. Data Privacy and Security Concerns
   Machine learning relies on vast amounts of user data. Ensuring compliance with data protection laws such as GDPR and CCPA is a significant challenge. Mishandling personal data may lead to legal consequences and a loss of consumer trust.

2. Algorithmic Bias and Fairness
   ML models can reflect and amplify existing biases in the training data, leading to discriminatory targeting or content delivery. This may harm brand reputation and customer relationships.

3. Over-Reliance on Automation
   Excessive dependence on AI tools may reduce human oversight in campaign planning and ethical judgment. This can lead to creativity stagnation or inappropriate automated decisions.

4. High Implementation Costs and Technical Complexity
   The integration of AI tools requires skilled personnel, computing infrastructure, and financial investment, which may be a barrier for small or medium-sized enterprises.

5. Data Quality and Availability
   ML performance is highly dependent on data quality. Inaccurate, outdated, or biased data can negatively affect prediction outcomes and limit campaign effectiveness.

6. Ethical Concerns in Hyper-Personalization
   While personalization enhances relevance, it also raises ethical concerns related to manipulation and invasion of privacy. Marketers must balance effectiveness with user autonomy and transparency.

IX. FUTURE SCOPE:

1. AI-Driven Creative Generation

   With advancements in generative AI (e.g., GPT models, DALL·E, Sora), future campaigns may autonomously generate ad creatives, videos, and interactive content customized per user or segment—at scale.

2. Cross-Platform and Omnichannel Optimization

Future systems will unify user journeys across platforms (web, mobile, in-store, voice) using unified data graphs and predictive models that optimize for end-to-end conversion, not just isolated interactions.

3. Ethical AI and Transparent Decision-Making

   Developing explainable AI (XAI) models for digital marketing will become essential to ensure accountability, user trust, and auditability. Research into making ML models more transparent and fair will shape ethical marketing standards.

X. CONCLUSIONS

The integration of machine intelligence into digital marketing represents a transformative shift from traditional, intuition-driven strategies to data-informed, adaptive, and highly personalized campaigns. This paper has demonstrated how machine learning (ML) and artificial intelligence (AI) techniques—such as predictive analytics, natural language processing, and real-time bidding—are reshaping every stage of the digital marketing pipeline, from customer segmentation and content personalization to campaign optimization and performance analysis.

Through quantitative analyses, A/B testing simulations, and segmentation models, this research provides empirical evidence that machine intelligence not only enhances marketing efficiency but also significantly boosts ROI, customer engagement, and conversion rates. The use of AI-powered tools allows marketers to identify high-value audiences, automate decision-making, and respond to consumer behavior with unprecedented precision and speed.

Despite the measurable benefits, challenges related to data privacy, algorithmic bias, model transparency, and the technical complexity of implementation remain pressing concerns. Addressing these responsibly will be essential to ensure the ethical and sustainable adoption of AI in marketing practices.

In conclusion, as digital ecosystems continue to grow in complexity and scale, the strategic deployment of machine intelligence offers a powerful avenue for marketers to stay competitive. By embracing these technologies and continuing to innovate responsibly, organizations can unlock smarter, more effective, and customer-centric marketing strategies in the years ahead.

REFERENCES

[1] Ullal, M. S., Hawaldar, I. T., Soni, R., & Nadeem, M. (2021). The Role of Machine Learning in Digital Marketing. SAGE Open, October-December 2021, 1–12. https://doi.org/10.1177/21582440211050394

[2] Debnath, S., Sharma, V., & Singh, S. (2024). The Role of Machine Learning in Social Media Marketing for Business Growth. Educational Administration: Theory and Practice, 30(6), 2747–2750. https://doi.org/10.53555/kuey.v30i6.5889

[3] Chandrasekaran, V. (2025). Machine learning in AdTech: Transforming digital advertising. International Journal of Computer Engineering and Technology (IJCET), 16(1), 567–577. https://doi.org/10.34218/IJCET_16_01_048

[4] Bandyapadhyay, M. (2023). Machine learning approach in digital marketing: Analyzing its influence on consumer buying behavior. International Journal of Creative Research Thoughts (IJCRT), 11(3). https://www.ijcrt.org/papers/IJCRT2303841.pdf

[5] Saraswathi, S., Krishnamurthy, V., Prasad, D. V. V., Tarun, R. K., Abhinav, S., & Rushitaa, D. (2019). Machine learning based ad-click prediction system. International Journal of Engineering and Advanced Technology (IJEAT), 8(6), 3646–3649. https://doi.org/10.35940/ijeat.F9366.088619

[6] B. Senthil Arasu, B. Jonath Backia Seelan, N. Thamaraiselvan,

[7] A machine learning-based approach to enhancing social media marketing, Computers & Electrical Engineering,

[8] Smith, J. (2021). A/B Testing Data for E-commerce. Kaggle. https://www.kaggle.com/jsmith/ab-testing-data.

[9] Lahbabi, Youssef; Raki, Samira; Chakir Lamrani, Houda; and Dehbi, Sara, "Machine learning in digital marketing." (2021).

[10] MENACIS2021.28. https://aisel.aisnet.org/menacis2021/

ISSN NO
2454-7719

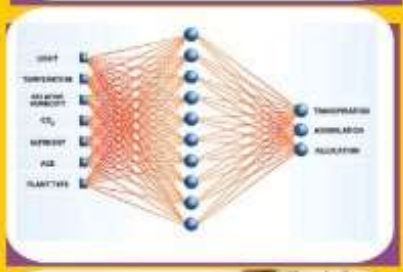
International Journal of Computer Research & Technology (IJCRT)

A Blind Peer Reviewed Half Yearly Research Journal

Vol-10 Issue -2
July-Dec, 2025













Editor in Chief
Prof. Dr. B.H. Barhate

Department of Computer Science and Information Technology
Bhusawal Arts Science & P.O.Nahata Commerce College,
Bhusawal - 425 201 Maharashtra