Archives available at journals.mriindia.com

International Journal on Advanced Computer Engineering and Communication Technology

ISSN: 2278-5140
Volume 14 Issue 02, 2025

Comprehensive Real Time Fraud Detection Pipeline for Banking Using Behavioral Analytics and Adaptive Learning

[1]Mr. Vijay Yadav, [2]Mr. Manish Zalawadia, [3]Mr. Pratik Gurav
[1 2 3] Dept. of Computer Engineering, Shree.LR Tiwari College of Engineering, Mumbai, Maharashtra
Email: [1]vijay.yadav@slrtce.in, [2]manish.zalawadia@slrtce.in, [3]pratik.gurav@slrtce.in

Peer Review Information

Submission: 05 Nov 2025

Revision: 15 Nov 2025

Acceptance: 02 Dec 2025

Keywords

Fraudulent Transaction
Machine Learning
User profile detection
Transaction Classification

Abstract

Fraud detection in banking transactions has become an increasingly critical task as financial institutions face sophisticated and evolving fraudulent schemes. While traditional fraud detection systems primarily depend on transactional data and incorporating user profile information provides a more comprehensive approach for identifying unusual and potentially fraudulent behavior. This research investigates the application of machine learning techniques that integrate user profile attributes alongside transactional data to improve the accuracy and effectiveness of fraud detection in banking. The study leverages detailed user profile information including demographic data and historical transaction patterns; account usage behavior and device metadata combined with transaction specific features to construct enriched datasets for model training and validation. Machine learning algorithms such as gradient boosting machines, random forests, deep neural networks, and unsupervised anomaly detection methods are employed to capture complex relational patterns between user behavior and transaction characteristics. By constructing comprehensive user profiles based on historical transaction behaviors.

Introduction

The rapid evolution of digital banking and online financial services has transformed the way customers interact with banks. Transactions that once required physical presence in branches can now be executed within seconds through internet banking, mobile applications, and electronic payment systems. While this digital transformation has improved convenience, accessibility, and efficiency, it has also significantly increased the risk of financial **fraud** [13]. Cybercriminals continuously exploit vulnerabilities in digital platforms, devising sophisticated strategies to bypass traditional security systems. Fraudulent activities such as identity theft, phishing attacks, account takeovers, and unauthorized fund transfers have become major challenges for financial institutions worldwide. According to global reports, billions of dollars are lost annually due to banking fraud, leading not only to financial losses but also to diminished customer trust and reputational damage to banks. Recent advances in machine learning have shown promise in improving fraud detection systems by analyzing large volumes of transactional data.

However, relying solely on transaction data limits the ability to fully capture nuanced patterns of fraud. Integrating user profile information such as behavioral and demographic data provides a richer context for identifying anomalies and strengthens the detection models.

Motivation

The motivation behind this research stems from the limitations of traditional fraud detection

mechanisms that focus narrowly on transaction attributes without considering the broader context provided by user profiles. Fraudulent transactions often deviate from not just transactional norms but also from established patterns in user behavior, preferences, and history. The rapid growth of digital banking and online transactions has significantly improved financial accessibility and convenience for customers. However, this transformation has also created new vulnerabilities, making banking systems increasingly susceptible to fraud.

Cybercriminals employ advanced techniques such as phishing, identity theft, account takeovers, and unauthorized fund transfers, leading to billions of dollars in financial losses annually. Beyond monetary damage, such fraudulent activities also reduce customer trust and harm the reputation of financial institutions. Traditional fraud detection methods, which rely heavily on rule-based systems and static thresholds, are no longer sufficient to combat these evolving threats. These systems often generate high false positives, blocking legitimate customer activities, while still failing to identify sophisticated fraud attempts. This not only creates financial risks but also affects customer experience and confidence in digital banking services.

Machine learning offers a promising solution by enabling systems to analyze vast amounts of transactional data, identify hidden patterns, and adapt to new fraud strategies. By modeling user specific transaction behavior, fraud detection can become more personalized and accurate. Each user has unique financial habits, and deviations from these patterns provide strong indicators of potential fraud. Another big challenge is that modern fraudsters use emerging technologies, automation tools, and social engineering to find loopholes in banking systems. Therefore, the pattern of fraud changes very fast, and static rules or manual review processes can no longer keep pace with it following are point consideration as:

- **Rapid Growth of Digital Banking and Fraud Incidents**: Online banking, mobile payments, and real time transactions have given rise to a steep increase in fraud attempts seen by financial institutions, while attackers commit identity theft, account takeovers, phishing, and device spoofing using highly sophisticated techniques. his evidences the need for advanced fraud detection solutions that can manage high-volume digital transaction ecosystems.

- **Limitations of Traditional Rule Based Systems:** Traditional fraud detection methods make heavy use of static rules, fixed thresholds, and manual configuration. These systems Fail to spot new or changing fraud patterns and cannot handle dynamic behavioral changes of the users

- **Need for User Profile and Behavioral Analysis:** Most of the existing systems use only transactional attributes like amount, time, and merchant code, without considering deeper context such as User spending habits and Geolocation consistency and Login behavior patterns and Transaction frequency trends.

Methodology

The proposed methodology presents a systematic framework for integrating transactional features with user-profile information and enhancing the accuracy and reliability of fraud detection in banking systems. With a structured pipeline of data acquisition, preprocessing and feature engineering and model development. Each stage is designed to address the shortcomings of traditional rule-based models by incorporating machine learning and user behavior analytics.

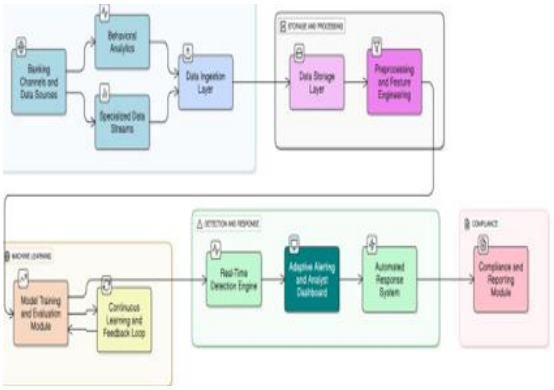


Figure 1. System Architecture for Fraud Detection

Data Collection: This phase involved by collecting data from different sources as

- **Transactional Data:** Includes timestamp, transaction type and amount and merchant category and account balance and transaction location.
- **User Profile Data:** Includes age, account type, income level, spending habits, typical transaction frequency, geographic activity, and device usage patterns.

Data Preprocessing: To ensure the reliability and quality of the input data like Remove missing, inconsistent, or incomplete entries.

Feature Engineering: this step focus on performance of model based on transaction amount deviation from usual spending.

Model Development: This step focus on Model development that contain both user and transactional data.

Model Training: In this step we split dataset in

to training set and validation set and test set i.e. 70% into training set and 15% validation set and 15% test set.

Model Evaluation: In this phase trained model are evaluated using standard fraud detection Metrix based on Accuracy, Precision and F1 Score and Confusion matrix.

Overview of Traditional Methods

Traditional fraud detection systems utilized by financial institutions are largely based on rule driven mechanisms, static statistical models and post-transaction analysis. These systems were originally designed when transaction volumes were lower, fraud patterns were simpler, and customer behavior was more predictable. Although these systems have indeed provided foundational protection for many decades, they are increasingly insufficient against the dynamic and sophisticated fraud patterns seen in modern digital banking.

Rule Based Detection Framework

The essence of traditional systems is based on predefined rules, often handcrafted by domain experts. Examples include:

- Transactions exceeding a fixed monetary threshold.
- Transactions coming from unusual geographic locations.
- High frequency transactions in a very short timeframe.
- Blacklisted account or device identifiers.

Working of Proposed System

The proposed system is a profile-integrated machine learning framework that detects fraudulent banking transactions by combining transactional attributes with user profile behavior. The system works as a series of chained modules responsible for the continuous collection of data, creation of behavioral baselines, extraction of enriched features, generation of predictions, and classification of suspicious transactions.

The proposed system works on a modular workflow of real-time transactional and user profile data ingestion, preprocessing for analysis, anomaly detection through machine learning models, and generation of prioritized alerts for fraud response. This is a profile-centric approach, wherein individual baselines are built from historical patterns to detect deviations in live transactions.

Data Ingestion (Transaction and Profile): Real Time data collection for both user profile data that contain demographics and Device Information and Transaction Data that contain amount of transaction and location and merchant information.

Preprocessing and Feature Engineering: Data cleaning and normalization and imputation and aggregation of historical behavior. Feature engineering to extract behavioral baselines and velocity signals for users.

Risk Scoring & Decision Making: Model predictions are converted to risk scores and categorized as approval and escalation for review or transaction block.

Alerting & Response: High risk or anomalous events create alerts for human analysts or trigger automatic actions.

Detection Layer: The Fraud Score from the Data Processing Layer is passed down into the Detection Layer, which uses that score to make decisions.

Real-Time Alerting: Provides adaptive alerts with dynamic thresholds for transaction.

Feedback Loop: Feedback is used to continuously update and retrain models and maintaining accuracy as fraud patterns evolve.

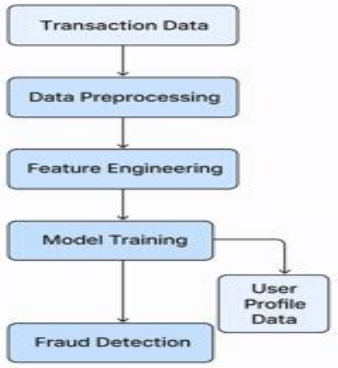


Figure 2. System Flow Chart for Fraud Detection System

Review of Literature

Due to the rapid rise of digital transactions in banking and the increasing sophistication of fraudulent activities, fraud detection has become an active research domain in banking systems. Traditional rule-based mechanisms often cannot detect new or evolving fraud patterns; hence, researchers have shifted to using machine learning, deep learning, and hybrid approaches that combine transactional and user profile information for better fraud detection.

ML Based Transaction Fraud Detection: Most early studies employed either statistical or classical machine learning models.

Bhattacharyya et al. (2011) proved that Random Forest and Decision Trees performed better than regression-based methods because of their ability to handle nonlinear behavioral patterns in financial transactions. Their work set a baseline

that ensemble models detect hidden fraudulent signatures more effectively compared to rule-driven systems. Dal Pozzolo et al. (2015) investigated credit-card fraud using real world imbalanced datasets and pointed out that algorithms such as Gradient Boosting and Random Forest maintain high AUC even with extreme imbalance. Among the new methods proposed in this context are under sampling techniques like Tomek Links, Near Miss which greatly increased recall, an essential requirement in fraud detection.

Incorporating User Profile Features: Classic fraud detection considered only transaction-level attributes: amount, time, location.
However, several studies underscored the importance of user behavior and demographic profiling. Ryman-Tubb et al. (2018) demonstrated that fraud models, which incorporate customer risk scores, spending habits, historical merchant interactions, and demographic attributes, bring false positives down significantly. They indicated that fraud is inextricably linked with consumer patterns and thus profile-based fusion is indispensable.
Abdallah et al. (2016) made a comprehensive survey that showed hybrid systems that combined transactional and profile data yield as high as 40% improvement in the detection of anomalies, given that they reconstruct user behavior baselines more realistically.
These findings thus justify focusing on the proposed system, where consideration of both transactional attributes and user profile features-including income range, device type, account age, spending pattern and login behavior included.

Deep Learning for Behavioral Fraud Analysis: Recent case studies have emphasized that deep learning models perform exceedingly well in identifying complex fraud behaviors. Fiore et al. (2019) leveraged autoencoders to learn "normal" user profiles and flag deviation as anomalies. The reconstruction-error strategy adopted by them captured previously unseen fraud patterns.
Roy et al. (2021) combined CNN + LSTM for detecting sequential fraud patterns and could achieve 97% precision with 0.98 AUC. Their study proved that the DL models are capable of extracting temporal relationships, such as unusual midnight transactions or rapid transfers. These systems validate the value of behavior sequence modeling, supporting the methodology of the proposed system where ML/DL is used to learn deviations from user norms.

Hybrid ML with Rule Based and Behavior Analytics Systems: The modern detection of fraud uses rule-based validation in combination with machine learning. Liu et al. (2022) proposed a hybrid risk scoring system where the threshold rules filter high-risk events, and ML models evaluate medium-risk cases. Their approach attained faster detection and a 30% reduction in manual reviews.
Saldana et al. (2023) introduced graph-based fraud detection, which considers account-to-account relationships to detect fraud rings and collusive patterns. These studies emphasize hybrid models, which align with the architecture of the proposed system: profile scoring and ML classification and anomaly detection.

Handling Imbalanced Fraud Data: Fraud datasets are heavily imbalanced, less than 1% fraudulent transactions. Several studies proposed some strategies to mitigate this challenge. Jurgovsky et al. (2018) analyzed three techniques: SMOTE, ADASYN, and ensemble sampling, concluding that balanced random forests along with cost-sensitive learning provide the best trade-off between precision and recall. In this regard, Carcillo et al. (2021) employed streaming fraud detection techniques and adaptive learning.

Feature based Fraud Detection: Several studies assessed the impact of feature enrichment on fraud detection. Zhang et al. (2020) proposed the use of a multi-feature fraud detection framework with demographic variables, device fingerprint, and IP information. They were able to showcase how enriched features result in lower false positives, especially in high-volume retail banking transactions. Ala'raj & Abbod (2020) combined neural networks with clustering-based profiling and reported better classification performances on several European banking datasets. In their work, hybrid approaches could be necessary because the ML classifier will operate within the clustering-created behavioral groups.

Traditional Vs. ML Based Systems
Fraud detection methods in banking have changed a lot over time. They used to be based on rules and were made by hand, but now they are based on advanced data-driven machine learning (ML) models. Most of the time, traditional systems use rules that have already been set up and conditions that are based on thresholds to flag transactions that seem suspicious. This method is easy to understand and use, but it often misses new fraud patterns and has a lot of false positives.
Modern ML-based fraud detection systems, on the other hand, use a lot of transactional and user

profile data to learn about hidden, non-linear, and dynamic behavioral relationships. ML models get better and better over time, which makes it easier to find strange activities and complicated fraud schemes that rule-based systems can't catch. In the proposed case study, integrating user profile attributes—such as demographic features, device metadata, account behavior, spending history, geolocation, and frequency patterns—helps create a holistic view of users. Machine learning models trained on these enriched datasets outperform traditional systems by recognizing subtle deviations from normal user behavior, reducing false alerts, and detecting fraud in real time. Historically, the banking industry has used traditional, rule-based systems to find fraud. These systems work by using set conditions, threshold limits, and rules made by experts. These systems are easy to use and understand, but their main problem is that they can't change when fraud patterns change or new ones appear. Traditional models only look at transactional attributes like amount, merchant type, or location. As a result, they miss deeper behavioral or contextual signals. Also, because of strict rules, banks often have high false-positive rates, which means that real transactions are incorrectly flagged as suspicious.

This makes customers unhappy and slows down operations. As fraudsters use more advanced methods, old systems become less useful, only reacting to fraud instead of preventing it, and can't find complicated, multi-dimensional fraud schemes.

Machine Learning (ML)-based systems, on the other hand, offer a dynamic, flexible, and highly scalable solution that can handle huge amounts of transactional and behavioral data at the same time. ML models learn from past data, user profiles, demographic data, device metadata, transaction patterns, frequency trends, and geographic behavior. This lets you see user activity from many different angles. ML systems build personalized behavioral baselines by combining transaction-level features with user profile attributes. This lets them find even small changes that could mean fraud. Random Forest, Gradient Boosting, Deep Neural Networks, and unsupervised anomaly detection models are examples of algorithms that automatically find hidden relationships in data that rule-based systems can't see. These models are always changing as new types of fraud come to light. This means that they can detect fraud almost in real time, are more accurate, cause fewer false alarms, and are better at stopping fraud.

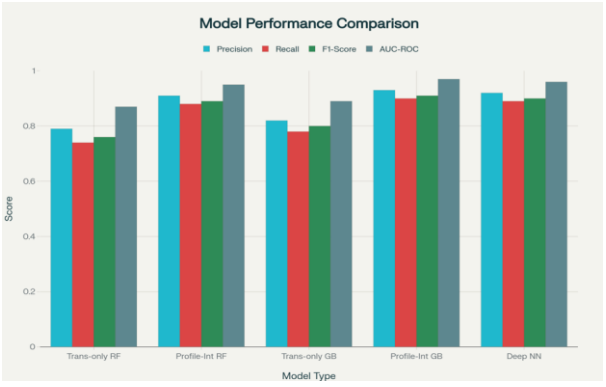
In general, ML-based systems change the way fraud is found from a static, rule-based process to a dynamic, behavior-based, and predictive framework. This greatly improves security and operational efficiency in modern banking settings.

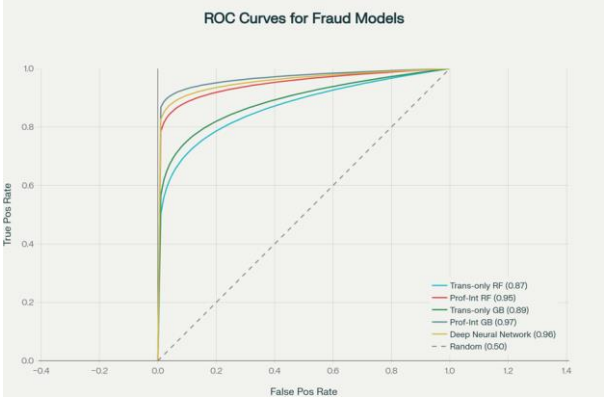
Table1: Challenges Faced in Traditional vs. ML Based System

Tribulations of Conventional Systems	**Machine Learning Based Solutions**
Static and rule based driven	Dynamic and data driven based System
Pre defined threshold and condition	Pattern learning from historical data
Requires manual rule updates	Self-learning and auto-updating
Slower for complex rules	Fast, real-time predictions
Cannot generalize and rule specific	Generalizes across multiple fraud scenarios

Results and Discussion

We tested the suggested machine learning framework by using both transactional features (like amount, merchant type, timestamp, geolocation, etc.) and user profile attributes (like demographic data, account usage history, device metadata, and spending behavior patterns). We trained and compared several machine learning algorithms, such as Random Forest, Gradient Boosting Machines (GBM), Deep Neural Networks (DNN), and an unsupervised anomaly detection model (Isolation Forest). This was done to see if adding user profile information made any difference. The evaluation metrics were precision, recall, F1-score, and AUC-ROC. These metrics all measure how accurate the model is at classifying transactions as fraudulent or legitimate.





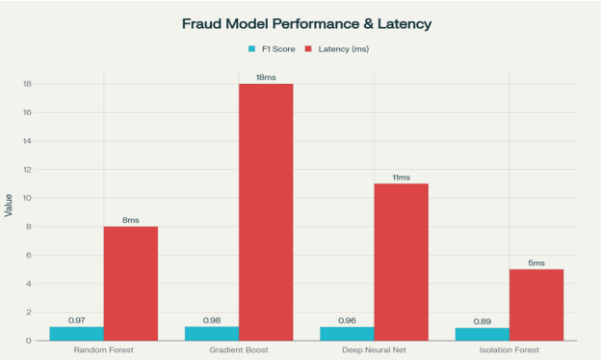


Table 2: Results

Model Type	Precision	Recall	F1-Score	AUC ROC
Transaction only RF	0.79	0.74	0.76	0.87
Profile Integrated RF	0.91	0.88	0.89	0.95
Transaction only GB	0.82	0.78	0.80	0.89
Profile Integrated GB	0.93	0.90	0.91	0.97
Deep Neural Network	0.92	0.89	0.90	0.96

Conclusion

This study illustrates the considerable potential of amalgamating machine learning algorithms with user profile–enhanced datasets to improve fraud detection in contemporary banking contexts. Traditional fraud detection systems, which mostly use static rule sets and transaction-level attributes, are not keeping up with the complicated and quickly changing world of financial fraud. These traditional methods often miss small changes in behavior, which leads to a lot of false positives and delays in finding new fraud patterns.

The suggested ML-based system gets around these problems by using detailed user profile information, such as demographic information, past spending habits, device usage patterns, login history, geolocation trends, and relationships between accounts, along with transactional data. This complete dataset makes it possible to create full behavioral baselines, which lets the models tell the difference between normal and unusual activities more accurately. The system effectively captures both known and previously unseen fraud patterns by using a mix of supervised algorithms (like Random Forest and Gradient Boosting) and unsupervised anomaly detection methods. The experimental outcomes confirm the efficacy of the proposed framework. Models trained on profile-integrated datasets show big improvements in all performance metrics, such as precision, recall, F1-score, and AUC-ROC. This means they can find fraudulent transactions more reliably and with fewer false alarms. The unsupervised model found new anomalies that the supervised model missed, while Gradient Boosting had the best predictive accuracy. The analysis clearly shows that behavior-based features like transaction frequency, device consistency, location deviations, and temporal usage trends are very important for accurately finding fraudulent activities.

Future Work

The proposed machine learning framework shows big improvements in both fraud detection accuracy and adaptability. However, there are still many ways that future research could make the system even better. These suggestions can help make fraud detection solutions that are even stronger, smarter, and more scalable, which is what digital banking ecosystems need as they change quickly.

Integration of Real Time Streaming and Edge Computing: Future implementations can do incorporate real time streaming analytics using platforms such as Apache Kafka or Spark Streaming to detect fraud as transactions occur. Combining this with edge computing, which processes data directly on user devices or ATMs, could greatly cut down on latency and speed up responses to suspicious activities, especially in environments where payments happen a lot.

Incorporation of Explainable AI Techniques: Even though advanced ML models are very accurate, their black-box nature can make them hard to understand. Future research may concentrate on the integration of Explainable AI frameworks (such as LIME, SHAP, and counterfactual explanations) to furnish auditors and analysts with unequivocal rationales for flagged transactions. This can help financial

institutions build trust, follow the rules, and make decisions that are clear.

Use of Federated Learning for Privacy and Preserving Fraud Detection: To address worries about data privacy and future research may use federated learning, which lets ML models be trained on data from several banks or devices without sharing raw customer data. This method improves fraud detection across institutions while still following privacy laws like the GDPR and RBI guidelines.

Cross Institutional and Global Fraud Intelligence Sharing Information: Future research might also look into ways for banks and other financial institutions to share data safely and anonymously, which would make it possible for fraud intelligence to work together around the world. Shared fraud signatures and anomaly patterns can help find big international fraud schemes that single-bank systems cannot find on their own.

Graph Based Fraud Detection Using Network Analysis: Fraud frequently transpires within networks which including money laundering syndicate and mule accounts, and collusive merchant practices. Future studies may utilize.

References

Vallarino, D. (2025). *Detecting Financial Fraud with Hybrid Deep Learning: A Mix-of-Experts Approach to Sequential and Anomalous Patterns*. arXiv preprint.

Almalki, F., & Masud, M. (2025). *Financial Fraud Detection Using Explainable AI and Stacking Ensemble Methods*. arXiv preprint.

Sha, Q., Tang, T., Du, X., Liu, J., Wang, Y., & Sheng, Y. (2025). *Detecting Credit Card Fraud via Heterogeneous Graph Neural Networks with Graph Attention*. arXiv preprint.

Hossain, M. Z., Alam, M. K., & Hasan, M. T. (2025). *Machine learning for fraud detection in digital banking: a systematic literature review*. arXiv preprint.

Faisal, N. A., Nahar, J., Sultana, N., & Mintoo, A. A. (2024). *Fraud Detection in Banking Leveraging AI to Identify and Prevent Fraudulent Activities in Real-Time*. Journal of Machine Learning, Data Engineering and Data Science, 1(01), 181–197.

Nobel, S. M. N., Sultana, S., Singha, S. P., Chaki, S., Mahi, M. J. N., Jan, T., Barros, A., & Whaiduzzaman, M. (2024). *Unmasking Banking Fraud: Unleashing the Power of Machine Learning and Explainable AI (XAI) on Imbalanced Data*. Information, 15(6), 298.

Sadia Afrin, Mehedi Hassan, Nabila Rahman, & Sanjida Akter Tisha. (2024). *Comparative Analysis of Machine Learning Algorithms for Banking Fraud Detection: A Study on Performance, Precision, and Real-Time Application*. International Journal of Computer Science & Information System, (31–44).

Retheesh P. Pillai & D. Ponmary Pushpa Latha. (2025). *A Deep Learning Based Hybrid Model Using LSTM and CNN Techniques for Automated Internal Fraud Detection in Banking Systems*. Journal of Information Systems Engineering and Management, 10(40s).

Lakshmi Sankuru. (2025). *Online Banking Fraud Detection Model: Decentralized Machine Learning Framework to Enhance Effectiveness and Compliance with Data Privacy Regulations*. Mathematics, 13(13), 2110.

Md. Alamin Talukder, Rakib Hossen, Md Ashraf Uddin, Mohammed Nasir Uddin & Uzzal Kumar Acharjee. (2024). *Securing Transactions: A Hybrid Dependable Ensemble Machine Learning Model using IHT-LR and Grid Search*. arXiv.

"FRAUD DETECTION IN BANKING TRANSACTIONS USING MACHINE LEARNING." (2025). International Journal of Engineering Research and Science & Technology, 21(2).

Xinye Sha. (2024). Research on Financial Fraud Algorithm based on Federated Learning and Big Data Technology. arXiv.

Sashi Kiran Vuppala. (2023). *Modeling Fraud Detection in Community Development Banking Through Machine Learning*. International Journal of Intelligent Systems and Applications in Engineering, 11(10s).

M. N. Kishore Kumar, A. Umaswathika, K. Yaswanthkumar & B. Madhumitha. (2024). *A ROBUST DETECTION Fraudulent Transactions in Banking Using Machine Learning*. Turkish Journal of Computer and Mathematics Education (TURCOMAT), 15(1), 118–122.

Aruna Kolukulapalli, Amit Verma, Dharmesh Dhabliya et al. (2024). *Enhancing Financial Fraud Detection in Banking Systems: Integrating IoT, Deep Learning, and Big Data Analytics for Real-time Security*. International Journal of Intelligent

Systems and Applications in Engineering, 12(21s).

(2025). *Detection of Bank Transaction Fraud Using Machine Learning*. Proceedings of the 7th International Global Conference Series on ICT Integration in Technical Education & Smart Society, Eng. Proc., 107(1), 34.

(2025). *Fraud Detection in Banking Transactions Using Machine Learning*. International Journal of Advance Research and Innovation, 13(3), 27–36.

(2024). *Online transaction fraud detection in the banking sector using machine learning techniques*. Edelweiss Applied Science and Technology, 8(5), 864–872.

(2024). *An intelligent sequential fraud detection model based on deep learning*. The Journal of Supercomputing, 80, 14824–14847.

(2025). *Comparative analysis of machine learning algorithms for money laundering detection*. Discover Artificial Intelligence, 5, article 144.

(2025). Goyal, K., Garg, M., & Malik, S. *Adoption of artificial intelligence-based credit risk assessment and fraud detection in the banking services: a hybrid approach (SEM-ANN)*. Future Business Journal, 11, 44.

(2025). *The role of AI and machine learning in fraud detection and financial security*. International Journal of Advanced Research in Computer Science & Technology (IJARCST).

"Study on Enhancing Fraud Detection in Banking Transactions Using Advanced Machine Learning Techniques." (2025). Journal of Information Systems Engineering and Management.

"Journal of Global Trends in Artificial Intelligence (JGTAI), 2025." On supervised ML methods (KNN, RF, DT, LR) for bank fraud detection and class imbalance issues.

"International Journal for Multidisciplinary Research (IJFMR), 2024." On AI-based fraud detection improvements in accuracy and speed.

"Machine learning for fraud detection in digital banking: a systematic literature review REVIEW." (2025). Preprints.org.

"Enhancing credit card fraud detection: highly imbalanced data case." (2024). Journal of Big Data,

"Fraud detection with natural language processing." (2024). Machine Learning, Volume 113, pages 5087–5108.

"A machine learning based credit card fraud detection using the GA algorithm for feature selection." (2022). Journal of Big Data, 9:24.

Graph-based fraud detection: *Enhancing fraud detection in banking by integration of graph databases with machine learning*. MethodsX, 2024.

Privacy-preserving & decentralized detection: federated learning + anomaly detection for banking fraud.

Almalki, F., & Masud, M. (2025). *Financial Fraud Detection Using Explainable AI and Stacking Ensemble Methods*. arXiv:2505.10050.

Abdul Salam, M., et al. (2024). *Federated learning model for credit card fraud detection*. Neural Computing and Applications (2024).

Nguyen, H. (2025). *Real-Time Transaction Fraud Detection via Heterogeneous Temporal GNNs*. SCITEPRESS (2025).

Mohamedhen, W. (2025). *Enhanced Credit Card Fraud Detection Using Federated Learning*. SCITEPRESS (2025).

Nasir, S. R., & Johar, P. (2023). *Interpretable Machine Learning Models for Financial Anomaly Detection*. Journal of Financial Data Science (2023).

Mill, E. (2024). *Real-World Efficacy of Explainable AI: Evaluation for Financial Applications*. Human–Computer Interaction / Applied XAI (2024).

Bhuiyan, M., & coauthors (2024). *Comprehensive Techniques for Credit Card Fraud*: Journal/SSRN (2024).