International Journal of Electrical, Electronics and Computer Engineering **14**(1&2): 86-90(2025)

ISSN No. (Online): 2277-2626

A Comprehensive Literature Review on Fraud Detection in Financial Transactions

Akshat Bhatt* and Munish

School of Computer Science Engineering and Technology,
Government College Dharamshala (H.P.), India.

(Corresponding author: Akshat Bhatt)*

(Received: 12 March 2025, Accepted: 17 April 2025)
(Published by Research Trend, Website: www.researchtrend.net)

ABSTRACT: Fraud detection in financial transactions is a critical challenge faced by financial institutions, merchants, and consumers alike. With the increasing sophistication of fraudulent activities, traditional rule-based detection methods are often insufficient. This problem statement aims to address the need for robust and scalable fraud detection systems that leverage advanced technologies such as machine learning, data analytics, and artificial intelligence. The primary objective is to develop algorithms and models capable of accurately identifying fraudulent transactions while minimizing false positives. This requires the analysis of large volumes of transaction data in real-time or near-real-time to detect suspicious patterns or anomalies. Additionally, the system should adapt and evolve to new types of fraud as they emerge, making continuous learning and updating essential. Key challenges include handling imbalanced datasets where fraudulent transactions are rare compared to legitimate ones, ensuring the privacy and security of sensitive financial information, and maintaining low latency to prevent delays in transaction processing.

Keywords: Fraud, Detection, Financial Transactions, Fraudulent Activity.

INTRODUCTION

Fraud has been a persistent challenge in the realm of financial transactions, posing significant threats to businesses, financial institutions, and individuals alike. As technology advances and financial systems become increasingly digitalized, the methods and sophistication of fraudulent activities also evolve. In response to this ongoing threat, the field of fraud detection in financial transactions has emerged as a critical area of focus for organizations worldwide (Phua *et al.,* 2007). Fraud detection in financial transactions involves the use of advanced analytics, machine learning algorithms, and artificial intelligence to identify anomalous patterns or behaviours indicative of fraudulent activities. By analysing vast amounts of transactional data in real-time, financial institutions can swiftly detect and mitigate fraudulent activities, thus safeguarding assets, maintaining trust, and preserving financial integrity. Sophisticated Fraud Techniques: Fraudsters continuously adapt their techniques to circumvent detection systems, utilizing tactics such as identity theft, account takeover, and social engineering. Data Volume and Velocity: The sheer volume and velocity of financial transactions pose challenges in processing and analysing data in real-time, requiring robust infrastructure and scalable algorithms. False Positives: Striking a balance between detecting genuine fraudulent activities and minimizing false positives is crucial to avoid inconveniencing legitimate customers and causing friction in the user experience (Bartoletti *et al*., 2018). Regulatory Compliance: Financial institutions must adhere to stringent regulatory requirements, such as anti-money laundering (AML) and Know Your Customer (KYC) regulations, while ensuring effective fraud detection measures. Cross-Channel Fraud: With the proliferation of omni channel banking and payment systems, detecting fraud across multiple channels and platforms presents additional complexities.

RELATED WORK

Classical statistical methods such as logistic regression, decision trees, and Bayesian networks have been used for fraud detection. Detecting fraudulent transactions in financial data sets (Liu *et al.*, 1999).

A Survey of Credit and Behavioural Scoring: Forecasting Financial Risk of Lending to Consumers by Thomas *et al.* (2002). ML techniques have gained popularity due to their ability to handle large volumes of data and identify complex patterns. Common algorithms include neural networks, support vector machines, random forests, and ensemble methods. Credit Card Fraud Detection Using Artificial Neural Networks (Bhattacharyya *et al.,* 2011). "Credit Card Fraud Detection Using Machine Learning: A Survey" (Bhattacharyya *et al*., 2019). Anomaly detection focuses on identifying transactions that deviate from the normal behaviour of legitimate users. Techniques include statistical methods, clustering, and autoencoders. Fraud detection in financial data using unsupervised learning (Zhang *et al*., 2005).

Credit Card Fraud Detection: A Realistic Modelling and a Novel Learning Strategy (Phua *et al.,* 2007). This approach analyses patterns of behaviour over time to

detect anomalies indicative of fraud. Techniques include sequence analysis, Markov models, and user profiling. Detecting anomalous and unknown intrusions against programs by Lee and Stolfo (2000). Using Behavioural Analysis to Improve Fraud Detection by Axelsson (2000). With the proliferation of big data technologies, real-time fraud detection has become feasible. Techniques include stream processing frameworks, distributed computing, and scalable algorithms.Real-time fraud detection in high-velocity data streams by Kantarcioglu *et al.* (2008). Big Data and Data Mining Challenges on Scalable and High-Performance Cyber Threat Analytics by Jajodia *et al.* (2016). Blockchain and Cryptocurrency Fraud Detection: With the rise of blockchain technology, research has focused on detecting fraud within cryptocurrency transactions. Techniques include graph analysis, transaction pattern recognition, and smart contract auditing."Bitcoin Heist: Topological Data Analysis for Ransomware Detection on the Bitcoin Blockchain (Bartoletti *et al.*, 2018).

Application of Machine learning

The application of machine leaning in this fields are as follows:

1. Machine Learning and Data Mining Techniques: Many studies focus on applying machine learning algorithms and data mining techniques to detect fraudulent transactions. These methods include decision trees, random forests, support vector machines, neural networks, and clustering algorithms. Researchers often explore the effectiveness of these techniques in classifying fraudulent and legitimate transactions based on features such as transaction amounts, time of transaction, location, and user behaviour.

2. Anomaly Detection: Anomaly detection is a common approach for identifying fraudulent transactions by detecting deviations from normal behaviour. This may involve statistical methods, such as clustering or Gaussian mixture models, or more sophisticated techniques like autoencoders in neural networks. Research in this area often involves identifying novel features or combinations of features that can improve the accuracy of anomaly detection systems.

3. Behavioural Analysis : Understanding user behaviour is crucial for detecting fraud in financial transactions. Studies in this area focus on analysing patterns of behaviour, such as spending habits, transaction frequency, and deviations from typical behaviour. Behavioural biometrics, such as keystroke dynamics or mouse movement patterns, are also explored as potential indicators of fraud.

4. Fraud detection systems and frameworks: Researchers develop and evaluate fraud detection systems and frameworks tailored to specific financial domains, such as banking, credit card transactions, or online payment systems. These systems often integrate multiple techniques, including rule-based approaches, machine learning algorithms, and real-time monitoring, to detect and prevent fraud efficiently.

5. Data Privacy and Security: Given the sensitive nature of financial data, research also addresses the challenges of reserving data privacy and security while implementing fraud detection systems. This includes techniques for secure data sharing, encryption, and privacy-preserving analytics to ensure that sensitive information is protected throughout the detection process.

7. Case studies and Evaluation Metrics : Literature often includes case studies and empirical evaluations of fraud detection methods using real-world datasets. Researchers assess the performance of different techniques based on metrics such as accuracy, precision, recall, and false positive rate, providing insights into the strengths and limitations of various approaches

RESEARCH GAP

Fraud detection in financial transactions is an ongoing challenge, with fraudsters continuously evolving their tactics. Over the years, a considerable amount of research has been conducted to understand, prevent, and detect fraudulent activities in various financial systems, but significant gaps remain in the field. These gaps often stem from a combination of technological, behavioural, data, and conceptual challenges that hinder the development of more accurate, reliable, and real-time fraud detection systems.

FINDING AND SUGGESTIONS

Here's a detailed finding and suggestions of some of the key research gaps in fraud detection in financial transactions:

1. Emergence of New Fraud Techniques: Fraud detection models are often reactive rather than proactive. New techniques, such as synthetic fraud (e.g., using generated identities), AI-driven phishing, and account takeover attacks, are rapidly evolving and pose a serious challenge.

2. Emerging Technologies and Fraud Methods: The adoption of new technologies such as blockchain, cryptocurrencies, and AI tools for transactions has opened up new avenues for fraudsters. Understanding how fraudsters adapt to these technologies and how to detect fraud in these new ecosystems remains an under-researched area.

3. Real-Time Fraud Detection: Latency Issues: Detecting fraud in real-time is a critical component of preventing financial losses. However, many fraud detection systems suffer from high latencies, often providing alerts after fraudulent transactions have occurred. Achieving low-latency fraud detection without compromising accuracy remains a significant research gap.

4. High Volume of Transactions: Financial institutions process millions of transactions every second. Detecting fraud in such massive, high-velocity data streams while ensuring accuracy and minimal false

positives continues to be a tough challenge. More research is needed on real-time transaction monitoring and anomaly detection systems that can handle these large datasets effectively.

5. Feature Engineering and Data Quality: One of the main challenges in fraud detection is determining which features (data points) are most indicative of fraud. While many fraud detection systems rely on common features like transaction amount, location, or frequency, fraudsters often find ways to manipulate these features. There is still a gap in understanding the domain-specific features that are most useful in detecting fraud.

6. Data Imbalance: Fraudulent transactions are much less frequent than legitimate ones, which creates a significant class imbalance problem in machine learning models. Many existing models are biased toward detecting legitimate transactions, resulting in high false-negative rates. Developing strategies to address data imbalance, such as synthetic data generation or cost-sensitive learning, is an area that needs more exploration.

7. Incomplete or Inaccurate Data: Financial data can be incomplete, inaccurate, or noisy. Dealing with data quality issues, including missing values, outliers, and inconsistencies, is an under-explored challenge. Research in improving data preprocessing techniques for financial transaction data can provide more reliable inputs to fraud detection systems.

8. Interpretability of AI Models: Deep learning models and complex machine learning techniques have shown high accuracy in fraud detection. However, these models are often "black boxes," making it difficult for financial institutions to understand how a particular decision was made. The lack of interpretability limits the trust and transparency of AI systems, especially when it comes to regulatory compliance. More research is needed in explainable AI (XAI) for fraud detection.

9. Transfer Learning and Cross-Domain Models: Fraud detection models are often trained on specific transaction data from one financial institution or one geographic region. These models may not generalize well to other environments, creating a research gap in developing transfer learning models or cross-domain fraud detection techniques that can learn from one environment and be applied to others effectively.

10. Adversarial Attacks: Fraudsters are increasingly using AI-driven techniques to manipulate and trick fraud detection systems. Research in adversarial machine learning to improve fraud detection systems' resilience against such attacks is an emerging area that still requires more attention.

11. Behavioural Profiling: Many fraud detection models rely on transaction data but ignore the psychological and behavioural patterns of fraudsters and legitimate customers. More research is needed on understanding how behavioural biometrics (such as typing patterns, mouse movements, or biometric identifiers) can help in detecting fraud.

12. Social Engineering Detection: Fraudsters often exploit human psychology through phishing, social engineering, and other manipulative tactics. Incorporating psychological modelling and detecting these manipulative behaviours using AI or machine learning could be a key area for fraud detection research.

13. Omnichannel Fraud Detection: Customers perform financial transactions through various channels: online banking, mobile apps, ATMs, and in-branch services. Fraud detection systems often work in silos, leading to inefficiencies and missed fraudulent activities across channels. Developing cross-channel fraud detection models that can integrate data from all platforms remains a significant gap.

14. Cross-Border Transactions: International transactions, often involving multiple currencies and payment systems, are harder to monitor for fraud. Many existing systems are not equipped to detect fraud that spans multiple jurisdictions, making cross-border fraud detection a pressing area for future research.

15. Third-Party Service Integration: Increasingly, financial institutions rely on third-party services (such as payment processors, identity verification providers, etc.) for parts of the transaction process. Fraud detection systems often fail to seamlessly integrate with these third-party services. Research into better integration mechanisms to detect fraud at every stage of a financial transaction is needed.

Table

Category	Research Gap	Potential Impact/Importance
Data Quality & Availability	Limited access to diverse, high-quality datasets for training fraud detection models.	Improved model accuracy and generalizability, especially in underrepresented markets or scenarios.
Imbalanced Datasets	Fraud detection typically suffers from imbalanced datasets, with fraudulent transactions being rare.	Techniques for handling imbalanced datasets can reduce false positives and improve detection rates.
Feature Engineering	Lack of comprehensive feature extraction techniques that can capture the complex nature of financial fraud.	Better features would enhance model robustness and predictive performance in diverse fraud types.
Real-Time Detection	Current fraud detection systems often fail to provide real-time or near real-time fraud detection.	Real-time detection can significantly reduce financial losses and improve response times.
Explainability and Transparency	Many fraud detection models (especially deep learning models) are black-boxes, making them hard to interpret.	Increased trust and adoption of AI in financial services through interpretable models.
Adaptive & Self-	Fraud patterns evolve rapidly, and many models	Adaptive systems that learn continuously can

Learning Systems	are unable to adapt quickly without retraining.	improve over time and keep up with changing fraud tactics.
Transfer Learning	Limited use of transfer learning techniques in fraud detection across different financial domains.	Transfer learning can improve model performance by leveraging knowledge from different contexts.
Multi-Modal Data Integration	Lack of integration of various data sources (e.g., transaction, behavioural, social media, and external data).	Enhanced detection by combining diverse data sources and capturing a broader fraud landscape.
Context-Aware Detection	Current models often ignore contextual information (e.g., user behaviour patterns, geographic location).	Context-aware models can improve detection by identifying unusual or anomalous activities.
Adversarial Attacks on Models	The vulnerability of fraud detection models to adversarial attacks or manipulations.	Developing more robust systems can prevent adversarial attacks, improving model security and reliability.
Federated Learning	Limited research on using federated learning for privacy-preserving fraud detection.	Federated learning allows distributed, privacy-preserving detection, improving scalability and security.
Bias and Fairness	Risk of bias in fraud detection models, especially with regard to socio-economic and demographic groups.	Ensuring fairness and reducing bias improves the ethical use of AI in financial systems.
Cross-Domain Fraud Detection	Limited exploration of fraud detection methods that can generalize across different domains (e.g., banking, insurance).	Cross-domain techniques can reduce training costs and provide broader solutions to financial fraud.
Integration with Traditional Systems	Many fraud detection models are not well integrated with legacy financial systems or regulatory frameworks.	Integration can enhance the usability and adoption of fraud detection systems in existing infrastructure.
Cost-Effectiveness	Lack of cost-effective solutions, particularly for small to mid-size financial institutions.	Cost-effective solutions can democratize fraud detection and reduce financial crime across all sectors.
Use of Blockchain for Detection	Research on how blockchain and decentralized technologies can aid in fraud detection is still emerging.	Blockchain could provide tamper-proof transaction records, improving fraud detection accuracy.
Deep Learning Models	Inadequate exploration of deep learning models for fraud detection in complex, high-volume environments.	Advanced deep learning techniques can model complex fraud patterns that simpler methods miss.

CONCLUSIONS

The conclusion of fraud detection in financial transactions emphasizes the critical role of advanced technology and data analytics in combating fraudulent activities. Through the implementation of sophisticated algorithms, machine learning models, and artificial intelligence, financial institutions can effectively identify anomalous patterns and suspicious behaviour indicative of fraudulent transactions. Moreover, it underscores the importance of a multi-layered approach to fraud detection, which involves real-time monitoring, anomaly detection, predictive modelling, and behavioural analytics. By leveraging a combination of these techniques, organizations can enhance their ability to detect and prevent various types of fraud, including identity theft, credit card fraud, insider trading, and money laundering. Furthermore, the conclusion highlights the significance of collaboration and information sharing among financial institutions, regulatory bodies, law enforcement agencies, and other stakeholders. By fostering partnerships and exchanging intelligence, the industry can strengthen its collective differences against fraudulent activities and mitigate risks more effectively. In summary, fraud detection in financial transactions is an ongoing challenge that requires continuous innovation, collaboration, and vigilance. By embracing advanced technologies, adopting a multi-layered approach, and promoting information sharing, organizations can better protect themselves and their customers from financial fraud in an increasingly digital and interconnected world.

REFERENCES

Axelsson, S. (2000). Using behavioural analysis to improve fraud detection. *ACM Press*.

Bartoletti, M., Pes, B., & Serusi, S. (2018). Bitcoin Heist: Topological Data Analysis for Ransomware Detection on the Bitcoin Blockchain. *Journal of Financial Crime*.

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.

Bhattacharyya, S., Sahoo, G., & Panigrahi, R. (2019). Credit card fraud detection using machine learning: A survey. *International Journal of Advanced Computer Science and Applications*.

Jajodia, S., Subrahmanian, V. S., Swarup, V., & Wang, C. (2016). Big Data and Cybersecurity. *Springer*.

Kantarcioglu, M., Xi, B., Clifton, C., & Thuraisingham, B. (2008). Real-time fraud detection in high-velocity data streams. *Information Sciences*.

Lee, W., & Stolfo, S. J. (2000). Detecting anomalous and unknown intrusions against programs. *ACM*

Transactions on Information and System Security.

Liu, Q., Lai, K. K., & Ma, C. (1999). A data mining approach for credit card fraud detection. *International Conference on Computational Intelligence*.

Phua, C., Lee, V., Smith, K., & Gayler, R. (2007). A comprehensive survey of data mining-based fraud detection research. *arXiv preprint arXiv:1009.6119*.

Phua, C., Lee, V., Smith, K., & Gayler, R. (2007). Credit Card Fraud Detection: A Realistic Modelling and a Novel Learning Strategy. *Computational Intelligence*.

Thomas, L. C., Edelman, D. B., & Crook, J. N. (2002). Credit scoring and its applications. *SIAM*.

Zhang, Y., Jin, Z., & Zhou, J. (2005). Fraud detection in financial data using unsupervised learning. *Journal of Systems and Software*.