International Journal of Advanced Trends in Multidisciplinary Research
ISSN: 3139-0986, Volume 2 Issue 7
July 2026, PP 1-6

The Role of Artificial Intelligence in Detecting Financial Frauds in Digital Banking

Dr. Manisha Kaushal Arora
Associate Professor, Gitarattan International Business School

***Abstract* – Financial services have changed as a result of the quick growth of digital banking, which has increased client convenience, efficiency, and accessibility. Financial frauds have become more common and sophisticated as a result of this digital revolution, which presents serious difficulties for regulators and financial institutions. By evaluating massive amounts of transactional data in real time, spotting odd trends, and more accurately forecasting possible threats than conventional rule-based systems, artificial intelligence (AI) has become a valuable tool for identifying and stopping fraudulent activity. With an emphasis on important technologies including machine learning, deep learning, natural language processing, and anomaly detection, this study investigates the significance of AI in identifying financial frauds in digital banking. Additionally, it looks at how AI-driven fraud detection systems improve customer trust, boost cybersecurity, decrease false positives, and increase operational efficiency. The report emphasises the difficulties in implementing AI despite its benefits, such as algorithmic bias, explainability, data privacy issues, regulatory compliance, and the dynamic nature of cyberthreats. The study comes to the conclusion that although AI cannot totally eradicate financial fraud, it can greatly improve fraud detection capabilities and aid in the creation of safe and resilient digital banking ecosystems when combined with strong governance frameworks, human expertise, and ongoing model improvement. For researchers, banking experts, legislators, and tech developers looking to improve fraud risk management in the digital age, the results offer insightful information.**

***Keywords* – Artificial Intelligence, Cybersecurity, Digital Banking, Financial Fraud Detection, Machine Learning**

I. INTRODUCTION

The quick digitisation of banking services has completely changed how consumers deal with their money and how financial institutions function. Financial services are now more quick, convenient, and accessible than ever thanks to digital banking platforms including contactless payments, smartphone apps, online banking, and API-driven open banking ecosystems. The sophistication, scope, and variety of financial fraud, however, have evolved in tandem with this shift at an equally quick pace. As the number of digital transactions has increased dramatically, so too have the ways in which bad actors might take advantage of weaknesses in these systems, leading to significant financial losses, a decline in customer confidence, and heightened regulatory scrutiny for banks throughout the globe.

Card-not-present fraud, account takeover, identity theft, synthetic identity fraud, phishing-induced transactions, and money laundering schemes are just a few of the ways that financial fraud appears in the context of digital banking. In order to combat these risks, traditional fraud detection methods—which mostly rely on static, rule-based systems—have become less and less effective. These systems rely on predetermined thresholds and heuristics that fraudsters may readily understand and go around, such as flagging transactions from particular geographic areas or exceeding a set amount. Furthermore, rule-based methods frequently produce significant false-positive rates, which result in needless transaction rejects, a worse client experience, and an ineffective use of investigative resources.

In this regard, artificial intelligence (AI) has become a revolutionary force in digital banking fraud detection and prevention. AI-driven methods, including as machine learning, deep learning, anomaly detection, behavioural biometrics, and graph-based network analysis, can learn intricate, non-linear patterns from enormous amounts of transactional and behavioural data, in contrast to traditional systems. These algorithms can detect tiny irregularities that would otherwise go unnoticed, adjust to new fraud typologies in almost real time, and dramatically lower false-positive rates while increasing detection accuracy.

The use of AI in fraud detection is not without difficulties, despite these benefits. The broad and successful implementation of these technologies is severely hampered by problems like model explainability, algorithmic bias, data privacy, regulatory compliance, and the adversarial adaption of fraudsters who also use AI tools.

1. Problem Statement

Financial institutions continue to suffer increasing losses as a result of fraudulent operations that take advantage of the speed, anonymity, and complexity of digital transaction channels, despite notable improvements in digital banking security architecture. Despite being widely used, traditional rule-based fraud detection systems are finding it more and more difficult to keep up with the constantly changing strategies used by scammers to get beyond static detection limits. This leads to two serious issues: a high number of fraudulent transactions that go unnoticed and result in direct financial harm (false negatives) and a high rate of false positives that strain institutional resources and annoy real customers.

Artificial intelligence's capacity to learn adaptive patterns and identify anomalies in real time presents exciting solutions, but its use poses unanswered questions about model openness, fairness, data privacy, and regulatory compliance. By methodically analysing the use, efficacy,

International Journal of Advanced Trends in Multidisciplinary Research
ISSN: 3139-0986, Volume 2 Issue 7
July 2026, PP 1-6

and difficulties of AI-driven fraud detection systems in the digital banking industry, this study aims to close this gap.

2. Objectives of the Study

The following are the main goals of this study:

- To investigate the shortcomings of conventional rule-based fraud detection systems in relation to contemporary online banking.
- To examine the many AI methods used to identify financial fraud.
- To assess how well AI-based systems work to lower false-positive rates and increase the accuracy of fraud detection.
- To determine the main obstacles to the adoption of AI, such as explainability, bias, privacy, and regulatory compliance.
- To investigate new developments like explainable AI (XAI) and federated learning.
- To offer suggestions on appropriate AI deployment to financial firms.

3. Scope of the Study

The use of artificial intelligence to identify financial fraud in digital banking settings, such as online, mobile, and digital payment systems, is the particular emphasis of this study. Card fraud, account takeover, identity theft, synthetic identity fraud, and money laundering are the key fraud types that are pertinent to this field and are identified using AI-driven systems. Although the study discusses ethical and regulatory issues, it does not cover jurisdiction-specific legal analysis or more general cybersecurity topics like network intrusion detection unless they are directly related to fraud in digital banking.

II. CONCEPTUAL FRAMEWORK

This paper suggests a five-layer conceptual framework that explains how AI functions within a digital banking fraud detection pipeline, from raw data ingestion to controlled, human-supervised decision-making, in order to provide the review with a logical analytical framework. This framework creates a single operational model by combining the mechanisms discussed in the evaluated literature (Figure 1).

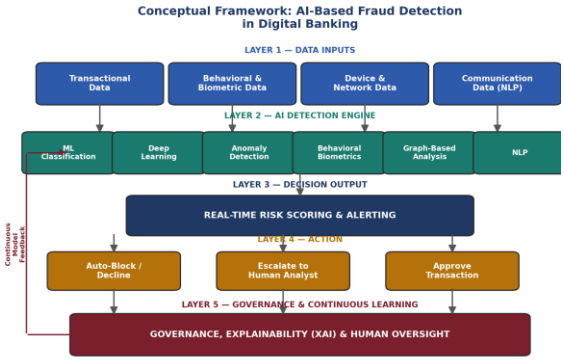

Figure 1. Conceptual Framework of AI-Based Fraud Detection in Digital Banking.

The paradigm emphasises a crucial aspect that has been highlighted in the literature: fraud detection is a closed-loop system rather than a single-pass classification exercise. The AI detection engine (Layer 2) receives outputs from the governance and human-oversight layer (Layer 5), such as explainability audits and analyst-confirmed fraud labels. This allows for ongoing model retraining and adaption to new fraud typologies.

III. LITERATURE REVIEW

Over the past 20 years, research on fraud detection has changed significantly, following the general transition from rule-based systems to intelligent, data-driven methods.

statistical and rule-based methods. Early fraud detection systems mostly relied on simple statistical techniques and guidelines established by experts. These methods have been heavily criticised for their rigidity and incapacity to identify new fraud patterns, despite being computationally effective and comprehensible.

Detection using machine learning: Supervised learning methods for transaction classification, including as logistic regression, decision trees, random forests, and gradient boosting (e.g., XGBoost, LightGBM), have been thoroughly studied. Researchers observe ongoing issues with class disparity, which are frequently resolved by SMOTE or cost-sensitive learning.

Anomaly detection and deep learning: CNNs, RNNs/LSTMs, and autoencoders are highlighted in recent literature as methods for capturing intricate temporal patterns. Reconstruction error analysis and isolation forests, two unsupervised anomaly detection techniques, are useful for spotting fraud patterns that have never been seen before. graph-based analysis and behavioural biometrics.

For ongoing authentication, behavioural biometrics examines keystroke dynamics, touchscreen motions, and navigational habits. Money-mule networks and organised fraud rings are discovered by graph neural networks and link-analysis algorithms.

Regulations and explainable: Research into explainable AI (XAI) methods like SHAP and LIME is fuelled by a substantial body of literature that tackles the "black box" issue of complicated AI models and its consequences for regulatory compliance.

1. Taxonomy of AI Techniques

The AI approaches found in the studied literature are arranged into a systematic taxonomy in Figure 2, which links each general technique category to its representative sub-methods.

International Journal of Advanced Trends in Multidisciplinary Research
ISSN: 3139-0986, Volume 2 Issue 7
July 2026, PP 1-6

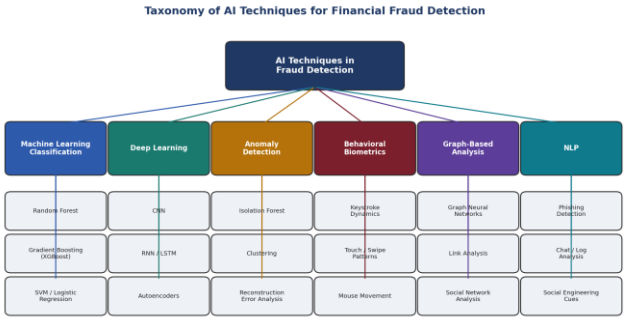

Figure 2. Taxonomy of AI Techniques for Financial Fraud Detection.

2. Summary of Reviewed Studies

Table 1 summarises the AI technique evaluated and the main findings reported by each of the fifteen empirical and review research covered in this paper's literature review.

Table 1. Summary Matrix of Key Reviewed Studies

S.No	Author(s) & Year	AI Technique / Focus	Key Finding
1	Abdallah et al. (2020)	Machine Learning (RF, SVM)	Supervised ML significantly outperforms rule-based systems; feature engineering and continuous updating are critical.
2	Sharma & Panigrahi (2020)	Behavioral Analytics / Anomaly Detection	AI enhances detection accuracy via behavioral analytics; imbalanced datasets and high false-positive rates remain key challenges.
3	Kou et al. (2021)	Deep Learning	Neural network models effectively detect complex fraud patterns in high-volume transactions; big data integration improves efficiency.
4	Singh & Best (2021)	AI Adoption in Banking	AI reduces operational costs, improves transaction monitoring and customer trust; explainable AI needed for transparency.
5	Bhatla & Prabhu (2021)	Ensemble Machine Learning	Ensemble models outperform individual algorithms; hybrid AI frameworks recommended for real-time banking.
6	West & Bhattacharya (2022)	Hybrid AI Models	Hybrid models combining ML, data mining, and behavioral analytics achieve superior accuracy;
			adaptive learning is important.
7	Ahmad et al. (2022)	Predictive Analytics / Anomaly Detection	Significantly improves fraud prevention; recommends integration with cloud computing and blockchain.
8	Ngai et al. (2023)	Real-Time Transaction Monitoring	Substantially reduces financial losses; AI provides scalability and speed traditional methods cannot achieve.
9	Alrashidi et al. (2023)	Explainable AI (XAI)	Explainability enhances user confidence, regulatory compliance, and decision transparency; accuracy-interpretability trade-off noted.
10	Xiao et al. (2025)	ML + Real-Time Analytics	Feature engineering combined with AI improves performance and reduces false alarms; continuous learning is essential.
11	George et al. (2025)	Systematic Review (Hybrid ML)	Hybrid supervised/unsupervised/deep learning approaches yield highest accuracy; explainability, scalability, and imbalance are key challenges.
12	Jagannarayan (2026)	AI Review (Banking Fraud)	AI-driven systems significantly outperform rule-based mechanisms for sophisticated frauds; continuous learning and real-time analytics are critical.
13	Buiya (2026)	Systematic Review (Ensemble/Graph-based)	Ensemble and hybrid models achieve superior precision, recall, and F1-scores; graph-based AI promising for organized fraud networks.
14	Islami & Palereng (2026)	AI + Blockchain / Big Data / AutoML	Integration significantly enhances detection capability; data privacy, explainability, and regulatory compliance remain barriers.

International Journal of Advanced Trends in Multidisciplinary Research
ISSN: 3139-0986, Volume 2 Issue 7
July 2026, PP 1-6

S.No	Author(s) & Year	AI Technique / Focus	Key Finding
15	Ibrahim et al. (2026)	Deep Learning, GNN, XAI	Deep learning, graph neural networks, and explainable AI identified as next-generation technologies; recommends trustworthy, ethical frameworks.

3. Research Gaps

Although the literature currently in publication covers individual AI techniques in great detail, there is still a dearth of consolidated analysis comparing their relative efficacy across various fraud typologies within digital banking specifically, as well as a lack of investigation into how institutions can strike a balance between detection performance and requirements for explainability, fairness, and privacy. The purpose of this study is to help close these gaps.

III. RESEARCH METHODOLOGY

A thorough evaluation of secondary sources, including peer-reviewed journal articles, conference papers, industry reports, and case studies published mostly within the last ten years, served as the foundation for this study's qualitative, descriptive research design.

Data collection: Using search terms like "AI fraud detection," "machine learning banking security," "anomaly detection financial transactions," and "explainable AI banking," literature was gathered from academic databases (IEEE Xplore, ScienceDirect, SpringerLink, Google Scholar) and trade publications.

Analytical Framework: Based on stated effectiveness measures, documented implementation obstacles, and fundamental AI approaches (ML classification, anomaly detection, behavioural biometrics, graph-based analysis, and NLP), the gathered literature is analysed thematically.
Comparative Evaluation: To evaluate the relative advantages and disadvantages of various AI techniques across fraud typologies, qualitative performance patterns recorded across studies are compared when available.

The methodology's limitations: Because this study uses secondary data, its conclusions are limited by the breadth, calibre, and reporting standards of the original literature. Banks' proprietary fraud detection technologies are frequently not fully disclosed to the public.

Findings and Analysis

Figures 3 and 4 below illustrate a number of recurring patterns found in the synthesis of the evaluated literature.

1. Effectiveness Across Fraud Typologies

A qualitative effectiveness matrix mapping each category of AI techniques against the main fraud typologies is shown in Figure 3. This matrix was created by synthesising the patterns seen in the examined papers. The authors' qualitative synthesis of relative strengths documented in the literature is shown in this matrix, which is not based on a single empirical benchmark and is meant to direct technique selection by type of fraud.

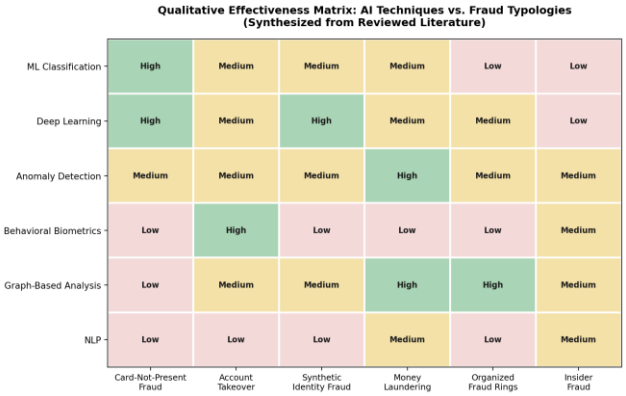

Figure 3. Qualitative Effectiveness Matrix — AI Techniques vs. Fraud Typologies.

The matrix shows that no single method is superior for all forms of fraud: machine learning classification and deep learning are particularly good at detecting card-not-present fraud and synthetic identities; behavioural biometrics is best at account takeover; and graph-based analysis is best at money laundering and organised fraud rings. These findings support the idea of hybrid, ensemble architectures.

2. Thematic Synthesis of Benefits and Challenges

A clear, empirically supported foundation for the discussion that follows is provided by Figure 4, which measures the frequency with which important benefit and difficulty themes were identified throughout the fifteen reviewed research summarised in Table 1.

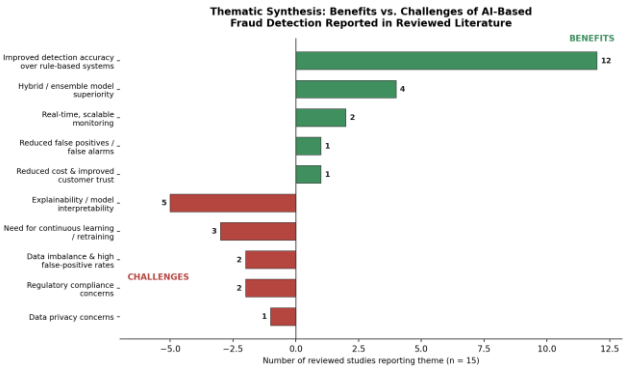

Figure 4. Thematic Synthesis of Benefits and Challenges Reported Across Reviewed Studies (n = 15).

3. Key Findings

- Better detection results compared to rule-based systems: Compared to rule-based engines, machine learning-based systems consistently exhibit improved

fraud detection accuracy and reduced false-positive rates; ensemble approaches often provide the best precision-recall balance.

- The advantage of deep learning for intricate, sequential fraud patterns. When applied to transaction sequences, LSTM networks and autoencoders enhance the identification of fraud patterns that emerge over several transactions or sessions.
- Anomaly detection's value in cold-start conditions. In order to identify new fraud types without labelled previous samples, unsupervised methods are crucial.
- A powerful defence against account takeover is behavioural biometrics. Behavioural biometrics-based continuous authentication enhances the detection of credential-based takeover and session hijacking.
- Techniques for organised fraud based on graphs. Coordinated fraud structures that are hidden by transaction-level models are revealed by graph neural network and link-analysis techniques.
- Enduring difficulties. In almost every studied source, the explainability gap, algorithmic bias risk from skewed training data, and the requirement for ongoing retraining reoccur.

These results collectively imply that no single AI strategy is adequate on its own; the research increasingly suggests that the most efficient and reliable method for detecting fraud in digital banking is to use hybrid, ensemble-based architectures that combine many techniques.

IV. CONCLUSION

With capabilities much beyond those of conventional rule-based systems, artificial intelligence has completely changed the landscape of financial fraud detection in digital banking. Financial institutions can now identify fraudulent activity more quickly, accurately, and adaptably thanks to machine learning, deep learning, anomaly detection, behavioural biometrics, and graph-based analysis. At the same time, the false positives that previously plagued both customers and fraud analysts are decreased.

Adopting AI in this field, however, is not a comprehensive solution on its own. Model explainability, data bias, regulatory compliance, and the adversarial evolution of fraud strategies are still major issues that need constant attention. The most successful fraud detection strategies incorporate several complementary AI techniques within a continuously monitored, governed security architecture rather than depending solely on one method, as demonstrated by the conceptual framework and effectiveness matrix presented in this paper (Figures 1 and 3).

The necessity of developing fraud detection systems that are not only accurate but also transparent, equitable, and compliant with changing regulatory norms will only grow as digital banking continues to spread throughout the world. Explainable AI approaches, privacy-preserving strategies like federated learning, and adaptive systems that can react instantly to fraud trends should be given top priority in future research. In the end, financial institutions, tech companies, and regulators must work together to make sure these systems are reliable and strong in order for AI to continue to be helpful in preventing financial fraud.

REFERENCES

1. Abdallah, A., Maarof, M. A., & Zainal, A. (2016). Fraud detection system: A survey. Journal of Network and Computer Applications, 68, 90–113. https://doi.org/10.1016/j.jnca.2016.04.007
2. Ahmad, Z., Shahid, M., & Khan, S. (2022). Artificial intelligence-enabled cybersecurity for digital banking: Challenges and opportunities. Journal of King Saud University – Computer and Information Sciences, 34(10), 8240–8253.
3. Bao, Y., Hilary, G., & Ke, B. (2022). Artificial intelligence and fraud detection. In Innovative Technology at the Interface of Finance and Operations (pp. 223–247). Springer.
4. George, A., Thomas, P., & Nair, S. (2025). Machine learning techniques for financial fraud detection: A systematic literature review. arXiv. https://arxiv.org/abs/2510.05167
5. Ibrahim, M., Hassan, R., & Ali, S. (2026). AI-driven financial fraud detection: Recent advances, challenges, and future directions. Applied Sciences, 16(4), 1931.
6. Jagannarayan, S. (2026). Fraud detection in banking using artificial intelligence: A systematic review. ResearchGate Preprint.
7. Kou, Y., Peng, Y., Wang, G., & Shi, Y. (2021). Deep learning techniques for financial fraud detection: A review. Expert Systems with Applications, 184, 115490.
8. Mehana, A., & Nuci, K. P. (2020). Fraud detection using data-driven approach. arXiv. https://arxiv.org/abs/2009.06365
9. Ngai, E. W. T., Hu, Y., Wong, Y. H., Chen, Y., & Sun, X. (2011). The application of data mining techniques in financial fraud detection: A classification framework and an academic review of literature. Decision Support Systems, 50(3), 559–569. https://doi.org/10.1016/j.dss.2010.08.006
10. Ryman-Tubb, N. F., Krause, P., & Garn, W. (2018). How artificial intelligence and machine learning research impacts payment card fraud detection: A survey and industry benchmark. Engineering Applications of Artificial Intelligence, 76, 130–157.
11. Singh, S., & Best, P. (2021). Artificial intelligence applications in banking: Opportunities and challenges. Journal of Financial Crime, 28(3), 793–812.

International Journal of Advanced Trends in Multidisciplinary Research
ISSN: 3139-0986, Volume 2 Issue 7
July 2026, PP 1-6