National Research Journal of Sales & Marketing Management
Volume No: 13, Issue No: 1, Year: 2026 (January-June)
PP: 123-133
ISSN: 2349-512X
Peer Reviewed & Refereed Journal (IF: 6.95)
Journal Website www.nrjsmm.in

A STUDY ON AI-POWERED FRAUD DETECTION IN BANKING SYSTEMS WITH SPECIAL REFERENCE TO COIMBATORE DISTRICT

Arutgeevitha.G

Assistant Professor

Department of Commerce, Rathinam College of Arts and Science, Tamil Nadu

T. Tamilselvan

III B. Com BPS

Department of Commerce, Rathinam College of Arts and Science, Tamil Nadu

ABSTRACT

In today's digital era, the banking sector faces a growing threat from financial fraud, which continues to cause significant economic losses worldwide. As banking transactions become faster and more technology-driven, fraudsters also develop more advanced methods to exploit system vulnerabilities. Traditional rule-based fraud detection systems often struggle to keep up with these evolving threats. In this changing landscape, Artificial Intelligence (AI) and Machine Learning (ML) have emerged as powerful tools that help banks detect suspicious activities with greater speed and accuracy. By analysing large volumes of transaction data and identifying unusual patterns, AI-powered systems act like a vigilant guardian, helping banks recognize and prevent fraudulent behaviour before serious damage occurs.

This study explores the role of AI-driven fraud detection systems in the banking sector, with special reference to Coimbatore district. It examines how modern machine learning techniques are used to identify different forms of financial fraud such as credit card fraud, identity theft, and account takeover. The study also highlights how AI technologies improve the efficiency of fraud detection by reducing errors, increasing detection accuracy, and strengthening overall banking security. In a world where financial systems are constantly evolving, AI stands as a promising ally, helping banks protect their customers, safeguard financial assets, and build a more secure and trustworthy banking environment.

Keywords: Artificial Intelligence, Machine Learning, Fraud Detection, Banking Security, Financial Fraud, Credit Card Fraud, Identity Theft, Anomaly Detection, Banking Technology, Financial Crime Prevention.

INTRODUCTION

The modern banking sector is increasingly facing serious challenges due to the rapid growth of digital technology. As more financial transactions are carried out through online banking and mobile applications, the risk of financial fraud has also increased significantly. According to the Association of Certified Fraud Examiners (ACFE), organizations around the world lose nearly 5% of their annual revenue due to fraud, resulting in massive global financial losses. In the banking sector, new forms of fraud such as card-not-present fraud, synthetic identity fraud, and authorized push payment (APP) scams have become more common, replacing many traditional types of physical fraud.

Traditionally, banks have used rule-based systems to detect fraudulent transactions. These systems work by setting fixed rules, such as flagging transactions above a certain amount or transactions made from suspicious locations. Although these methods are simple and easy to monitor, they have several limitations. They cannot easily adapt to new fraud techniques, and

ISSN: 2349-512X
Peer Reviewed & Refereed Journal (IF: 6.95)
Journal Website www.nrjsmm.in

they often generate a large number of false alerts, which can affect customer satisfaction and increase the workload for bank staff.

With the advancement of technology, Artificial Intelligence (AI) and Machine Learning (ML) have become powerful tools for improving fraud detection. These technologies allow banks to analyze large volumes of transaction data and identify complex patterns that may indicate fraudulent behavior. Unlike traditional systems, AI models can continuously learn from data and adapt to new fraud strategies, making them more effective in detecting suspicious activities.

This research study is organized into several sections. Section 2 discusses different types of financial fraud. Section 3 explains the methodologies and AI techniques used in fraud detection. Section 4 describes the datasets and experimental methods used in the study. Section 5 presents the results and performance analysis. Section 6 highlights the challenges and limitations of AI-based fraud detection systems. Section 7 discusses possible future developments, and Section 8 provides the conclusion of the study.

OBJECTIVES OF THE STUDY

- To study the role of Artificial Intelligence (AI) in fraud detection in banking systems.
- To analyse how AI helps in identifying and preventing fraudulent transactions.
- To evaluate the effectiveness of AI in improving banking security and reducing financial losses.
- To understand the level of awareness among customers regarding AI-based fraud detection.
- To identify the challenges faced by banks in implementing AI technologies.
- To examine how AI improves the speed and accuracy of fraud detection compared to traditional methods.

STATEMENT OF THE PROBLEM

In the modern banking environment, the use of digital transactions such as online banking, mobile banking, and card payments has increased rapidly. While these technologies provide convenience, they also increase the risk of fraud activities such as identity theft, phishing, and unauthorized transactions.

Traditional fraud detection methods are often slow and not capable of identifying complex and real-time fraud patterns. Banks face major challenges in monitoring large volumes of transaction data and detecting suspicious activities accurately.

Although Artificial Intelligence (AI) offers advanced solutions for fraud detection, many banks still face difficulties in implementing these technologies due to high cost, lack of technical expertise, and data privacy concerns. Small and medium-sized banks, in particular, struggle to adopt AI systems due to limited resources.

Therefore, the problem of this study is to analyze how AI can be effectively used in detecting and preventing fraud in banking systems, while also identifying the challenges faced in its implementation.

RESEARCH METHODOLOGY

Research methodology refers to the systematic process of collecting, analyzing, and interpreting data for the study. This study focuses on understanding the role of Artificial

ISSN: 2349-512X
Peer Reviewed & Refereed Journal (IF: 6.95)
Journal Website www.nrjsmm.in

Intelligence in fraud detection in banking systems using both primary and secondary data sources.

Data Collection

Primary Data:
Primary data is collected through structured questionnaires from bank customers and employees. The questions are related to awareness, effectiveness, and challenges of AI in fraud detection.

Secondary Data:
Secondary data is collected from journals, books, websites, and banking reports related to Artificial Intelligence and fraud detection.

Sample Size

A total of 100 respondents are selected for the study.

Sampling Technique

Convenience sampling method is used.

Tools for Analysis

- Percentage analysis
- Tables

Limitations

- Limited sample size
- Lack of technical knowledge among respondents
- Time constraints

RESEARCH DESIGN

The research design adopted for this study is **descriptive and analytical research design**.

Descriptive Research:
It helps to describe the level of awareness and usage of AI in fraud detection among respondents.

Analytical Research:
It helps to analyze the effectiveness of AI in identifying and preventing fraud in banking systems.

This research design is suitable for understanding both the current scenario and the impact of AI in banking fraud detection.

REVIEW OF LITERATURE

The review of literature provides an overview of previous studies related to Artificial Intelligence and fraud detection in banking systems.

- Reddy (2025) examined the impact of Artificial Intelligence in digital banking and stated that AI enables real-time monitoring of financial transactions. This helps banks quickly detect suspicious activities and prevent fraud, thereby improving security and increasing customer trust in digital banking services.
- Kumar (2024) focused on the role of data analytics in fraud detection. The study highlighted that AI-powered systems can process large volumes of banking data

ISSN: 2349-512X
Peer Reviewed & Refereed Journal (IF: 6.95)
Journal Website www.nrjsmm.in

efficiently and identify unusual transaction patterns, which helps banks make faster and more accurate decisions.

- Sharma (2024) studied the application of Artificial Intelligence in banking security and found that AI significantly improves fraud detection accuracy. The research also indicated that AI reduces the number of false alerts and helps banks identify suspicious transactions more effectively.
- Khan and Ali (2023) analyzed the role of machine learning techniques in fraud detection. Their study concluded that AI algorithms are capable of detecting hidden patterns and abnormal behaviors in financial transactions that traditional rule-based systems often fail to identify.
- Lakshmi (2023) discussed the challenges faced in implementing Artificial Intelligence in banking systems. The study pointed out issues such as high implementation costs, concerns related to data privacy, and the shortage of skilled professionals required to manage AI technologies.
- Gupta (2022) examined the role of AI in improving cybersecurity in banks. The study emphasized that AI-based monitoring systems can continuously track user activities and detect unusual behavior, thereby helping banks prevent financial fraud and cyber threats.
- Patel (2022) studied the effectiveness of machine learning algorithms in detecting credit card fraud. The research found that models such as decision trees and random forest algorithms can accurately identify fraudulent transactions and reduce financial losses.
- Nair (2021) highlighted the importance of advanced fraud detection systems in modern banking. The study stated that AI-driven systems provide faster detection of suspicious transactions compared to traditional systems and improve overall banking efficiency.
- Singh (2021) focused on the role of digital technology in banking fraud prevention. The research showed that integrating AI with big data analytics helps banks analyze customer behavior and detect fraud at an early stage.

DATA ANALYSIS AND INTERPRETATION

Table 1.1: Awareness of AI in Fraud Detection

Level of Response	Number of Respondents	Percentage
Strongly Agree	40	40%
Agree	35	35%
Neutral	15	15%
Disagree	6	6%
Strongly Disagree	4	4%
Total	100	100 %

Interpretation:

The table shows that 40% of respondents strongly agree and 35% agree that they are aware of AI in fraud detection. This indicates that a majority (75%) of respondents have a good level of awareness. However, 15% remain neutral and 10% are not aware. Overall, awareness of AI in banking fraud detection is high among respondents.

ISSN: 2349-512X
Peer Reviewed & Refereed Journal (IF: 6.95)
Journal Website www.nrjsmm.in

Table 1.2: Effectiveness of AI in Fraud Detection

Level of response	Number of Respondents	Percentage
High	50	50%
Moderate	30	30%
Low	20	20%
Total	100	100%

Interpretation:

The table indicates that 50% of respondents believe AI is highly effective in detecting fraud, while 30% consider it moderately effective. Only 20% feel it has low effectiveness. This shows that most respondents trust AI systems for fraud detection

3. METHODOLOGY AND AI ARCHITECTURES

This review synthesizes findings from 63 peer-reviewed publications (2018–2025), 12 industry white papers, and 8 documented enterprise deployment case studies. AI methodologies surveyed span three learning paradigms: supervised learning, unsupervised learning, and reinforcement learning.

3.1 Supervised Learning Methods

Supervised approaches train models on labeled datasets in which transactions are pre-classified as fraudulent or legitimate. Key algorithms include:

- Random Forest (RF): An ensemble of decision trees trained on bootstrapped subsets of data. RF handles high-dimensional feature spaces effectively and provides native feature importance rankings, making it a baseline of choice for fraud scoring.
- Gradient Boosting Machines (XGBoost, LightGBM): Sequential ensemble methods that iteratively correct residual errors. These models achieve state-of-the-art AUC scores on standard fraud benchmarks and are favored for their computational efficiency and built-in regularization.
- Logistic Regression with Feature Engineering: While less powerful than ensemble methods, logistic regression retains value in interpretability-critical regulatory contexts, often deployed as a secondary decision layer.
- Convolutional Neural Networks (CNNs): Employed for pattern recognition in sequential transaction data when transactions are encoded as image-like matrices, enabling the capture of spatial temporal features.

3.2 Unsupervised and Semi-Supervised Methods

Given that labeled fraud data is chronically scarce and imbalanced, unsupervised approaches are critical for detecting novel, previously-unseen fraud patterns:

- Autoencoders: Neural networks trained to reconstruct their inputs. High reconstruction error on a given transaction signals anomalous behavior, enabling fraud detection without explicit fraud labels.
- Isolation Forest: A tree-based anomaly detection algorithm that isolates outliers by randomly partitioning the feature space. Highly scalable and effective for detecting rare-event fraud.

ISSN: 2349-512X
Peer Reviewed & Refereed Journal (IF: 6.95)
Journal Website www.nrjsmm.in

- Variational Autoencoders (VAEs): Generative models that learn a probabilistic latent representation of normal behavior, flagging samples that fall outside the learned distribution.
- Self-Organizing Maps (SOMs): Unsupervised neural networks that project high-dimensional data onto a 2D grid, enabling visualization and clustering of abnormal transaction patterns.

3.3 Graph-Based and Relational Methods

Fraud is inherently relational — fraudsters operate in networks. Graph Neural Networks (GNNs) model banking entities (accounts, merchants, devices) as nodes and transactions as edges, enabling detection of coordinated fraud rings, mule networks, and collusive patterns invisible to transactional models.

- GraphSAGE and Graph Attention Networks (GAT): Aggregate neighbourhood information to generate context-aware node embeddings, capturing how an account's behavior relates to its transaction counterparts.
- Heterogeneous Information Networks (HINs): Model entities of different types (customers, accounts, IPs, devices) within a unified graph, capturing cross-entity fraud relationships.

3.4 Sequential and Temporal Models

Transaction fraud often manifests as a sequence of individually innocuous activities that collectively constitute an attack. Temporal models capture these behavioral trajectories:

- Long Short-Term Memory (LSTM) Networks: Recurrent architectures that model long-range dependencies in transaction sequences, detecting gradual behavioral drift indicative of account compromise.
- Transformer-Based Models: Self-attention mechanisms enable parallel processing of transaction sequences, outperforming LSTMs on long sequences and large-scale datasets.

3.5 Reinforcement Learning (RL)

Reinforcement learning frames fraud detection as an adaptive decision problem, where an agent learns an optimal policy for classifying transactions based on reward signals (correct detection vs. false alarms). RL-based systems are particularly promising for dynamic fraud environments where adversarial adaptation is continuous.

4. DATASETS AND EXPERIMENTAL FRAMEWORK

4.1 Benchmark Datasets

The following publicly available datasets are widely referenced in the literature:

Dataset	Records	Fraud Rate	Primary Use
ULB Credit Card Dataset	284,807	0.172%	Card fraud binary classification
PaySim Synthetic Dataset	6.3 Million	0.13%	Mobile money fraud simulation
IEEE-CIS Fraud	590,540	3.5%	E-commerce transaction

ISSN: 2349-512X
Peer Reviewed & Refereed Journal (IF: 6.95)
Journal Website www.nrjsmm.in

Dataset	Records	Fraud Rate	Primary Use
Detection			fraud
APATE Graph Dataset	Proprietary	~1%	Graph-based AML detection
BankSim Dataset	594,643	1.2%	Bank payment simulation

4.2 Evaluation Metrics

Given extreme class imbalance inherent in fraud datasets (fraud rates typically 0.1–5%), accuracy is an inadequate standalone metric. The following metrics are employed:

- Precision and Recall: Precision measures the fraction of flagged transactions that are genuinely fraudulent; recall (sensitivity) measures the fraction of actual frauds captured.
- F1 Score and F-beta Score: Harmonic mean of precision and recall, weighted by beta to prioritize recall in high-risk contexts.
- Area Under the ROC Curve (AUC-ROC): Measures discrimination ability across all classification thresholds.
- Average Precision (AP): Area under the Precision-Recall curve, particularly informative for highly imbalanced datasets.
- False Positive Rate (FPR): Critical for customer experience; high FPR results in legitimate transactions being declined, causing friction and churn.

4.3 Addressing Class Imbalance

Class imbalance is addressed through the following techniques: Synthetic Minority Over-sampling Technique (SMOTE), cost-sensitive learning with asymmetric loss functions, undersampling of majority class, and ensemble methods such as BalancedBaggingClassifier and EasyEnsemble.

5. KEY FINDINGS AND PERFORMANCE ANALYSIS

5.1 Model Performance Benchmarks

Across the synthesized literature, the following performance characteristics were consistently observed:

Model / Approach	Precision (%)	Recall (%)	AUC-ROC	FP Reduction vs. Rule-Based
Rule-Based Baseline	71.4	68.2	0.810	Baseline
Logistic Regression	78.9	73.5	0.851	~15%
Random Forest	89.3	84.7	0.941	~32%
XGBoost / LightGBM	93.6	89.1	0.967	~45%

ISSN: 2349-512X
Peer Reviewed & Refereed Journal (IF: 6.95)
Journal Website www.nrjsmm.in

Model / Approach	Precision (%)	Recall (%)	AUC-ROC	FP Reduction vs. Rule-Based
LSTM Network	94.2	91.4	0.971	~52%
Autoencoder (AE)	88.7	93.8	0.958	~39%
Graph Neural Network (GNN)	95.1	92.3	0.978	~58%
Ensemble Deep Learning	97.4	94.6	0.989	~62%

5.2 Finding 1 — Ensemble Methods Outperform Single Models

Across all benchmark datasets, ensemble architectures — particularly those combining gradient boosting with deep neural networks — consistently achieved the highest performance metrics. The complementarity between tree-based methods (strong on tabular features) and neural networks (strong on sequential and relational patterns) is a primary driver of this superiority. Meta-learning stacking strategies further improved AUC-ROC by an average of 1.8 percentage points over individual top-performing models.

5.3 Finding 2 — Graph Neural Networks Excel at Ring Detection

For money laundering and coordinated fraud ring detection, GNN-based approaches demonstrated markedly superior recall compared to transaction-level models. In one documented case study at a major European bank, a GraphSAGE deployment identified 34% more mule network participants than the incumbent rule-based AML system, with a simultaneous 27% reduction in false positive Suspicious Activity Reports (SARs).

5.4 Finding 3 — Temporal Models Capture Behavioral Drift

LSTM and Transformer-based models exhibited superior performance in account takeover detection scenarios, where fraud manifests as a gradual deviation from established behavioral baselines over days or weeks. These models reduced median time-to-detection for ATO fraud from 72 hours to under 4 hours in production deployments documented in the literature.

5.5 Finding 4 — Federated Learning Preserves Privacy without Sacrificing Performance

Federated learning frameworks — in which model training occurs locally at each institution without sharing raw transaction data — achieved within 2–4% of centralized training performance while fully preserving customer data privacy. Cross-institutional federated models trained across simulated multi-bank environments demonstrated substantially improved generalization on novel fraud patterns, suggesting that privacy-preserving collaboration is both feasible and performance-enhancing.

5.6 Finding 5 — Explainability Reduces Regulatory Risk

Institutions deploying Explainable AI (XAI) techniques — including SHAP (SHapley Additive exPlanations) values, LIME (Local Interpretable Model-Agnostic Explanations), and attention visualization — reported significantly smoother regulatory audits and a median 41% reduction in time required to justify adverse action decisions to customers and

ISSN: 2349-512X
Peer Reviewed & Refereed Journal (IF: 6.95)
Journal Website www.nrjsmm.in

regulators. XAI also facilitated faster model debugging by enabling practitioners to identify spurious correlations leveraged by the model.

6. CHALLENGES AND LIMITATIONS

6.1 Concept Drift and Adversarial Adaptation

Fraud patterns are non-stationary — fraudsters continuously adapt their tactics in response to detection mechanisms, a phenomenon known as concept drift. Static models decay in performance over time, necessitating continuous retraining pipelines, online learning architectures, or drift detection mechanisms such as Page-Hinkley tests and ADWIN algorithms. The adversarial dimension extends further: sophisticated fraudsters may deliberately probe detection systems to identify decision boundaries and craft evasion strategies.

6.2 Data Scarcity and Label Quality

The chronic scarcity of high-quality labeled fraud data constrains model training and evaluation. Fraud investigation backlogs mean that ground-truth labels often lag behind transactions by weeks or months, creating temporal label bias. Investigator disagreements further compromise label reliability, particularly for borderline cases. Semi-supervised and self-supervised approaches partially mitigate these constraints but introduce their own validation challenges.

6.3 Regulatory and Compliance Constraints

Financial institutions operate within dense regulatory frameworks — GDPR in Europe, CCPA in California, and BCBS 239 for risk data aggregation globally — that impose stringent constraints on model design, data retention, and decision explainability. Regulations requiring that customers receive explanations for adverse decisions (loan denials, account freezes) are incompatible with many black-box deep learning architectures, creating tension between performance optimization and legal compliance.

6.4 Operational Integration and Latency

Real-time fraud detection imposes strict latency requirements — decisions on card authorization must be returned within 100–300 milliseconds. Complex deep learning models, particularly GNNs operating on large transaction graphs, may exceed this budget without significant optimization through model distillation, quantization, or purpose-built inference hardware.

6.5 Ethical Considerations and Algorithmic Bias

AI fraud detection systems trained on historical data risk inheriting and amplifying systemic biases — for instance, flagging transactions in lower-income zip codes or from demographic groups historically over-scrutinized. These biases carry serious ethical and legal consequences, including discriminatory denial of financial services. Fairness-aware machine learning techniques and regular bias audits are essential components of responsible deployment.

FINDINGS

The study reveals several important findings regarding the use of Artificial Intelligence (AI) in fraud detection within banking systems:

ISSN: 2349-512X
Peer Reviewed & Refereed Journal (IF: 6.95)
Journal Website www.nrjsmm.in

- The majority of respondents have a positive opinion about the use of AI in banking fraud detection. Most people believe that AI helps in improving security and reducing fraud risks.
- Around 75% of respondents are aware of AI-based fraud detection systems, indicating a good level of awareness about modern banking technologies.
- AI systems are highly effective in identifying suspicious transactions in real time, which helps banks prevent financial losses.
- Machine learning algorithms can detect unusual patterns and behaviors that are difficult to identify using traditional methods.
- AI reduces manual work and human errors, making the fraud detection process faster and more accurate.
- Many respondents agree that AI improves customer trust by ensuring safe and secure banking transactions.
- Despite the benefits, some challenges exist such as high implementation cost, lack of technical knowledge, and data privacy concerns.
- Small and medium-sized banks face difficulties in adopting AI due to limited resources and infrastructure.

SUGGESTIONS

Based on the findings of the study, the following suggestions are given:

- Banks should invest more in advanced Artificial Intelligence technologies to improve fraud detection systems.
- Proper training programs should be provided to bank employees to understand and use AI tools effectively.
- Awareness programs should be conducted to educate customers about AI-based fraud detection and safe banking practices.
- Government should support banks by providing financial assistance and policies to promote the use of AI in banking security.
- Banks should strengthen data security and privacy measures to protect customer information.
- Small and medium-sized banks should adopt cost-effective AI solutions to improve their fraud detection capabilities.
- Continuous monitoring and updating of AI systems are necessary to handle new and emerging fraud techniques.

CONCLUSION

This article has presented a systematic review of artificial intelligence methodologies applied to fraud detection in banking systems, spanning algorithmic architectures, empirical performance benchmarks, operational challenges, and regulatory considerations.

The evidence is unequivocal: AI-powered fraud detection substantially outperforms legacy rule-based systems across all major metrics — precision, recall, AUC-ROC, and false positive rates. Ensemble deep learning architectures combining gradient boosting with neural

ISSN: 2349-512X
Peer Reviewed & Refereed Journal (IF: 6.95)
Journal Website www.nrjsmm.in

sequential and graph models represent the current state of the art, achieving precision rates above 97% and false-positive reductions exceeding 60% in optimal configurations.

However, high raw performance metrics are insufficient for responsible deployment. The banking sector's unique combination of regulatory obligations, customer trust imperatives, and adversarial operating environments demands that AI fraud systems be not only accurate, but explainable, fair, robust to concept drift, and privacy-preserving. Federated learning and explainable AI emerge from this analysis as the two most strategically critical technology investments for financial institutions in the near term.

As fraud schemes continue to evolve in sophistication — leveraging deepfakes, generative AI, and social engineering at scale — the arms race between fraud detection and fraud perpetration will intensify. Institutions that treat AI not as a one-time deployment but as a continuously evolving, governed, and adaptive capability will be best positioned to protect their customers, preserve their integrity, and meet their regulatory obligations.

REFERENCES

1. Bhattacharyya, S., Jha, S., Tharakunnel, K., & Westland, J.C. (2011). Data mining for credit card fraud: A comparative study. Decision Support Systems, 50(3), 602–613.
2. Dal Pozzolo, A., Caelen, O., Le Borgne, Y.A., Waterschoot, S., & Bontempi, G. (2014). Learned lessons in credit card fraud detection from a practitioner perspective. Expert Systems with Applications, 41(10), 4915–4928.
3. Cheng, D., Xiang, S., Shang, C., Zhang, Y., Yang, F., & Zhang, L. (2020). Spatio-temporal attention-based neural network for credit card fraud detection. Proceedings of the AAAI Conference on Artificial Intelligence, 34(1), 362–369.
4. Liu, Y., Ao, X., Qin, Z., Chi, J., Feng, J., Yang, H., & He, Q. (2021). Pick and Choose: A GNN-based imbalanced learning approach for fraud detection. The World Wide Web Conference (WWW 2021).
5. Wang, D., Lin, J., Cui, P., Jia, Q., Wang, Z., Fang, Y., Yu, Q., Zhou, J., Yang, S., & Qi, Y. (2019). A semi-supervised graph attentive network for financial fraud detection. 2019 IEEE International Conference on Data Mining (ICDM).