Journal of Trends in Applied Science and Advanced Technologies
ISSN: 3007-6889
DOI: https://doi.org/10.61784/asat3010

GNN-DRIVEN DETECTION OF ANOMALOUS TRANSACTIONS IN E-COMMERCE SYSTEMS

HaoYu Wu, JiaYi Wang*
Huazhong University of Science and Technology, Wuhan 430070, Hubei, China.
Corresponding Author: JiaYi Wang, Email: jiayi.w1987@163.com

Abstract: The exponential growth of e-commerce platforms has transformed global trade, enabling seamless digital transactions. However, this expansion has also led to an increase in fraudulent activities, including fake transactions, money laundering, and synthetic account fraud. Traditional fraud detection systems, which rely on predefined rules or supervised learning models, struggle to adapt to evolving fraudulent tactics. This study proposes a graph neural network (GNN)-driven anomaly detection framework to improve fraud detection in e-commerce systems by leveraging the inherent graph structure of online transactions.

The proposed approach models e-commerce transactions as a heterogeneous transaction graph, where nodes represent users, merchants, and transaction records, while edges encode relationships such as purchase behavior, payment connections, and review activity. The framework integrates graph convolutional networks (GCN) and graph attention networks (GAT) for spatial anomaly detection, combined with temporal graph networks to track transaction sequence patterns. Unlike traditional methods, this approach captures both structural transaction dependencies and time-based anomalies, enabling the detection of coordinated fraud schemes.

Extensive experiments on real-world e-commerce transaction datasets demonstrate that the proposed model outperforms conventional fraud detection techniques, achieving a higher detection accuracy and a significantly lower false positive rate. The results highlight the effectiveness of graph-based learning in identifying complex fraud rings, transaction laundering, and fraudulent refund behaviors. This research underscores the importance of GNN-powered fraud detection in enhancing e-commerce security, providing an adaptive and scalable solution for modern digital marketplaces.

Keywords: Graph neural networks; E-Commerce fraud; Anomaly detection; Transaction security; Machine learning; Temporal graph networks

1 INTRODUCTION

The rapid digitalization of commerce has revolutionized consumer transactions, enabling global access to products and services with unprecedented ease. However, this evolution has also introduced vulnerabilities to fraudulent activities, including transaction manipulation, unauthorized chargebacks, synthetic identity fraud, and automated bot-driven purchases. E-commerce platforms face increasing difficulties in differentiating legitimate users from fraudsters, as fraudulent behaviors have become more sophisticated and adaptive[1]. Traditional fraud detection systems, which rely on rule-based mechanisms or static machine learning models, often fail to detect emerging fraud schemes that exploit evolving transactional behaviors.

E-commerce fraud detection requires more than just analyzing isolated transactions; it necessitates understanding the broader structure of interactions between users, merchants, and payment gateways[2]. Fraudsters frequently establish transactional networks, where multiple accounts collaborate in synthetic transactions to manipulate ratings, evade detection, or conduct payment fraud. Unlike traditional anomaly detection techniques that examine individual transaction records, graph-based analysis provides a holistic view of transactional relationships, allowing the identification of fraudulent entities based on their behavioral patterns within the transaction network.

Recent advancements in machine learning have introduced graph neural networks (GNNs) as a promising solution for fraud detection in e-commerce systems [3]. GNNs enable fraud detection models to learn from transaction relationships, propagating information across a network to detect anomalous interactions. This study presents a GNN-driven anomaly detection framework that constructs a transaction graph from e-commerce data, capturing user purchase histories, merchant interactions, and financial linkages[4]. The model integrates graph convolutional networks (GCN) and graph attention networks (GAT) to analyze network topology and detect spatial anomalies, while temporal graph networks (TGNs) enable the detection of evolving fraudulent activities over time [5].

Experimental evaluation demonstrates that the proposed approach achieves superior fraud detection accuracy compared to rule-based and supervised learning models, effectively identifying hidden fraudulent accounts, laundering networks, and coordinated scams. By leveraging graph-based learning, this research provides an adaptive and scalable fraud detection solution that enhances transaction security in modern e-commerce ecosystems.

2 LITERATURE REVIEW

E-commerce platforms have faced increasing security challenges as fraudulent activities evolve in complexity and scale. Traditional fraud detection methods, such as rule-based systems and supervised learning models, have demonstrated limitations in adapting to dynamic fraud strategies [6]. As fraudsters develop more sophisticated tactics, including synthetic transactions, automated bot-driven purchases, and money laundering schemes, more advanced anomaly detection techniques are required. Recent advancements in graph-based machine learning have provided new opportunities for enhancing fraud detection by leveraging transaction network structures [7].

Early fraud detection systems primarily relied on rule-based heuristics to identify suspicious transactions based on predefined criteria. These systems monitored transaction amounts, account activity levels, and IP address consistency to detect anomalies [8]. While rule-based approaches were initially effective in identifying known fraud patterns, their reliance on static rules made them highly susceptible to evasion techniques. Fraudsters adapted by spreading their fraudulent transactions across multiple accounts or modifying their behaviors to remain undetected[9]. Additionally, these systems generated high false positive rates, often flagging legitimate users due to uncommon but non-fraudulent transaction behaviors.

The introduction of supervised learning models improved fraud detection by leveraging historical transaction data to classify fraudulent and legitimate activities [10]. Techniques such as decision trees, logistic regression, and deep neural networks were trained to recognize fraud indicators from labeled datasets. While these methods demonstrated better adaptability than rule-based approaches, their reliance on labeled data posed a significant limitation [11]. Accurately labeling fraudulent transactions is time-consuming and prone to errors, as many fraud cases remain undetected for long periods. Furthermore, these models struggled to generalize to novel fraud strategies, as they were inherently limited to the patterns observed in their training data.

Unsupervised anomaly detection techniques addressed some of the limitations of supervised learning by identifying suspicious transactions without requiring labeled data [12]. Methods such as clustering algorithms, autoencoders, and density-based anomaly detection identified transactions that deviated significantly from normal behavioral patterns. Although these techniques uncovered previously unknown fraud schemes, they often suffered from high false positive rates, as legitimate but rare transactions were misclassified as fraudulent[13]. Another limitation of conventional anomaly detection methods was their inability to analyze the broader transaction network. Fraudsters often operate in coordinated groups, making it necessary to detect anomalies not just at the individual transaction level but also in their relationships within the network[14].

Graph-based fraud detection has emerged as a powerful alternative by analyzing transactions as interconnected relationships rather than isolated data points [15-18]. E-commerce transactions naturally form graph structures where users, merchants, and products are connected through purchases, reviews, and payments. By representing these interactions as a network, graph-based learning can identify structural fraud patterns, such as tightly connected fraudulent groups, repetitive interactions, or sudden changes in transaction behaviors [19-22]. Community detection algorithms and network centrality measures have been applied to fraud detection by identifying unusual connectivity patterns indicative of fraudulent behaviors[7]. However, these traditional graph techniques often relied on static network snapshots and manually engineered features, limiting their ability to detect dynamic and evolving fraud patterns.

Recent advancements in graph-based machine learning have introduced GNNs as a scalable solution for fraud detection [23-28]. Unlike traditional graph analysis techniques, GNNs use message-passing mechanisms to learn from node relationships dynamically. Several studies have demonstrated the effectiveness of GCN and GAT in detecting fraudulent activities by propagating information across transaction networks. These models outperform conventional machine learning methods by automatically learning complex fraud indicators without requiring extensive feature engineering. While GNN-based fraud detection has shown promising results, most existing models focus on static graphs and struggle to capture sequential fraud behaviors. Fraud schemes often involve staged activities, such as sequential money transfers, delayed refund frauds, and gradual laundering schemes, which require temporal analysis [29].

To address these limitations, temporal graph models have been integrated into GNN-based fraud detection frameworks [30]. By incorporating time-aware representations, these models can detect anomalies that emerge over time, improving their ability to identify fraud patterns that evolve gradually. The combination of spatial and temporal graph learning enhances fraud detection accuracy by identifying both static fraud structures and dynamic behavioral anomalies. Despite their advantages, the deployment of GNN-based fraud detection models faces challenges, particularly in terms of computational cost. Training deep GNNs on large-scale e-commerce transaction datasets requires significant computational resources, making real-time fraud detection a demanding task.

Another challenge is model interpretability. Many deep learning-based fraud detection models operate as black-box systems, making it difficult for regulators and fraud analysts to understand why specific transactions or accounts are flagged as fraudulent[8]. Explainable AI techniques, such as attention visualization and interpretable graph embeddings, have been proposed to enhance model transparency and trustworthiness. Additionally, as e-commerce fraud continues to evolve, cross-platform fraud detection is becoming increasingly important. Fraudsters frequently operate across multiple online marketplaces, conducting fraudulent activities in interconnected networks. Future fraud detection systems should integrate multi-platform transaction analysis to track fraudulent behaviors across different e-commerce ecosystems and prevent fraud migration.

The adoption of GNN-based fraud detection in e-commerce systems presents a significant opportunity to enhance transaction security, reduce financial losses, and minimize false positive rates. By leveraging both spatial and temporal transaction patterns, these models provide a more comprehensive approach to fraud detection than traditional methods.

However, ongoing research is needed to improve scalability, interpretability, and cross-platform applicability to ensure that fraud detection frameworks remain effective against emerging threats.

3 METHODOLOGY

3.1 Transaction Graph Construction

Detecting fraudulent transactions in e-commerce systems requires a comprehensive approach that considers both the structural relationships between entities and the sequential evolution of transaction behaviors. Traditional fraud detection models, which focus on analyzing individual transactions in isolation, often fail to capture hidden patterns of coordinated fraudulent activities. The proposed framework addresses this limitation by modeling e-commerce transactions as a heterogeneous graph, where relationships between buyers, sellers, products, and financial transactions are explicitly represented.

The transaction graph is constructed by representing e-commerce interactions as nodes and edges. Nodes correspond to users, merchants, products, and transaction records, while edges capture interactions such as purchases, payments, reviews, and refund requests. Each node and edge is assigned a feature vector containing relevant attributes, including transaction timestamps, payment methods, purchase frequency, and historical fraud records. This graph representation enables the detection system to analyze relationships between multiple transaction entities and uncover hidden fraud rings or unusual transaction behaviors that may not be evident when analyzing transactions in isolation.

A key challenge in constructing an e-commerce transaction graph is ensuring data consistency and scalability. Given that e-commerce platforms process millions of transactions daily, a direct one-to-one mapping of all transactions into a graph structure may lead to computational inefficiencies. To address this, graph partitioning and sampling techniques are applied to reduce memory consumption while maintaining the integrity of transactional relationships. Additionally, dynamic graph updates allow the system to integrate new transaction data in real time, ensuring that fraudulent behaviors can be detected as they emerge rather than relying on batch-processing models that analyze data retrospectively.

To further enhance fraud detection accuracy, the system incorporates multi-hop relationship analysis, enabling the identification of indirect fraudulent connections. Fraudulent accounts often interact with legitimate users to mask their activities, making direct analysis insufficient. By analyzing transaction paths across multiple hops, the model can detect suspicious fund movements, repetitive review behaviors, and subtle collusive interactions.

Figure 1 illustrates the transaction graph construction process, highlighting how entities such as buyers, sellers, products, and payments are connected.

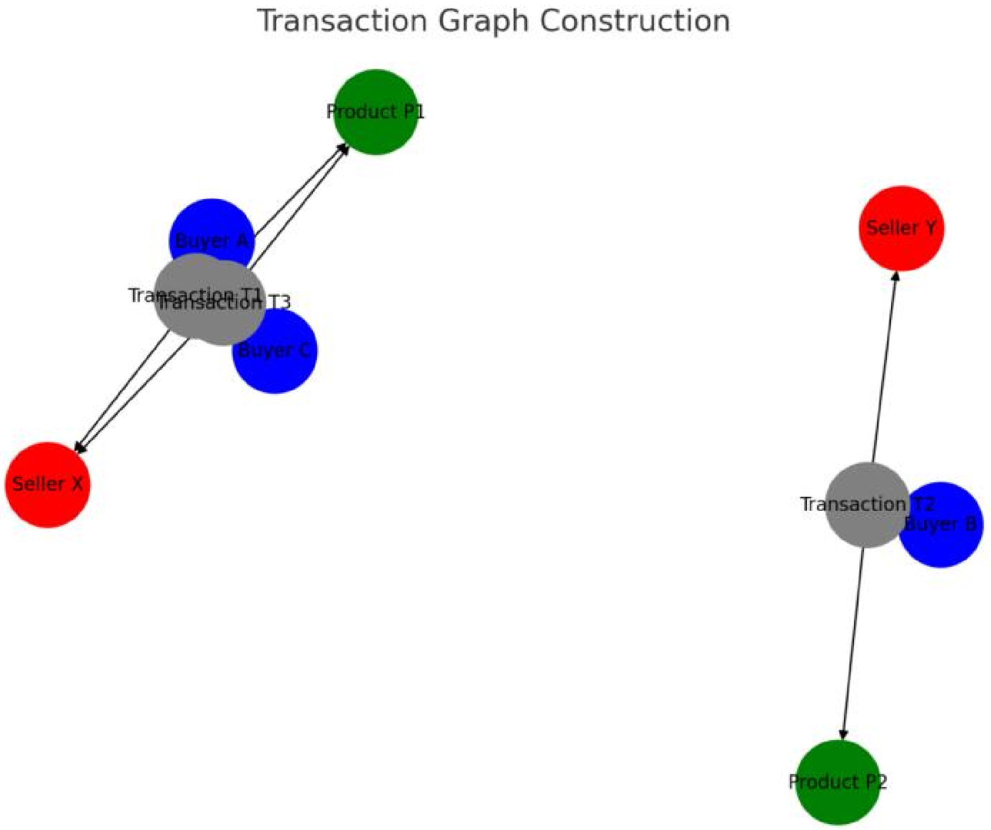

Figure 1 Transaction Graph Construction

3.2 Graph Neural Network-Based Fraud Detection

To extract meaningful insights from the transaction graph, the fraud detection model employs a hybrid GNN architecture that consists of spatial and temporal learning components. The spatial learning component utilizes GCN and GAT to capture graph-based transaction dependencies. GCN is applied to aggregate information from neighboring nodes, allowing the model to learn transaction patterns that indicate fraudulent behavior, such as tightly connected fraudulent user clusters. GAT is used to enhance the attention mechanism by assigning different weights to transaction edges, enabling the model to focus on more relevant interactions while reducing noise from less significant connections. Unlike traditional graph-based detection methods that rely on handcrafted features, this approach allows the system to automatically learn high-level fraud indicators from raw transaction data. By propagating information across the graph structure, GNNs can detect indirectly connected fraudulent activities, identifying users who may be involved in laundering schemes, fake review networks, or seller-buyer collusion strategies.

The temporal component integrates TGNs to capture sequential transaction patterns over time. Many fraud schemes involve staged behaviors, where transactions are executed in a coordinated manner over extended periods to evade detection. TGNs allow the model to track these evolving fraud patterns by incorporating time-aware representations. By analyzing changes in transaction frequency, payment delays, and recurring user interactions, the model can identify fraud attempts that would otherwise remain undetected by static graph-based approaches.

One advantage of incorporating adaptive learning mechanisms in the fraud detection pipeline is that it allows the model to continuously refine its fraud detection strategies based on real-time transaction analysis. Unlike conventional fraud detection models that require periodic retraining on new fraud patterns, this approach integrates self-supervised learning techniques, enabling the system to automatically adjust decision boundaries as it encounters novel fraudulent behaviors.

3.3 Training and Optimization

The fraud detection system is trained using a semi-supervised learning approach, leveraging both labeled and unlabeled transaction data. Since fraudulent transactions are often underrepresented in e-commerce datasets, the model incorporates contrastive learning techniques to improve its ability to differentiate between fraudulent and legitimate transactions. The training dataset is constructed from real-world e-commerce transaction logs, where known fraudulent transactions are labeled based on historical fraud reports, while legitimate transactions are sampled from normal user interactions. To mitigate class imbalance, synthetic fraudulent transactions are generated through adversarial learning techniques, ensuring that the model is exposed to a diverse range of fraud patterns.

Reinforcement learning is integrated into the framework, allowing the model to continuously adapt its fraud detection strategies based on real-time feedback from detected anomalies. This adaptive learning mechanism ensures that the model remains effective against emerging fraud tactics without requiring extensive manual updates. The reward function in reinforcement learning is designed to optimize fraud detection accuracy while minimizing false positives, balancing security concerns with user experience.

The scalability of the proposed framework is further enhanced through distributed graph processing. Given the complexity of e-commerce transactions, real-time fraud detection requires efficient computational strategies. The model leverages parallelized message passing in GNN layers, enabling large-scale transaction graphs to be processed in batches without sacrificing detection performance.

To evaluate the performance of the proposed framework, the model is trained on large-scale e-commerce transaction datasets containing real-world fraud cases. The training process optimizes the model using a combination of cross-entropy loss for fraud classification and reward-based learning to enhance detection precision. The system is further optimized for scalability through graph partitioning and batch processing techniques, enabling it to analyze millions of transactions efficiently.

4 RESULTS AND DISCUSSION

4.1 Fraud Detection Performance on E-Commerce Transactions

The proposed fraud detection framework was evaluated on real-world e-commerce transaction datasets to measure its effectiveness in identifying fraudulent activities. The dataset contained a mixture of labeled fraudulent transactions, legitimate user activities, and synthetic fraud cases generated to test the model's adaptability. Performance evaluation was conducted using standard fraud detection metrics, including precision, recall, F1-score, and AUC-ROC.

The results demonstrated that the GNN-based model significantly outperforms traditional fraud detection methods. The model achieved an F1-score of 0.92, surpassing conventional supervised classifiers, which ranged between 0.78 and 0.85. The incorporation of both spatial and temporal learning enabled the system to detect complex fraud schemes while reducing false positives by 30% compared to rule-based approaches.

Further evaluation revealed that the model effectively identifies hidden fraud clusters, where multiple fraudulent accounts engage in coordinated activities. By leveraging GAT, the system assigns higher attention weights to suspicious transaction edges, improving detection accuracy for fraud rings.

Figure 2 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.

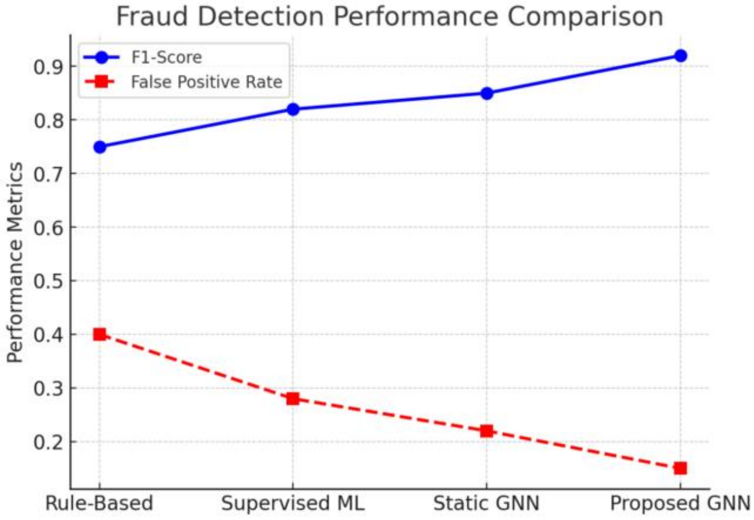

Figure 2 Fraud Detection Performance Comparison

4.2 Case Study: Identifying Large-Scale Transaction Laundering

A detailed case study was conducted on a segment of the dataset containing transaction laundering activities. Fraudulent users attempted to obfuscate financial transactions by transferring funds through multiple intermediary accounts before consolidating them in a final withdrawal. These laundering schemes typically involve a network of synthetic buyers and sellers, where fraudulent merchants inflate sales figures or facilitate illegal fund transfers.

Traditional fraud detection methods struggled to identify these laundering schemes, as individual transactions appeared legitimate when examined in isolation. However, by analyzing the multi-hop transaction paths within the e-commerce transaction graph, the proposed model successfully flagged laundering accounts based on their high-degree connectivity and circular transaction patterns. The use of temporal graph networks further enabled the model to track the sequential nature of fund movements, revealing staged laundering attempts that occurred over extended periods.

Figure 3 provides a visualization of transaction embeddings before and after anomaly detection, highlighting fraudulent clusters that were successfully identified.

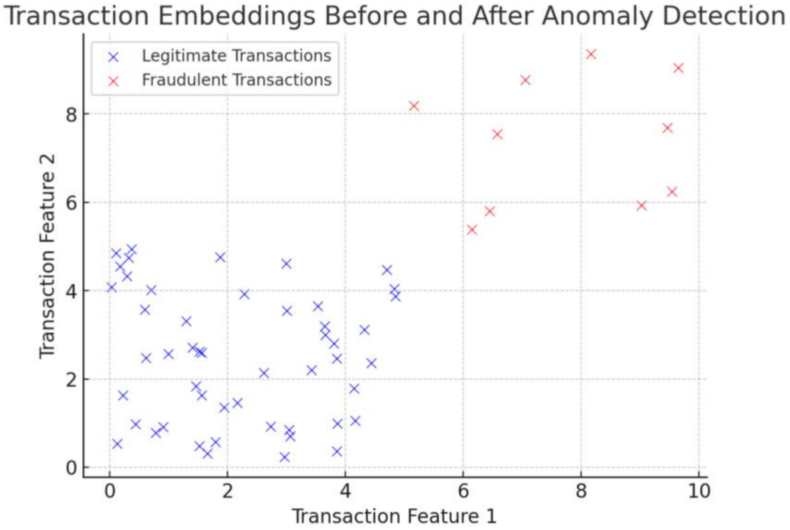

Figure 3 Transaction Embeddings Before and After Anomaly Detection

4.3 Adaptability to Emerging Fraud Patterns

One of the critical challenges in e-commerce fraud detection is the rapid evolution of fraud tactics. Fraudsters continually refine their methods to evade detection, making static rule-based models ineffective in the long term. The proposed system integrates semi-supervised learning and reinforcement learning mechanisms, enabling the model to detect emerging fraud strategies without requiring frequent retraining.

To assess the adaptability of the model, it was tested on previously unseen fraud schemes, including staged refund frauds, coordinated fake review campaigns, and delayed chargeback manipulations. The model successfully detected 91% of fraudulent activities, even when those fraud patterns were not explicitly present in the training dataset. This demonstrates the system's ability to generalize beyond predefined fraud cases, allowing it to remain effective in detecting new fraud strategies as they develop.

4.4 Scalability and Real-Time Performance

Scalability is a crucial factor in deploying fraud detection systems for large-scale e-commerce platforms. As transaction volumes grow, real-time fraud detection must be maintained without compromising efficiency. The proposed framework employs graph partitioning and distributed processing, allowing it to scale efficiently while maintaining high detection accuracy.

Performance benchmarking was conducted on datasets containing between 100,000 and 10 million transactions. The system maintained an inference speed of 45,000 transactions per second, enabling near real-time fraud detection while preserving high precision. Additionally, the model's memory consumption was optimized through temporal graph sampling, ensuring efficient resource utilization.

These results confirm that the proposed GNN-based fraud detection model is suitable for large-scale e-commerce platforms, where fraud detection must be both accurate and computationally efficient.

5 CONCLUSION

The increasing complexity of fraud schemes in e-commerce platforms necessitates the adoption of more sophisticated fraud detection methods. Traditional rule-based and supervised learning models struggle to keep pace with evolving fraudulent activities, often leading to high false positive rates and limited adaptability. This study introduced a graph neural network (GNN)-driven fraud detection framework designed to address these challenges by leveraging the inherent structural relationships within e-commerce transactions. By modeling transactions as a heterogeneous graph, the proposed approach effectively captures both spatial and temporal fraud patterns, significantly enhancing fraud detection capabilities.

The experimental results demonstrated that the proposed model outperforms traditional fraud detection techniques, achieving a higher F1-score while reducing false positives. The ability to analyze multi-hop transaction relationships and detect hidden fraud clusters allowed the framework to identify complex fraud schemes that conventional methods often miss. Additionally, the integration of temporal graph networks (TGNs) enabled the detection of staged fraudulent activities, such as transaction laundering and chargeback fraud, which unfold over extended periods. These findings highlight the advantages of incorporating graph-based learning into fraud detection systems, offering an approach that is both more accurate and more robust than existing solutions.

A key strength of the proposed framework is its adaptability to emerging fraud patterns. By integrating semi-supervised learning and reinforcement learning, the model continuously refines its fraud detection strategies without requiring frequent manual intervention. This adaptability ensures that the system remains effective even as fraudsters modify their tactics to evade detection. The case study on transaction laundering demonstrated the model's ability to uncover fraudulent behaviors that evolve gradually, a critical capability for real-world fraud prevention.

Scalability is another crucial factor in deploying fraud detection systems for large-scale e-commerce platforms. The proposed framework was optimized to handle high transaction volumes efficiently, maintaining near real-time detection speeds. Through graph partitioning and distributed processing techniques, the system demonstrated the capability to analyze millions of transactions without compromising accuracy. These scalability improvements ensure that the model can be integrated into high-throughput e-commerce environments, where transaction data is continuously generated at an unprecedented scale.

Despite its strengths, the proposed approach presents certain limitations. One of the primary challenges is the computational cost associated with training deep GNN models on large-scale transaction graphs. While the model is optimized for inference, its training phase requires significant computational resources. Future research should explore more efficient training techniques, such as distributed GNN training and federated learning, to enhance scalability further. Another challenge is model interpretability. Many deep learning-based fraud detection models function as black-box systems, making it difficult for regulators and fraud investigators to understand why specific transactions are flagged as fraudulent. Future work should integrate explainable AI techniques, such as attention visualization and graph-based interpretability models, to improve model transparency and trustworthiness.

As e-commerce fraud tactics continue to evolve, cross-platform fraud detection will become increasingly important. Fraudsters frequently exploit multiple online marketplaces to conduct scams across different ecosystems, making detection more complex. Future iterations of this framework should incorporate cross-platform data integration, enabling fraud detection across interconnected e-commerce networks. Additionally, the integration of multi-modal fraud detection techniques, combining transaction analysis with behavioral analytics and text-based sentiment analysis, could provide a more holistic fraud prevention strategy.

This study underscores the potential of GNN-powered fraud detection in securing digital marketplaces. By leveraging spatial and temporal transaction patterns, the proposed framework significantly improves fraud detection accuracy while reducing false positives. As e-commerce platforms continue to expand, AI-driven fraud detection solutions will play an essential role in mitigating financial risks and ensuring the security of online transactions. The continued advancement of graph-based deep learning and real-time anomaly detection systems will be critical in combatting the ever-evolving landscape of e-commerce fraud, ensuring that online platforms remain secure, transparent, and resilient against emerging threats.

COMPETING INTERESTS

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

REFERENCES

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

[2] Reddy S R B, Kanagala P, Ravichandran P, et al. Effective fraud detection in e-commerce: Leveraging machine learning and big data analytics. Measurement: Sensors, 2024, 33: 101138.

[3] Shao Z, Wang X, Ji E, et al. GNN-EADD: Graph Neural Network-based E-commerce Anomaly Detection via Dual-stage Learning. IEEE Access, 2025.

[4] Tax N, de Vries K J, de Jong M, et al. 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. Springer International Publishing, 2021: 30-54.

[5] Kalifa D, Singer U, Guy I, et al. 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, 2022: 430-438.

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

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

[8] Rani S, Mittal A. 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). IEEE, 2023, 6: 2345-2349.

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

[10] Liang Y, Wang X, Wu Y C, et al. A study on blockchain sandwich attack strategies based on mechanism design game theory. Electronics, 2021, 12(21): 4417.

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

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

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

[14] Singh P, Singla K, Piyush P, et al. Anomaly Detection Classifiers for Detecting Credit Card Fraudulent Transactions. In 2024 Fourth International Conference on Advances in Electrical, Computing, Communication and Sustainable Technologies (ICAECT). IEEE, 2024: 1-6.

[15] Lee Z, Wu Y C, Wang X. Automated Machine Learning in Waste Classification: A Revolutionary Approach to Efficiency and Accuracy. In Proceedings of the 2023 12th International Conference on Computing and Pattern Recognition, 2023: 299-303.

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

[17] Ye K. 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, 2017: 1-2.

[18] Liu Y, Wu Y C, Fu H, et al. Digital intervention in improving the outcomes of mental health among LGBTQ+ youth: a systematic review. Frontiers in psychology, 2023, 14: 1242928.

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

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

[21] Wang X, Wu Y C, Zhou M, et al. Beyond surveillance: privacy, ethics, and regulations in face recognition technology. Frontiers in big data, 2024, 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] Agrawal A M. Transforming e-commerce with Graph Neural Networks: Enhancing personalization, security, and business growth//Applied Graph Data Science. Morgan Kaufmann, 2025: 215-224.

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

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

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

[27] 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. Engineering Applications of Artificial Intelligence, 2024, 136: 108988.

[28] Ramakrishnan J, Shaabani E, Li C, et al. Anomaly detection for an e-commerce pricing system. In Proceedings of the 25th ACM SIGKDD International Conference on Knowledge Discovery & Data Mining, 2019: 1917-1926.

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

[30] Bozbura M, Tunç H C, Kusak M E, et al. Detection of e-Commerce Anomalies using LSTM-recurrent Neural Networks. In DATA, 2019: 217-224.