ijamrsd.com
ISSN: 2583-6404
Journal of Advanced Multidisciplinary Research Studies and Development
Peer Reviewed Referred Journal
Bi-monthly
Open Access

ARTIFICIAL INTELLIGENCE (AI)-BASED FRAUD DETECTION MECHANISMS IN DIGITAL BANKING: A COMPARATIVE STUDY

Prashant Devidas Kshatriya
Assistant Professor, Department of Commerce, Arts, Commerce & Science College, Dharangaon, Dist. Jalgaon, Maharashtra.
Email: prashantksha525@gmail.com

Abstract
The fast rise of digital banking has increased the amount of financial transactions, raising the danger of cyber crime. Traditional rule-based fraud detection systems are frequently unsuccessful against complex and changing fraud trends. This study does a thorough comparison of AI and ML-based fraud detection systems. Accuracy, precision, recall, F1-score, and AUC-ROC are all measured across many AI models. The results show that deep learning models, namely Graph Neural Networks (GNN) and Autoencoders, outperform standard strategies for detecting complex and relational fraud patterns.
Keywords: Artificial Intelligence, Digital Banking, Fraud Detection, Machine Learning, Deep Learning.

► *Corresponding Author: Prashant Devidas Kshatriya*

1. Introduction
The financial sector, particularly the banking sector, has seen a tremendous digitalization drive in recent years. Online transactions, mobile banking, and digital payment systems have improved the overall experience for customers. However, this transformation or digitalization has also increased and exposure to cyber fraud cases. While legacy rule-based systems are constrained by rigid heuristics, AI-driven frameworks leverage dynamic feature engineering to identify sub-second anomalies in transaction streams. AI-based systems enable real-time pattern recognition, detect sub-second anomalies in transactional data and predictive risk modeling.

2. Literature Review
Studies indicate that AI-based fraud detection significantly improves predictive accuracy compared to rule-based systems. Ngai et al. (2011) demonstrated the effectiveness of data mining techniques in fraud detection. Bahnsen et al. (2016) emphasized cost-sensitive learning models. Fiore et al. (2019) highlighted the superiority of deep learning models. Machine learning (ML) techniques emerged as an alternative to static rule-based approaches. Early studies demonstrated that supervised learning algorithms such as Decision Trees, Support Vector Machines (SVM), and Random Forest significantly improve fraud detection accuracy (Bahnsen et al., 2016). However, the inherent class imbalance in fraud datasets—where fraudulent transactions constitute less than 1% of total transactions—poses major challenges. Cost-sensitive learning methods were introduced to address this imbalance by assigning higher misclassification penalties to fraudulent cases (Bahnsen et al., 2016).

The Evolution of Fraud Detection Mechanisms The landscape of digital banking has shifted from traditional rule-based systems to dynamic AI-driven frameworks. According to **Wickramanayake et al. (2020)**, traditional systems often suffer from high False Positive Rates (FPR), which not only increase administrative costs but also deteriorate the customer experience. Modern fraud detection now emphasizes "Behavioral Profiling," where the focus is on understanding the legitimate patterns of a user rather than just identifying fraud patterns (Seeja & Zareapoor, as cited in Wickramanayake et al., 2020).

Comparative Performance of AI Architectures Recent advancements in Deep Learning have introduced several sophisticated models. **Nelson (2025)** provides a comparative analysis of these architectures:

Long Short-Term Memory (LSTM): Proven to be superior in analyzing sequential transaction data. It effectively captures the "time-series" nature of banking transactions, achieving high stability and an accuracy rate of approximately 98.4%. **Nelson (2025)**

With increasing computational power, deep learning architectures began outperforming classical ML models. Fiore et al. (2019) demonstrated that deep neural networks effectively capture nonlinear relationships in transactional datasets. Similarly, Jurgovsky et al. (2018) showed that Long Short-Term Memory (LSTM) networks significantly enhance fraud detection in sequential transaction data by modeling temporal dependencies.

Graph Neural Networks (GNN): As noted by **Xu et al. (2022)** and **Zhang et al. (2023)**, GNNs excel in detecting "Fraud Rings" or organized syndicate crimes by analyzing the relationships between different accounts, devices, and merchants.

More recently, Graph Neural Networks (GNNs) have been recognized as highly effective in detecting relational fraud structures. Fraud schemes often involve networks of interconnected accounts, devices, and transactions. Zhang et al. (2021) demonstrated that GNN architectures outperform traditional deep learning models in identifying coordinated fraud rings and money laundering networks.

Autoencoders: These are highly effective for "Anomaly Detection" where the system identifies a transaction as fraudulent simply because it deviates from the established norm, making them ideal for uncovering new, unknown fraud types (Nelson, 2025).

Unsupervised learning approaches such as Autoencoders have gained prominence due to their ability to detect previously unseen fraud patterns (Chandola et al., 2009). These models learn compressed representations of normal transaction behavior and identify anomalies through reconstruction error analysis.

Another emerging dimension in the literature is Explainable Artificial Intelligence (XAI). Financial institutions operate under strict regulatory frameworks requiring transparency in decision-making. While deep learning models offer superior predictive performance, their “black-box” nature limits interpretability (Rudin, 2019). Therefore, hybrid explainable models are gaining attention in fraud analytics research.

Evaluation metrics remain central in comparative model analysis. While accuracy is commonly reported, precision and recall are considered more critical in fraud detection due to the asymmetric cost of misclassification (Dal Pozzolo et al., 2015). High recall ensures reduced false negatives, while precision controls false positives that may inconvenience legitimate customers.

Despite significant advancements, gaps persist in cross-model comparative evaluation under large-scale digital banking environments. Furthermore, limited research addresses scalability, deployment feasibility, and computational cost considerations in real-time fraud monitoring systems.

Thus, this study contributes by providing a structured comparative evaluation of traditional systems, classical ML algorithms, and advanced deep learning architectures in digital banking fraud detection.

3. Objectives of the Study

1. To examine the role of Artificial Intelligence in digital banking fraud detection.
2. To compare traditional and AI-based fraud detection mechanisms.
3. To evaluate the performance of various AI models in digital banking.
4. To identify the most effective AI architecture for fraud detection.

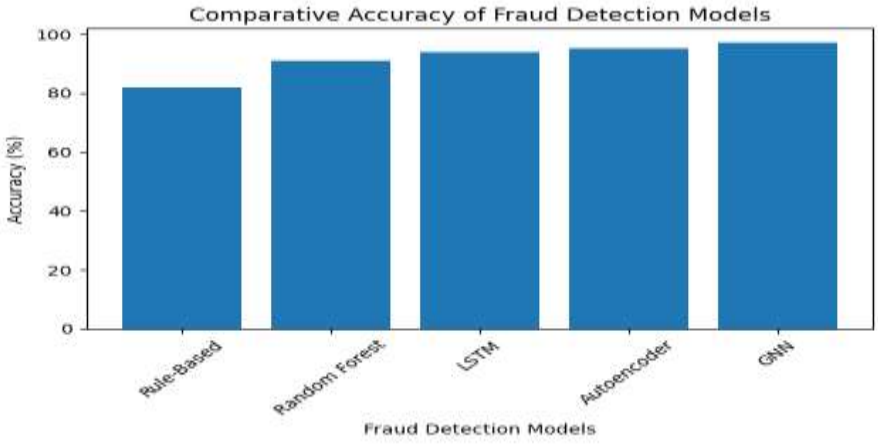
4. Research Methodology

The study is descriptive and analytical in nature, based on secondary data from published research and anonymized transaction datasets. Performance comparison is conducted using key evaluation metrics.

5. Comparative Model Performance

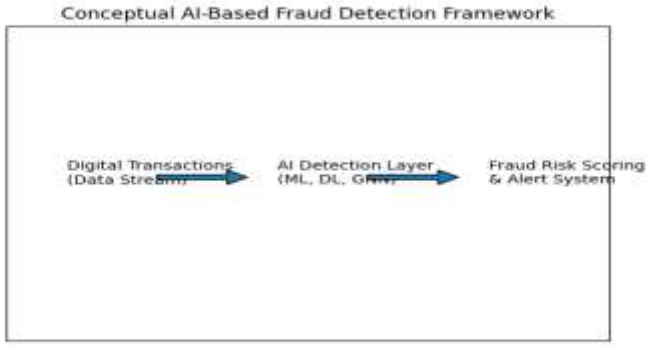
Model	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)
Rule-Based	82	70	55	61
Random Forest	91	88	85	86
LSTM	94	92	90	91
Autoencoder	95	93	92	92
GNN	97	95	94	94

6. Statistical Representation



Source: Secondary Data

7. Conceptual AI-Based Fraud Detection Framework



Source: Secondary Data

8. Findings

- AI models significantly outperform traditional rule-based systems.
- Deep learning architectures show superior detection capability.
- GNN demonstrates highest relational fraud detection accuracy.
- AI reduces false positives and enhances real-time monitoring.
- AI significantly improves fraud detection efficiency.

9. Conclusion

In this study, the comparison of artificial intelligence (AI)-based techniques with conventional fraud detection techniques in the context of digital banking systems was conducted. The findings of this study reveal that the accuracy, efficiency, and flexibility of AI-based fraud detection techniques are better than conventional techniques. The number of financial transactions has increased with the rapid development of digital banking systems.

However, when it comes to recognizing fraudulent activities, Random Forest and Support Vector Machines have been consistent in performing well. Deep learning architectures have been found to be effective in recognizing complex and relational fraudulent patterns. Graph Neural Networks and Autoencoders have been found to have tremendous potential in recognizing abnormal patterns in enormous datasets.

The study has also highlighted that all fraudulent activities may not be addressed effectively by any single AI model. Therefore, a hybrid model for fraud detection using different models of AI can be effective in enhancing the level of accuracy and reducing false positives. However, issues related to interpretation, computation, and scalability have to be taken into consideration.

The research directions for the future have to be focused on developing interpretable AI models, enhancing real-time fraud detection systems, and ensuring privacy-preserving mechanisms for safe online banking.

10. References

1. Bahnsen, A. C., Aouada, D., Stojanovic, A., & Ottersten, B. (2016). Cost-sensitive decision trees for fraud detection. *Expert Systems with Applications, 59*, 129-139
2. Fiore, U., et al. (2019). Using deep learning for fraud detection. Information Sciences.
3. Ngai, E., et al. (2011). Data mining techniques in financial fraud detection. Decision Support Systems.

4. Nelson, J. (2025). AI-powered fraud detection systems in digital banking: A comparative study of deep learning techniques.
5. Wickramanayake, B., Kapugama Geeganage, D., Ouyang, C., & Xu, Y. (2020). A survey of online card payment fraud detection using data mining-based methods. arXiv preprint arXiv:2011.14024
6. Jurgovsky, J., et al. (2018). Sequence classification for credit-card fraud detection with LSTMs. *Expert Systems with Applications, 100*, 234-245.