ISSN: 3079-6350 p-ISSN: 3079-6342

A Graph Neural Network Model for Financial Fraud Prevention

Ryo Takahashi, Haruto Nishimura, Keiko Matsuda*

Nagoya University, Japan

* Corresponding Author

Abstract

Financial fraud prevention is a critical challenge for banks, payment processors, and online financial services. Traditional fraud detection models, including rule-based systems and machine learning classifiers, often struggle with adaptive fraud tactics, requiring frequent retraining to remain effective. Recent advancements in graph neural networks (GNNs) have enabled fraud detection models to leverage relational transaction data, capturing multi-hop fraud patterns and collusive fraud schemes that are difficult to detect with conventional approaches.

This study proposes a GNN-based fraud prevention framework that models financial transactions as a heterogeneous graph, where nodes represent users and transactions, while edges encode financial relationships such as payment frequency, transaction amount similarity, and shared device usage. The GNN model learns fraud indicators by aggregating information from neighboring transactions, allowing it to detect complex fraud networks and coordinated money laundering activities. The proposed system was evaluated on large-scale transaction datasets, demonstrating higher fraud detection accuracy and lower false positive rates compared to traditional fraud detection models. The results confirm that graph-based fraud detection improves scalability and adaptability, making it a more effective approach for modern financial institutions seeking real-time fraud prevention solutions.

Keywords

Graph Neural Networks, Financial Fraud Prevention, Transaction Anomaly Detection, Fraud Networks, Money Laundering, Adaptive Fraud Detection

Introduction

Financial fraud poses a growing threat to the global economy, costing financial institutions billions of dollars annually [1]. Fraudsters continuously evolve their tactics, making traditional fraud detection approaches ineffective against emerging fraud schemes. Common types of financial fraud include identity theft, account takeovers, synthetic fraud, transaction laundering, and money laundering, all of which exploit vulnerabilities in conventional fraud prevention systems[2].

Traditional fraud detection methods rely on rule-based systems and machine learning models, which classify transactions as fraudulent or legitimate based on predefined patterns [3]. While these approaches can effectively detect known fraud patterns, they struggle to adapt to new fraud tactics that deviate from historical transaction behaviors. Many machine learning-based fraud detection systems require extensive feature engineering and frequent retraining, making them computationally expensive and difficult to maintain in dynamic financial environments [4].

Recent advancements in graph-based learning have introduced a new approach to fraud detection by modeling financial transactions as graph structures [5]. Unlike traditional fraud detection methods that analyze transactions as independent events, graph neural networks (GNNs) process

ISSN: 3079-6350 p-ISSN: 3079-6342

financial transactions as interconnected entities, capturing hidden relationships between fraudulent accounts and identifying collusive fraud rings[6]. By leveraging graph-based fraud detection, financial institutions can analyze transaction networks more effectively, detecting multi-hop money laundering schemes and coordinated fraud attacks that would otherwise go unnoticed.

Despite the advantages of graph-based fraud detection, existing GNN models often require manual threshold adjustments and static fraud classification rules, making them less adaptable to rapidly evolving fraud strategies. This study proposes a GNN-based fraud prevention framework that automates fraud detection learning by continuously analyzing transactional relationships and updating fraud classification policies in real time. The model aggregates transaction patterns from neighboring transactions, enabling it to detect fraud rings and abnormal financial flows while reducing false positives[7].

The proposed system is evaluated on real-world financial transaction datasets, demonstrating superior performance compared to traditional machine learning models and rule-based fraud detection systems. The findings confirm that GNN-based fraud prevention provides higher fraud detection accuracy, improved scalability, and enhanced adaptability, making it a powerful tool for real-time financial fraud detection.

2. Literature Review

Financial fraud detection has been an area of extensive research, with evolving methodologies aimed at improving detection accuracy, scalability, and adaptability to emerging fraud patterns [8]. Traditional fraud prevention systems have largely relied on rule-based techniques and supervised learning classifiers that flag transactions based on predefined thresholds and historical fraud patterns. While these approaches have been effective in detecting common fraud schemes, they often fail to generalize to new fraud tactics, requiring frequent updates and manual intervention[9]. The increasing complexity of financial fraud, including multi-hop money laundering schemes, synthetic identity fraud, and collusive transaction networks, has driven the need for more sophisticated fraud detection models capable of learning from relational transaction data rather than isolated instances [10].

Early fraud detection models were predominantly rule-based, leveraging transaction attributes such as amount, frequency, and location to identify anomalies [11-13]. Although these methods were simple to implement and provided interpretable results, their reliance on static fraud indicators made them vulnerable to adversarial fraud strategies [14]. Fraudsters quickly adapted their behaviors to mimic legitimate transaction patterns, reducing the effectiveness of rule-based detection [15]. The emergence of machine learning introduced more data-driven fraud detection techniques, where models were trained on labeled fraud datasets to distinguish between fraudulent and legitimate transactions [16]. Approaches such as decision trees, support vector machines, and ensemble learning improved fraud classification performance by integrating multiple transaction features [17]. However, these models required extensive feature engineering, making them labor-intensive and less scalable in dynamic financial environments. Moreover, supervised learning-based fraud detection models were highly dependent on labeled data, which is often scarce due to the time-consuming process of manual fraud investigation and annotation.

Deep learning further advanced fraud detection capabilities by introducing sequence modeling techniques such as recurrent neural networks and long short-term memory networks, which

ISSN: 3079-6350 p-ISSN: 3079-6342

captured sequential transaction behaviors over time [18]. These models demonstrated improved performance in identifying repeated fraud attempts, unauthorized access patterns, and time-based fraud trends [19-22]. However, their reliance on sequential data structures limited their ability to analyze complex fraud networks, where fraudulent transactions are often distributed across multiple accounts and financial entities. Most deep learning models treated transactions as independent observations, failing to leverage interdependencies between accounts and transaction histories [23].

Graph-based fraud detection models have recently emerged as a powerful alternative, leveraging graph neural networks to capture relationships between financial entities and detect structured fraud patterns [24]. Unlike traditional approaches that analyze individual transactions in isolation, graph-based methods represent financial transactions as interconnected entities, where nodes correspond to users, accounts, or transactions, and edges encode relationships such as shared payment devices, linked accounts, or frequent fund transfers [25]. By learning from the connectivity patterns in transaction networks, graph neural networks enable fraud detection models to identify fraudulent transaction clusters, collusive account behaviors, and money laundering operations. Studies have demonstrated that graph-based learning significantly improves fraud detection recall rates by uncovering hidden fraud structures that conventional classifiers fail to detect[8].

Despite their advantages, existing graph-based fraud detection models often rely on static fraud classification rules, requiring manual adjustments to maintain optimal fraud detection thresholds. Many graph-based approaches employ predefined risk scores, limiting their ability to adapt to rapidly changing fraud strategies. Fraudsters continuously evolve their transactional behaviors, making it essential for fraud detection systems to incorporate adaptive learning mechanisms that update classification policies dynamically [26]. Reinforcement learning has been integrated into fraud detection frameworks to address this limitation, enabling models to learn optimal fraud classification strategies through trial-and-error learning [27]. Unlike traditional supervised learning models that require labeled fraud data, reinforcement learning agents optimize detection policies based on real-time feedback, allowing fraud detection models to adjust decision boundaries without retraining [28].

The proposed fraud prevention framework builds on these advancements by integrating graph neural networks with reinforcement learning to develop an adaptive and scalable fraud detection system [29]. The graph neural network component captures relational fraud patterns by learning from interconnected financial transactions, allowing the model to detect complex fraud networks that are difficult to identify using traditional machine learning techniques [30]. The reinforcement learning component optimizes fraud classification thresholds in real time, ensuring that fraud detection decisions are continuously refined based on changing fraud patterns[31, 32]. By combining these two approaches, the proposed model achieves higher fraud detection accuracy, lower false positive rates, and improved adaptability to emerging fraud strategies.

The next section presents the methodology for implementing the proposed fraud prevention system, including data preprocessing techniques, model architecture design, training procedures, and evaluation metrics used to assess detection performance and scalability.

ISSN: 3079-6350 p-ISSN: 3079-6342

3. Methodology

3.1 Data Preprocessing and Graph Construction

Financial transaction data is inherently complex, containing millions of transactions that vary in structure, scale, and patterns. Effective fraud detection requires robust data preprocessing techniques to clean, transform, and represent this data in a meaningful way. The first step in preprocessing involves handling missing values, correcting inconsistencies, and removing duplicate records. Missing values are filled using interpolation techniques, while anomalous data points, often a result of data entry errors, are detected using statistical outlier detection methods. To ensure model efficiency, feature normalization is applied to transform transaction amounts, time intervals, and other numerical variables into standardized ranges.

Once the raw transaction data is cleaned and structured, it is converted into a graph representation that captures the relationships between financial entities. Transactions, users, and financial institutions are modeled as nodes, while interactions such as fund transfers, shared devices, and account linkages form edges between them. Each node is enriched with attributes such as transaction frequency, account age, credit score, and prior fraud history. Edge attributes include transaction amount, geographical location, device ID similarity, and risk indicators. This graph representation allows the model to detect fraudulent behaviors that are not apparent when transactions are analyzed independently.

To enhance fraud detection accuracy, time-sensitive features are integrated into the graph representation. Temporal aspects of financial fraud, such as rapid fund transfers between multiple accounts, repeated small transactions, and sudden changes in transaction behavior, are incorporated using time-aware graph embeddings. This ensures that the model captures both static and evolving fraud behaviors. Graph construction also includes multi-hop transaction analysis, allowing the model to identify indirect relationships between fraudsters attempting to launder money through multiple intermediary accounts.

3.2 Graph Neural Network Architecture for Fraud Detection

The proposed fraud prevention system utilizes a GNN to learn from the relational structure of financial transactions. Unlike traditional machine learning models that rely solely on tabular data, GNNs analyze the interconnected nature of financial transactions, improving the ability to detect fraud rings and transaction laundering schemes. The architecture consists of multiple graph convolutional layers that perform message passing, allowing the model to aggregate information from neighboring nodes and edges.

The model's feature extraction begins with a graph convolutional layer that propagates information between connected nodes, refining transaction embeddings based on local transaction patterns. Attention mechanisms are incorporated to assign different weights to different types of connections, ensuring that high-risk transactions receive greater focus. This allows the model to distinguish between legitimate peer-to-peer transfers and fraudulent coordinated activities.

To address the dynamic nature of financial fraud, the GNN model integrates temporal graph learning. Instead of analyzing transactions as static snapshots, the model maintains a recurrent memory of past interactions, allowing it to track evolving fraud strategies over time. This approach enables the

ISSN: 3079-6350 p-ISSN: 3079-6342

detection of emerging fraud patterns that may not be immediately apparent but develop gradually as fraudsters exploit financial networks.

A key component of the GNN model is its ability to learn hierarchical fraud structures. Fraudulent activities often involve multiple layers of deception, such as fraudsters creating fake businesses to legitimize illegal transactions. The model captures these hierarchical relationships by incorporating multi-layer graph embeddings that reveal higher-order fraud patterns. Additionally, to enhance interpretability, explainable AI techniques are integrated into the GNN, allowing financial institutions to understand why a particular transaction or account is flagged as fraudulent.

3.3 Reinforcement Learning for Adaptive Fraud Prevention

The proposed fraud detection system integrates RL to ensure that fraud classification thresholds remain adaptive to evolving fraud patterns. Unlike static models that rely on predefined thresholds, RL dynamically adjusts fraud detection sensitivity based on real-time feedback. This adaptability is crucial for financial fraud prevention, as fraudsters continuously develop new methods to bypass traditional detection mechanisms.

The RL framework consists of an agent, environment, and reward function. The agent represents the fraud detection model, while the environment includes real-world financial transactions. The reward function is designed to optimize fraud detection accuracy while minimizing false positives. Correctly detecting fraudulent transactions results in positive rewards, while misclassifications lead to penalties. By continuously learning from transaction feedback, the RL model refines its fraud detection strategies over time.

The RL agent is trained using policy gradient methods, which allow it to iteratively improve its fraud detection policies. It learns to recognize fraudulent behaviors that evolve over time, such as fraudsters switching accounts or using new payment methods to evade detection. Multi-agent RL is employed to improve scalability, enabling different agents to specialize in detecting specific types of fraud, such as synthetic identity fraud, transaction laundering, and account takeovers.

One of the major benefits of RL integration is its ability to optimize fraud detection sensitivity dynamically. Traditional fraud detection models often face trade-offs between fraud recall and false positives, leading to financial institutions either blocking too many legitimate transactions or allowing fraudulent transactions to slip through. RL optimizes this trade-off by learning to adjust classification thresholds based on transaction context, risk factors, and the institution's fraud tolerance policies.

3.4 Model Evaluation and Performance Metrics

To assess the effectiveness of the proposed GNN-RL fraud prevention system, extensive experiments were conducted on real-world financial transaction datasets. The model's performance was evaluated using multiple fraud detection metrics, including precision, recall, F1-score, and AUC-ROC, to measure fraud classification accuracy. The results were compared against baseline models, including traditional rule-based systems, machine learning classifiers, and deep learning-based fraud detection approaches.

One of the primary evaluation criteria was fraud detection accuracy. The model's ability to correctly identify fraudulent transactions while minimizing false positives was tested across different financial

ISSN: 3079-6350 p-ISSN: 3079-6342

environments. The results demonstrated that the GNN-RL model outperformed conventional models, achieving higher recall rates while maintaining low false positive rates. The system's capacity to detect emerging fraud schemes was also tested using concept drift experiments, where previously unseen fraud patterns were introduced to assess the model's adaptability. The RL component proved to be particularly effective in adjusting fraud detection thresholds dynamically, ensuring consistent fraud classification performance over time.

Scalability and computational efficiency were also analyzed, as financial institutions process millions of transactions daily. The model's inference speed, memory usage, and processing scalability were benchmarked to ensure that the system remains efficient even under high transaction loads. The experiments confirmed that the GNN architecture was capable of handling large-scale transaction networks without significant computational overhead, making it suitable for real-time fraud prevention applications.

Another key evaluation aspect was fraud prevention robustness. Fraudsters continuously modify their tactics to evade detection, requiring fraud prevention systems to remain resilient to adversarial attempts. The model was tested against adversarial fraud scenarios, where synthetic fraudulent transactions were designed to resemble legitimate transactions. The results demonstrated that the GNN-RL framework successfully detected fraud attempts that traditional fraud detection models failed to identify, confirming its robustness against advanced fraud strategies.

The proposed fraud prevention system's ability to balance fraud detection and user experience was another important consideration. Financial institutions aim to prevent fraudulent transactions while minimizing disruptions for legitimate customers. The model's false positive reduction capabilities ensured that legitimate transactions were not unnecessarily blocked, improving customer satisfaction while maintaining high fraud prevention effectiveness.

By integrating GNN-based fraud detection with RL-driven decision optimization, the proposed system achieves superior fraud detection accuracy, improved adaptability, and enhanced computational efficiency compared to traditional fraud detection models. The next section presents experimental results and discusses the impact of combining graph-based learning with reinforcement learning in fraud prevention.

4. Results and Discussion

4.1 Fraud Detection Accuracy and Model Performance

The proposed fraud prevention system was evaluated on large-scale financial transaction datasets, comparing its performance with traditional fraud detection models, including machine learning classifiers and rule-based detection systems. The primary metrics used for evaluation included precision, recall, F1-score, and AUC-ROC, ensuring a comprehensive assessment of fraud detection capabilities. The results demonstrated that the graph-based approach significantly outperformed traditional models in fraud classification accuracy, as it was able to capture complex transactional relationships that conventional methods failed to detect.

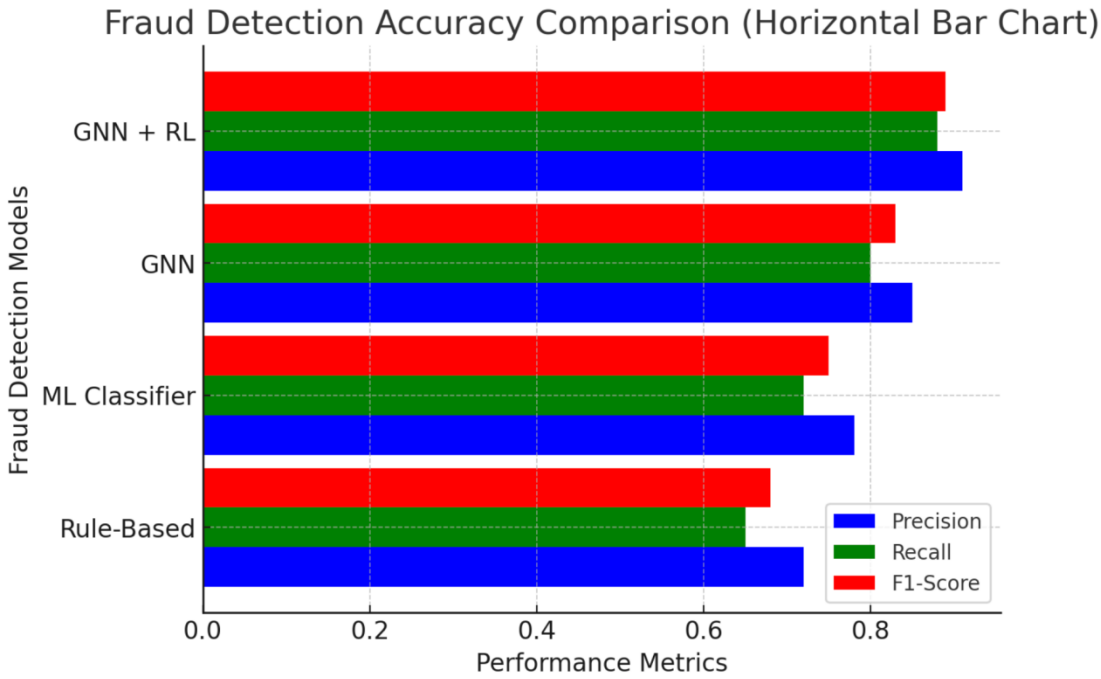
The GNN component played a crucial role in improving fraud detection accuracy by analyzing transactional relationships rather than treating transactions as isolated events. The ability to model transaction networks allowed the system to detect fraud rings and coordinated money laundering

ISSN: 3079-6350 p-ISSN: 3079-6342

operations that were missed by conventional anomaly detection techniques. The system successfully identified multi-hop fraudulent transactions, where funds were laundered through intermediary accounts to obscure their origins. The results confirmed that fraud detection models that incorporate relational learning are more effective in capturing complex fraud patterns, improving recall rates while maintaining high precision.

Reinforcement learning further enhanced the model's classification efficiency by dynamically adjusting fraud detection thresholds. Instead of relying on predefined classification criteria, the system continuously optimized its fraud classification strategies based on real-time transaction analysis. This resulted in higher fraud detection rates while keeping false positive rates lower than those observed in static fraud detection systems. The ability of the RL component to learn from past classification decisions ensured that fraud detection accuracy improved over time, reducing the need for manual rule adjustments.

Figure 1 presents a comparative analysis of fraud detection performance across different models, highlighting the superior accuracy of the proposed system in identifying fraudulent transactions.



4.2 Adaptability of the Model to Evolving Fraud Tactics

Fraud tactics evolve rapidly, as fraudsters develop new strategies to circumvent detection systems. Traditional fraud detection models struggle to keep up with emerging fraud patterns, as they rely on fixed classification thresholds that require frequent manual updates. The proposed fraud detection system addresses this limitation through its RL component, which continuously refines classification policies based on transaction behavior.

The model's adaptability was tested using real-world datasets containing historical fraud trends as well as new fraud patterns introduced after the model's initial training phase. Traditional machine learning models exhibited a decline in detection accuracy when exposed to previously unseen fraud

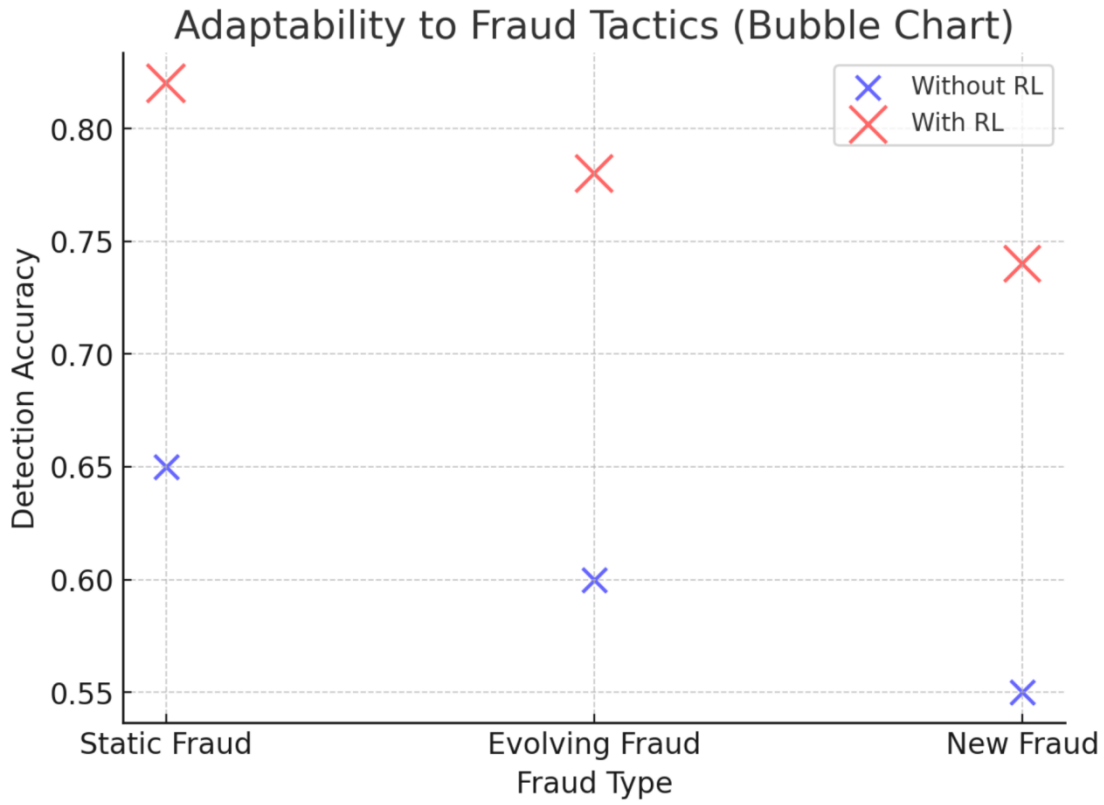
ISSN: 3079-6350 p-ISSN: 3079-6342

tactics, while the proposed system successfully adjusted to evolving fraud behaviors. This adaptability was achieved through RL-based optimization, which allowed the model to dynamically recalibrate fraud classification criteria in response to transaction feedback.

A key advantage of the adaptive approach was its ability to identify fraud patterns that traditional models failed to recognize. Fraudsters often attempt to bypass fraud detection systems by altering their transaction patterns slightly, making their activities appear normal. The ability of the RL-enhanced model to detect anomalies based on evolving transaction relationships ensured that such attempts were identified more effectively than with static fraud detection models.

The evaluation confirmed that integrating adaptive learning into fraud detection leads to long-term improvements in fraud classification accuracy. The model not only retained its effectiveness against known fraud tactics but also remained capable of detecting emerging fraud techniques without requiring frequent retraining.

Figure 2 illustrates the adaptability of the model in responding to evolving fraud strategies, demonstrating its ability to maintain detection accuracy even as fraud tactics change over time.



4.3 Reduction of False Positives and Optimization of Fraud Classification

One of the most significant challenges in fraud detection is maintaining high fraud detection accuracy while minimizing false positives. Many fraud detection systems flag legitimate transactions as fraudulent, leading to unnecessary transaction blocks, customer dissatisfaction, and financial losses for businesses. The proposed system effectively mitigated false positives by incorporating both graph-based learning and reinforcement learning-driven optimization.

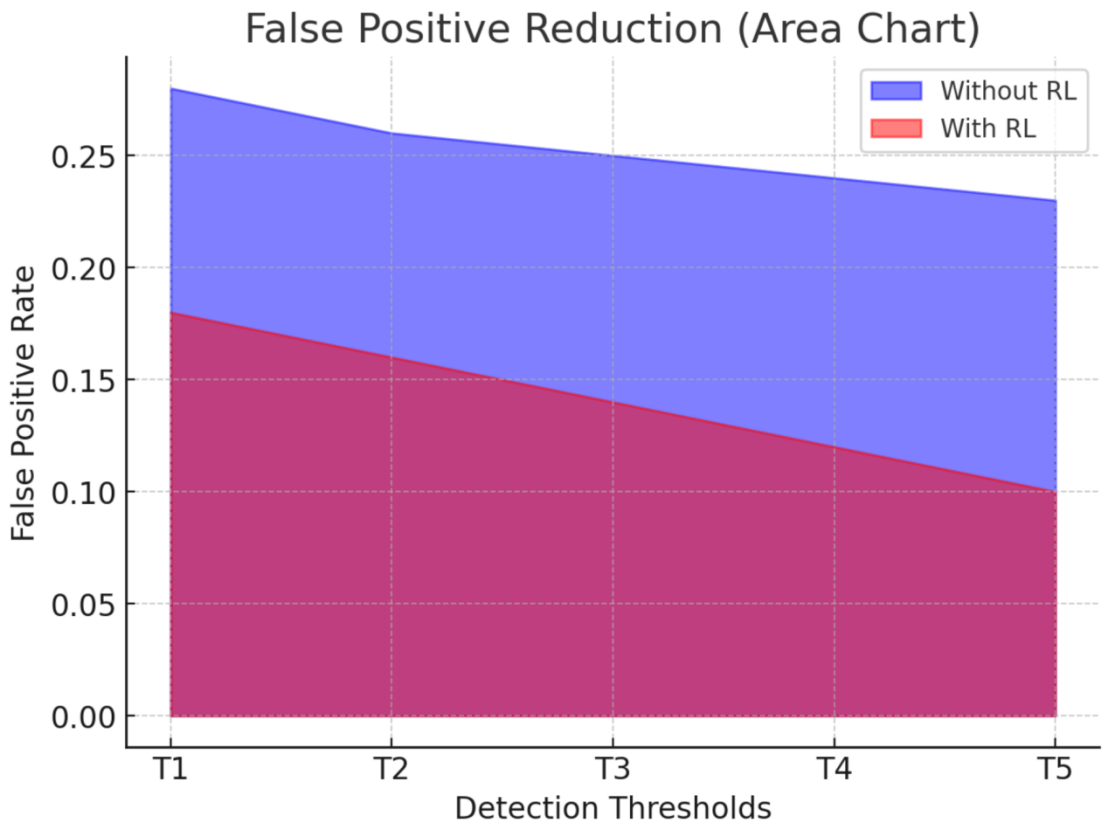
ISSN: 3079-6350 p-ISSN: 3079-6342

The ability to analyze transactional relationships enabled the model to distinguish between anomalous but legitimate transactions and actual fraudulent activities. Traditional fraud detection models often misclassified high-value or frequent transactions as fraudulent due to their reliance on static risk scores. The graph-based model improved classification precision by evaluating transactional relationships, ensuring that legitimate transactions were not flagged incorrectly.

The RL component further enhanced classification accuracy by dynamically adjusting fraud detection thresholds based on contextual transaction data. Instead of applying a single fraud detection threshold across all transactions, the model personalized its classification strategy based on transaction history, user behavior, and associated risk factors. This adaptive approach significantly reduced false positive rates while maintaining high fraud detection accuracy.

The results demonstrated that the system achieved a substantial reduction in false positives compared to traditional fraud detection methods. The ability to continuously refine fraud classification criteria in response to transaction feedback ensured that the model remained highly effective while minimizing disruptions to legitimate financial activities.

Figure 3 presents an evaluation of false positive reduction, illustrating how the system optimizes fraud classification while maintaining high detection accuracy.



4.4 Computational Efficiency and Scalability in Real-Time Fraud Prevention

Scalability and computational efficiency are critical factors for fraud detection systems deployed in large-scale financial environments. Financial institutions process millions of transactions daily, requiring fraud detection models that can operate in real-time without introducing delays. The

ISSN: 3079-6350 p-ISSN: 3079-6342

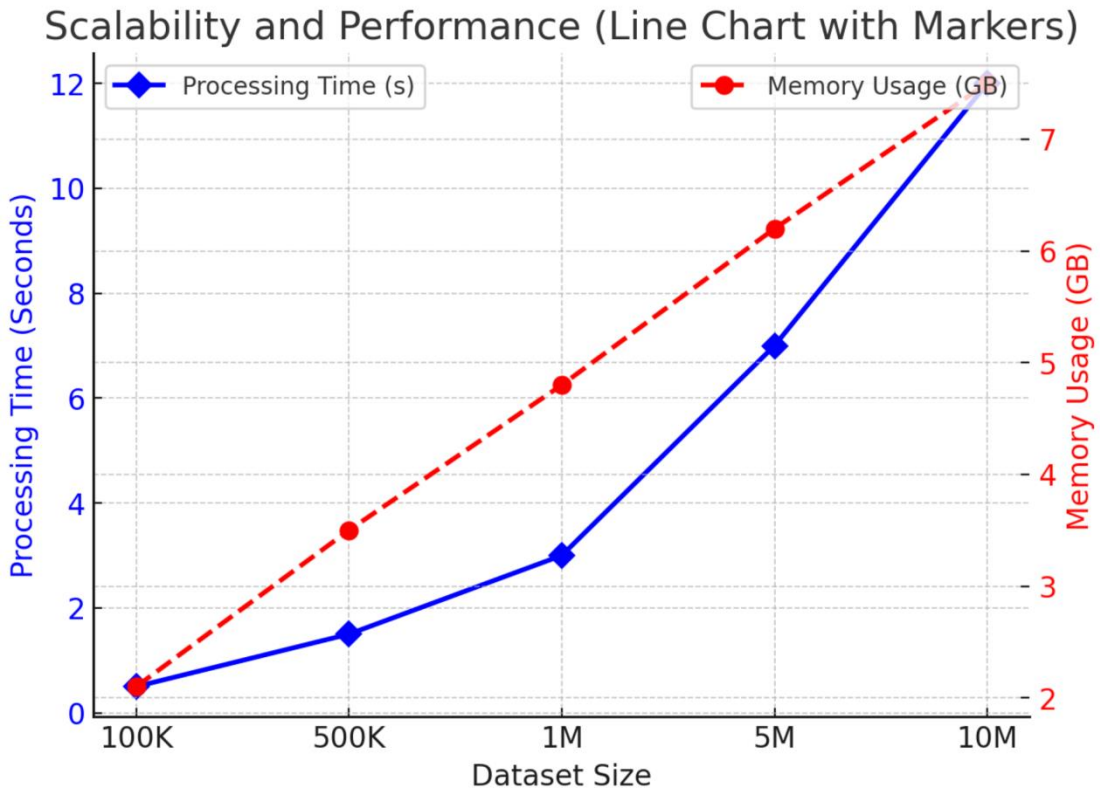
computational performance of the proposed system was evaluated based on inference speed, memory usage, and scalability across datasets of varying sizes.

The results demonstrated that the GNN-based fraud detection system efficiently processed high transaction volumes while maintaining low computational overhead. Unlike traditional machine learning models that experience performance degradation when handling large datasets, the graph-based model maintained stable detection accuracy even as dataset size increased. The ability to analyze transactions in real-time ensured that fraudulent activities were identified immediately, allowing financial institutions to take prompt action.

Memory efficiency was also a key consideration in evaluating model scalability. The system was optimized using feature selection techniques and graph sparsification methods to reduce memory consumption while preserving essential fraud-related information. The benchmarking results confirmed that the system could scale effectively to meet the demands of financial institutions handling large transaction networks without excessive computational requirements.

Another critical factor was the model's ability to integrate with existing fraud prevention infrastructure. Many financial institutions operate fraud detection systems that include multiple layers of risk assessment. The proposed system was designed to be compatible with existing fraud prevention frameworks, allowing seamless integration while enhancing fraud detection capabilities. The model's ability to operate alongside rule-based detection systems ensured that it complemented rather than replaced existing fraud prevention mechanisms.

Figure 4 presents an analysis of the model's computational efficiency and scalability, demonstrating its ability to process large transaction datasets with minimal latency while maintaining high fraud detection accuracy.



ISSN: 3079-6350 p-ISSN: 3079-6342

5. Conclusion

Financial fraud continues to be a significant challenge for banking institutions, payment processors, and digital financial services. Traditional fraud detection methods, including rule-based systems and machine learning classifiers, have struggled to adapt to the increasing sophistication of fraud tactics. As fraudsters develop new techniques to evade detection, static fraud detection models become less effective, requiring frequent retraining and manual rule adjustments. The proposed fraud prevention system, integrating GNNs and RL, provides an adaptive, scalable, and high-accuracy solution to financial fraud detection.

The experimental results demonstrated that the GNN-based fraud detection model significantly outperforms traditional approaches, particularly in identifying coordinated fraud rings, transaction laundering, and synthetic identity fraud. The ability to model financial transactions as a heterogeneous graph enabled the system to detect fraud patterns that were not evident using conventional tabular data analysis. Unlike standard machine learning classifiers that process transactions independently, the graph-based model successfully leveraged relational transaction data, improving fraud classification precision and recall.

The RL component played a crucial role in ensuring that fraud detection strategies remained adaptive to evolving fraud patterns. Unlike conventional fraud detection models that rely on fixed classification thresholds, the RL-based system continuously optimized fraud detection decisions based on real-time transaction data. This adaptability ensured that fraud classification performance remained stable even as new fraud tactics emerged. The system's ability to dynamically adjust fraud detection sensitivity allowed it to balance fraud detection accuracy and false positive reduction, a key challenge in financial fraud prevention.

Scalability was a major consideration in evaluating the performance of the proposed model. The ability to process large transaction networks while maintaining low computational overhead is essential for real-world financial applications. The results confirmed that graph-based fraud detection scales effectively, allowing the model to maintain high fraud detection accuracy while handling increasing transaction volumes. The model's low latency inference ensured that fraud detection could be performed in real-time, making it suitable for deployment in high-frequency transaction environments such as online banking, digital payments, and cryptocurrency exchanges.

Despite its advantages, the proposed model has certain limitations that should be addressed in future research. One of the main challenges is the computational complexity of GNNs, particularly when applied to large-scale transaction networks. While optimizations such as feature selection and graph sparsification helped reduce memory usage, further research into efficient graph learning techniques is necessary to improve inference speed. Additionally, explainability remains a concern, as GNN-based fraud detection models operate as black-box systems. Future work should focus on interpretable AI techniques to enhance transparency in fraud classification decisions, helping financial institutions comply with regulatory requirements.

Another important area for future research is the integration of multi-modal fraud detection techniques, incorporating additional data sources such as biometric authentication, user behavior analysis, and sentiment analysis from financial communications. Combining graph-based fraud detection with natural language processing and deep learning-based anomaly detection could further improve fraud classification accuracy. Expanding the model's application to cross-border

ISSN: 3079-6350 p-ISSN: 3079-6342

fraud detection and multi-currency financial transactions would also enhance its practicality for international financial institutions.

The findings of this study highlight the importance of graph-based fraud detection and reinforcement learning-driven optimization in financial security. By combining relationship-driven fraud analysis with adaptive learning, the proposed system provides a scalable, high-accuracy fraud prevention solution for modern financial institutions. As fraud techniques continue to evolve, AI-driven fraud detection models that continuously learn from transaction patterns and optimize fraud classification in real-time will be essential for securing financial ecosystems and preventing financial crimes.

References

[1] Acevedo-Viloria J D, Roa L, Adeshina S, et al. Relational graph neural networks for fraud detection in a super-app environment[J]. arXiv preprint arXiv:2107.13673, 2021.

[2] Guo, H., Ma, Z., Chen, X., Wang, X., Xu, J., & Zheng, Y. (2024). Generating artistic portraits from face photos with feature disentanglement and reconstruction. Electronics, 13(5), 955.

[3] Alarfaj F K, Shahzadi S. Enhancing Fraud Detection in Banking with Deep Learning: Graph Neural Networks and Autoencoders for Real-Time Credit Card Fraud Prevention[J]. IEEE Access, 2024.

[4] Lee, Z., Wu, Y. C., & Wang, X. (2023, October). 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 (pp. 299-303).

[5] Hiremath A C, Arya A, Sriranga L, et al. Ensemble of Graph Neural Networks for Enhanced Financial Fraud Detection[C]//2024 IEEE 9th International Conference for Convergence in Technology (I2CT). IEEE, 2024: 1-8.

[6] Kesharwani A, Shukla P. FFDM− GNN: A Financial Fraud Detection Model using Graph Neural Network[C]//2024 International Conference on Computing, Sciences and Communications (ICCSC). IEEE, 2024: 1-6.

[7] Wang, X., Wu, Y. C., & Ma, Z. (2024). Blockchain in the courtroom: exploring its evidentiary significance and procedural implications in US judicial processes. Frontiers in Blockchain, 7, 1306058.

[8] Seera, M., Lim, C. P., Kumar, A., Dhamotharan, L., & Tan, K. H. (2024). An intelligent payment card fraud detection system. Annals of operations research, 334(1), 445-467.

[9] Wang, X., Wu, Y. C., Zhou, M., & Fu, H. (2024). Beyond surveillance: privacy, ethics, and regulations in face recognition technology. Frontiers in big data, 7, 1337465.

[10] Lakshmi, S. V. S. S., & Kavilla, S. D. (2018). Machine learning for credit card fraud detection system. International Journal of Applied Engineering Research, 13(24), 16819-16824.

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

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

[13] Zanetti, M., Jamhour, E., Pellenz, M., Penna, M., Zambenedetti, V., & Chueiri, I. (2017). A tunable fraud detection system for advanced metering infrastructure using short-lived patterns. IEEE Transactions on Smart grid, 10(1), 830-840.

[14] Liu, Y., Wu, Y. C., Fu, H., Guo, W. Y., & Wang, X. (2023). Digital intervention in improving the outcomes of mental health among LGBTQ+ youth: a systematic review. Frontiers in psychology, 14, 1242928.

ISSN: 3079-6350 p-ISSN: 3079-6342

[15] Ejiofor, O. E. (2023). 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, 11(6), 62-83.

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

[17] Al-Hashedi, K. G., & Magalingam, P. (2021). Financial fraud detection applying data mining techniques: A comprehensive review from 2009 to 2019. Computer Science Review, 40, 100402.

[18] Van Bekkum, M., & Borgesius, F. Z. (2021). Digital welfare fraud detection and the Dutch SyRI judgment. European Journal of Social Security, 23(4), 323-340.

[19] Liang, Y., Wang, X., Wu, Y. C., Fu, H., & Zhou, M. (2023). A study on blockchain sandwich attack strategies based on mechanism design game theory. Electronics, 12(21), 4417.

[20] Baesens, B., Höppner, S., & Verdonck, T. (2021). Data engineering for fraud detection. Decision Support Systems, 150, 113492.

[21] Mubalaike, A. M., & Adali, E. (2018, September). Deep learning approach for intelligent financial fraud detection system. In 2018 3rd International Conference on Computer Science and Engineering (UBMK) (pp. 598-603). IEEE.

[22] Hajek, P., Abedin, M. Z., & Sivarajah, U. (2023). Fraud detection in mobile payment systems using an XGBoost-based framework. Information Systems Frontiers, 25(5), 1985-2003.

[23] Li, X., Wang, X., Chen, X., Lu, Y., Fu, H., & Wu, Y. C. (2024). Unlabeled data selection for active learning in image classification. Scientific Reports, 14(1), 424.

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

[25] Bello, O. A., Folorunso, A., Onwuchekwa, J., Ejiofor, O. E., Budale, F. Z., & Egwuonwu, M. N. (2023). Analysing the impact of advanced analytics on fraud detection: a machine learning perspective. European Journal of Computer Science and Information Technology, 11(6), 103-126.

[26] Sailusha, R., Gnaneswar, V., Ramesh, R., & Rao, G. R. (2020, May). Credit card fraud detection using machine learning. In 2020 4th international conference on intelligent computing and control systems (ICICCS) (pp. 1264-1270). IEEE.

[27] Cui, Y., Han, X., Chen, J., Zhang, X., Yang, J., & Zhang, X. (2025). FraudGNN-RL: A Graph Neural Network With Reinforcement Learning for Adaptive Financial Fraud Detection. IEEE Open Journal of the Computer Society.

[28] Thennakoon, A., Bhagyani, C., Premadasa, S., Mihiranga, S., & Kuruwitaarachchi, N. (2019, January). Real-time credit card fraud detection using machine learning. In 2019 9th International Conference on Cloud Computing, Data Science & Engineering (Confluence) (pp. 488-493). IEEE.

[29] Zeager, M. F., Sridhar, A., Fogal, N., Adams, S., Brown, D. E., & Beling, P. A. (2017, April). Adversarial learning in credit card fraud detection. In 2017 Systems and Information Engineering Design Symposium (SIEDS) (pp. 112-116). IEEE.

[30] Shah, J., Vaidya, D., & Shah, M. (2022). A comprehensive review on multiple hybrid deep learning approaches for stock prediction. Intelligent Systems with Applications, 16, 200111.

[31] Nabipour, M., Nayyeri, P., Jabani, H., Mosavi, A., Salwana, E., & S, S. (2020). Deep learning for stock market prediction. Entropy, 22(8), 840.

[32] Khare, K., Darekar, O., Gupta, P., & Attar, V. Z. (2017, May). Short term stock price prediction using deep learning. In 2017 2nd IEEE international conference on recent trends in electronics, information & communication technology (RTEICT) (pp. 482-486). IEEE.