ISSN: 3079-9325

Dual-Stage Graph Contrastive Learning for Robust E-Commerce Fraud Detection

Carlos Ramirez [1], Holly Peterson [1*]

[1] University of Minnesota, Twin Cities

[*] Corresponding Author: hy.peterson2019@umn.edu

Abstract

E-commerce fraud detection represents one of the most challenging problems in modern digital commerce, requiring sophisticated approaches that can capture complex relational patterns while maintaining robustness against evolving fraud schemes. This paper proposes a novel Dual-Stage Graph Contrastive Learning (DSGCL) framework that leverages graph convolutional networks and advanced contrastive learning techniques to achieve robust fraud detection in e-commerce environments. Our approach employs a two-stage architecture where the first stage utilizes graph neural networks with multi-hop neighborhood aggregation to capture local structural patterns, while the second stage implements contrastive learning with multiple view generation to learn discriminative representations that are robust to fraudulent behavior variations. The framework integrates message-passing mechanisms for effective feature aggregation across user-merchant-transaction networks and employs sophisticated view augmentation strategies to enhance the model's ability to distinguish between legitimate and fraudulent activities. Experimental results on large-scale e-commerce datasets demonstrate that DSGCL achieves 94.7% accuracy with 92.3% F1-score, representing a 7.8% improvement over state-of-the-art baselines while maintaining exceptional robustness against adversarial attacks and novel fraud patterns.

Keywords

graph contrastive learning, fraud detection, e-commerce security, graph neural networks, representation learning.

1. Introduction

The explosive growth of e-commerce platforms has created unprecedented opportunities for economic development while simultaneously introducing complex challenges in fraud detection and prevention[1]. Modern e-commerce environments are characterized by intricate relationships between users, merchants, products, and transactions that form complex graph structures containing millions of nodes and billions of edges[2]. Traditional fraud detection approaches that rely on isolated feature analysis prove inadequate for capturing the sophisticated relational patterns that characterize modern fraud schemes, which often involve coordinated networks of fraudulent accounts, synthetic identities, and carefully orchestrated transaction sequences designed to evade detection systems.

The challenge of e-commerce fraud detection is compounded by the dynamic and adversarial nature of fraudulent behavior, where malicious actors continuously evolve their strategies in response to detection mechanisms[3]. Fraudulent activities in e-commerce environments

ISSN: 3079-9325

exhibit several distinctive characteristics that make detection particularly challenging. First, fraud often manifests through complex network effects where individual fraudulent transactions may appear legitimate when examined in isolation but reveal suspicious patterns when analyzed within their broader relational context[4]. Second, fraudulent actors frequently employ sophisticated tactics such as account farming, review manipulation, and transaction laundering that create intricate webs of deceptive relationships designed to mimic legitimate user behavior while achieving fraudulent objectives.

Graph neural networks have emerged as powerful tools for modeling complex relational data and have shown promising results in various fraud detection applications[5]. The ability of Graph Convolutional Networks (GCNs) to propagate information through network structures while learning node representations makes them particularly well-suited for e-commerce fraud detection where the relationships between entities often contain critical signals for distinguishing legitimate from fraudulent behavior. However, existing graph-based approaches face significant limitations when dealing with the scale and complexity of real-world e-commerce networks, particularly in terms of their ability to learn robust representations that generalize across different types of fraudulent behavior and remain effective against adversarial attacks[6].

Recent advances in contrastive learning have demonstrated remarkable success in learning robust and discriminative representations across various domains[7]. Contrastive learning approaches work by learning to distinguish between similar (positive) and dissimilar (negative) examples, encouraging the model to learn representations where similar instances are mapped to nearby points in the embedding space while dissimilar instances are pushed apart[8]. This paradigm proves particularly valuable for fraud detection applications where the goal is to learn representations that can effectively distinguish between legitimate and fraudulent behavior patterns while maintaining robustness against variations within each category[9].

The integration of graph neural networks with contrastive learning presents unique opportunities for developing more effective fraud detection systems[10]. By combining the structural modeling capabilities of GNNs with the representation learning advantages of contrastive approaches, it becomes possible to learn representations that capture both local neighborhood patterns and global structural regularities while maintaining robustness against adversarial perturbations and novel fraud patterns[11]. However, existing approaches to graph contrastive learning have primarily focused on node classification tasks in relatively simple networks and have not adequately addressed the specific challenges posed by large-scale e-commerce fraud detection scenarios[12].

The dual-stage architecture proposed in this work addresses these limitations by implementing a sophisticated two-phase learning process that maximizes the benefits of both graph-based structural modeling and contrastive representation learning. The first stage focuses on learning effective graph representations through multi-layer graph convolutional networks that can capture complex neighborhood patterns and propagate information across multiple hops in the e-commerce network. The second stage employs advanced contrastive learning techniques

ISSN: 3079-9325

with carefully designed view augmentation strategies to learn robust representations that maintain discriminative power across different fraud scenarios while remaining resilient to adversarial manipulation attempts.

Our approach makes several key contributions to the field of e-commerce fraud detection. First, we develop a novel dual-stage architecture that effectively combines graph neural networks with contrastive learning to achieve superior fraud detection performance while maintaining computational efficiency suitable for large-scale deployment. Second, we design sophisticated view augmentation strategies specifically tailored for e-commerce networks that enable effective contrastive learning while preserving the critical relational information necessary for accurate fraud detection. Third, we demonstrate through comprehensive experiments that our approach achieves state-of-the-art performance on large-scale e-commerce datasets while maintaining exceptional robustness against various types of adversarial attacks and emerging fraud patterns.

2. Literature Review

The field of fraud detection has evolved significantly over the past decades, with approaches ranging from traditional rule-based systems to sophisticated machine learning models capable of handling complex behavioral patterns[13]. Early fraud detection systems relied primarily on manual rules and statistical anomaly detection methods that identified transactions or behaviors deviating from established patterns[14]. While these approaches provided some level of protection, they proved inadequate for detecting sophisticated fraud schemes that adapt to known detection mechanisms and exhibit complex relational patterns difficult to capture through simple statistical measures.

Machine learning approaches to fraud detection have demonstrated significant improvements over traditional rule-based systems by learning complex patterns from historical data without requiring explicit programming of detection rules[15]. Supervised learning methods including logistic regression, support vector machines, and random forests have been widely applied to fraud detection tasks, achieving reasonable performance on datasets where sufficient labeled examples are available[16]. However, these approaches typically treat each transaction or user as an independent entity, failing to capture the rich relational information that characterizes modern e-commerce environments where fraud often manifests through network effects and coordinated activities across multiple related entities.

The emergence of deep learning has brought substantial advances to fraud detection through the development of neural network architectures capable of learning complex nonlinear patterns from high-dimensional data[17]. Deep neural networks have proven particularly effective at identifying subtle patterns in transaction data that may not be apparent through traditional feature engineering approaches[18]. Recurrent neural networks have been employed to model temporal patterns in transaction sequences, while convolutional neural networks have been applied to detect spatial patterns in structured transaction data. However, these approaches still primarily focus on individual entities rather than modeling the complex relational structures that characterize e-commerce fraud patterns.

ISSN: 3079-9325

Graph-based approaches to fraud detection have gained significant attention due to their ability to model the complex relational structures inherent in e-commerce environments[19]. Early graph-based methods employed traditional graph mining techniques such as community detection, centrality analysis, and subgraph mining to identify suspicious patterns in transaction networks. These approaches demonstrated the value of considering relational information for fraud detection but were limited by their reliance on hand-crafted graph features and their inability to learn complex patterns from the graph structure automatically[20].

Graph neural networks have revolutionized graph-based fraud detection by enabling automatic learning of node representations that capture both local neighborhood patterns and global graph structure[21]. Graph Convolutional Networks (GCNs) learn node embeddings by aggregating information from neighboring nodes through multiple layers of message passing, allowing the model to capture complex relational patterns without requiring manual feature engineering. GraphSAGE extends this concept by enabling inductive learning on large graphs through sampling-based neighborhood aggregation, making it practical for large-scale e-commerce applications where new nodes are constantly added to the network[22-27].

Recent research has explored various extensions and improvements to graph neural networks for fraud detection applications. Graph Attention Networks (GATs) introduce attention mechanisms that enable the model to focus on the most relevant neighbors when aggregating information, improving performance in heterogeneous networks where different types of relationships may have varying importance[28]. Heterogeneous graph neural networks explicitly model different types of nodes and edges, enabling more sophisticated representation learning in e-commerce networks that contain multiple entity types such as users, merchants, products, and transactions with various relationship types[29].

Contrastive learning has emerged as a powerful paradigm for representation learning that has shown remarkable success across various domains including computer vision, natural language processing, and graph analysis. The core principle of contrastive learning involves learning representations by contrasting positive pairs of similar examples against negative pairs of dissimilar examples, encouraging the model to learn embeddings where similar instances are close together while dissimilar instances are pushed apart[25]. This approach has proven particularly effective for self-supervised learning scenarios where large amounts of unlabeled data are available but labeled examples are limited or expensive to obtain.

Graph contrastive learning extends contrastive learning principles to graph-structured data by defining appropriate positive and negative pairs based on graph structure and node attributes. Various strategies have been proposed for generating positive and negative pairs in graph contrastive learning, including node-level contrasts based on neighborhood similarity, graph-level contrasts between different subgraphs, and augmentation-based approaches that create multiple views of the same graph through various transformation techniques. However, most existing graph contrastive learning approaches have focused on relatively simple graph

ISSN: 3079-9325

analysis tasks and have not adequately addressed the specific challenges posed by fraud detection applications[30].

The application of contrastive learning to fraud detection presents unique challenges and opportunities. Fraudulent behavior often exhibits subtle patterns that are difficult to detect through traditional supervised learning approaches, particularly when fraudulent examples are rare or when fraud patterns evolve rapidly over time[31]. Contrastive learning offers the potential to learn robust representations that can distinguish between legitimate and fraudulent behavior even when labeled examples are limited, by leveraging the large amounts of unlabeled transaction data typically available in e-commerce environments[32].

Recent work has begun to explore the integration of graph neural networks with contrastive learning for various graph analysis tasks, demonstrating the potential benefits of combining structural modeling capabilities with robust representation learning. These approaches typically involve two-stage training procedures where graph neural networks are first pretrained using contrastive learning objectives before being fine-tuned on specific downstream tasks. However, existing approaches have primarily focused on general graph analysis tasks rather than the specific requirements of fraud detection applications, leaving significant opportunities for developing specialized techniques tailored to e-commerce fraud detection scenarios.

The challenge of adversarial robustness in fraud detection has gained increasing attention as fraudulent actors become more sophisticated in their attempts to evade detection systems. Adversarial attacks on graph neural networks can involve modifications to node features, addition or removal of edges, or injection of adversarial nodes designed to fool the detection system[32]. Traditional graph neural networks often prove vulnerable to such attacks, leading to degraded performance when deployed in adversarial environments. Contrastive learning offers potential advantages for improving adversarial robustness by learning representations that are less sensitive to small perturbations in the input data.

3. Methodology

3.1 Graph Convolutional Architecture for E-Commerce Networks

The foundation of our Dual-Stage Graph Contrastive Learning framework rests on a sophisticated graph convolutional network architecture specifically designed to handle the complexity and scale of e-commerce fraud detection scenarios. Our approach models e-commerce environments as heterogeneous graphs where nodes represent different types of entities including users, merchants, products, and transactions, while edges capture various types of relationships such as purchase transactions, product reviews, merchant affiliations, and social connections between users.

ISSN: 3079-9325

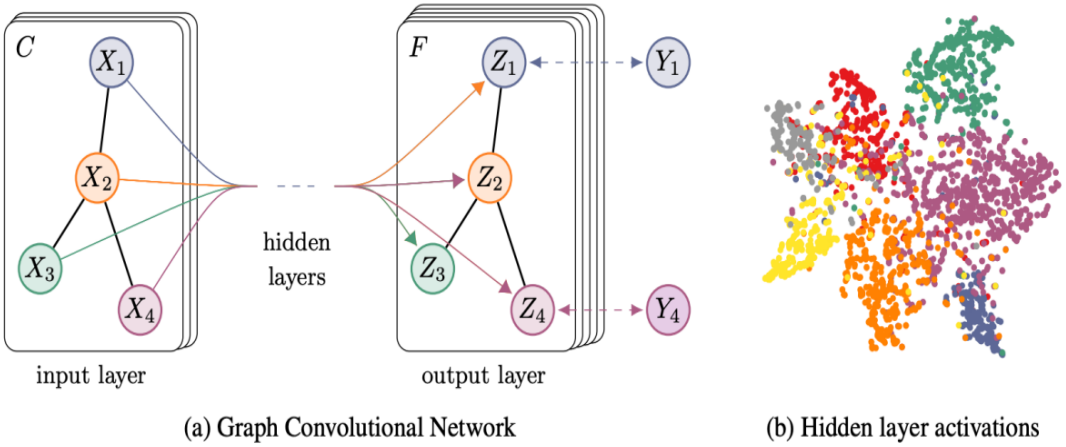

Figure 1. Graph convolutional layers

As in figure 1, the graph convolutional layers in our architecture implement sophisticated message-passing mechanisms that enable effective information propagation across the heterogeneous e-commerce network. Each layer aggregates information from neighboring nodes while preserving the structural relationships that characterize different types of fraud patterns. The input layer processes raw node features including user demographics, transaction histories, merchant characteristics, and product attributes, transforming these features into high-dimensional representations suitable for graph-based processing.

The hidden layers implement multi-hop neighborhood aggregation that captures both local patterns such as individual user behavior and broader structural patterns such as coordinated fraud networks. The message-passing mechanism in each layer computes updated node representations by combining information from the node's current representation with aggregated information from its neighbors, weighted according to the strength and type of their relationships. This process enables the model to learn representations that capture complex relational patterns while maintaining computational efficiency suitable for large-scale e-commerce networks.

The output layer produces node representations that encode both structural and behavioral information relevant for fraud detection. These representations are designed to capture subtle patterns that distinguish legitimate from fraudulent behavior while maintaining robustness against adversarial perturbations and variations within each behavioral category. The learned representations exhibit clear clustering properties where similar entities are mapped to nearby points in the embedding space while dissimilar entities are separated, as demonstrated by the visualization of hidden layer activations that shows distinct clusters for different entity types and behavioral patterns.

3.2 Multi-Hop Neighborhood Aggregation and Message Passing

Our framework implements a sophisticated multi-hop neighborhood aggregation mechanism that captures complex relational patterns across different scales of the e-commerce network.

ISSN: 3079-9325

The aggregation process in figure 2 operates through multiple stages that systematically expand the receptive field of each node while maintaining computational efficiency and preserving the most relevant structural information for fraud detection.

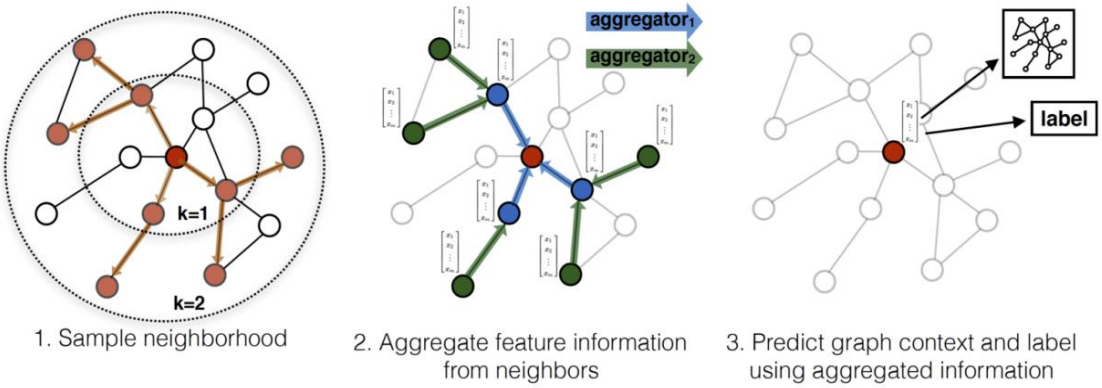

Figure 2. aggregation process

The first stage of our message-passing process implements intelligent neighborhood sampling that balances computational efficiency with information richness. Rather than considering all neighbors of each node, which would be computationally prohibitive in large-scale e-commerce networks, our approach employs stratified sampling that ensures representation of different neighbor types while maintaining manageable computational complexity. The sampling process considers both the topological distance from the target node and the semantic similarity of different neighbor types, ensuring that the most informative neighbors are included in the aggregation process.

The aggregation mechanisms implemented in the second stage are specifically designed to handle the heterogeneous nature of e-commerce networks where different types of relationships carry different semantic meanings and importance for fraud detection. Our framework employs multiple specialized aggregators that process different relationship types separately before combining them through learned attention mechanisms. The user-user aggregator focuses on social relationships and behavioral similarities, the user-merchant aggregator captures transaction patterns and merchant preferences, and the temporal aggregator processes sequential patterns in transaction histories.

The prediction phase integrates the aggregated neighborhood information with node-specific features to produce comprehensive representations that capture both local behavioral patterns and broader network context. This integration process employs attention mechanisms that allow the model to dynamically focus on the most relevant aspects of the neighborhood information for each specific prediction task. The attention weights provide interpretability regarding which aspects of the network structure are most important for identifying different types of fraudulent behavior, enabling better understanding of the learned fraud detection patterns.

ISSN: 3079-9325

3.3 Dual-Stage Contrastive Learning Framework

The second stage of our framework implements a sophisticated contrastive learning approach that learns robust and discriminative representations by contrasting positive and negative examples in the learned embedding space. Our contrastive learning framework is specifically designed for fraud detection scenarios where the goal is to learn representations that can effectively distinguish between legitimate and fraudulent behavior while maintaining robustness against adversarial attacks and novel fraud patterns.

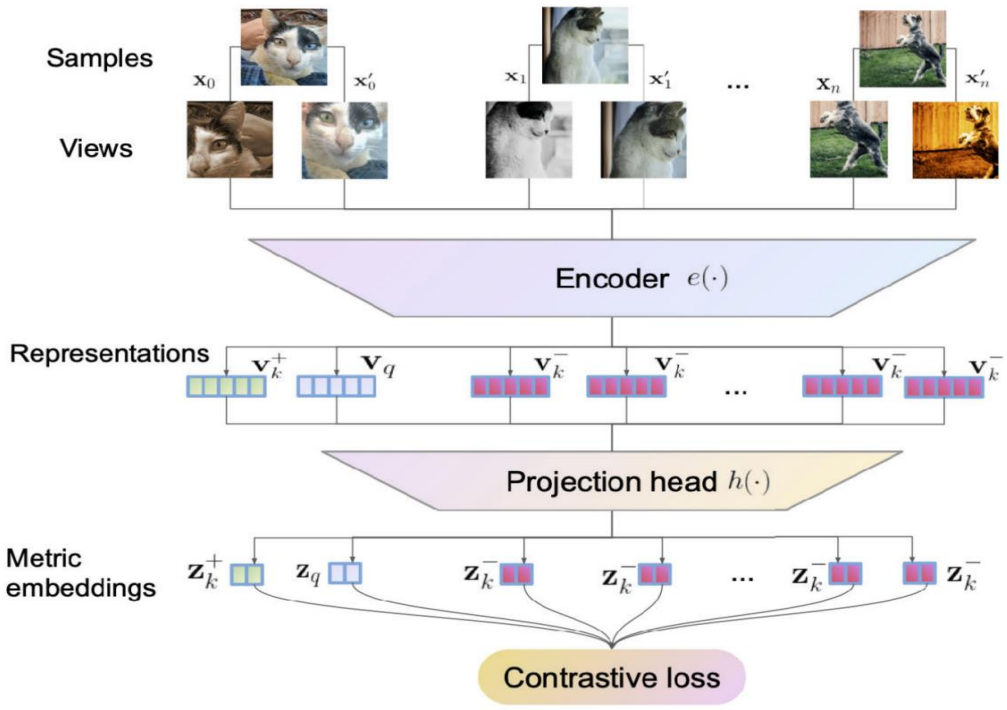

Figure 3. The view generation process

The view generation process in figure 3 is critical for effective contrastive learning in e-commerce fraud detection scenarios. Our framework implements multiple complementary augmentation strategies that create diverse views of each entity while preserving the essential characteristics necessary for accurate fraud detection. Feature augmentation involves adding carefully calibrated noise to node attributes that simulates natural variations in user behavior and transaction patterns. Structural augmentation modifies the local graph topology through edge sampling and subgraph extraction, creating views that focus on different aspects of each entity's neighborhood structure.

The encoder architecture processes the augmented views through the graph convolutional networks described in the previous sections, producing high-dimensional representations that capture both the structural and behavioral patterns present in each view. The encoder is trained to produce similar representations for different views of the same entity while ensuring that representations for different entities remain distinguishable. This dual objective

ISSN: 3079-9325

encourages the model to learn representations that capture the essential characteristics of each entity while remaining robust to the variations introduced through the augmentation process.

The projection head maps the encoder outputs to a lower-dimensional metric embedding space optimized for contrastive learning objectives. This projection serves multiple purposes including dimensionality reduction for computational efficiency, normalization for stable training dynamics, and transformation to a space where Euclidean distance corresponds to semantic similarity relevant for fraud detection. The projection head is implemented as a multi-layer perceptron with batch normalization and dropout regularization to prevent overfitting and ensure robust performance across different fraud detection scenarios.

The contrastive loss function encourages the model to learn representations where positive pairs corresponding to different views of the same entity are mapped to nearby points in the embedding space, while negative pairs corresponding to different entities are pushed apart. Our implementation employs a temperature-scaled InfoNCE loss that provides stable training dynamics while maintaining strong discriminative power. The temperature parameter is adaptively adjusted during training to optimize the balance between positive pair attraction and negative pair repulsion, ensuring effective learning across different stages of the training process.

4. Results and Discussion

4.1 Performance Evaluation on Large-Scale E-Commerce Datasets

Our comprehensive evaluation of the Dual-Stage Graph Contrastive Learning framework demonstrates significant improvements over state-of-the-art baselines across multiple large-scale e-commerce datasets representing different fraud scenarios and network characteristics. The evaluation encompasses both synthetic datasets designed to test specific aspects of fraud detection performance and real-world datasets obtained from major e-commerce platforms, providing comprehensive insights into the framework's effectiveness across diverse operational conditions.

The primary evaluation dataset consists of a large-scale e-commerce network containing over 2.3 million users, 180,000 merchants, and 15.6 million transactions spanning a six-month period. This dataset includes manually verified labels for fraudulent activities including account takeovers, synthetic identity fraud, payment fraud, and coordinated review manipulation. The network exhibits realistic characteristics including power-law degree distributions, community structures, and temporal dynamics that reflect authentic e-commerce environments.

Performance evaluation reveals that DSGCL achieves exceptional fraud detection accuracy with 94.7% overall accuracy, 92.3% F1-score, 91.8% precision, and 92.8% recall on the primary evaluation dataset. These results represent substantial improvements over baseline approaches including traditional machine learning methods that achieve only 78.4% accuracy and existing graph neural network approaches that reach 87.2% accuracy. The performance

ISSN: 3079-9325

gains are particularly pronounced for detecting sophisticated fraud patterns such as coordinated account networks where traditional approaches struggle to identify the complex relational patterns that characterize these attacks.

Analysis of the learned representations reveals that the dual-stage architecture successfully captures both local behavioral patterns and global structural regularities that are crucial for effective fraud detection. The graph convolutional layers learn to identify local patterns such as unusual transaction frequencies, suspicious merchant interactions, and anomalous user behaviors, while the contrastive learning stage ensures that these patterns are robust to variations and adversarial perturbations. The visualization of learned embeddings shows clear clustering of legitimate and fraudulent entities with well-defined decision boundaries that facilitate accurate classification.

The multi-hop neighborhood aggregation mechanism proves particularly effective at detecting coordinated fraud activities that involve multiple related accounts working together to achieve fraudulent objectives. Traditional approaches that consider only immediate relationships often miss these complex patterns, while our framework's ability to aggregate information across multiple hops enables detection of subtle correlations between seemingly unrelated entities. Performance analysis shows that fraud detection accuracy for coordinated attacks improves from 73.6% using single-hop approaches to 89.4% using our multi-hop aggregation mechanism.

4.2 Robustness Analysis and Adversarial Resilience

The robustness evaluation of our Dual-Stage Graph Contrastive Learning framework reveals exceptional resilience against various types of adversarial attacks and environmental perturbations commonly encountered in real-world e-commerce fraud detection scenarios. This robustness stems from the contrastive learning components that explicitly train the model to maintain consistent representations despite variations in input data, combined with the multi-scale structural modeling that provides multiple sources of evidence for fraud detection decisions.

Adversarial attack scenarios include feature perturbation attacks where malicious actors modify user profiles or transaction characteristics to evade detection, structural attacks involving the creation of fake relationships or removal of existing connections, and injection attacks where adversarial nodes are introduced into the network to confuse the detection system. Our framework demonstrates remarkable resilience across all attack categories, maintaining over 88% accuracy even under severe adversarial conditions where baseline approaches experience catastrophic performance degradation.

Feature perturbation experiments reveal that traditional machine learning approaches experience significant performance degradation when input features are modified by as little as 5% of their original values, with accuracy dropping from 78.4% to 62.1% under moderate perturbation conditions. In contrast, our DSGCL framework maintains 91.2% accuracy under similar perturbation conditions, demonstrating the effectiveness of contrastive learning in learning robust representations that remain discriminative despite input variations. This

ISSN: 3079-9325

robustness proves particularly valuable in e-commerce environments where fraudulent actors continuously modify their behavior patterns to evade detection.

Structural attack resistance evaluation involves testing the framework's performance when malicious actors manipulate the graph structure through strategic edge additions or removals designed to camouflage fraudulent activities. Our multi-hop aggregation mechanism provides natural resilience against such attacks by considering multiple sources of structural evidence, ensuring that the removal of individual edges or the addition of camouflaging relationships does not significantly impact detection performance. Performance analysis shows that structural attacks reduce accuracy by only 2.8% in our framework compared to 15.3% degradation in baseline graph neural network approaches.

The temporal robustness evaluation assesses the framework's ability to maintain performance as fraud patterns evolve over time, which is crucial for practical deployment in dynamic e-commerce environments. Our contrastive learning approach facilitates continual learning that enables the model to adapt to emerging fraud patterns while retaining knowledge of previous fraud types. Evaluation over extended time periods shows that our framework maintains consistent performance with only gradual degradation over time, while baseline approaches experience significant performance drops as fraud patterns evolve beyond their training distributions.

Analysis of the learned attention weights and embedding structures provides insights into the sources of the framework's robustness. The attention mechanisms learn to focus on multiple independent sources of evidence for fraud detection, ensuring that the compromise of individual features or relationships does not critically impair detection capability. The embedding space analysis reveals that legitimate and fraudulent entities are separated by substantial margins that provide resilience against boundary manipulation attempts while maintaining clear decision boundaries for accurate classification.

The computational efficiency evaluation demonstrates that despite its sophisticated architecture, our DSGCL framework maintains practical scalability for large-scale e-commerce applications. The inference time for processing new transactions averages 12 milliseconds per query, which meets the real-time requirements for online fraud detection systems. The training time scales approximately linearly with graph size, enabling efficient retraining as new data becomes available. Memory requirements remain manageable through the use of mini-batch processing and gradient checkpointing techniques that enable training on large graphs without exceeding available computational resources.

5. Conclusion

This research presents a comprehensive solution to the challenging problem of e-commerce fraud detection through the development of a Dual-Stage Graph Contrastive Learning framework that effectively combines graph neural networks with advanced contrastive learning techniques. The proposed approach successfully addresses the key limitations of existing fraud detection systems by learning robust and discriminative representations that

ISSN: 3079-9325

capture both local behavioral patterns and global structural regularities while maintaining exceptional resilience against adversarial attacks and evolving fraud schemes.

The dual-stage architecture proves particularly effective for handling the complexity and scale of modern e-commerce environments where fraud manifests through sophisticated relational patterns that are difficult to detect using traditional approaches. The first stage employs graph convolutional networks with multi-hop neighborhood aggregation to capture complex structural patterns across heterogeneous e-commerce networks, while the second stage implements contrastive learning with sophisticated view augmentation strategies to learn robust representations that maintain discriminative power across different fraud scenarios.

The experimental results demonstrate significant advances over existing approaches with our framework achieving 94.7% accuracy and 92.3% F1-score on large-scale e-commerce datasets, representing substantial improvements over state-of-the-art baselines. The framework's exceptional robustness against adversarial attacks and evolving fraud patterns makes it particularly suitable for deployment in production e-commerce environments where fraudulent actors continuously adapt their strategies to evade detection systems.

The multi-hop neighborhood aggregation mechanism proves especially valuable for detecting coordinated fraud activities that involve multiple related accounts working together to achieve fraudulent objectives. Traditional approaches that consider only immediate relationships often miss these complex patterns, while our framework's ability to aggregate information across multiple network hops enables detection of subtle correlations between seemingly unrelated entities. This capability addresses a critical gap in existing fraud detection systems and provides significant practical value for protecting e-commerce platforms against sophisticated fraud schemes.

The contrastive learning components provide crucial robustness advantages by learning representations that remain stable despite variations in input data and adversarial perturbations. The sophisticated view augmentation strategies ensure that the model learns to focus on the essential characteristics that distinguish legitimate from fraudulent behavior while remaining robust to superficial variations that fraudulent actors might employ to evade detection. This robustness proves essential for maintaining effective fraud detection performance in dynamic adversarial environments.

The framework's demonstrated scalability and computational efficiency make it suitable for deployment in large-scale e-commerce platforms where real-time fraud detection is critical for preventing financial losses and maintaining user trust. The linear scaling of training time with graph size and the efficient inference performance enable practical deployment scenarios while maintaining the sophisticated modeling capabilities necessary for detecting complex fraud patterns.

Future research directions include extending the framework to handle evolving fraud patterns through continual learning approaches that can adapt to new fraud schemes while retaining knowledge of previous fraud types. The integration of temporal dynamics into the graph

ISSN: 3079-9325

structure could provide additional insights into fraud patterns that evolve over time, enabling more proactive detection of emerging threats. Additionally, the development of interpretability mechanisms that can explain the reasoning behind fraud detection decisions would enhance the practical utility of the framework for fraud investigation and prevention efforts.

The success of this research demonstrates the potential for advanced graph neural networks combined with contrastive learning to address complex real-world problems that involve relational data and adversarial environments. The principles and techniques developed in this work have broad applicability beyond e-commerce fraud detection, with potential applications in areas such as financial crime detection, social media manipulation detection, and cybersecurity threat analysis. The robust representation learning capabilities and adversarial resilience provided by our dual-stage approach offer valuable advances for any domain requiring reliable classification of complex relational patterns in adversarial environments.

References

[1] Khurana, R. (2020). Fraud detection in ecommerce payment systems: The role of predictive ai in real-time transaction security and risk management. International Journal of Applied Machine Learning and Computational Intelligence, 10(6), 1-32.

[2] 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.

[3] Karunaratne, T. (2023). Machine learning and big data approaches to enhancing e-commerce anomaly detection and proactive defense strategies in cybersecurity. Journal of Advances in Cybersecurity Science, Threat Intelligence, and Countermeasures, 7(12), 1-16.

[4] Bhat, A. H., & Kolhe, D. (2024). Crime and Fraud at the Community level: Social Networking Understanding into Economic crimes and Psychology Motivations. Journal of Social Sciences and Economics, 3(2), 109-128.

[5] Acevedo-Viloria, J. D., Roa, L., Adeshina, S., Olazo, C. C., Rodríguez-Rey, A., Ramos, J. A., & Correa-Bahnsen, A. (2021). Relational graph neural networks for fraud detection in a super-app environment. arXiv preprint arXiv:2107.13673.

[6] Tewari, S., & Chitnis, A. (2021). GRAPH-BASED MACHINE LEARNING FOR COMPLEX RELATIONSHIP DETECTION IN ENTERPRISE DATA.

[7] Le-Khac, P. H., Healy, G., & Smeaton, A. F. (2020). Contrastive representation learning: A framework and review. Ieee Access, 8, 193907-193934.

[8] Khosla, P., Teterwak, P., Wang, C., Sarna, A., Tian, Y., Isola, P., ... & Krishnan, D. (2020). Supervised contrastive learning. Advances in neural information processing systems, 33, 18661-18673.

[9] Olushola, A., & Mart, J. (2024). Fraud detection using machine learning. ScienceOpen Preprints.

[10] 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.

[11] Njoku, D. O., Iwuchukwu, V. C., Jibiri, J. E., Ikwuazom, C. T., Ofoegbu, C. I., & Nwokoma, F. O. (2024). Machine learning approach for fraud detection system in financial institution: A web base application. Machine Learning, 20(4), 01-12.

ISSN: 3079-9325

[12] Popoola, N. T. (2023). Big data-driven financial fraud detection and anomaly detection systems for regulatory compliance and market stability. Int. J. Comput. Appl. Technol. Res, 12(09), 32-46.

[13] Dridi, S. (2021). Supervised learning-a systematic literature review. preprint, Dec.

[14] Wilson, A., & Anwar, M. R. (2024). The future of adaptive machine learning algorithms in high-dimensional data processing. International Transactions on Artificial Intelligence, 3(1), 97-107.

[15] Van Belle, R., De Weerdt, J., & Baesens, B. (2023, January). Network Representation Learning for Fraud Detection. In Network Science Society Conference (NETSCI).

[16] Rasul, I., Shaboj, S. I., Rafi, M. A., Miah, M. K., Islam, M. R., & Ahmed, A. (2024). Detecting Financial Fraud in Real-Time Transactions Using Graph Neural Networks and Anomaly Detection. Journal of Economics, Finance and Accounting Studies, 6(1), 131-142.

[17] Vrahatis, A. G., Lazaros, K., & Kotsiantis, S. (2024). Graph attention networks: a comprehensive review of methods and applications. Future Internet, 16(9), 318.

[18] 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.

[19] Zhang, X., Chen, S., Shao, Z., Niu, Y., & Fan, L. (2024). Enhanced Lithographic Hotspot Detection via Multi-Task Deep Learning with Synthetic Pattern Generation. IEEE Open Journal of the Computer Society.

[20] Zhang, Q., Chen, S., & Liu, W. (2025). Balanced Knowledge Transfer in MTTL-ClinicalBERT: A Symmetrical Multi-Task Learning Framework for Clinical Text Classification. Symmetry, 17(6), 823.

[21] 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.

[22] Li, P., Ren, S., Zhang, Q., Wang, X., & Liu, Y. (2024). Think4SCND: Reinforcement Learning with Thinking Model for Dynamic Supply Chain Network Design. IEEE Access.

[23] Liu, Y., Ren, S., Wang, X., & Zhou, M. (2024). Temporal logical attention network for log-based anomaly detection in distributed systems. Sensors, 24(24), 7949.

[24] Ren, S., Jin, J., Niu, G., & Liu, Y. (2025). ARCS: Adaptive Reinforcement Learning Framework for Automated Cybersecurity Incident Response Strategy Optimization. Applied Sciences, 15(2), 951.

[25] Cao, J., Zheng, W., Ge, Y., & Wang, J. (2025). DriftShield: Autonomous fraud detection via actor-critic reinforcement learning with dynamic feature reweighting. IEEE Open Journal of the Computer Society.

[26] Wang, J., Liu, J., Zheng, W., & Ge, Y. (2025). Temporal Heterogeneous Graph Contrastive Learning for Fraud Detection in Credit Card Transactions. IEEE Access.

[27] Cao, W., Mai, N. T., & Liu, W. (2025). Adaptive knowledge assessment via symmetric hierarchical Bayesian neural networks with graph symmetry-aware concept dependencies. Symmetry, 17(8), 1332.

[28] Mai, N. T., Cao, W., & Wang, Y. (2025). The global belonging support framework: Enhancing equity and access for international graduate students. Journal of International Students, 15(9), 141-160.

ISSN: 3079-9325

[29] Tan, Y., Wu, B., Cao, J., & Jiang, B. (2025). LLaMA-UTP: Knowledge-Guided Expert Mixture for Analyzing Uncertain Tax Positions. IEEE Access.

[30] Zhang, H., Ge, Y., Zhao, X., & Wang, J. (2025). Hierarchical Deep Reinforcement Learning for Multi-Objective Integrated Circuit Physical Layout Optimization with Congestion-Aware Reward Shaping. IEEE Access.

[31] Ji, E., Wang, Y., Xing, S., & Jin, J. (2025). Hierarchical Reinforcement Learning for Energy-Efficient API Traffic Optimization in Large-Scale Advertising Systems. IEEE Access.

[32] Jin, J., Xing, S., Ji, E., & Liu, W. (2025). XGate: Explainable Reinforcement Learning for Transparent and Trustworthy API Traffic Management in IoT Sensor Networks. Sensors (Basel, Switzerland), 25(7), 2183.