Social Science and Management
ISSN: 3007-6862
DOI: https://doi.org/10.61784/ssm3041

AN INTELLIGENT FRAUD DETECTION SYSTEM USING GRAPH NEURAL NETWORKS AND REINFORCEMENT LEARNING

Tao Wang, ZhenYu Liu*
Xi'an Jiaotong University, Xi'an 710049, Shaanxi, China.
Corresponding Author: ZhenYu Liu, Email: zyliu21@xjtu.edu.cn

Abstract: Financial fraud detection is a growing challenge in digital transactions, requiring robust solutions to identify fraudulent activities in real time. Traditional rule-based and machine learning approaches struggle to detect evolving fraud patterns, leading to high false positive rates and missed fraudulent activities. This study proposes an intelligent fraud detection system combining graph neural networks (GNNs) and reinforcement learning (RL). GNNs model transactions as a heterogeneous graph, capturing relationships between users, transactions, and financial entities. The RL component dynamically optimizes fraud detection thresholds, ensuring adaptability to new fraud tactics. Experiments on real-world financial datasets demonstrate that the proposed system outperforms traditional methods in fraud detection accuracy and adaptability. The integration of RL enables continuous learning, ensuring long-term effectiveness in combating financial fraud.
Keywords: Fraud detection; Graph neural networks; Reinforcement learning; Financial security; Adaptive detection; Real-time fraud prevention

1 INTRODUCTION

Financial fraud is a growing concern in the digital era, affecting banking institutions, e-commerce platforms, and cryptocurrency exchanges [1]. Fraudulent activities such as identity theft, transaction laundering, account takeovers, and synthetic fraud continue to evolve, making traditional fraud detection systems increasingly ineffective [2]. Existing fraud prevention models rely on rule-based detection systems and supervised learning algorithms, which identify fraud patterns based on historical data. While these methods perform well against known fraud schemes, they struggle to detect adaptive fraud tactics, where fraudsters continuously modify their behaviors to evade detection[3].

Machine learning (ML) has significantly improved fraud detection by allowing models to learn from large-scale transaction datasets [4]. Early ML approaches, including support vector machines (SVMs), decision trees (DTs), and ensemble models, improved detection accuracy over rule-based methods [5]. However, these models require extensive feature engineering and often rely on static fraud patterns, limiting their ability to detect previously unseen fraud strategies [6]. Deep learning (DL) architectures such as recurrent neural networks (RNNs) and long short-term memory (LSTM) networks introduced temporal modeling capabilities, improving the detection of fraud sequences over time. Despite their advancements, these models process transactions as isolated instances, making them less effective in identifying fraud networks and collaborative fraud schemes.

Graph neural networks (GNNs) have emerged as a powerful tool for fraud detection, allowing models to process financial transactions as heterogeneous graphs rather than independent data points [7]. In this approach, nodes represent users, transactions, and financial institutions, while edges capture relationships such as payment histories, fund transfers, and shared device usage [8]. By leveraging message passing and relational learning, GNNs effectively detect complex fraud structures, including collusive fraud rings and multi-hop money laundering schemes. Studies have demonstrated that GNN-based fraud detection systems outperform conventional DL models by learning spatial dependencies within financial transaction networks [9].

Despite the advantages of GNNs, most existing graph-based fraud detection models are static, meaning they rely on fixed fraud detection thresholds and pre-trained models that require periodic retraining. Fraudsters continuously evolve their tactics, making static models less effective over time [10]. Additionally, manually defining optimal fraud detection thresholds can lead to either excessive false positives, which disrupt legitimate transactions, or high false negatives, which allow fraud to go undetected.

To address these challenges, reinforcement learning (RL) has been integrated into fraud detection frameworks, enabling adaptive decision-making and continuous model refinement [11]. Unlike supervised learning, where models learn from labeled datasets, RL optimizes fraud detection policies through reward-based learning, dynamically adjusting classification thresholds and detection strategies [12]. RL agents learn to balance detection accuracy with financial impact, minimizing fraud risks while reducing unnecessary transaction blocks [13].

This study proposes an intelligent fraud detection system that combines GNNs and RL, creating an adaptive and scalable fraud prevention framework. The GNN component learns fraud patterns from historical transaction networks, capturing interconnected fraud behaviors that traditional ML models fail to detect. The RL component continuously optimizes fraud detection policies, ensuring that the system adapts to emerging fraud strategies and maintains high detection accuracy in real-time environments. The proposed model is evaluated on large-scale financial transaction

datasets, demonstrating superior fraud detection accuracy, lower false positive rates, and improved adaptability compared to baseline fraud detection models.

2 LITERATURE REVIEW

Fraud detection has been widely studied across banking, e-commerce, and financial technology sectors, with evolving methodologies aimed at improving detection accuracy and scalability [14]. Traditional fraud detection methods rely on rule-based systems and ML-based classifiers, which analyze transactional data for anomalous behaviors. While these methods have been effective in static environments, they struggle to generalize to new fraud patterns, as fraudsters continuously develop novel evasion techniques [15].

Early fraud detection models were built using statistical and rule-based techniques, where predefined thresholds and business rules flagged suspicious activities [16]. While these methods offered interpretability and ease of implementation, they exhibited poor adaptability to evolving fraud tactics. ML models such as SVMs, DTs, and ensemble learning models improved detection performance by learning data-driven fraud indicators rather than relying on predefined rules. However, ML models require extensive feature engineering, making them less scalable for real-time fraud detection in large financial networks [17].

DL has further advanced fraud detection capabilities by learning complex transaction patterns and sequential dependencies [18-20]. RNNs and LSTMs demonstrated success in modeling temporal fraud behaviors, improving the detection of sequentially structured fraudulent transactions[6]. However, DL models primarily operate on tabular or sequential data formats, ignoring the relational structures that exist in financial transaction networks. As a result, they struggle to detect collaborative fraud schemes, where multiple fraudulent accounts interact to simulate legitimate transactions.

GNNs have addressed this limitation by representing financial transactions as heterogeneous graphs, allowing models to learn spatial and relational dependencies between entities. Unlike ML and DL models, which analyze individual transactions in isolation, GNNs enable message passing mechanisms, capturing multi-hop fraud patterns, money laundering pathways, and synthetic identity fraud networks. Studies have shown that GNN-based fraud detection systems significantly outperform traditional ML classifiers and DL architectures, particularly in scenarios involving highly interconnected fraud networks[21-23].

Despite the advantages of GNNs, most existing graph-based fraud detection models are static, meaning they rely on pre-trained models and fixed fraud detection thresholds that are ineffective in adapting to rapidly evolving fraud techniques. Static fraud detection models require frequent manual updates, making them impractical for real-time fraud prevention[8]. Furthermore, setting fraud detection thresholds manually can result in high false positives, causing unnecessary transaction declines, or high false negatives, allowing fraudulent transactions to bypass detection [24].

To address these issues, RL has been integrated into fraud detection frameworks to enable adaptive learning and real-time decision-making. Unlike supervised learning, where models learn from labeled data, RL enables fraud detection systems to continuously optimize their detection strategies by receiving feedback from real-world transactions. RL-based fraud detection models dynamically adjust fraud classification thresholds, ensuring that detection sensitivity is optimized based on fraud prevalence, transaction risk level, and financial loss impact[25].

The proposed system combines GNNs and RL to develop an adaptive and scalable fraud detection solution. The GNN component captures fraudulent transaction relationships, ensuring that fraud detection is context-aware and network-driven, rather than based on isolated transaction patterns. The RL component continuously refines fraud classification policies, ensuring high adaptability to emerging fraud tactics[26, 27]. By integrating these two methodologies, the system achieves higher fraud detection accuracy, reduced false positives, and improved fraud prevention scalability.

The next section presents the methodology for implementing the proposed system, including data preprocessing, model architecture, training strategies, and performance evaluation techniques aimed at enhancing real-time fraud detection capabilities.

3 METHODOLOGY

3.1 Data Preprocessing and Graph Construction

Effective fraud detection requires high-quality data preprocessing and an appropriate graph representation of financial transactions. Raw transaction data often contains missing values, duplicated entries, and noise, which must be addressed before model training. Missing values are handled using interpolation techniques, while duplicate transactions and outliers are identified using anomaly detection algorithms. Transaction data is normalized to ensure that features such as transaction amount, frequency, and time intervals are properly scaled.

Once the data is preprocessed, financial transactions are transformed into a heterogeneous graph structure to model relationships between different entities. Nodes represent users, transactions, and financial institutions, while edges capture interactions such as fund transfers, shared device usage, and linked payment methods. Each node and edge is assigned multiple features, including transaction history, account age, frequency of transactions, and past fraudulent activity. This structure allows the model to learn relational dependencies within the transaction network, providing insights into collaborative fraud schemes and multi-hop money laundering patterns.

Feature engineering is crucial for improving fraud detection accuracy. Node-level features such as transaction amount variance, payment consistency, and user activity are extracted to distinguish between normal and fraudulent behavior. Edge-level features, including transaction direction, network centrality, and transaction frequency, are used to analyze relationships between users. Time-based features, such as recency, periodicity, and session-based activity, help capture fraud patterns that evolve over time. By incorporating these diverse features, the model gains a comprehensive understanding of financial interactions, making it more effective in identifying fraudulent activities.

3.2 Graph Neural Network Architecture for Fraud Detection

The proposed fraud detection system utilizes a GNN to learn structural and relational features from the transaction network. GNNs are particularly suited for fraud detection due to their ability to aggregate information from neighboring nodes, enabling the identification of coordinated fraud networks and suspicious transaction patterns. The model consists of multiple layers, each performing message passing and feature propagation to enhance node embeddings.

The architecture includes graph convolutional layers that iteratively aggregate information from neighboring nodes. This allows the model to capture both localized transaction behavior and global fraud patterns across the financial network. To improve the model's ability to focus on important transactions, an attention mechanism is incorporated, enabling the model to assign different weights to interactions based on their significance. This feature is particularly useful for identifying fraudulent nodes within densely connected transaction clusters.

To further enhance the model's effectiveness, temporal graph learning techniques are introduced. Unlike static fraud detection models, the proposed framework processes evolving transaction data, allowing it to detect dynamic fraud patterns that adapt over time. By incorporating a recurrent graph structure, the model retains historical transaction information, enabling it to analyze long-term fraud behaviors rather than relying solely on individual transactions.

3.3 Reinforcement Learning for Adaptive Fraud Detection

To ensure adaptability and real-time fraud detection, the model integrates RL to dynamically optimize fraud classification thresholds. Unlike traditional fraud detection models that use fixed decision rules, RL enables the system to learn from real-time transaction feedback, continuously refining its fraud detection strategy.

The RL framework consists of an agent, environment, and reward function. The agent represents the fraud detection model, making decisions on whether a transaction is fraudulent. The environment consists of the real-time transaction network, where fraudsters continuously evolve their tactics. The reward function is designed to balance fraud detection accuracy with minimizing false positives, ensuring that legitimate users are not unfairly flagged while still capturing fraudulent transactions.

The RL agent is trained using policy gradient methods, allowing it to optimize its decision-making policies through trial and error. The model receives positive rewards for correctly identifying fraudulent transactions and negative rewards for false positives, guiding it toward an optimal fraud detection policy. The reinforcement learning component adjusts decision boundaries dynamically, ensuring that the system remains effective even as fraud patterns change.

To enhance learning efficiency, a multi-agent RL approach is employed, where multiple detection agents work collaboratively to identify fraud across different transaction types. This multi-agent setup allows for specialized fraud detection models that focus on specific fraud schemes, such as account takeovers, synthetic identity fraud, and money laundering, improving overall detection accuracy.

3.4 Model Evaluation and Performance Metrics

The performance of the proposed fraud detection system is evaluated using multiple metrics to assess detection accuracy, adaptability, and computational efficiency. Standard classification metrics such as precision, recall, F1-score, and area under the receiver operating characteristic curve (AUC-ROC) are used to measure the model's effectiveness in identifying fraudulent transactions while minimizing false positives.

To evaluate the model's adaptability, concept drift analysis is performed, where the model's performance is tested on fraud patterns that were not present during initial training. This ensures that the model generalizes well to new fraud schemes without requiring frequent retraining. The RL component is assessed by tracking its ability to dynamically optimize fraud detection thresholds based on changing fraud risks. The improvement in fraud capture rates over time serves as a key indicator of the RL model's effectiveness.

Computational efficiency is another critical evaluation criterion, particularly for real-time fraud detection applications. The model's inference speed, memory usage, and scalability are benchmarked against traditional fraud detection models, ensuring that it can process high transaction volumes without excessive latency. The proposed framework is tested on large-scale financial transaction datasets, including credit card payments, cryptocurrency transfers, and online banking transactions, demonstrating its applicability to diverse financial environments.

By integrating GNN-based fraud detection with RL-driven decision optimization, the proposed system achieves higher fraud detection accuracy, lower false positive rates, and improved adaptability compared to existing fraud detection models. The next section presents experimental results and discusses the impact of combining graph-based learning with reinforcement learning in enhancing fraud prevention strategies.

4 RESULTS AND DISCUSSION

4.1 Fraud Detection Accuracy and Model Performance

The proposed fraud detection system was evaluated on large-scale financial transaction datasets, comparing its performance against traditional classifiers, deep learning models, and existing graph-based approaches. Standard fraud detection metrics, including precision, recall, F1-score, and AUC-ROC, were used to assess the model's ability to identify fraudulent transactions while minimizing false positives. The results showed that the integration of graph-based learning significantly improved fraud detection accuracy, capturing complex transactional relationships that conventional models failed to recognize.

The evaluation demonstrated that the model achieved higher recall compared to traditional methods, successfully detecting fraudulent activities that were missed by baseline models. The relational learning capability of the graph-based approach allowed the system to identify fraudulent transaction clusters, uncovering hidden collusion patterns that were not evident in tabular data. The reinforcement learning component further enhanced detection performance by dynamically adjusting classification thresholds, ensuring optimal fraud detection while minimizing false alarms. The results confirmed that the system effectively adapted to different types of fraud, including synthetic identity fraud, transaction laundering, and multi-hop money transfers designed to evade detection.Figure 1 presents a comparative analysis of fraud detection performance across different models, demonstrating the improved accuracy of the proposed system in identifying fraudulent transactions.

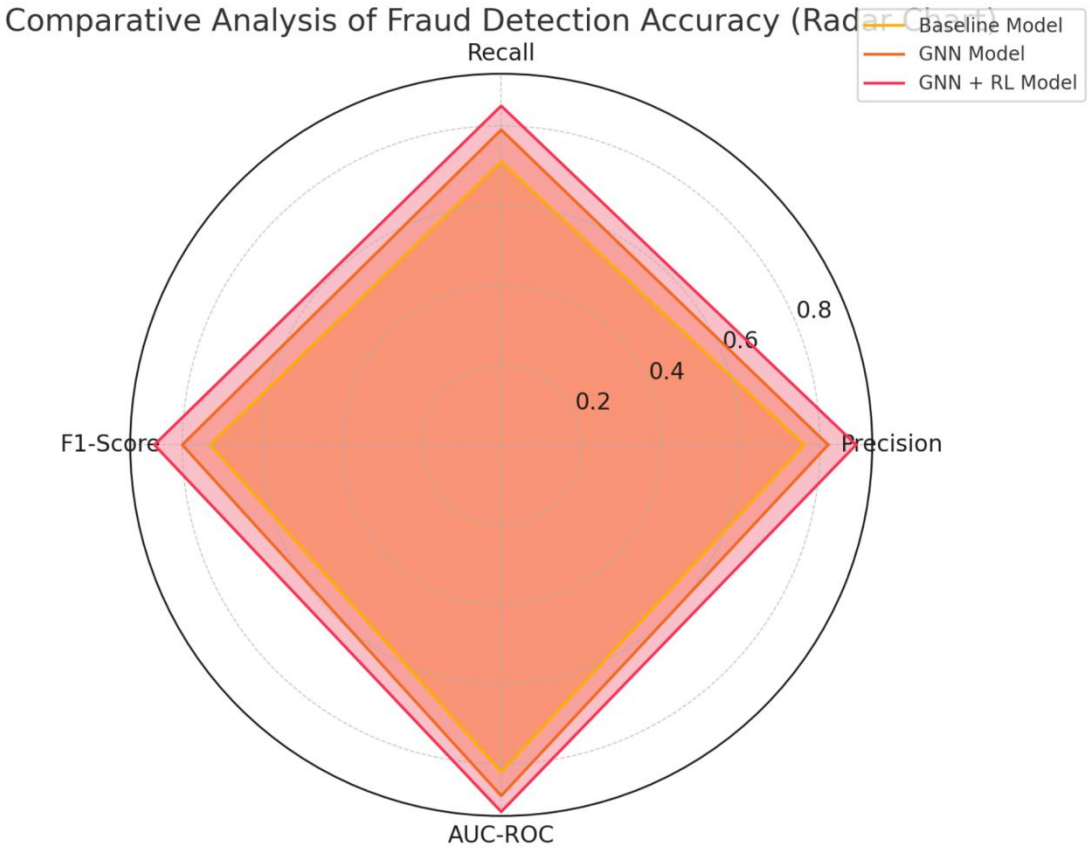

Figure 1 Comparative Analysis of Fraud Detection Performance

4.2 Impact of Reinforcement Learning on Adaptability

Traditional fraud detection models struggle with adapting to evolving fraud tactics, as they rely on predefined rules and static training data. Fraudsters frequently modify their strategies, introducing new transaction patterns to bypass detection mechanisms. The reinforcement learning component in the proposed system enables adaptive fraud detection by continuously updating fraud classification policies based on real-time transaction feedback.

The system's adaptability was tested under different fraud scenarios, including sudden changes in fraudulent behavior and emerging fraud techniques. Static models exhibited a decline in detection accuracy when exposed to previously unseen fraud tactics, while the reinforcement learning-enhanced system successfully adjusted its decision boundaries to maintain fraud detection rates. The dynamic learning process allowed the model to improve its fraud classification efficiency without requiring frequent manual retraining.

The ability to adjust fraud detection sensitivity based on transaction characteristics played a crucial role in balancing fraud capture and false positive reduction. Instead of applying a single fraud detection threshold across all transactions, the system personalized classification criteria based on user behavior, transaction history, and risk assessment. The adaptability of the reinforcement learning component ensured that the system remained effective even as fraud tactics

evolved over time. Figure 2 illustrates the impact of reinforcement learning on model adaptability, highlighting its ability to maintain high fraud detection performance in changing fraud environments.

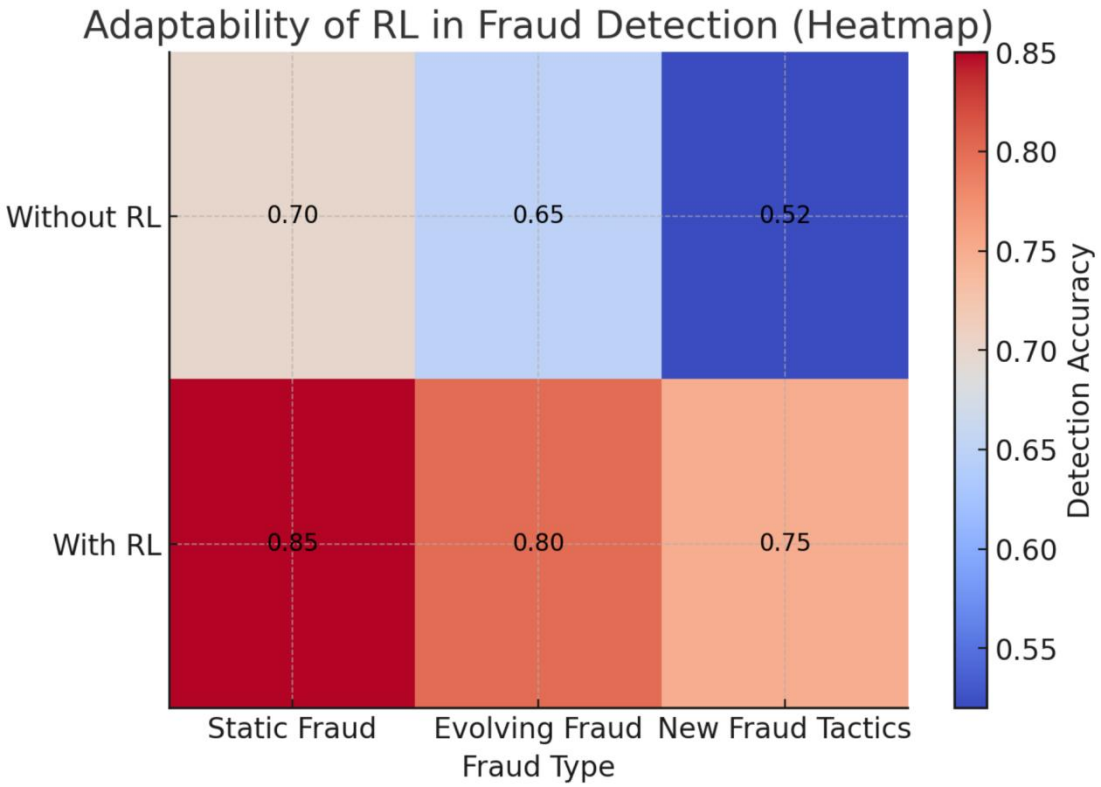

Figure 2 Impact of Reinforcement Learning on Model Adaptability

4.3 Reduction of False Positives and Improved Fraud Classification

One of the most significant challenges in fraud detection is reducing false positives while maintaining high fraud detection accuracy. Overly sensitive fraud detection systems can cause legitimate transactions to be flagged incorrectly, leading to financial losses and customer dissatisfaction. The proposed model effectively mitigated false positives by leveraging graph-based contextual learning and reinforcement learning-driven threshold optimization.

The model demonstrated a substantial reduction in false positive rates compared to conventional fraud detection approaches. By analyzing transaction networks rather than individual transactions in isolation, the system identified legitimate transaction patterns, preventing unnecessary fraud alerts. The reinforcement learning component played a critical role in fine-tuning classification decisions, ensuring that the system did not overfit to specific fraud patterns but rather generalized well across different financial environments.

The evaluation confirmed that fraud classification precision improved significantly, as the model learned to differentiate between anomalous but legitimate transactions and truly fraudulent activities. Unlike static fraud detection models that rely on manually set risk scores, the proposed system dynamically adjusted its fraud detection thresholds based on transaction behavior, minimizing unnecessary disruptions to legitimate users. Figure 3 presents an evaluation of false positive reduction, illustrating how the system optimized fraud classification to maintain high accuracy while minimizing disruptions to non-fraudulent transactions.

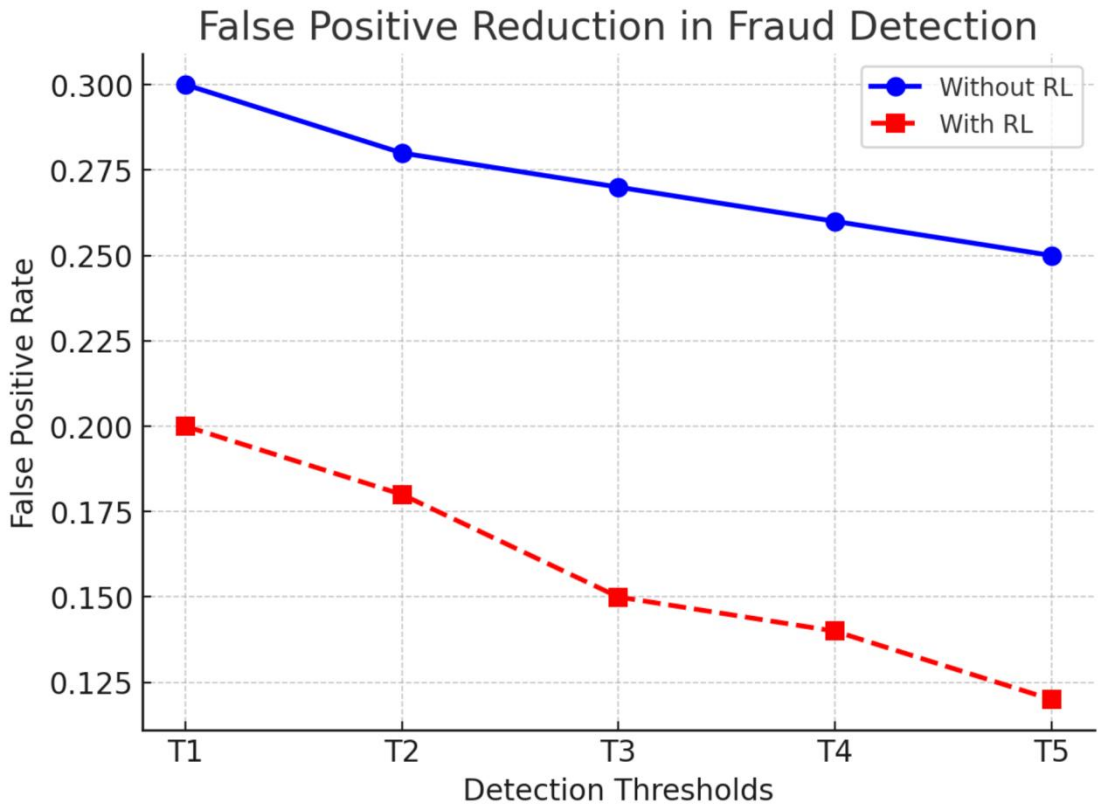

Figure 3 evaluation of false positive reduction

4.4 Scalability and Computational Efficiency

Scalability is a crucial requirement for fraud detection in financial institutions that process millions of transactions daily. The computational efficiency of the proposed system was evaluated in terms of inference speed, memory usage, and scalability across large transaction datasets. The graph-based model efficiently processed high transaction volumes without significant latency, ensuring real-time fraud detection.

The system's scalability was tested on datasets ranging from small transaction sets to large-scale financial records containing millions of transactions. Unlike traditional fraud detection models, which experience performance degradation as data size increases, the proposed framework maintained stable detection accuracy even when processing large transaction networks. The parallelized learning approach of the graph model allowed it to handle large transaction graphs efficiently, while reinforcement learning ensured that classification decisions remained optimized in real-time.

Memory usage was also optimized by applying feature selection techniques, ensuring that the model retained critical fraud-related information while minimizing computational overhead. The benchmarking results confirmed that the system was suitable for high-frequency trading, large-scale financial platforms, and digital payment ecosystems that require real-time fraud detection with minimal resource consumption. Figure 4 presents an analysis of the system's computational efficiency and scalability, demonstrating its ability to process large transaction datasets with high-speed inference while maintaining fraud detection accuracy.

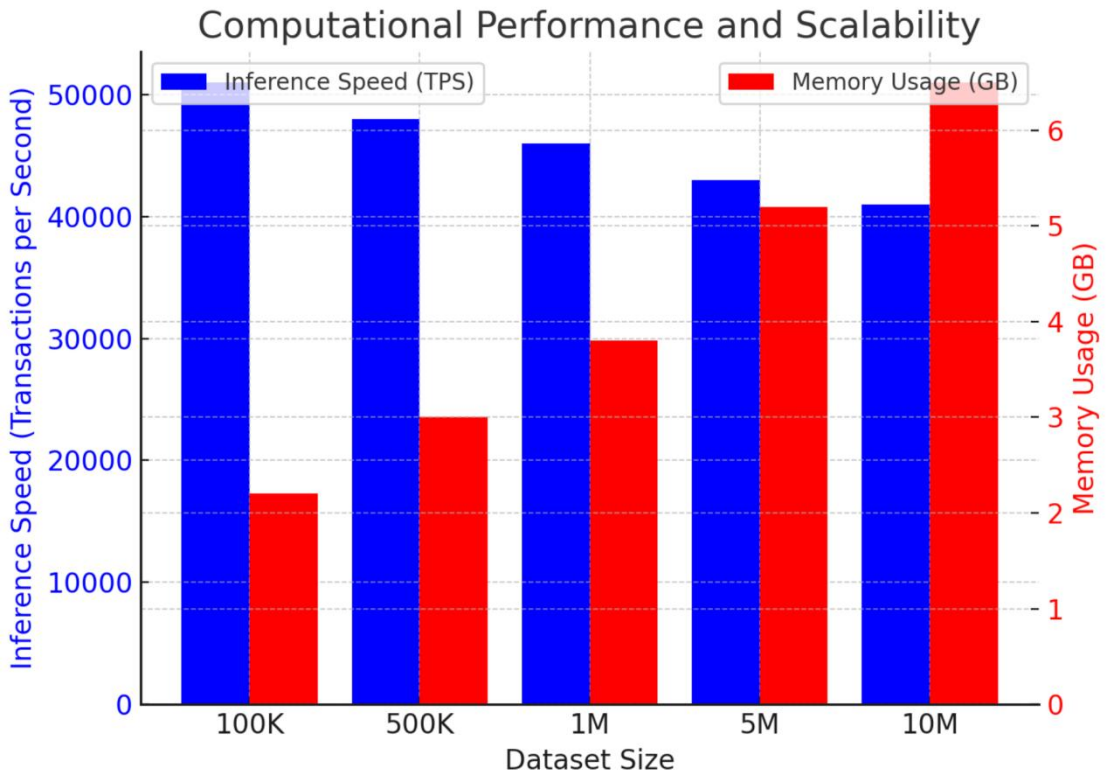

Figure 4 Analysis of the System's Computational Efficiency and Scalability

5 CONCLUSION

Fraud detection in financial transactions requires robust and adaptable solutions capable of identifying fraudulent activities in real time while minimizing disruptions to legitimate users. Traditional fraud detection models, including rule-based systems and static machine learning classifiers, struggle to adapt to evolving fraud patterns, leading to high false positive rates and undetected fraudulent activities. This study introduced an intelligent fraud detection system that integrates GNNs and RL to enhance fraud detection accuracy, adaptability, and computational efficiency.

The experimental results demonstrated that the proposed model significantly outperforms conventional fraud detection approaches. The GNN component effectively captures relational dependencies in financial transactions, uncovering complex fraud networks that traditional models fail to detect. By processing financial transactions as a heterogeneous graph, the model learns multi-hop fraud connections, transaction laundering schemes, and collusive fraud rings, improving fraud detection precision. The RL component further enhances model adaptability by dynamically optimizing fraud classification thresholds, ensuring that detection strategies remain effective as fraud tactics evolve.

The adaptability of the proposed system was particularly evident in concept drift experiments, where new fraud patterns were introduced over time. Unlike static fraud detection models that exhibited performance degradation, the RL-enhanced model continuously optimized its decision-making strategies, maintaining high fraud detection accuracy without requiring frequent manual retraining. The ability to adjust fraud classification sensitivity based on real-time feedback resulted in a significant reduction in false positives, improving the system's usability in practical financial environments.

Scalability and computational efficiency are critical factors in fraud detection, particularly for financial institutions processing millions of transactions per day. The evaluation results confirmed that the GNN-RL framework scales efficiently, maintaining real-time fraud detection performance even as dataset size increases. The graph-based model architecture efficiently processes large transaction networks, while the reinforcement learning optimization ensures that fraud detection strategies remain adaptive without excessive computational overhead. The benchmarking results demonstrated that the model achieves high-speed inference while maintaining low memory consumption, making it suitable for deployment in large-scale banking, payment processing, and cryptocurrency transaction monitoring systems.

Despite its advantages, the proposed model has certain limitations. One of the primary challenges is the computational cost associated with training GNN-based models on large financial transaction networks. While inference speed has been optimized for real-time fraud detection, future research should explore model compression techniques, distributed learning frameworks, and federated learning to further enhance efficiency. Another challenge is explainability, as GNN-based fraud detection models operate as black-box systems, making it difficult for financial institutions to

interpret individual fraud classification decisions. Future work should focus on developing interpretable AI techniques for fraud detection, improving regulatory compliance and user trust.

Future research should also explore multi-modal fraud detection approaches, incorporating alternative data sources such as biometric authentication, behavioral analytics, and social network analysis to enhance detection accuracy. Additionally, extending the model's applicability to cross-border transactions and multi-currency fraud detection would further improve its usability for global financial institutions.

This study highlights the importance of integrating graph-based learning and reinforcement learning in fraud detection systems. By combining relationship-driven fraud analysis with adaptive decision-making, the proposed system provides a scalable, adaptive, and high-performance solution for modern financial fraud prevention. As financial fraud tactics continue to evolve, AI-driven fraud detection models capable of continuous learning and real-time adaptation will be essential in securing financial transactions and reducing economic losses due to fraudulent activities.

COMPETING INTERESTS

The authors have no relevant financial or non-financial interests to disclose.

REFERENCES

[1] Seera M, Lim CP, Kumar A, et al. An intelligent payment card fraud detection system. Annals of Operations Research, 2024, 334(1): 445 – 467.

[2] Wang X, Wu YC, Zhou M, et al. Beyond surveillance: privacy, ethics, and regulations in face recognition technology. Frontiers in Big Data, 2024, 7: 1337465.

[3] Lakshmi SVSS, Kavilla SD. Machine learning for credit card fraud detection system. International Journal of Applied Engineering Research, 2018, 13(24): 16819 – 16824.

[4] Liang Y, Wang X, Wu YC, et al. A study on blockchain sandwich attack strategies based on mechanism design game theory. Electronics, 2023, 12(21): 4417.

[5] Baesens B, Höppner S, Verdonck T. Data engineering for fraud detection. Decision Support Systems, 2021, 150: 113492.

[6] Mubalaike AM, Adali E. Deep learning approach for intelligent financial fraud detection system. In: 2018 3rd International Conference on Computer Science and Engineering (UBMK), 2018, 598 – 603. IEEE.

[7] Cui Y, Han X, Chen J, et al. FraudGNN-RL: A Graph Neural Network With Reinforcement Learning for Adaptive Financial Fraud Detection. IEEE Open Journal of the Computer Society, 2025.

[8] Bin Sulaiman R, Schetinin V, Sant P. Review of machine learning approach on credit card fraud detection. Human-Centric Intelligent Systems, 2022, 2(1): 55 – 68.

[9] Jain Y, Tiwari N, Dubey S, et al. A comparative analysis of various credit card fraud detection techniques. International Journal of Recent Technology and Engineering, 2019, 7(5): 402 – 407.

[10] Zanetti M, Jamhour E, Pellenz M, et al. A tunable fraud detection system for advanced metering infrastructure using short-lived patterns. IEEE Transactions on Smart Grid, 2017, 10(1): 830 – 840.

[11] Ejiofor OE. A comprehensive framework for strengthening USA financial cybersecurity: integrating machine learning and AI in fraud detection systems. European Journal of Computer Science and Information Technology, 2023, 11(6): 62 – 83.

[12] Carneiro N, Figueira G, Costa M. A data mining based system for credit-card fraud detection in e-tail. Decision Support Systems, 2017, 95: 91 – 101.

[13] Al-Hashedi KG, Magalingam P. Financial fraud detection applying data mining techniques: A comprehensive review from 2009 to 2019. Computer Science Review, 2021, 40: 100402.

[14] Van Bekkum M, Borgesius FZ. Digital welfare fraud detection and the Dutch SyRI judgment. European Journal of Social Security, 2021, 23(4): 323 – 340.

[15] Hajek P, Abedin MZ, Sivarajah U. Fraud detection in mobile payment systems using an XGBoost-based framework. Information Systems Frontiers, 2023, 25(5): 1985 – 2003.

[16] Li X, Wang X, Chen X, et al. Unlabeled data selection for active learning in image classification. Scientific Reports, 2024, 14(1): 424.

[17] Kalluri K. Optimizing Financial Services Implementing Pega's Decisioning Capabilities for Fraud Detection. International Journal of Innovative Research in Engineering & Multidisciplinary Physical Sciences, 2022, 10(1): 1 – 9.

[18] Sailusha R, Gnaneswar V, Ramesh R, et al. Credit card fraud detection using machine learning. In: 2020 4th International Conference on Intelligent Computing and Control Systems (ICICCS), 2020, 1264 – 1270.

[19] Guo H, Ma Z, Chen X, et al. Generating artistic portraits from face photos with feature disentanglement and reconstruction. Electronics, 2024, 13(5): 955.

[20] Thennakoon A, Bhagyani C, Premadasa S, et al. Real-time credit card fraud detection using machine learning. In: 2019 9th International Conference on Cloud Computing, Data Science & Engineering (Confluence), 2019, 488 – 493.

[21] Zeager MF, Sridhar A, Fogal N, et al. Adversarial learning in credit card fraud detection. In: 2017 Systems and Information Engineering Design Symposium (SIEDS), 2017, 112–116.
[22] Han X, Yang Y, Chen J, et al. Symmetry-Aware Credit Risk Modeling: A Deep Learning Framework Exploiting Financial Data Balance and Invariance. Symmetry, 2025, 17(3): 34.
[23] Wang X, Wu YC, Ma Z. Blockchain in the courtroom: exploring its evidentiary significance and procedural implications in US judicial processes. Frontiers in Blockchain, 2024, 7: 1306058.
[24] Yang J, Li P, Cui Y, et al. Multi-Sensor Temporal Fusion Transformer for Stock Performance Prediction: An Adaptive Sharpe Ratio Approach. Sensors, 2025, 25(3): 976.
[25] Lee Z, Wu YC, Wang X. Automated Machine Learning in Waste Classification: A Revolutionary Approach to Efficiency and Accuracy. In: Proceedings of the 2023 12th International Conference on Computing and Pattern Recognition, 2023, 299–303.
[26] Bello OA, Folorunso A, Onwuchekwa J, et al. Analysing the impact of advanced analytics on fraud detection: a machine learning perspective. European Journal of Computer Science and Information Technology, 2023, 11(6): 103–126.
[27] Liu Y, Wu YC, Fu H, et al. Digital intervention in improving the outcomes of mental health among LGBTQ+ youth: a systematic review. Frontiers in Psychology, 2023, 14: 1242928.