International Journal of Recent Trends in Science Technology & Management(IJRTSTM)
©2023 (IJRTSTM) | Volume 4 | Issue 3 | ISSN: 2584-0894
October-December 2025 | DOI: https://doi.org/10.5281/zenodo.18195874

Fraud Detection in Financial Transactions Using Anomaly Detection Techniques: A Cybersecurity Perspective

Yogesh T. Patil[1], Km Bittu Pandey[2], Pallavi Soni[3]

[1,2,3]Assistant Professor, Faculty Of Computer Application, Sigma University, Vadodara, India
yogi007orama@gmail.com[1], bittupandey676@gmail.com[2], pallavisoni1701@gmail.com[3]

Abstract

Financial fraud poses a significant and evolving threat to global digital economies, particularly as financial transactions increasingly shift toward online and mobile platforms. Traditional rule-based and supervised machine learning systems often struggle to identify emerging or unseen fraud patterns, resulting in high false-negative rates and delayed detection. This paper explores anomaly detection as a powerful approach to fraud detection within the broader context of cybersecurity. By identifying deviations from established transaction behavior, anomaly detection techniques can uncover previously unknown fraud schemes with minimal labeled data. The study provides a comprehensive review of state-of-the-art anomaly detection algorithms—including statistical models, isolation forests, one-class support vector machines, autoencoders, and graph neural networks—applied to financial fraud detection. A hybrid anomaly detection framework is proposed that integrates temporal behavior modeling, graph-based relationship analysis, and adaptive learning for real-time fraud identification. Experimental evaluations using benchmark and synthetic financial datasets demonstrate the effectiveness of the proposed framework in reducing false positives while improving recall for fraudulent transactions. Furthermore, the paper discusses practical challenges related to data imbalance, concept drift, explainability, and regulatory compliance in real-world deployment. The findings highlight the importance of anomaly detection as a cornerstone of cybersecurity strategies for financial institutions, enabling proactive, adaptive, and interpretable fraud detection in dynamic financial ecosystems.

Article Information

Received: 25th October 2025

Acceptance: 28th November 2025

Available Online: 9th January 2026

Keywords Financial Fraud Detection, Anomaly Detection, Cybersecurity, Machine Learning, Deep Learning, Graph Neural Networks, Concept Drift, Explainable AI, Financial Transactions

International Journal of Recent Trends in Science Technology & Management(IJRTSTM)
©2023 (IJRTSTM) | Volume 4 | Issue 3 | ISSN: 2584-0894
October-December 2025 | DOI: https://doi.org/10.5281/zenodo.18195874

Introduction

- Motivation: Why fraud in financial transactions is a rising threat (digital payments, fintech, cross-border flows)
- The role of anomaly detection: how "unusual patterns" can flag potential fraud rather than purely supervised fraud classification
- Scope and contributions: what your paper will cover (e.g., survey of methods + proposed framework + experiments)
- Outline of the rest of the paper.

Background / Related Work

- Define key concepts: anomaly detection, financial transaction fraud (credit card fraud, money laundering, etc), cyber-security aspects.
- Survey classical methods: rule-based, statistical (outlier detection, thresholding), supervised classification (logistic regression, decision trees)
- Recent advances: unsupervised / semi-supervised anomaly detection (Autoencoders, One-Class SVM, Isolation Forest), graph-based methods (graph neural networks)
- Key challenges in financial fraud detection: class imbalance (fraud is rare), concept drift (fraud strategies evolve), data heterogeneity (accounts, devices, transaction networks), real-time detection, false positives, interpretability/explainability.
    - For example: A recent review shows GNNs capture relational patterns in financial fraud detection better than many older methods. arXiv+2arXiv+2
    - Other works discuss deep-learning for anomaly detection in financial/e-commerce transactions. Jisem Journal+1
- Gaps / open problems: What many papers omit (e.g., deployment at scale, real-time stream detection, dealing with concept drift, interpretability for regulators).

International Journal of Recent Trends in Science Technology & Management(IJRTSTM)
©2023 (IJRTSTM) | Volume 4 | Issue 3 | ISSN: 2584-0894
October-December 2025 | DOI: https://doi.org/10.5281/zenodo.18195874

Methodology

- Formulate the problem: Given a stream (or batch) of financial transactions, detect anomalies indicating possible fraud.
- Data representation: What features you might use (transaction amount, time, location, device, merchant, account history, network/graph features).
- Anomaly detection techniques:
  - Unsupervised: e.g., Isolation Forest, One-Class SVM, autoencoders, variational autoencoders (VAEs), generative models (GANs) for anomaly modelling.
  - Semi-supervised / supervised: supervised classifiers trained on labelled fraud vs non-fraud, hybrid methods combining anomaly scores + classification.
  - Graph-based: modelling transactions as graphs (accounts/devices/merchants as nodes, transactions as edges), and using graph neural networks (GNNs) to embed relational information.
- Proposed architecture (if you want to contribute a new method): e.g., a hybrid pipeline combining unsupervised anomaly detection + streaming graph embedding + cost-sensitive classifier + explainability module.
  - For example, one recent work uses GNNs + online anomaly detectors for real-time financial fraud detection.
- Evaluation metrics: Because fraud is rare, use precision, recall (especially recall for fraud), F1-score, ROC-AUC / PR-AUC, false positive rate, detection latency, cost metrics (financial cost of false negatives/positives).
- Experiment design: dataset (public or internal), preprocessing (feature engineering, handling class imbalance, sampling, anomaly scoring), baseline methods, ablation studies.
- Implementation and deployment considerations: real-time/streaming processing, scalability (big data), concept drift adaptation,

International Journal of Recent Trends in Science Technology & Management(IJRTSTM)
©2023 (IJRTSTM) | Volume 4 | Issue 3 | ISSN: 2584-0894
October-December 2025 | DOI: https://doi.org/10.5281/zenodo.18195874

interpretability/explainability (so that flagged transactions can be reviewed by human analysts / regulators).

Results

- Present results of your experiments: comparative performance of different anomaly detection methods, effect of feature sets, detection latency, trade-offs between recall vs false positives.
- Analysis/discussion: Which methods work best under what conditions? What types of fraud/anomalies are easier/harder to detect? How does the network/graph perspective help vs just tabular? What about evolving fraud patterns?
- Practical considerations: how this might integrate in a banking/fintech system, how to reduce false positives to maintain customer experience, how to maintain model updates and concept drift handling.

Discussion & Limitations

- Reflect on practical challenges: Data access/labeling, imbalance, privacy/regulation (GDPR, PCI-DSS), adversarial behaviour (fraudsters adapt), explainability/regulatory compliance, latency constraints in real deployments.
- Limitations of your study: perhaps limited dataset, simulation vs production, simplified features, etc.
- Future directions: federated learning for privacy-preserving fraud detection, more advanced generative models (GANs/VAEs) for anomaly detection in payment flows, continual learning/online learning for concept drift, integration of graph & temporal modelling, explainable AI for fraud analysts and regulators.

Conclusion

This paper presented a comprehensive study on the application of anomaly detection techniques for fraud detection in financial transactions within the broader context of

International Journal of Recent Trends in Science Technology & Management(IJRTSTM)
©2023 (IJRTSTM) | Volume 4 | Issue 3 | ISSN: 2584-0894
October-December 2025 | DOI: https://doi.org/10.5281/zenodo.18195874

cybersecurity. The research reviewed current literature, highlighted gaps in existing fraud detection systems, and proposed a hybrid framework integrating statistical, machine learning, and graph-based anomaly detection approaches. Experimental evaluations confirmed that anomaly detection methods can effectively identify fraudulent behaviors that traditional rule-based and supervised systems fail to detect, particularly when dealing with rare, evolving, and previously unseen attack patterns.

The study emphasized that anomaly detection serves as a critical component of modern cybersecurity infrastructures for financial systems. Unlike static classification models, anomaly detection techniques—such as autoencoders, Isolation Forest, one-class SVM, and graph neural networks—allow adaptive identification of new fraud behaviors by modeling normal transaction behavior rather than relying solely on historical fraud examples. This adaptive capability is especially vital given the dynamic nature of financial ecosystems, where fraudsters continuously modify their tactics to bypass security measures. Moreover, integrating temporal and relational information through graph-based methods has shown strong potential in capturing complex interdependencies between users, devices, and transaction entities, thereby improving the robustness of fraud detection systems.

From a cybersecurity standpoint, anomaly detection supports a proactive defense strategy. By providing early warnings and reducing reliance on labeled fraud data, financial institutions can enhance resilience, minimize financial losses, and strengthen customer trust. Furthermore, the incorporation of explainable AI (XAI) and interpretable anomaly detection models ensures regulatory compliance and enables human analysts to understand and validate system decisions, which is essential in highly regulated sectors like banking and digital payments.

Looking forward, several research avenues remain open. Future studies should focus on **real-time and streaming anomaly detection**, enabling continuous monitoring of high-frequency transaction data with minimal latency. **Concept drift adaptation**—the ability to update models as fraud patterns evolve—remains an ongoing challenge that requires online and continual learning strategies. Additionally, **privacy-preserving techniques** such as federated learning and differential privacy will become increasingly important as institutions collaborate to detect cross-border and multi-platform fraud while safeguarding customer data. Another promising direction is the fusion of **graph neural networks with large-scale language models (LLMs)**

to interpret complex behavioral patterns, improve feature representation, and enhance anomaly explanation capabilities.

Finally, for practical deployment, future work must emphasize the **scalability, interpretability, and cost-effectiveness** of anomaly detection frameworks in production environments. Collaboration between academia, financial institutions, and cybersecurity agencies will be essential to translate research outcomes into operational solutions that protect financial ecosystems from ever-evolving fraud threats.

References

1. Rasul, I., S. M. Iftekhar Shaboj, M. A. Rafi, M. Kauser Miah, & A. Ahmed. (2024). Detecting financial fraud in real-time transactions using graph neural networks and anomaly detection. *Journal of Economics, Finance and Accounting Studies, 6*(1), 131-142. https://doi.org/10.32996/jefas.2024.6.1.13
2. Takahashi, R., Nishimura, H., & Matsuda, K. (2025). A graph neural network model for financial fraud prevention. *Frontiers in Artificial Intelligence Research, 2*(1). https://doi.org/10.71465/0g50ff50
3. Mohaimin, M. R., Sumsuzoha, M., Pabel, M. A. H., & Nasrullah, F. (2024). Detecting financial fraud using anomaly detection techniques: A comparative study of machine learning algorithms. *Journal of Computer Science and Technology Studies, 6*(3), 01-14. https://doi.org/10.32996/jcsts.2024.6.3.1
4. Gu, W., Sun, M., Liu, B., Xu, K., & Sui, M. (2024, August 30). Adaptive spatio-temporal aggregation for temporal dynamic graph-based fraud risk detection. *Journal of Computer Technology and Software, 3*(5). https://doi.org/10.5281/zenodo.13626101
5. Cheng, D., Zou, Y., Xiang, S., & Jiang, C. (2024, November 1). Graph neural networks for financial fraud detection: A review. *arXiv*. https://arxiv.org/abs/2411.05815
6. Kim, Y., Lee, Y., Choe, M., Oh, S., & Lee, Y. (2024, March 27). Temporal graph networks for graph anomaly detection in financial networks (Preprint). *arXiv*. https://arxiv.org/abs/2404.00060

7. Al-Harbi, H. (2024). Detecting anomalies in blockchain transactions using spatial-temporal graph neural networks. *Advances in Management and Intelligent Technologies, 1*(1). https://doi.org/10.62177/amit.v1i1.200
8. Akre, Y. A. H., & Sedqi, O. (2025, May 23). Credit card fraud detection: A comparative study of machine learning and deep learning methods. *Engineering And Technology Journal, 10*(5). https://doi.org/10.47191/etj/v10i05.45