Role of Ai in Detecting Financial Frauds in Digital Banking

[1]Aditya Dhiman, [2]Dr. Ritu Bharti
[1]Student, Quantum University, Roorkee, Uttarakhand
[2]Associate Professor, QSB, Quantum University, Roorkee, Uttarakhand
doi.org/10.64643/JATIRV2I6-140458-001

***Abstract*—In 2025, the rapid expansion of digital banking has significantly transformed the financial sector by providing fast, convenient, and accessible financial services. However, this digital transformation has also led to a sharp rise in financial frauds such as phishing, identity theft, credit card fraud, and unauthorized transactions. Traditional rule-based fraud detection systems have proven inadequate in dealing with the increasing complexity and sophistication of cyber threats.**

Artificial Intelligence (AI) has emerged as an advanced and effective solution for detecting and preventing financial fraud in digital banking. By utilizing machine learning, deep learning, and predictive analytics, AI enables real-time transaction monitoring, anomaly detection, and risk assessment. AI systems can process vast amounts of data, identify hidden patterns, and detect suspicious activities with greater accuracy and speed compared to conventional methods.

This study focuses on the role of AI in enhancing fraud detection mechanisms in digital banking. It highlights the key techniques, benefits, and challenges associated with AI implementation. While issues such as data privacy, high costs, and model transparency remain concerns, AI continues to play a crucial role in strengthening banking security and ensuring safer digital financial transactions.

***Index Terms*—Artificial Intelligence (AI), Digital Banking, Financial Fraud Detection, Machine Learning, Cyber Fraud, Anomaly Detection, Predictive Analytics, Banking Security, Fraud Prevention, Deep Learning**

I. INTRODUCTION

The digital banking sector has witnessed remarkable growth over the past few years, particularly from 2020 to 2026, driven by technological advancements, increased internet penetration, and the widespread use of smartphones. In 2020, the COVID-19 pandemic acted as a major catalyst for digital transformation, as lockdowns and social distancing measures forced customers to shift

from traditional banking methods to digital platforms such as mobile banking, internet banking, and digital payment systems.

In 2020, digital payment adoption in India increased significantly, with platforms like UPI recording over 2 billion transactions per month. However, this rapid adoption also led to a rise in cyber fraud cases, including phishing attacks and OTP scams. Moving into 2021, digital banking usage continued to grow, with UPI transactions crossing 4 billion per month, while fraud cases also increased due to lack of user awareness and weak cybersecurity practices.

By 2022, the digital banking ecosystem became more mature, with enhanced security measures implemented by banks and regulatory authorities. Despite this, financial frauds became more sophisticated, involving techniques such as social engineering, SIM swap fraud, and fake banking apps. During this period, fraud cases in digital payments showed a steady increase, highlighting the limitations of traditional rule-based fraud detection systems.

In 2023, banks began integrating Artificial Intelligence (AI) and machine learning technologies more actively to combat fraud. AI-based systems enabled real-time transaction monitoring, anomaly detection, and predictive analysis. UPI transactions surged beyond 8 billion per month, reflecting the growing dependence on digital payment systems.

The year 2024 marked a significant shift toward AI-driven fraud detection mechanisms. Financial institutions increasingly relied on AI to analyze customer behavior, detect unusual transaction patterns, and prevent unauthorized access. Reports indicated that AI adoption helped reduce fraud detection time by nearly 30–40%, although challenges such as false positives and data privacy concerns persisted.

In 2025, the digital banking landscape has become highly advanced, with widespread adoption of AI technologies. As mentioned earlier, digital banking provides fast, convenient, and secure services; however, financial frauds such as phishing, identity theft, and credit card fraud have also increased. AI plays a crucial role in analyzing large volumes of transaction data in real time, identifying suspicious activities, and improving detection accuracy through continuous learning.

Looking ahead to 2026, the future of digital banking is expected to be even more secure and intelligent, with the integration of advanced AI technologies such as deep learning, behavioral biometrics, and Explainable AI (XAI). These technologies will not only enhance fraud detection but also improve transparency and trust in AI systems. It is expected that AI-driven systems will become the backbone of fraud prevention strategies in digital banking, significantly reducing financial losses and cyber threats.

II. LITERATURE REVIEW

The literature on financial fraud detection has evolved significantly with the advancement of Artificial Intelligence (AI) and machine learning technologies. Researchers have extensively studied the limitations of traditional fraud detection systems and emphasized the importance of intelligent, data-driven approaches.

Early studies on fraud detection primarily relied on rule-based systems and manual verification processes. These methods were found to be time-consuming, costly, and inefficient in detecting complex fraud patterns. According to a systematic review published in 2022, traditional methods lack accuracy and are not suitable for handling large volumes of financial data, leading to increased fraud risks in the banking sector .

With the emergence of AI, researchers have focused on machine learning (ML) techniques for fraud detection. The 2022 systematic literature review by Abdulalem Ali et al. analyzed 93 research papers and found that algorithms such as Support Vector Machines (SVM) and Artificial Neural Networks (ANN) are widely used for detecting financial fraud, particularly in credit card transactions . These models improve detection accuracy by learning patterns from historical transaction data.

Further advancements were observed in studies conducted between 2023 and 2025, where researchers emphasized the use of supervised and unsupervised learning models. A 2025 systematic review of 118 studies highlighted that supervised learning techniques like decision trees and logistic regression remain dominant due to their interpretability, while unsupervised anomaly detection methods are increasingly used to detect unknown fraud patterns . This shift reflects the need to identify new and evolving fraud techniques that do not follow predefined patterns.

In addition to traditional ML models, recent research has explored the use of deep learning techniques. Studies indicate that deep learning models, such as Recurrent Neural Networks (RNNs) and Convolutional Neural Networks (CNNs), are highly effective in analyzing sequential transaction data and detecting complex fraud patterns. However, these models face challenges related to interpretability and real-time implementation .

A 2024 study on AI-based fraud detection emphasized that AI systems outperform conventional methods by enabling real-time monitoring, predictive analysis, and behavioral pattern recognition. The study also highlighted that AI reduces false positives and enhances operational efficiency, making it a preferred solution for modern banking systems .

More recent research in 2026 has further strengthened the role of AI in fraud detection. A comprehensive review published in 2026 analyzed AI-based fraud detection systems developed between 2015 and 2025 and concluded that AI has become a core tool in financial fraud detection. The study identified key challenges such as data imbalance, lack of labeled datasets, and the trade-off between accuracy and interpretability, which continue to influence research in this field .

Another important area of research focuses on Explainable AI (XAI), which aims to make AI decisions more transparent and understandable. A 2025 study on deep learning in banking fraud detection emphasized that while AI models are highly accurate, their “black-box” nature can create trust issues, making explainability a critical factor in real-world applications .

Furthermore, recent literature highlights the growing complexity of fraud due to technologies like deepfakes and identity fraud. Studies in 2025 indicate that AI is not only used for fraud

detection but is also being exploited by fraudsters, increasing the need for more advanced and adaptive AI systems.

Overall, the literature clearly shows a transition from traditional fraud detection methods to AI-driven intelligent systems. Machine learning, deep learning, and hybrid models have significantly improved fraud detection accuracy and efficiency. However, challenges such as data privacy, model transparency, and evolving fraud techniques remain key areas for future research.

III. OBJECTIVES OF THE STUDY

1. To analyze the role of Artificial Intelligence (AI) in detecting and preventing financial frauds in digital banking.
2. To evaluate the effectiveness of AI techniques (such as machine learning and predictive analytics) in improving fraud detection accuracy and reducing financial risks.

IV. RESEARCH METHODOLOGY

The present study adopts a systematic and analytical approach to examine the role of Artificial Intelligence in detecting financial frauds in digital banking during the period from 2020 to 2026. This time frame is particularly significant as it captures the rapid transformation of the digital banking ecosystem, especially after the COVID-19 pandemic, which accelerated the adoption of online financial services. The research is descriptive as well as analytical in nature, focusing on understanding trends, patterns, and the effectiveness of AI in fraud detection across these years.

The study is based on both primary and secondary data. Primary data has been collected through a structured questionnaire administered to respondents who actively use digital banking services such as mobile banking, internet banking, and UPI-based transactions. The survey captures user experiences related to digital transactions, exposure to fraud, awareness of AI technologies, and trust in AI-based fraud detection systems. Secondary data has been collected from research journals, banking reports, and digital payment statistics to provide a broader perspective on the growth of digital banking and fraud trends between 2020 and 2026.

The period from 2020 onwards marks a significant shift in digital financial behavior. In 2020, digital transactions increased sharply due to pandemic-related restrictions, with UPI transactions crossing billions annually. This growth continued in 2021 and 2022, where digital payments expanded rapidly, supported by government initiatives and increased smartphone penetration. However, this expansion also led to a rise in financial fraud cases such as phishing and OTP scams. By 2023 and 2024, digital payment systems became more deeply integrated into daily life, with UPI emerging as the dominant mode of payment, accounting for a major share of retail digital transactions. During this period, fraud techniques also became more advanced, requiring more sophisticated detection systems.

By 2025, digital banking reached a highly advanced stage, with transactions reaching unprecedented levels. For instance, UPI recorded over 228 billion transactions in 2025, reflecting

massive adoption across the country . The trend continued into 2026, where UPI alone processed 22.64 billion transactions in March 2026, indicating the scale and speed of digital financial activities . Such exponential growth in transaction volume has made traditional fraud detection methods inadequate, as they are unable to process large datasets in real time or identify complex fraud patterns.

Overall, the research methodology combines empirical data with real-world digital payment trends from 2020 to 2026 to provide a comprehensive understanding of how Artificial Intelligence contributes to fraud detection in digital banking. The integration of primary survey data with secondary statistical evidence strengthens the reliability and relevance of the study.

V. ROLE OF AI IN FINANCIAL FRAUDS IN DIGITAL BANKING

1. Real-Time Transaction Monitoring and Fraud Detection

Real-time transaction monitoring is one of the most important roles of Artificial Intelligence (AI) in detecting financial fraud in digital banking. In modern banking systems, millions of transactions are processed every second through platforms such as mobile banking, internet banking, and UPI. Monitoring such a massive volume of data manually or through traditional rule-based systems is not only difficult but also inefficient. This is where AI plays a transformative role.

AI-powered systems continuously track and analyze every transaction as it occurs. These systems use advanced machine learning algorithms to evaluate multiple factors simultaneously, such as transaction amount, location, time, device information, frequency of transactions, and user behavior patterns. Based on this analysis, AI can instantly determine whether a transaction is normal or suspicious.

For example, if a customer usually makes small transactions within a specific city and suddenly a large transaction is initiated from a different country, the AI system immediately identifies this as unusual behavior. It can then take instant action, such as blocking the transaction, sending an alert to the user, or asking for additional verification like OTP or biometric authentication. This rapid response helps in preventing fraud before any financial loss occurs.

Another key advantage of real-time monitoring is speed and accuracy. Traditional systems often detect fraud after the transaction is completed, which makes recovery difficult. In contrast, AI systems work in real time, reducing the chances of successful fraud. They also minimize false positives by learning from past transaction data and continuously improving their decision-making process.

2. Anomaly Detection and Pattern Recognition

Anomaly detection and pattern recognition is a core function of Artificial Intelligence (AI) in identifying financial fraud in digital banking. Unlike traditional systems that depend on fixed rules, AI systems learn from historical data and continuously analyze user behavior to establish a

"normal pattern" for each customer. This includes transaction habits such as average spending amount, preferred transaction time, location, device usage, and frequency of transactions.

Once these patterns are established, AI algorithms—especially machine learning models—continuously compare real-time transactions with past behavior. If any deviation or unusual activity is detected, the system flags it as a potential fraud. For instance, if a user typically performs small daily transactions within a local area and suddenly initiates a high-value transaction from a different state or country, the system identifies this as an anomaly.

Pattern recognition further strengthens fraud detection by identifying hidden relationships and trends within large datasets. AI can detect complex fraud patterns that may not be visible to human analysts or traditional systems. For example, it can identify coordinated fraud activities such as multiple accounts making similar transactions within a short time frame, which may indicate organized fraud attempts.

Another advantage of AI-based anomaly detection is its ability to handle unknown or new fraud types. Since fraudsters constantly change their methods, predefined rules often fail to detect new fraud patterns. AI overcomes this limitation by using unsupervised learning techniques that do not rely on prior fraud examples. Instead, they focus on identifying deviations from normal behavior, making the system more adaptive and intelligent.

Additionally, AI reduces false positives by refining its understanding of user behavior over time. This ensures that genuine transactions are not unnecessarily blocked, improving customer experience while maintaining security. The system becomes more accurate as it learns from each transaction and feedback.

3. Predictive Analytics and Risk Assessment

Predictive analytics and risk assessment represent a proactive role of Artificial Intelligence (AI) in detecting and preventing financial fraud in digital banking. Unlike traditional systems that react after fraud has occurred, AI uses historical data and advanced algorithms to predict the likelihood of fraudulent activity before it actually happens. This forward-looking approach significantly reduces financial losses and strengthens banking security.

AI systems analyze vast amounts of past transaction data, customer behavior, and known fraud patterns to identify trends and risk indicators. Using machine learning models such as logistic regression, decision trees, and neural networks, the system evaluates each transaction and assigns a risk score. This score represents the probability that a transaction is fraudulent. Transactions with higher risk scores are automatically flagged for further verification or temporarily blocked until confirmation is received.

For example, if a customer suddenly initiates multiple high-value transactions within a short period or attempts transactions from different geographical locations simultaneously, the AI system interprets this as high-risk behavior. Based on predictive analysis, the system may trigger alerts, require additional authentication, or decline the transaction to prevent fraud.

Risk assessment also helps banks prioritize their fraud investigation processes. Instead of manually reviewing all transactions, financial institutions can focus on high-risk cases identified

by AI. This improves operational efficiency, reduces workload, and ensures faster response times. Additionally, predictive models continuously learn from new data, which enhances their accuracy and ability to detect emerging fraud trends.

Another important advantage is that predictive analytics supports strategic decision-making. Banks can identify vulnerable areas, improve their fraud prevention policies, and allocate resources more effectively. It also helps in compliance with regulatory requirements by providing detailed risk analysis and reporting.

4. Behavioral Biometrics and Identity Verification

Behavioral biometrics and identity verification represent an advanced and highly secure application of Artificial Intelligence (AI) in detecting financial fraud in digital banking. Unlike traditional authentication methods such as passwords, PINs, or OTPs—which can be stolen or misused—behavioral biometrics focuses on the unique patterns of user behavior that are difficult for fraudsters to replicate.

AI systems continuously monitor how a user interacts with their device during digital banking activities. This includes parameters such as typing speed, keystroke dynamics, touchscreen pressure, scrolling behavior, mouse movements, and even the angle at which a mobile device is held. These behavioral traits form a unique "digital signature" for each user. When a transaction or login attempt is made, the AI system compares the current behavior with the stored behavioral profile. If any inconsistency or unusual deviation is detected, the system flags it as suspicious.

For example, even if a fraudster gains access to a user's login credentials, their interaction pattern—such as slower typing speed or unfamiliar navigation style—will differ from the original user. AI can instantly detect this mismatch and trigger security measures such as additional authentication, transaction blocking, or alert notifications. This makes behavioral biometrics a powerful tool in preventing account takeover fraud.

In addition to behavioral biometrics, AI also strengthens identity verification through advanced technologies such as facial recognition, voice recognition, and document verification. Facial recognition systems analyze facial features to confirm the identity of users, while voice recognition systems verify individuals based on their speech patterns. AI-based document verification ensures that identity proofs such as Aadhaar or PAN cards are authentic and not forged.

These AI-driven verification methods provide a multi-layered security approach, reducing reliance on traditional authentication systems. They not only enhance fraud detection but also improve user experience by enabling faster and more seamless verification processes.

VI. KEY FINDINGS

The study reveals that the rapid growth of digital banking has significantly increased the risk of financial fraud, making advanced security systems essential. With the widespread use of mobile banking and UPI-based transactions, users are more exposed to threats such as phishing, identity

theft, and unauthorized access. A considerable portion of respondents reported experiencing some form of financial fraud, indicating that the problem is both real and growing in the digital era.

The findings show that Artificial Intelligence plays a crucial role in improving fraud detection mechanisms. AI-based systems are capable of monitoring transactions in real time, which allows banks to detect and prevent suspicious activities instantly. This real-time capability is far more effective than traditional rule-based systems, which often detect fraud only after the transaction has been completed.

Another important finding is that AI significantly enhances anomaly detection and pattern recognition. By analyzing historical transaction data, AI can identify unusual behavior and detect new types of fraud that do not follow predefined patterns. This makes AI highly adaptable to evolving fraud techniques and more efficient in identifying complex fraud cases.

The study also highlights the effectiveness of predictive analytics in fraud prevention. AI systems can assess the risk level of transactions in advance and assign risk scores, enabling financial institutions to take preventive actions before fraud occurs. This proactive approach reduces financial losses and improves operational efficiency.

Furthermore, behavioral biometrics and AI-based identity verification have emerged as strong security measures. These technologies analyze user-specific behavior and biometric features, making it difficult for fraudsters to gain unauthorized access even if they have login credentials. This adds an additional layer of protection to digital banking systems.

The findings also indicate that while awareness of AI among users is moderate, the level of trust in AI-based fraud detection systems is relatively high. Most respondents believe that AI improves banking security and reduces fraud risks. However, some concerns still exist regarding data privacy, system transparency, and false alerts.

Overall, the study concludes that Artificial Intelligence has become an essential tool in detecting and preventing financial fraud in digital banking. It not only improves accuracy and efficiency but also enables a proactive approach to fraud management. As digital transactions continue to grow, the role of AI will become even more critical in ensuring secure and reliable banking systems.

VII. CONCLUSION

The study on the Role of Artificial Intelligence in Detecting Financial Frauds in Digital Banking clearly demonstrates that AI has become a critical component in ensuring the security and reliability of modern financial systems. With the rapid expansion of digital banking services from 2020 to 2026, the volume of online transactions has increased significantly, which has also led to a parallel rise in financial frauds such as phishing, identity theft, and unauthorized transactions. This growing threat has exposed the limitations of traditional fraud detection systems that rely on fixed rules and manual monitoring.

Artificial Intelligence provides an advanced and effective solution to these challenges by enabling real-time transaction monitoring, anomaly detection, predictive analytics, and behavioral biometrics. These capabilities allow financial institutions to detect suspicious activities instantly, identify unusual patterns, and prevent fraud before it occurs. AI systems continuously learn from data, making them more adaptive and accurate in dealing with evolving fraud techniques.

The findings of the study highlight that AI not only improves fraud detection accuracy but also enhances operational efficiency by reducing manual intervention and false alerts. Additionally, technologies such as biometric authentication and identity verification strengthen security measures and minimize the risk of unauthorized access. Although challenges such as data privacy concerns, high implementation costs, and lack of transparency still exist, the benefits of AI outweigh these limitations.

In conclusion, Artificial Intelligence has transformed fraud detection in digital banking from a reactive process to a proactive and intelligent system. As digital transactions continue to grow, the integration of advanced AI technologies will become increasingly important in safeguarding financial systems. Therefore, the adoption of AI is not just an option but a necessity for building a secure, efficient, and trustworthy digital banking environment in the future.

REFERENCES

[1] Shaban, K., Salleh, & Shaikh, J. M. (2021). The relationship between ethical leadership and the quality of work life in the hotel industry. Journal of Xidian University, 15(5), 679-695.

[2] Dyg Nurulsyazwany Izzaty, M. T., & Shaikh, J. M. (2021). Research study of people with disabilities in Brunei towards development of human capital: A case of disabilities. Journal of Critical Review, 8(2), 714-722.

[3] Mortimore, A. W. (2021). Independent assurance of ESG disclosures and the impact on investment decisions. Taras Shevchenko National University of Kyiv.

[4] Kangwa, D., Mwale, J. T., & Shaikh, J. M. (2021). Digital financial inclusion of Generation Z within complex adaptive systems. European Journal of Accounting, Finance and Investment, 6(10).

[5] Adrine, M., & Shaikh, J. M. (2021). Socio-economic impact of COVID-19 on higher education: A case of Chinhoyi University of Technology. 1st International e-Conference on Impact of COVID-19 on Global Business.

[6] Kangwa, D., Mwale, J. T., & Shaikh, J. M. (2021). COVID-19 and digital financial inclusion of Generation Z within complex adaptive systems. 1st International e-Conference on Impact of COVID-19 on Global Business.

[7] Linh Bao, D. T. (2021). Evaluation of stock listing impact on corporate performance of agrofood companies in Vietnam. Asia e University.

[8] Junaidi, H. (2021). Transition towards accrual accounting and disclosure requirements in the Malaysian public sector: A case of Sarawak. Curtin University

[9] Leek, Y. H., J. M. S., & Ho, P. (2021). Predicting financial distress amongst public listed companies in Malaysia—Evaluating the effectiveness of Altman's Z-Score model. Asian Journal of Knowledge Management, 5(1), 1-8.

[10] . Kumar, S. (2021). Impact of corporate governance on the financial performance of financial institutions in Malaysia. Curtin University.

[11] Mohamed Mihilar, M. S. (2021). Adoption and implementation of corporate sustainability strategy: Evidence from a mixed-method study. Curtin University.

[12] Karim, A. M. (2021). Australian Academy of Business Leadership (AABL) 8a Erica Lane, Minto, NSW 2566, Australia.

[13] Sor Tin, S. (2021). Taxpayer compliance in service tax: An indirect compliance study. Asia e University.

[14] Asif, M. K. (2021). Perception of creative accounting: Gap analysis solution among auditors and accountants in Bangladesh. Asia e University.

[15] Mahdi Tavassoli, J. M. S., & Oraee, K. (2021). Productivity and domestic economic factors: The case of the Australian mining industry. Proceedings of TheIRES 6th International Conference, Melbourne, Australia.

[16] Arif, Haroon, Aashesh Kumar, Muhammad Fahad, and Hafiz Khawar Hussain. "Multidisciplinary Sciences and Arts."

[17] Khan, Muhammad Ismaeel, Aftab Arif, Ali Raza A. Khan, Nadeem Anjum, and Haroon Arif. "The Dual Role of Artificial Intelligence in Cybersecurity: Enhancing Defense and Navigating Challenges." International Journal of Innovative Research in Computer Science and Technology 13, no. 1 (2025): 62-67.

[18] Arif, Aftab, Muhammad Ismaeel Khan, Ali Raza A. Khan, Nadeem Anjum, and Haroon Arif. "AI-Driven Cybersecurity Predictions: Safeguarding California's Digital Landscape." International Journal of Innovative Research in Computer Science and Technology 13, no. 1 (2025): 74-78.

[19] Khan, Ali Raza A., Muhammad Ismaeel Khan, Aftab Arif, Nadeem Anjum, and Haroon Arif. "Intelligent Defense: Redefining OS Security with AI." International Journal of Innovative Research in Computer Science and Technology 13, no. 1 (2025): 85-90.

[20] Arif, Haroon, Farazul Hoda, and Aashesh Kumar. "Establishing Cloud Security by Setting up Honeypot on Azure Services." (2023).

[21] Kumar, Aashesh, Muhammad Fahad, Haroon Arif, and Hafiz Khawar Hussain. "Advancements in Detection and Mitigation: Fortifying Against APTs-A Comprehensive Review." BULLET: Jurnal Multidisiplin Ilmu 3, no. 1 (2024): 141-150.

[22] Kumar, Aashesh, Muhammad Fahad, Haroon Arif, and Hafiz Khawar Hussain. "Navigating the Uncharted Waters: Exploring Challenges and Opportunities in Block chain-Enabled Cloud Computing for Future Research." BULLET: Jurnal Multidisiplin Ilmu 2, no. 6 (2023): 12971305.

[23] Fahad, Muhammad, Haroon Airf, Aashesh Kumar, and Hafiz Khawar Hussain. "Securing against apts: Advancements in detection and mitigation." BIN: Bulletin Of Informatics 1, no. 2 (2023).

[24] . Arif, Haroon, Aashesh Kumar, Muhammad Fahad, and Hafiz Khawar Hussain. "Future horizons: AI-enhanced threat detection in cloud environments: Unveiling opportunities for research." International Journal of Multidisciplinary Sciences and Arts 3, no. 1 (2024): 242251.