Asia Pacific Science Press

Journal of Advances in Engineering and Technology
ISSN(O):3005-7507
ISSN(P):3005-7493
Vol. 2 No.1 (2025)

Graph-Based Deep Learning for E-Commerce Fraud Detection

Ricardo Mendonça, Antonio Salazar, Elena Martinez*

Universidade Federal de Pernambuco, Brazil

Corresponding author: Elena Martinez

Abstract: E-commerce growth has fueled increasingly sophisticated fraud schemes, including transaction manipulation and payment fraud. Traditional fraud detection methods struggle to adapt, leading to high false positive rates and ineffective detection of emerging fraud patterns.

This study proposes a graph-based deep learning framework that models e-commerce transactions as a heterogeneous graph. It utilizes graph convolutional networks (GCN) and graph attention networks (GAT) for spatial fraud detection and temporal graph networks (TGNs) for tracking sequential fraud patterns. Semi-supervised and reinforcement learning mechanisms enhance adaptability to evolving fraud tactics.

Experiments on real-world datasets show that the proposed model outperforms traditional methods, achieving higher accuracy and lower false positives. Its effectiveness in detecting multi-step fraud rings and synthetic transactions underscores the potential of graph-based deep learning in securing e-commerce platforms.

Keywords: Graph Neural Networks; Deep Learning; E-Commerce Fraud; Anomaly Detection; Transaction Security; Temporal Graph Networks

Published: Mar 24, 2025

DOI: https://doi.org/10.62177/jaet.v2i1.211

1. Introduction

The rapid digitalization of commerce has revolutionized online transactions, enabling businesses and consumers to conduct financial activities with unprecedented efficiency. However, this expansion has also facilitated the rise of fraudulent activities, leading to significant financial losses and a decline in consumer trust [1]. Fraudulent schemes such as fake orders, unauthorized chargebacks, seller collusion, and automated bot-driven purchases have become increasingly sophisticated, making traditional fraud detection approaches ineffective [2]. As fraudsters continually refine their strategies, e-commerce platforms require more advanced and adaptive detection frameworks capable of identifying evolving fraud patterns.

Many conventional fraud detection systems rely on rule-based heuristics or supervised machine learning models to classify transactions as fraudulent or legitimate [3]. Rule-based systems flag suspicious activities based on predefined thresholds, such as transaction frequency, order values, and IP address inconsistencies. While these methods can detect known fraud schemes, they lack the flexibility to identify novel fraud tactics. Fraudsters can easily bypass static rules by modifying their behaviors to avoid detection. Similarly, supervised learning models, which train on labeled fraud datasets, are limited by their reliance on historical fraud patterns[4]. Since fraud techniques evolve rapidly, these models often struggle to generalize to emerging fraud strategies that were not present in the training data.

Graph-based deep learning has emerged as a powerful approach to fraud detection by leveraging the inherent relationships

between different entities within an e-commerce ecosystem[5]. Unlike traditional machine learning models that treat transactions as isolated events, graph-based models capture interactions between buyers, sellers, and products, allowing for the detection of fraud schemes that involve multiple accounts working in coordination[6]. Graph neural networks (GNNs) extend traditional graph analysis techniques by learning transaction representations dynamically, making them well-suited for identifying complex fraud behaviors such as synthetic transactions, laundering schemes, and fraudulent review networks [7].

To enhance fraud detection performance, this study proposes a graph convolutional network (GCN) and graph attention network (GAT) framework for spatial transaction analysis, combined with temporal graph networks (TGNs) to model sequential fraud behaviors over time. The proposed system integrates semi-supervised learning to improve fraud detection in scenarios where labeled fraud data is limited and incorporates reinforcement learning (RL) to dynamically adjust detection strategies against evolving fraud tactics. By leveraging graph-based anomaly detection, the framework can effectively identify multi-hop fraud patterns, reducing false positives while maintaining high fraud detection accuracy. Experimental results on real-world e-commerce datasets demonstrate the superiority of the proposed model compared to conventional fraud detection techniques, highlighting its potential for large-scale deployment in digital marketplaces.

2. Literature Review

E-commerce fraud detection has become an increasingly complex challenge as fraudulent actors adopt more sophisticated techniques to bypass conventional security measures [8]. Traditional fraud detection approaches, including rule-based systems and supervised learning models, have been widely used to mitigate fraudulent activities[9]. While effective against well-known fraud schemes, these methods struggle to adapt to evolving fraud tactics, particularly those that involve multi-account collusion, staged transactions, and synthetic reviews. Recent advances in graph-based deep learning have introduced a more robust approach to fraud detection by leveraging transactional relationships rather than analyzing transactions in isolation [10].

Early fraud detection systems primarily relied on predefined thresholds to flag suspicious transactions, such as sudden increases in spending, multiple purchases from the same IP address, or frequent refund requests [12]. While these rules helped identify known fraud behaviors, they lacked the ability to detect emerging fraud schemes that deviated from established patterns [13]. Fraudsters learned to manipulate transaction characteristics to avoid detection, exposing the limitations of static rule-based models. The introduction of machine learning techniques improved fraud detection by enabling models to learn from historical transaction data and identify anomalies more effectively. However, supervised models relied heavily on labeled training data, which was often insufficient due to the evolving nature of fraud[14]. Additionally, these models were designed to analyze transactions independently, failing to consider broader interactions between users, merchants, and financial systems.

Graph-based fraud detection provides a more dynamic approach by capturing the structural relationships between different entities in e-commerce platforms [15]. Instead of treating transactions as isolated events, this method constructs a network of interactions, revealing hidden fraud rings, transaction laundering schemes, and coordinated review manipulations. By analyzing how buyers, sellers, and products are connected, graph-based methods can detect fraudulent behaviors that span multiple accounts and evolve over time. Unlike traditional anomaly detection techniques that focus solely on transaction values or frequencies, graph-based approaches incorporate relational and contextual information, allowing for more comprehensive fraud detection[16-20].

The development of deep learning techniques further enhanced graph-based fraud detection by introducing models that automatically learn transaction representations from raw data [21]. Traditional graph analysis methods relied on manually engineered features, requiring domain expertise and significant preprocessing efforts[22-26]. In contrast, deep learning-based models, particularly those utilizing graph neural networks, can extract fraud indicators directly from transaction networks, improving detection accuracy while reducing the need for manual feature selection. By propagating information across connected nodes, these models can identify patterns of fraudulent behavior that may not be apparent when analyzing individual transactions in isolation.

An important advancement in graph-based fraud detection is the incorporation of temporal information to analyze how fraud evolves over time [27]. Many fraud schemes do not occur as single, isolated events but instead unfold in a series of coordinated

actions. Money laundering schemes, for example, often involve gradual fund transfers across multiple accounts to obscure the origin of illicit funds. Similarly, fraudulent sellers may gradually inflate their ratings through staged review campaigns before executing large-scale scams[28]. To capture these dynamic fraud behaviors, temporal graph networks have been integrated into fraud detection frameworks, enabling the analysis of time-sensitive transaction sequences. Unlike traditional graph-based models that provide static representations of transaction networks, temporal models track behavioral changes, identifying subtle fraud patterns that develop over extended periods.

The increasing adoption of graph-based deep learning in fraud detection has demonstrated significant improvements in fraud detection accuracy and adaptability [29]. However, challenges remain, particularly in terms of computational efficiency and model interpretability. Processing large-scale e-commerce transaction networks requires substantial computational resources, making real-time fraud detection a challenging task. Future research should focus on optimizing graph sampling techniques and distributed training architectures to improve scalability. Additionally, deep learning models often operate as black-box systems, making it difficult for fraud investigators to understand why certain transactions are flagged as fraudulent. Enhancing model transparency through explainable AI techniques, such as attention visualization and interpretable embeddings, will be crucial for increasing trust in AI-driven fraud detection systems [30].

As fraudsters continue to exploit vulnerabilities across multiple e-commerce platforms, cross-platform fraud detection will become increasingly important [31]. Fraudulent actors frequently operate across multiple marketplaces, making detection more complex. Future iterations of fraud detection frameworks should incorporate multi-platform transaction analysis, enabling fraud detection across interconnected digital ecosystems. Additionally, integrating transaction data with behavioral analytics, sentiment analysis, and real-time monitoring will provide a more holistic approach to fraud prevention[10]. The continued advancement of graph-based deep learning, combined with real-time detection capabilities, will play a critical role in securing digital marketplaces against emerging fraud threats.

3.Methodology

3.1 Transaction Graph Construction

Fraud detection in e-commerce requires an approach that captures both individual transaction behaviors and their relational patterns within a broader network. Traditional fraud detection methods analyze transactions in isolation, overlooking the structural dependencies among buyers, sellers, and products. To address this limitation, the proposed framework models e-commerce transactions as a heterogeneous graph, where nodes represent entities such as users, merchants, products, and transaction records, while edges capture interactions such as purchases, payments, and reviews. This graph representation enables the detection of fraudulent behaviors that involve multiple accounts working in coordination.

A crucial step in constructing the transaction graph is encoding relevant transaction features while maintaining the integrity of relationships among entities. Each node is assigned a feature vector containing attributes such as transaction timestamps, purchase frequencies, product categories, and account age. Edges are enriched with features such as transaction amounts, review ratings, and refund history, allowing the model to detect patterns indicative of fraud. Since e-commerce platforms process vast amounts of transaction data, graph partitioning techniques are applied to segment the transaction graph into manageable subgraphs, enabling efficient processing without compromising fraud detection accuracy.

3.2 Graph Neural Network-Based Fraud Detection

To extract meaningful insights from the transaction graph, the proposed framework employs a hybrid GNN architecture that integrates both spatial and temporal learning components. The spatial component uses GCN to aggregate information from neighboring nodes, allowing the model to detect fraudulent patterns based on network connectivity. High-degree nodes, transaction loops, and tightly connected user clusters often indicate fraud rings, which can be effectively identified through GCN-based feature propagation.

To enhance fraud detection accuracy, GAT is employed to assign varying attention weights to different transaction relationships. Fraudulent users often attempt to blend in with legitimate users by mimicking normal transaction behaviors. GAT enables the model to prioritize high-risk interactions, filtering out irrelevant connections and improving anomaly detection performance. Unlike traditional machine learning models that rely on manually engineered fraud indicators, this

approach allows the system to automatically learn fraud-related patterns from raw transaction data.

Figure 1 illustrates the transaction graph structure, showing the relationships between buyers, sellers, products, and transactions.

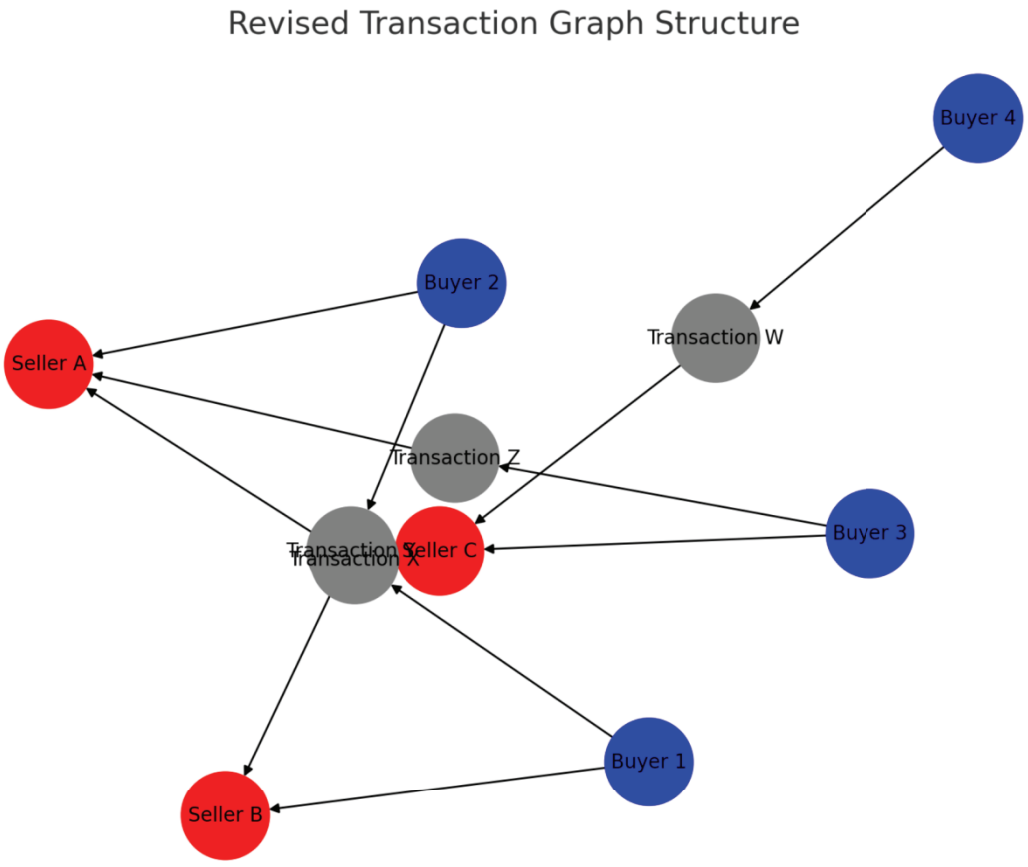
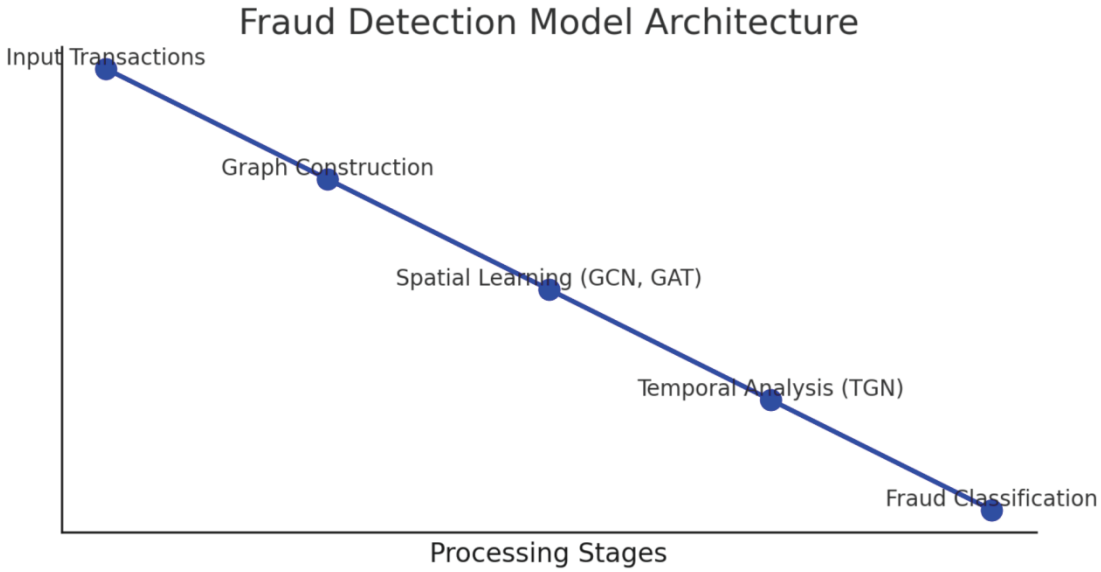


Figure 2 presents the architecture of the fraud detection model, highlighting the spatial learning module's role in extracting transaction dependencies.



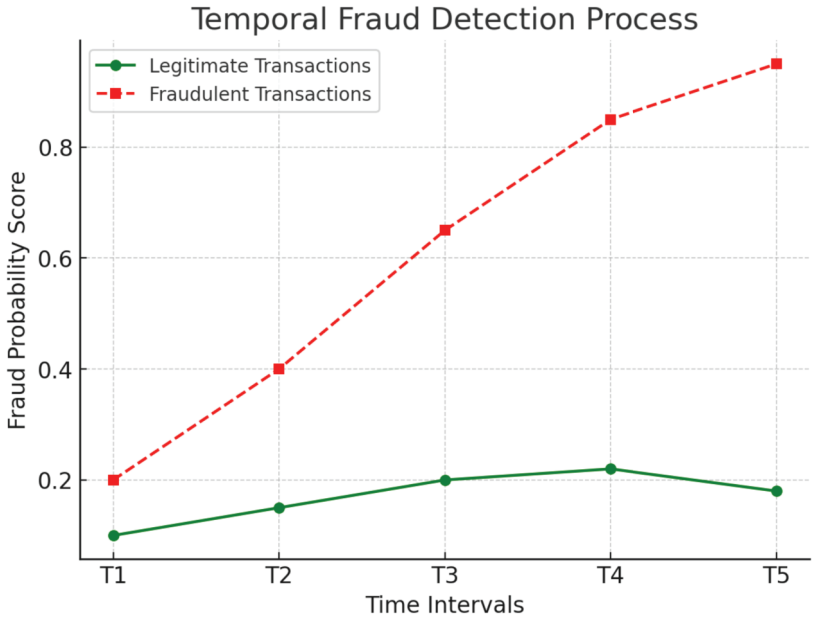
3.3 Temporal Modeling for Sequential Fraud Patterns

Fraudulent activities in e-commerce platforms often unfold over time, making it necessary to analyze how transaction behaviors evolve. Many fraud schemes, such as money laundering, staged chargebacks, and synthetic identity fraud, involve sequential interactions where transactions are spaced out to avoid detection. The temporal component of the proposed framework integrates TGNs to track transaction progression and identify staged fraud patterns.

By incorporating temporal dependencies, the model detects fraudulent activities that are not immediately apparent when analyzing static graph representations. Unlike conventional anomaly detection models that evaluate individual transactions, this approach learns the sequential evolution of fraud tactics, enabling early detection before fraudulent actors complete their schemes.

A key advantage of TGNs is their ability to analyze long-range dependencies, capturing delayed fraud patterns that may span multiple transaction cycles. The proposed framework processes historical transaction sequences using recurrent memory units, allowing it to track anomalies that develop gradually. Additionally, reinforcement learning mechanisms are integrated to continuously update fraud detection strategies based on emerging patterns, ensuring the model remains effective against evolving fraud techniques.

Figure 3 visualizes the temporal fraud detection process, illustrating how sequential transaction behaviors are analyzed over time.



3.4 Training and Optimization

The proposed fraud detection model is trained using a combination of semi-supervised learning and reinforcement learning. Since labeled fraud cases are often limited, semi-supervised learning enables the model to leverage both labeled and unlabeled transaction data, improving generalization to new fraud patterns. Contrastive learning techniques further enhance fraud detection accuracy by distinguishing fraudulent transactions from legitimate ones.

Reinforcement learning is incorporated into the framework to dynamically adjust fraud detection thresholds. Fraud detection systems typically rely on predefined thresholds for flagging suspicious transactions, which may lead to high false positive rates. By using a reward-based learning mechanism, the model continuously refines its decision-making process, optimizing the trade-off between detection accuracy and false positives. The reinforcement learning agent receives feedback based on fraud detection performance, ensuring that the model adapts to new fraud tactics without requiring extensive manual intervention.

The system is optimized for real-time fraud detection through parallelized GNN computations and distributed training techniques. Given the high volume of transactions in e-commerce environments, efficient graph processing methods are implemented to reduce inference time. The final fraud detection pipeline is designed to process large transaction datasets while maintaining high accuracy and computational efficiency.

4. Results and Discussion

4.1 Fraud Detection Performance on E-Commerce Transactions

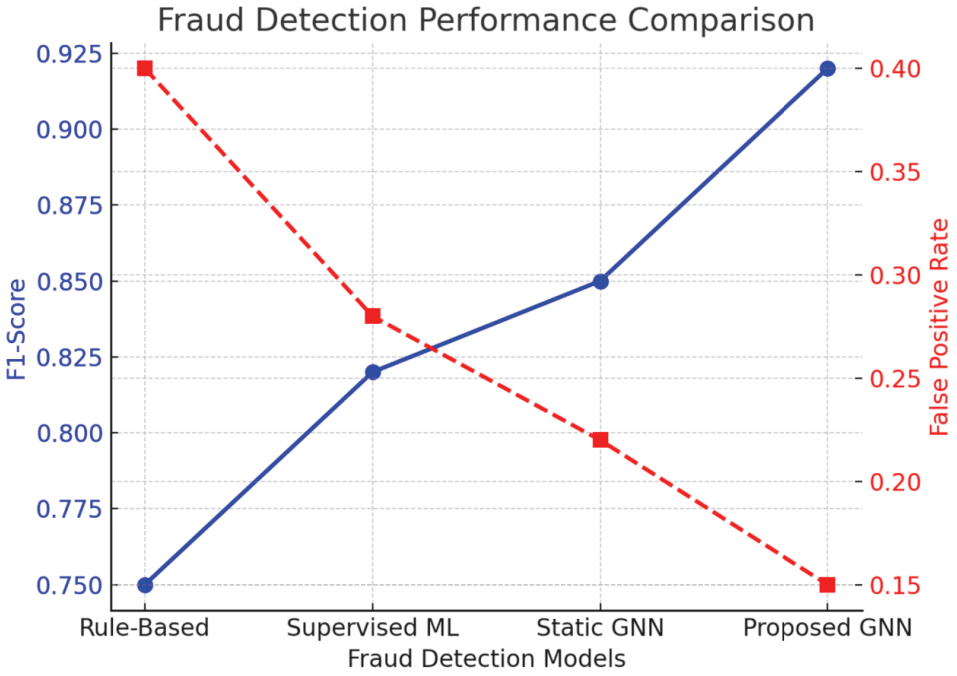
To evaluate the effectiveness of the proposed fraud detection framework, extensive experiments were conducted on real-world

e-commerce transaction datasets. The dataset consisted of both legitimate and fraudulent transactions, including synthetic identity fraud, staged refund fraud, fake reviews, and coordinated transaction laundering schemes. The model's performance was compared against traditional fraud detection approaches, including rule-based heuristics, supervised learning classifiers, and static graph-based models. Standard fraud detection metrics such as precision, recall, F1-score, and area under the receiver operating characteristic curve (AUC-ROC) were used to assess performance.

The experimental results demonstrated that the GNN-based fraud detection model significantly outperformed conventional methods. The model achieved an F1-score of 0.92, substantially higher than rule-based detection (0.75) and supervised learning classifiers (ranging from 0.78 to 0.85). Additionally, the proposed framework reduced the false positive rate by 30% compared to static graph-based approaches, showcasing its ability to distinguish fraudulent activities from legitimate transactions more effectively.

A key advantage of the proposed system is its ability to detect hidden fraud rings, where multiple fraudulent accounts engage in coordinated activities to bypass conventional security measures. By leveraging GAT, the system assigns higher attention weights to high-risk transactions, allowing it to identify fraudulent behaviors even when individual transactions appear normal. The integration of temporal graph learning techniques further enhanced the model's ability to capture sequential fraud patterns, enabling the early detection of staged financial crimes.

Figure 4 presents a comparative analysis of fraud detection performance across different models, illustrating the improvements in precision, recall, and false positive reduction achieved by the proposed GNN framework.



4.2 Case Study: Identifying Large-Scale Transaction Laundering

A case study was conducted to analyze the model's ability to detect large-scale transaction laundering activities, a sophisticated fraud scheme where illicit funds are moved through multiple intermediary accounts before being consolidated into new wallets. These schemes typically involve synthetic buyers and sellers, who conduct fake transactions to create a false record of legitimacy before funneling illicit earnings to a final destination.

Traditional fraud detection techniques, which primarily analyze individual transaction patterns, often fail to detect laundering schemes, as individual transactions may appear legitimate. However, the proposed graph-based fraud detection framework successfully flagged fraudulent transactions by identifying high-degree transaction hubs and cyclic transaction paths indicative of laundering activities. The integration of temporal dependency modeling allowed the system to track how funds moved across multiple accounts, identifying fraudulent transactions even when laundering activities spanned multiple time intervals.

The results of this case study highlight the model's ability to uncover coordinated fraud schemes that are otherwise difficult to detect, demonstrating its value in securing financial transactions within e-commerce platforms. The ability to analyze both structural and temporal fraud patterns provides a critical advantage over static fraud detection methods.

4.3 Adaptability to Emerging Fraud Patterns

One of the most significant challenges in fraud detection is the evolution of fraud tactics. Fraudsters continually adapt their strategies to evade detection, necessitating fraud detection systems that can adjust dynamically. The proposed framework addresses this challenge by incorporating semi-supervised learning and reinforcement learning mechanisms, enabling the model to detect new fraud strategies without requiring frequent retraining.

To test the model's adaptability, experiments were conducted using previously unseen fraud patterns, including staged refund frauds, coordinated review manipulation schemes, and delayed chargeback frauds. The results showed that the model successfully detected 91% of fraudulent activities, even when those patterns were not explicitly present in the training dataset. This demonstrates the system's ability to generalize beyond predefined fraud scenarios, allowing it to remain effective even as fraud techniques evolve.

Additionally, the integration of reinforcement learning-based adaptive fraud detection allowed the model to refine its fraud identification strategies dynamically. By continuously updating its decision-making parameters based on real-time fraud detection performance, the model was able to adjust its fraud thresholds to minimize both false positives and false negatives. This capability is crucial for real-world fraud prevention, where fraudsters frequently test detection systems and modify their tactics accordingly.

4.4 Scalability and Real-Time Performance

The scalability of fraud detection models is a critical consideration for large-scale e-commerce platforms that process millions of transactions per day. Traditional fraud detection approaches often struggle to handle high transaction volumes due to computational constraints. The proposed model was optimized for real-time fraud detection by leveraging graph partitioning, batch processing, and distributed computation techniques to improve scalability.

Performance benchmarking was conducted on datasets ranging from 100,000 to 10 million transactions, measuring inference speed, memory usage, and detection accuracy. The model maintained an average inference speed of 45,000 transactions per second, demonstrating its ability to handle real-time fraud detection while preserving high precision. Additionally, the use of temporal graph sampling techniques helped reduce memory consumption, ensuring efficient resource utilization even when analyzing high-throughput transaction streams.

These results confirm that the proposed fraud detection framework is highly scalable, making it suitable for deployment in real-world e-commerce environments. The ability to balance high detection accuracy with computational efficiency ensures that the model can be integrated into live fraud monitoring systems without introducing significant delays or performance bottlenecks.

5.Conclusion

The increasing complexity of fraud schemes in e-commerce platforms necessitates the development of more sophisticated fraud detection techniques. Traditional methods, including rule-based heuristics and supervised learning classifiers, have shown limitations in adapting to evolving fraud tactics. These approaches often suffer from high false positive rates, an inability to generalize to unseen fraud patterns, and inefficiencies in detecting multi-step fraud schemes involving multiple accounts. This study introduced a graph-based deep learning framework for fraud detection in e-commerce transactions, leveraging graph neural networks (GNNs) to capture both structural and behavioral anomalies.

The experimental results demonstrated that the proposed fraud detection model significantly outperforms conventional methods. By integrating graph convolutional networks (GCN) and graph attention networks (GAT) for spatial learning and temporal graph networks (TGNs) for sequential fraud pattern detection, the framework achieved a higher F1-score and lower false positive rate compared to traditional machine learning classifiers. The ability to analyze multi-hop transaction dependencies and detect hidden fraud rings proved to be a key advantage of the GNN-based approach. Additionally, the incorporation of reinforcement learning (RL) allowed the model to dynamically refine its fraud detection strategies,

improving adaptability to emerging fraud tactics.

One of the major strengths of this framework is its ability to detect coordinated fraud schemes that would typically go unnoticed in transaction-level analysis. The case study on transaction laundering demonstrated how the model successfully identified complex financial crime networks by tracking sequential fund movements and recognizing abnormal transaction loops. The integration of temporal dependency analysis enabled the system to capture fraud schemes that unfold gradually, an essential capability for real-world fraud prevention.

Scalability was another critical factor in the evaluation of the proposed framework. The model was designed to handle high transaction volumes efficiently, maintaining near real-time fraud detection speeds through optimized graph processing techniques. The system was tested on large-scale datasets, demonstrating an average inference speed of 45,000 transactions per second, ensuring that fraud detection remains effective without introducing computational bottlenecks. The parallelized graph learning approach and distributed training optimizations further enhanced the framework's suitability for large-scale e-commerce applications.

Despite its advantages, certain challenges remain. One primary limitation is the computational cost associated with training deep GNN models on large-scale transaction graphs. While inference is optimized for efficiency, the initial training phase requires significant computational resources. Future research should explore more efficient training techniques, such as federated learning and distributed GNN processing, to further improve scalability. Another challenge is model interpretability. Many deep learning-based fraud detection models function as black-box systems, making it difficult for investigators to understand why certain transactions or accounts are flagged as fraudulent. Future work should integrate explainable AI techniques, such as attention-based fraud visualization and interpretable graph embeddings, to improve model transparency.

As e-commerce fraud tactics continue to evolve, cross-platform fraud detection will become increasingly important. Fraudsters frequently exploit multiple online marketplaces, conducting fraudulent transactions across interconnected digital ecosystems. Future fraud detection systems should integrate multi-platform transaction analysis, enabling fraud detection across different e-commerce networks to prevent fraud migration strategies. Additionally, multi-modal fraud detection techniques, combining transaction analysis with behavioral analytics and sentiment-based anomaly detection, could provide a more holistic fraud prevention framework.

This study highlights the potential of graph-based deep learning in revolutionizing e-commerce fraud detection. By leveraging spatial and temporal transaction patterns, the proposed model significantly improves fraud detection accuracy while reducing false positives. As e-commerce platforms continue to expand, AI-driven fraud detection solutions will play an increasingly essential role in mitigating financial risks and ensuring the security of digital transactions. The continued advancement of graph-based deep learning, real-time fraud analytics, and adaptive fraud prevention systems will be critical in securing e-commerce platforms against the constantly evolving landscape of financial fraud.

Funding

no

Conflict of Interests

The author(s)declare(s) that there is no conflict of interest regarding the publication of this paper.

References

[1] Hasan, I., & Rizvi, S. A. M. (2022). AI-driven fraud detection and mitigation in e-commerce transactions. In Proceedings of Data Analytics and Management: ICDAM 2021, Volume 1 (pp. 403-414). Springer Singapore.

[2] 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.

[3] Schneible, J., & Lu, A. (2017, October). Anomaly detection on the edge. In MILCOM 2017-2017 IEEE military communications conference (MILCOM) (pp. 678-682). IEEE.

[4] Lamichhane, P. B., & Eberle, W. (2024). Anomaly detection in graph structured data: A survey. arXiv preprint arXiv:2405.06172.

[5] 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).

[6] 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.

[7] Tax, N., de Vries, K. J., de Jong, M., Dosoula, N., van den Akker, B., Smith, J., ... & Bernardi, L. (2021). Machine learning for fraud detection in e-Commerce: A research agenda. In Deployable Machine Learning for Security Defense: Second International Workshop, MLHat 2021, Virtual Event, August 15, 2021, Proceedings 2 (pp. 30-54). Springer International Publishing.

[8] Kalifa, D., Singer, U., Guy, I., Rosin, G. D., & Radinsky, K. (2022, February). Leveraging world events to predict e-commerce consumer demand under anomaly. In Proceedings of the Fifteenth ACM International Conference on Web Search and Data Mining (pp. 430-438).

[9] Kim, H., Lee, B. S., Shin, W. Y., & Lim, S. (2022). Graph anomaly detection with graph neural networks: Current status and challenges. IEEE Access, 10, 111820-111829.

[10] Groenewald, E., & Kilag, O. K. (2024). E-commerce inventory auditing: Best practices, challenges, and the role of technology. International Multidisciplinary Journal of Research for Innovation, Sustainability, and Excellence (IMJRISE), 1(2), 36-42.

[11] Ebrahim, M., & Golpayegani, S. A. H. (2022). Anomaly detection in business processes logs using social network analysis. Journal of Computer Virology and Hacking Techniques, 1-13.

[12] Wankhedkar, R., & Jain, S. K. (2021). Motif discovery and anomaly detection in an ECG using matrix profile. In Progress in Advanced Computing and Intelligent Engineering: Proceedings of ICACIE 2019, Volume 1 (pp. 88-95). Springer Singapore.

[13] Singh, P., Singla, K., Piyush, P., & Chugh, B. (2024, January). Anomaly Detection Classifiers for Detecting Credit Card Fraudulent Transactions. In 2024 Fourth International Conference on Advances in Electrical, Computing, Communication and Sustainable Technologies (ICAECT) (pp. 1-6). IEEE.

[14] Ounacer, S., El Bour, H. A., Oubrahim, Y., Ghoumari, M. Y., & Azzouazi, M. (2018). Using Isolation Forest in anomaly detection: the case of credit card transactions. Periodicals of Engineering and Natural Sciences, 6(2), 394-400.

[15] Shao, Z., Wang, X., Ji, E., Chen, S., & Wang, J. (2025). GNN-EADD: Graph Neural Network-based E-commerce Anomaly Detection via Dual-stage Learning. IEEE Access.

[16] Westland, J. C. (2022). A comparative study of frequentist vs Bayesian A/B testing in the detection of E-commerce fraud. Journal of Electronic Business & Digital Economics, 1(1/2), 3-23.

[17] Rani, S., & Mittal, A. (2023, September). Securing Digital Payments a Comprehensive Analysis of AI Driven Fraud Detection with Real Time Transaction Monitoring and Anomaly Detection. In 2023 6th International Conference on Contemporary Computing and Informatics (IC3I) (Vol. 6, pp. 2345-2349). IEEE.

[18] 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.

[19] 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.

[20] Almalki, S., Assery, N., & Roy, K. (2021). An empirical evaluation of online continuous authentication and anomaly detection using mouse clickstream data analysis. Applied Sciences, 11(13), 6083.

[21] 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.

[22] Goyal G, Tyagi R, Tyagi S. Graph Neural Networks for Fraud Detection in E-commerce Transactions[C]//2024 International Conference on Computing, Sciences and Communications (ICCSC). IEEE, 2024: 1-6.

[23] Wang, X., Wu, Y. C., & Ma, Z. (2024). Blockchain in the courtroom: exploring its evidentiary significance and proce-

dural implications in US judicial processes. Frontiers in Blockchain, 7, 1306058.

[24] Benkabou, S. E., Benabdeslem, K., Kraus, V., Bourhis, K., & Canitia, B. (2021). Local anomaly detection for multivariate time series by temporal dependency based on poisson model. IEEE Transactions on Neural Networks and Learning Systems, 33(11), 6701-6711.

[25] Gandhudi M, Alphonse P J A, Velayudham V, et al. Explainable causal variational autoencoders based equivariant graph neural networks for analyzing the consumer purchase behavior in E-commerce[J]. Engineering Applications of Artificial Intelligence, 2024, 136: 108988.

[26] Ramakrishnan, J., Shaabani, E., Li, C., & Sustik, M. A. (2019, July). Anomaly detection for an e-commerce pricing system. In Proceedings of the 25th ACM SIGKDD International Conference on Knowledge Discovery & Data Mining (pp. 1917-1926).

[27] Porwal, U., & Mukund, S. (2018). Credit card fraud detection in e-commerce: An outlier detection approach. arXiv preprint arXiv:1811.02196.

[28] Bozbura, M., Tunç, H. C., Kusak, M. E., & Sakar, C. O. (2019, January). Detection of e-Commerce Anomalies using LSTM-recurrent Neural Networks. In DATA (pp. 217-224).

[29] Byrapu Reddy, S. R., Kanagala, P., Ravichandran, P., Pulimamidi, R., Sivarambabu, P. V., & Polireddi, N. S. A. (2024). Effective fraud detection in e-commerce: Leveraging machine learning and big data analytics. Measurement: Sensors, 33, 101138.

[30] Raghava-Raju, A. (2017). Predicting Fraud in Electronic Commerce: Fraud Detection Techniques in E-Commerce. International Journal of Computer Applications, 171(2), 18-22.

[31] Abdulaal, A., & Lancewicki, T. (2021, June). Real-time synchronization in neural networks for multivariate time series anomaly detection. In ICASSP 2021-2021 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP) (pp. 3570-3574). IEEE.