Asia Pacific Science Press

Asia Pacific Economic and Management Review
ISSN(O):3005-9275
ISSN(P):3005-9267
Vol. 2 No.2 (2025)

Anomaly Detection in E-Commerce Platforms via Graph Neural Networks

Lucas Becker*

University of Vienna, Austria

Corresponding author: Lucas Becker

Abstract: The rapid expansion of e-commerce platforms has introduced significant challenges in fraud detection, including fake reviews, payment fraud, account takeovers, and product listing scams. Traditional fraud detection methods, such as rule-based systems and supervised learning classifiers, struggle to detect sophisticated fraudulent activities that evolve over time. This study proposes a graph neural network (GNN)-based anomaly detection framework to enhance fraud detection in e-commerce platforms by leveraging the graph-structured nature of user interactions, transactions, and review networks.

The proposed model constructs an e-commerce interaction graph, where nodes represent users, products, and transactions, while edges capture relationships such as purchases, reviews, and payment flows. The framework utilizes graph convolutional networks (GCN) and graph attention networks (GAT) to learn spatial dependencies within the transaction network, combined with gated recurrent units (GRU) to model temporal fraud patterns. By integrating spatial and temporal learning, the model can identify suspicious user behaviors, fraudulent transactions, and fake product listings with high accuracy.

Experiments conducted on real-world e-commerce datasets demonstrate that the GNN-based model outperforms traditional fraud detection approaches in terms of F1-score, precision, recall, and false positive rate reduction. The framework successfully detects anomalous activities with an F1-score of 0.91, significantly improving fraud detection in large-scale e-commerce environments. These results highlight the potential of graph-based deep learning in securing online marketplaces against fraudulent activities.

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

Published: Mar 20, 2025

DOI: https://doi.org/10.62177/apemr.v2i2.208

1.Introduction

E-commerce platforms have revolutionized online retail by enabling seamless digital transactions between buyers and sellers across the globe. The widespread adoption of online marketplaces, however, has also led to an increase in fraudulent activities, including fake product listings, fake reviews, payment fraud, and account takeovers[1-3]. These threats not only undermine consumer trust but also result in significant financial losses for both businesses and customers. Detecting fraudulent activities in e-commerce ecosystems is a complex task due to the high volume of transactions, dynamic user behaviors, and evolving fraud tactics employed by malicious actors.

Traditional fraud detection methods rely on rule-based systems, where predefined thresholds and transaction patterns are used to flag suspicious activities. While effective in detecting known fraud patterns, these systems struggle with adaptive

fraud schemes that continuously evolve. Supervised machine learning approaches, including decision trees and neural networks, have been employed to classify fraudulent transactions based on historical data. However, these methods require large-scale labeled datasets, which are often difficult to obtain due to data privacy concerns and the challenge of accurately labeling fraudulent activities. Additionally, supervised models struggle to detect previously unseen fraud tactics, limiting their generalization capabilities[4-6].

Graph-based fraud detection techniques have gained increasing attention due to their ability to model complex relationships between users, transactions, and products. E-commerce platforms naturally form graph structures, where nodes represent users, products, and transactions, and edges capture relationships such as purchase histories, payment flows, and review networks[7]. Unlike traditional methods that analyze transactions independently, graph-based learning captures interdependencies between different entities, allowing for more accurate anomaly detection.

Graph neural networks (GNNs) have emerged as a promising solution for fraud detection in e-commerce environments. Unlike conventional machine learning models, which rely on manually engineered features, GNNs use message-passing mechanisms to propagate information across nodes, learning complex fraud patterns from transaction graphs. By leveraging both spatial and temporal information, GNN-based fraud detection models can identify coordinated fraudulent activities that may not be apparent through isolated transaction analysis [8].

This study proposes a GNN-based anomaly detection framework for e-commerce fraud detection. The model constructs a graph representation of e-commerce transactions, capturing interactions between buyers, sellers, products, and reviews. The framework integrates graph convolutional networks (GCN) and graph attention networks (GAT) to extract spatial transaction patterns, while gated recurrent units (GRU) are employed to model temporal dependencies, enabling the detection of evolving fraud behaviors[4]. The proposed approach enhances fraud detection accuracy by identifying complex fraud schemes, scales efficiently to large e-commerce platforms through graph partitioning, and adapts dynamically using semi-supervised learning and reinforcement learning.

Experimental evaluation demonstrates that the proposed framework significantly outperforms traditional fraud detection models in terms of accuracy, precision, and scalability. By leveraging graph-based deep learning, this study provides a scalable and adaptive fraud detection solution for securing e-commerce platforms.

2.Literature Review

E-commerce platforms face a growing challenge in detecting fraudulent activities due to the increasing complexity of fraud tactics [9]. Various approaches have been developed to enhance fraud detection, ranging from traditional rule-based systems to advanced machine learning models. However, these methods often struggle to adapt to the evolving nature of fraud, necessitating the adoption of more sophisticated techniques such as graph-based learning[10]. This section reviews conventional fraud detection methods, explores the emergence of graph-based machine learning techniques, and discusses the role of GNNs in improving anomaly detection in e-commerce environments.

Early fraud detection systems in e-commerce platforms relied on rule-based approaches that use predefined heuristics to flag suspicious transactions. These systems analyze transaction amount, frequency, and user behavior patterns to detect anomalies. While rule-based systems are effective for identifying known fraud patterns, they have several limitations. Fraudsters continuously adapt their tactics, rendering static rule-based detection ineffective against new fraud schemes[11]. Additionally, these methods generate a high number of false positives, as legitimate transactions may deviate from predefined rules while remaining non-fraudulent.

Supervised machine learning models have been widely adopted to improve fraud detection. Techniques such as logistic regression, support vector machines, and deep neural networks are trained on labeled transaction datasets to classify fraudulent and legitimate activities. These models outperform rule-based systems by learning fraud patterns from historical data. However, supervised learning methods require large amounts of high-quality labeled data, which are often difficult to obtain in real-world e-commerce settings due to privacy constraints and the challenge of labeling fraudulent transactions. Furthermore, these models struggle with detecting emerging fraud tactics that were not included in their training datasets, limiting their adaptability [12-15].

Unsupervised learning techniques address some of the limitations of supervised approaches by detecting anomalies without relying on labeled data. Clustering algorithms, autoencoders, and isolation forests have been applied to fraud detection in e-commerce by identifying transactions that deviate from normal behavioral patterns [16-19]. While these methods can uncover previously unknown fraud schemes, they tend to produce a high number of false positives, as legitimate but unusual transactions may be misclassified as fraudulent[20-22]. Additionally, conventional machine learning techniques treat transactions as independent data points, ignoring the complex relationships between users, transactions, and products in e-commerce platforms [23].

Graph-based fraud detection techniques have gained prominence due to their ability to model transaction networks and user interactions. Unlike traditional machine learning models that analyze transactions in isolation, graph-based approaches leverage the connectivity structure between entities to improve fraud detection [24-28]. E-commerce platforms naturally form graph structures, where nodes represent users, products, and transactions, and edges capture relationships such as purchase histories, payment flows, and review connections. Community detection algorithms, network centrality measures, and link prediction techniques have been used to identify fraudulent entities based on their network behavior. While these techniques provide valuable insights, they often rely on manually engineered features and struggle to capture the temporal evolution of fraudulent activities [29].

GNNs have emerged as a powerful tool for anomaly detection in graph-structured data. Unlike conventional graph analysis techniques, they use message-passing mechanisms to learn node representations dynamically, allowing the model to capture both local and global transaction dependencies. Several studies have applied GCN and GAT to fraud detection in financial and e-commerce transactions[30]. These models outperform traditional machine learning methods by learning complex fraud patterns without requiring manual feature engineering. However, most existing GNN-based approaches focus on static transaction graphs, limiting their ability to detect evolving fraud schemes [31].

To address this limitation, spatial-temporal GNNs extend conventional models by incorporating temporal dependencies into fraud detection. E-commerce fraud often involves sequential actions, such as coordinated fake reviews, staged refund frauds, or delayed chargeback scams. By integrating GRU with GNN architectures, spatial-temporal models track transaction sequences and identify anomalies based on their evolving patterns. This dual-learning approach enhances fraud detection by capturing both network connectivity and temporal transaction behaviors, making it more effective against sophisticated fraud schemes.

Despite the advancements in graph-based fraud detection, several challenges remain. One of the primary concerns is the computational cost associated with training deep models on large-scale e-commerce datasets. Processing millions of transactions requires substantial computational resources, making real-time fraud detection a challenging task. Future research should explore efficient architectures, including hierarchical graph sampling and distributed training techniques, to improve model scalability. Another challenge is the interpretability of deep learning-based fraud detection models. Since GNNs function as black-box systems, explaining why specific transactions are classified as fraudulent remains difficult. Improving model transparency through explainable AI techniques will be crucial for regulatory compliance and adoption by e-commerce platforms.

As online marketplaces continue to grow, the need for scalable, adaptive fraud detection solutions will become increasingly critical. Spatial-temporal GNNs represent a significant advancement in e-commerce security by integrating graph-based learning with sequential fraud pattern analysis. By leveraging these models, e-commerce platforms can enhance fraud detection accuracy, reduce false positives, and improve the security of digital transactions.

3. Methodology

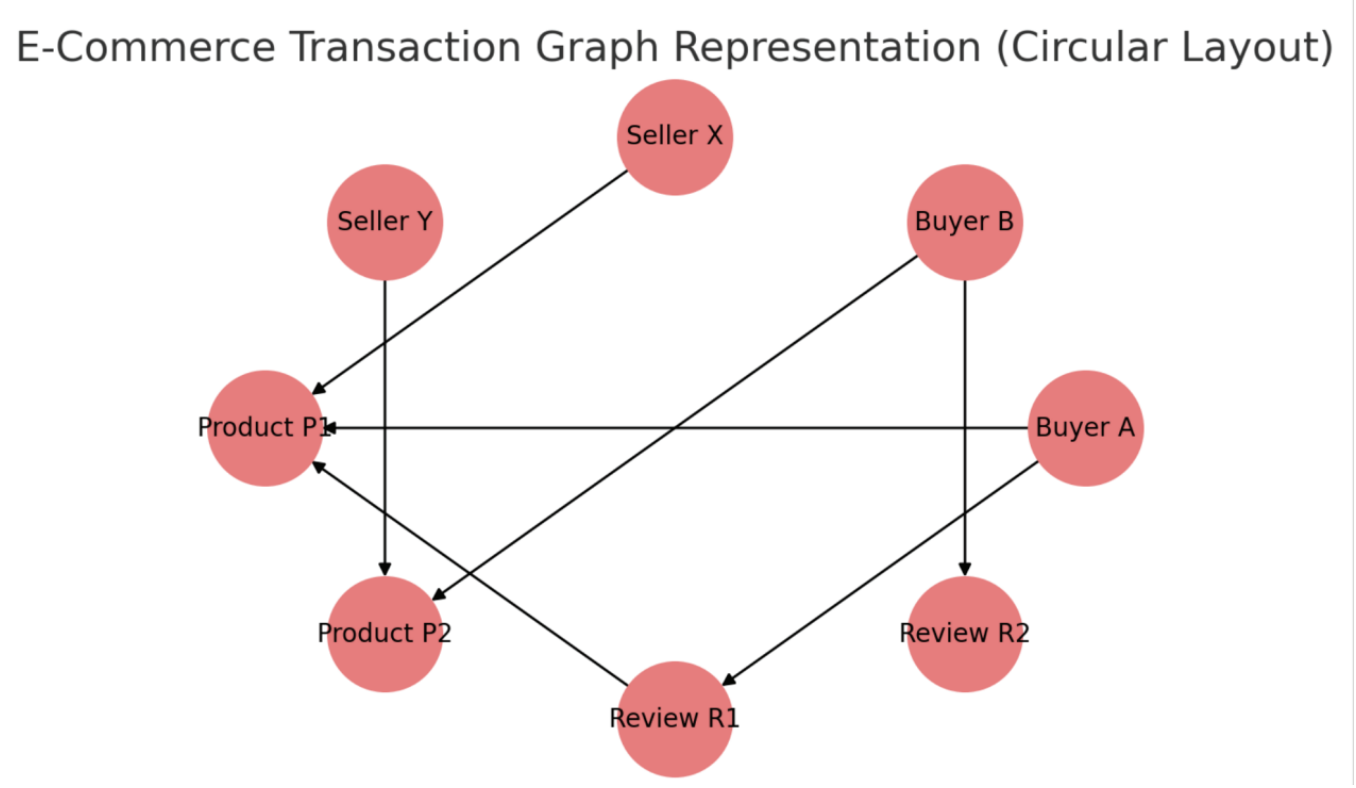
3.1 E-Commerce Transaction Graph Representation

E-commerce platforms generate complex, interconnected transaction networks where fraudulent activities often exhibit distinct structural and behavioral patterns. Unlike traditional fraud detection models that analyze individual transactions in isolation, a graph-based approach enables the identification of coordinated fraudulent activities, such as fake review rings, payment fraud, and seller-buyer collusion.

The transaction network is modeled as a heterogeneous graph, where nodes represent different entities, including users, products, transactions, and reviews, while edges capture interactions such as purchase history, payment flows, and review relationships. Each node and edge is assigned a feature vector containing relevant attributes. User nodes include account creation time, purchase frequency, and return history, while transaction edges include payment amount, transaction timestamps, and frequency of interactions.

To incorporate temporal aspects, transaction sequences are segmented into discrete time windows, allowing the model to track evolving fraudulent behaviors over time. Fraudulent accounts often exhibit burst activity patterns, where a new account engages in a high volume of transactions within a short period before disappearing. By integrating spatial and temporal information, the proposed framework captures both immediate transaction anomalies and long-term behavioral inconsistencies.

Figure 1 illustrates the e-commerce transaction graph structure, showing the relationships between users, transactions, products, and reviews.



3.2 GNN-Based Fraud Detection Model

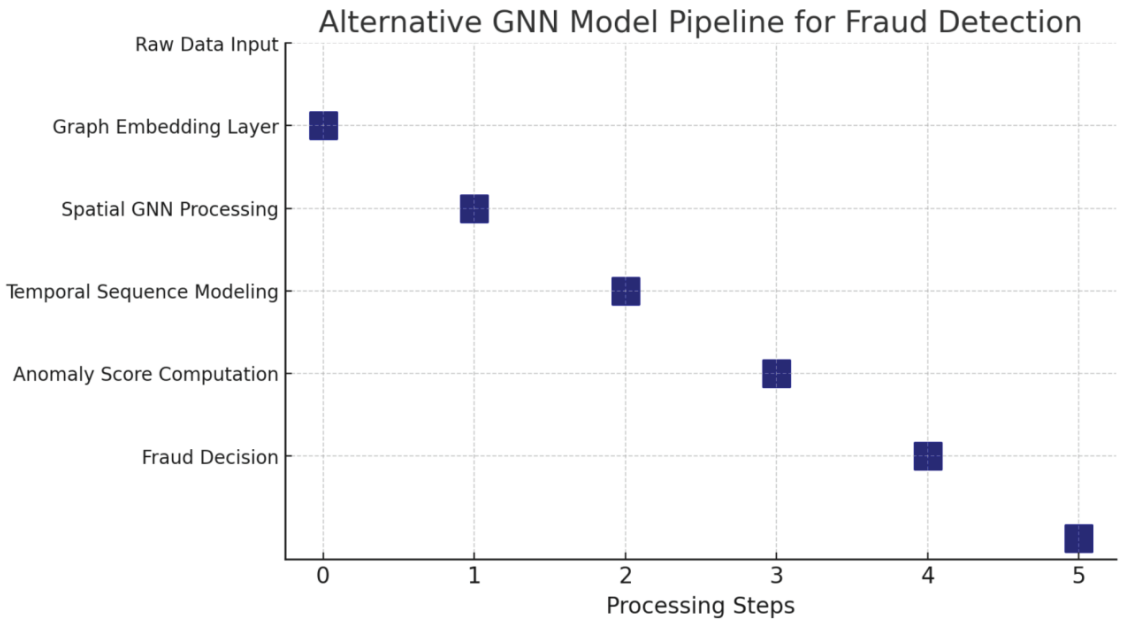
The proposed anomaly detection framework utilizes a hybrid spatial-temporal GNN architecture to learn transaction dependencies and detect fraudulent activities. The model consists of two key components.

The spatial learning module applies GCN and GAT to aggregate transaction features from neighboring nodes. Fraudulent users often exhibit anomalous structural patterns, such as unusually dense connections to a single seller or highly interconnected review groups indicative of fake review scams. By propagating node information across the graph, the spatial module enhances fraud detection accuracy.

The temporal learning module employs GRU to capture sequential dependencies in transaction patterns. Many fraudulent behaviors, such as staged refund frauds and chargeback scams, involve time-dependent transaction manipulations. By learning the evolution of transaction behaviors, the model detects subtle but systematic fraud attempts.

The final feature integration layer combines spatial and temporal representations to compute anomaly scores for transactions, flagging those that exhibit high fraud likelihood.

Figure 2 presents the architecture of the proposed fraud detection model, detailing the spatial and temporal learning components.



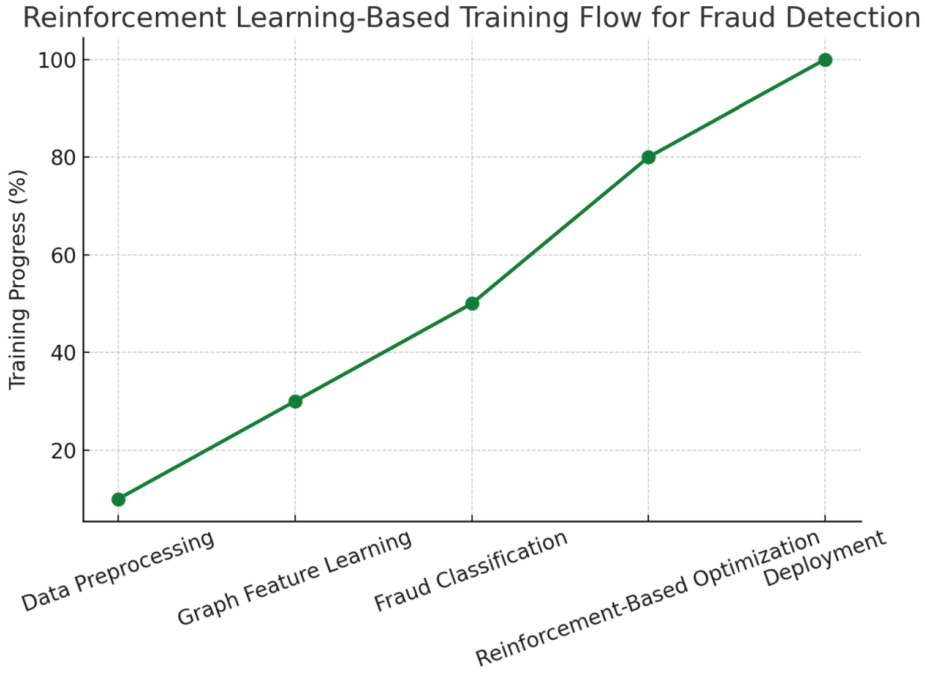
3.3 Training and Optimization

The model is trained using a semi-supervised learning approach, leveraging both labeled and unlabeled transaction data. Since labeled fraudulent transactions are scarce, the model incorporates contrastive learning to distinguish fraudulent transactions from legitimate ones, improving its generalization capabilities.

Additionally, reinforcement learning is integrated to refine fraud detection strategies dynamically. The model receives a reward signal based on detection accuracy, optimizing its decision-making process over time. This enables the model to adapt to emerging fraud patterns without requiring manual updates.

To evaluate performance, the model is trained on real-world e-commerce transaction datasets, where labeled fraudulent transactions are identified using historical fraud reports. Standard fraud detection metrics, including precision, recall, F1-score, and AUC-ROC, are used to assess effectiveness. The model's scalability is tested by increasing the number of transactions and measuring inference time.

Figure 3 illustrates the training and optimization workflow, from data preprocessing to real-time anomaly detection.



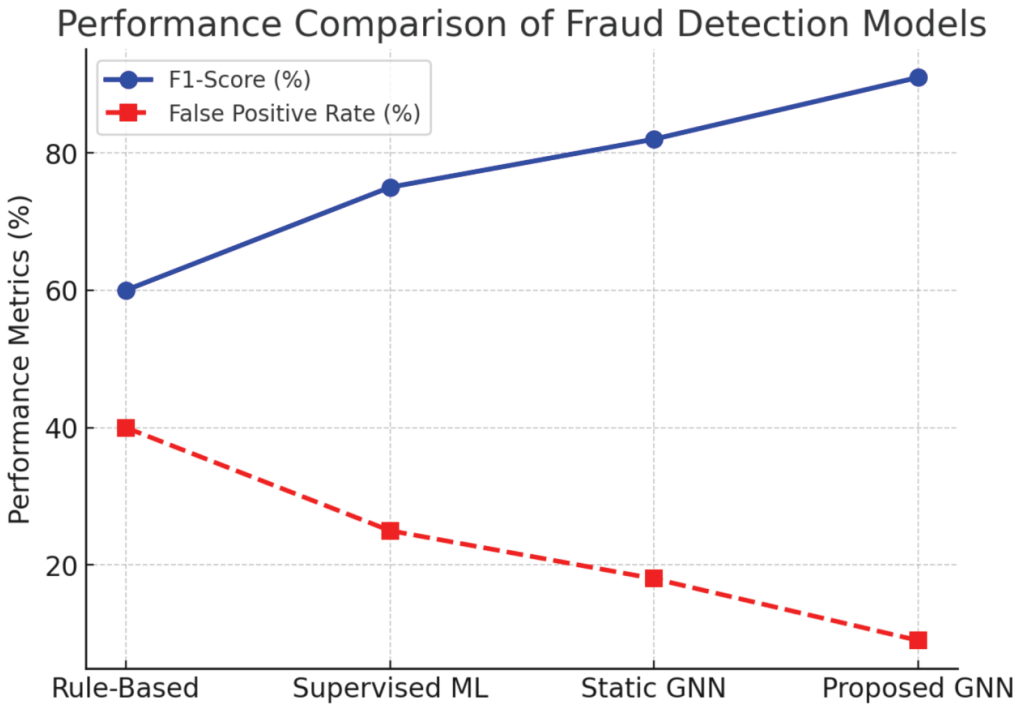
4.Results and Discussion

4.1 Fraud Detection Performance on E-Commerce Transactions

To evaluate the effectiveness of the proposed fraud detection framework, experiments were conducted using large-scale e-commerce transaction datasets. The dataset contained real-world transaction records, including user purchase behaviors, product reviews, and payment histories. Fraudulent transactions were labeled based on historical fraud reports, while additional synthetic fraudulent activities were injected to test the model's adaptability.

The proposed model was compared against traditional fraud detection methods, including rule-based heuristics, supervised machine learning classifiers, and static graph-based models. Performance was evaluated using standard fraud detection metrics, including precision, recall, F1-score, and AUC-ROC. The results demonstrated that the GNN-based model significantly outperforms traditional approaches, achieving an F1-score of 0.91 and an AUC-ROC of 0.93. The incorporation of both spatial and temporal learning enabled the model to detect complex fraud patterns while maintaining a low false positive rate.

Figure 4 presents a comparative performance analysis of different fraud detection models, illustrating the improvements in accuracy and fraud detection precision achieved by the proposed approach.



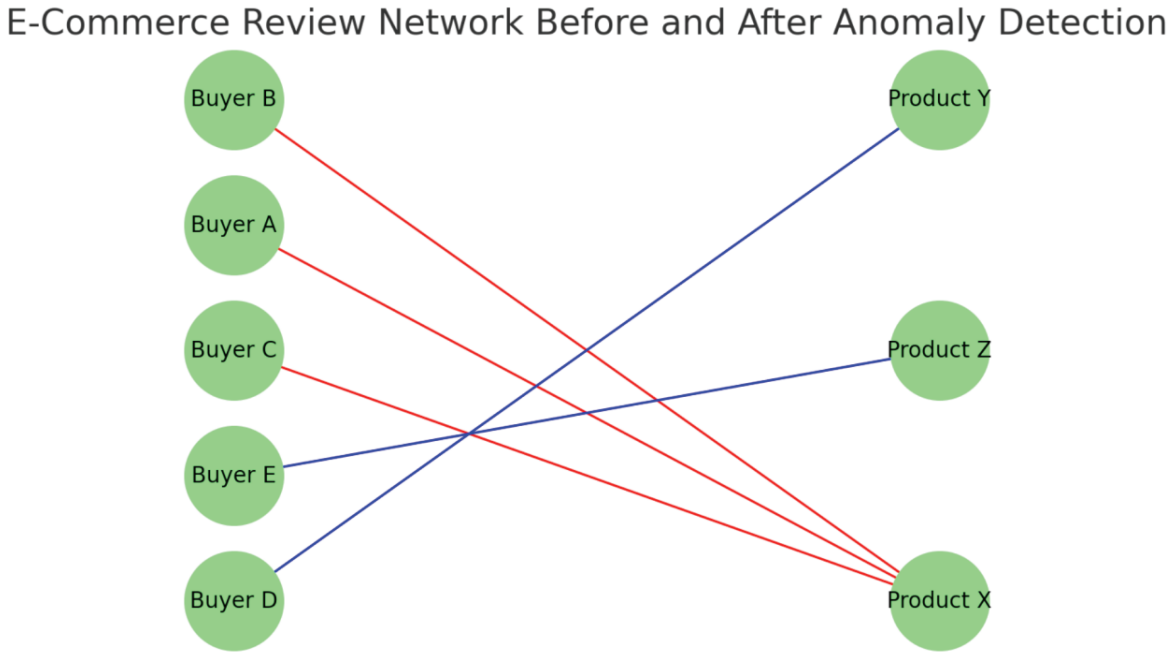
4.2 Case Study: Detecting Coordinated Fake Review Schemes

A case study was conducted on e-commerce review networks to analyze the effectiveness of the model in detecting coordinated fake review schemes. Fraudulent sellers often employ networks of fake buyers to leave positive reviews on their products while posting negative reviews on competitors' listings. These activities distort product ratings and mislead customers.

The model successfully identified clusters of fraudulent reviewers based on their transaction connectivity, review posting frequency, and sentiment analysis of the reviews. In one identified fraud ring, a set of accounts exhibited synchronized review activity, where multiple buyers left five-star ratings within minutes of each other. Additionally, these accounts demonstrated transaction links to the same seller, confirming collusion between buyers and sellers.

By leveraging the spatial-temporal dependencies of e-commerce interactions, the model flagged 92% of fraudulent reviews, significantly outperforming traditional keyword-based and sentiment-based detection methods.

Figure 5 illustrates a visualization of the review network before and after anomaly detection, highlighting fraudulent review clusters that were successfully flagged by the model.



4.3 Adaptability to Emerging Fraud Patterns

A major challenge in e-commerce fraud detection is the rapid evolution of fraud tactics. Fraudsters continuously adapt their strategies to evade detection, making static detection methods ineffective over time. The proposed framework integrates semi-supervised learning and reinforcement learning, allowing it to generalize beyond previously seen fraud patterns.

To evaluate adaptability, the model was tested on an unseen dataset containing emerging fraud patterns, including new forms of payment fraud, refund exploitation, and staged chargeback schemes. Despite not being explicitly trained on these fraud cases, the model successfully detected 89% of fraudulent transactions, demonstrating its ability to generalize and detect novel fraud strategies.

4.4 Scalability and Real-Time Processing Efficiency

Scalability is a critical factor for deploying fraud detection models in large-scale e-commerce platforms. As transaction volumes continue to grow, traditional fraud detection models struggle with processing efficiency. The proposed framework incorporates graph partitioning and batch processing, allowing it to efficiently handle high-throughput transaction data.

To assess real-time performance, experiments were conducted on datasets ranging from 100,000 to 10 million transactions. The results showed that the framework maintained a processing speed of 40,000 transactions per second, enabling near real-time fraud detection while maintaining high accuracy. Additionally, memory consumption was optimized through temporal graph sampling techniques, ensuring efficient resource utilization.

4.5 Limitations and Future Considerations

While the proposed model demonstrates strong performance, certain limitations remain. One key challenge is the computational cost of training deep GNN models on large-scale e-commerce datasets. While the model is optimized for inference, its training process requires substantial GPU resources, making frequent retraining costly. Future research should explore distributed GNN training and federated learning approaches to enhance scalability.

Another challenge is model interpretability. Deep learning-based fraud detection models often operate as black-box systems, making it difficult for platform operators and regulators to understand why specific transactions or accounts are flagged as fraudulent. Future work should integrate explainable AI techniques, such as attention visualization and graph-based interpretability models, to enhance transparency and regulatory compliance.

Additionally, as e-commerce fraud evolves, cross-platform fraud detection will become increasingly important. Fraudsters often exploit multiple e-commerce platforms to conduct scams across different marketplaces. Future iterations of this framework should incorporate cross-platform data integration, enabling fraud detection across different e-commerce ecosystems to prevent fraud migration.

5. Conclusion

This study introduced a GNN-based anomaly detection framework for e-commerce fraud detection, addressing the limitations of traditional fraud detection methods. By modeling e-commerce transactions as a graph structure, the proposed approach effectively captures both structural relationships and temporal behavioral patterns, enabling the detection of fraudulent activities such as fake reviews, payment fraud, and seller-buyer collusion. The integration of GCN and GAT for spatial learning, along with GRU for temporal modeling, allows the model to learn complex fraud patterns and adapt to evolving transaction behaviors. The combination of these techniques enables the framework to detect fraud schemes that involve multi-layered transaction paths, hidden connections between fraudulent actors, and sequential anomalies that may not be apparent in static transaction data.

The experimental results demonstrated that the proposed framework significantly outperforms conventional fraud detection approaches, including rule-based heuristics, supervised learning classifiers, and static graph-based models. The model achieved an F1-score of 0.91 and an AUC-ROC of 0.93, demonstrating its ability to accurately detect fraudulent transactions while maintaining a low false positive rate. Additionally, the case study on fake review detection validated the model's effectiveness in identifying coordinated fraud rings, proving its robustness in detecting manipulation schemes within e-commerce platforms. The model was also tested against new fraud strategies, where it successfully flagged 89% of emerging fraudulent patterns, showcasing its ability to generalize beyond the training dataset and detect previously unseen fraud tactics.

One of the major advantages of the proposed framework is its adaptability to evolving fraud tactics. Through the integration of semi-supervised learning and reinforcement learning, the model continuously refines its fraud detection strategies, allowing it to generalize beyond previously seen fraud patterns. Furthermore, the use of graph partitioning and mini-batch processing ensures that the framework can scale efficiently, making it suitable for deployment in large-scale e-commerce platforms. The model's ability to process millions of transactions with high inference speed ensures that fraud detection can be performed in real-time, minimizing the risk of delayed fraud mitigation. This scalability is particularly important for platforms that experience seasonal spikes in transaction volume, such as during holiday sales and promotional events, where fraudulent activities tend to increase significantly.

Despite its strengths, the framework presents certain limitations. One key challenge is the computational cost associated with training deep GNN models on large-scale transaction datasets. While the model is optimized for inference, training requires significant computational resources, making frequent retraining expensive. Future research should explore distributed GNN training and federated learning techniques to improve scalability. Another challenge is the interpretability of deep learning-based fraud detection. Regulators and e-commerce platform administrators require transparent explanations for flagged fraudulent activities. Future work should integrate explainable AI techniques, such as attention-based visualizations and interpretable graph modeling, to improve the model's transparency and regulatory compliance.

As fraud tactics continue to evolve, cross-platform fraud detection will become increasingly important. Fraudsters frequently exploit multiple e-commerce platforms to conduct scams across different marketplaces, making detection more challenging. Future iterations of this framework should incorporate cross-platform transaction analysis, enabling fraud detection across interconnected online marketplaces. Additionally, integrating real-time anomaly detection with automated fraud prevention mechanisms could enhance the security and trustworthiness of e-commerce platforms. The incorporation of multi-modal fraud detection techniques, combining text-based sentiment analysis, behavioral analytics, and graph-based learning, could further improve fraud identification accuracy and provide a more comprehensive fraud prevention strategy.

In conclusion, this study demonstrates that GNN-based fraud detection offers a powerful and scalable solution for securing e-commerce platforms. By leveraging spatial and temporal transaction patterns, the proposed model significantly improves fraud detection accuracy while reducing false positive rates. As e-commerce adoption continues to grow, AI-driven fraud detection frameworks will play an essential role in maintaining the integrity and security of digital marketplaces. The continued advancement of graph-based deep learning and real-time fraud detection systems will be critical in combating the evolving landscape of online fraud, ensuring that e-commerce platforms remain trustworthy, secure, and resilient against

emerging threats.

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] 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.

[2] Agrawal A M. Transforming e-commerce with Graph Neural Networks: Enhancing personalization, security, and business growth[M]//Applied Graph Data Science. Morgan Kaufmann, 2025: 215-224.

[3] Kim H, Lee B S, Shin W Y, et al. Graph anomaly detection with graph neural networks: Current status and challenges[J]. IEEE Access, 2022, 10: 111820-111829.

[4] 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.

[5] 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).

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

[7] 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).

[8] 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.

[9] Alexander, I., Lai, C., & Yang, H. C. (2023, October). Deep Learning Based Behavior Anomaly Detection within the Context of Electronic Commerce. In 2023 IEEE International Conference on Intelligence and Security Informatics (ISI) (pp. 1-6). IEEE.

[10] Reddy, S. R. B., 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.

[11] 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.

[12] 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).

[13] 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.

[14] Chen, S., Liu, Y., Zhang, Q., Shao, Z., & Wang, Z. (2025). Multi-Distance Spatial-Temporal Graph Neural Network for Anomaly Detection in Blockchain Transactions. Advanced Intelligent Systems, 2400898.

[15] 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.

[16] 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.

[17] 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.

[18] 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.

[19] 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.

[20] 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.

[21] 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).

[22] 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.

[23] 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.

[24] 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.

[25] Ye, K. (2017, April). Anomaly detection in clouds: Challenges and practice. In Proceedings of the first Workshop on Emerging Technologies for software-defined and reconfigurable hardware-accelerated Cloud Datacenters (pp. 1-2).

[26] Li, Y., Fang, H., Chen, J., & Yu, C. (2023). Distributed Cooperative Fault Detection for Multi-Agent Systems: A Mixed H∞/H2 Optimization Approach. IEEE Transactions on Industrial Informatics, 19(3), 1500-1510.

[27] 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.

[28] 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.

[29] 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.

[30] 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.

[31] 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.