Chapter

Fraud Detection in E-Commerce: A Systematic Review of Transaction Risk Prevention

Susie Xi Rao, Jiawei Jiang, Zhichao Han and Hang Yin

Abstract

We provide a systematic review of the endeavors of e-commerce companies in combating transaction risks that involve buyers, sellers, items, and transactions. There has been a paradigm shift from rule-based systems to simple machine learning-based systems to deep learning-based systems. This transformation has also involved multimodal data engineering efforts like rule extraction, feature engineering on text and image, graph-structured abstraction, etc. In this review, we not only reflect on the shifts in data and systems but also the role of human experts, as well as the infrastructure support for such shifts, which are oftentimes neglected in previous review articles. The key conclusions from this review are three. First, there has been an increasing focus on multimodal data engineering efforts, explainability, and human-in-the-loop systems. Second, despite certain contributions to the online scalability of fraud detection systems, this topic has remained understudied. Third, newer research trends are on federated learning and adversarial machine learning, reinforcement learning, large language models, and their applicability and feasibility to integrate into the existing e-commerce fraud detection systems.

Keywords: fraud detection, e-commerce, transaction risk, artificial intelligence, review

1. Introduction

Anomaly detection plays a crucial role in modern e-commerce platforms to mitigate transaction risks involving buyers, sellers, items, and transactions. This chapter systematically reviews the evolution from rule-based systems to machine learning and deep learning-based methods, along with the infrastructure and human expertise needed for their deployment.

Traditional rule-based fraud detection systems rely on predefined heuristics and domain expertise to flag suspicious activities. While effective for well-known fraud patterns, these systems struggle with adapting to evolving fraudulent tactics. The advent of machine learning and deep learning approaches has significantly improved fraud detection by leveraging large-scale transactional data, behavioral patterns, and graph-based representations. Graph-based anomaly detection has emerged as a

powerful tool for capturing relational structures in fraud detection, which strengthens the ability to model complex interactions between entities such as users, devices, and transactions.

This chapter explores various aspects of fraud detection in e-commerce, including feature engineering, which plays a crucial role in constructing informative representations for anomaly detection models. Explainability and human-in-the-loop systems highlight the need for transparency and interpretability in AI-driven fraud detection, ensuring regulatory compliance and building trust among fraud analysts. Scalability challenges are discussed in the context of real-time fraud detection, where millions of transactions must be processed efficiently.

Additionally, we examine federated learning, which enables multiple e-commerce platforms to collaboratively train fraud detection models while preserving data privacy. Adversarial machine learning is another emerging area, addressing fraudsters' ability to manipulate detection systems by generating synthetic transaction patterns or evading anomaly detection models. We also critically assess the feasibility to utilize large language models in facilitating fraud detection workloads.

As fraud tactics become increasingly sophisticated, the integration of advanced graph-based learning, adversarial training, large language models, and privacy-preserving techniques will be essential in strengthening fraud detection capabilities across diverse e-commerce environments. This chapter provides a comprehensive review of these advancements, identifying key challenges and future research directions in anomaly detection for e-commerce fraud prevention.

2. Fundamentals of anomaly detection in e-commerce

Anomalies refer to instances that deviate significantly from normal patterns. These anomalies can manifest as fraudulent transactions, fake reviews, identity theft, or collusive seller-buyer activities. The primary challenge in anomaly detection lies in differentiating between genuine outliers and fraudulent activities, as well as handling evolving fraud patterns that adapt to detection mechanisms. This differentiation is usually contingent on automatically generated metrics or/and human judgment and varies according to use cases.

Early fraud detection systems relied on predefined rules and expert knowledge. These systems flagged transactions based on thresholds for parameters such as transaction amount, frequency, and location [1]. While effective for detecting known fraud patterns, rule-based systems struggle with adaptive fraud strategies. Additionally, they require constant updates from fraud analysts to stay relevant against emerging threats.

However, rule extraction techniques are not obsolete. They serve as basic building blocks for advanced fraud detection systems, some of which rely on predefined rules to construct their graphs, especially on criteria of node connections [2, 3]; others utilize the rules in post-detection to explain the system output [4–6]. The newly extracted rules will be augmented to the existing rule-based engines that have already been implemented on the platform.

Machine learning techniques offer more flexibility, leveraging feature engineering and (mostly) supervised learning models to detect fraudulent transactions [7]. Simple algorithms such as decision trees, random forests, and support vector machines are adopted to analyze historical transaction data to identify suspicious patterns. In practice, tree-based models such as gradient boosting decision tree (GBDT) are extremely

powerful in large-scale e-commerce applications [5, 8]. These models reduce reliance on manual rule updates by learning from labeled datasets. However, their effectiveness depends on high-quality labeled data and well-engineered features.

Advanced fraud detection systems integrate deep learning models and graph-based representations, including graph neural networks (GNNs), to enhance accuracy and scalability. Recurrent neural networks (RNNs) and convolutional neural networks (CNNs) have been used to detect fraud based on sequential transaction data [5, 6, 9–12]. Graph-based models analyze relationships between users, transactions, and payment methods in scenarios such as anti-money laundering [13–18], credit card fraud detection [19], user onboarding [20], transaction risks [2–4, 8, 21–25], and risky accounts [25–28].

Graph structures help detect fraud rings and suspicious relationships among users, transactions, and payment details. By constructing transaction/user/device networks, anomalies can be detected through graph analytics techniques such as community detection and centrality measures. For example, fraudsters often use multiple fake accounts to artificially boost product ratings or conduct money laundering activities, which can be identified through dense subgraph patterns.

3. Case studies in e-commerce fraud detection

Now we zoom in on the aspects that are of special focus in both academia and industry on state-of-the-art fraud detection performance. We provide (**Table 1**) as a reference for readers to retrieve the relevant literature items.

We survey the publications on e-commerce fraud detection from the top-ranked venues on machine learning, deep learning, data mining, and graph representation learning between the years 2017 and 2024, including but not limited to AAAI, CIKM, Expert Systems with Applications, ICDE, ICDM, ICLR, IEEE venues, IJCAI, KDD, NeurIPS, TKDE, VLDB, WSDM, and WWW.[1] There has been a surge in increasing usage of advanced machine learning techniques and deep learning techniques with the further development of sufficient infrastructures and the abundance of data availability. Since the year 2018, there has been an increase in using graph representation learning (with GNNs as examples) to further advance pattern detection based on the existing infrastructures.

Table 1 summarizes key studies on fraud detection in this review. The *Graph* column specifies the type of graph used, such as transaction networks or account networks. The *Construction Method* describes how each graph was built, following the taxonomy in Ref. [36], including sources such as external knowledge bases, raw data, similarity metrics, or multimodal content. *Graph Type* characterizes the graph's structural properties, such as bipartite, homogeneous, heterogeneous, dynamic, or multimodal. The *Data* column lists the dataset(s) used and the public availability.[2] In the column *Application*, we specify the fraud detection domain, such as anti-money laundering or risky account detection. The *Method* column outlines the modeling

[1] For a more comprehensive survey of the fraud detection landscape that includes over 180 publications, we refer the readers to Rao et al. [35]. Another source that is actively curated is https://github.com/safe-graph/graph-fraud-detection-papers.

[2] Since many publications do not document dataset links, or provided links are outdated, the authors have made an effort to locate accessible sources.

Graph	Construction method	Graph type	Data	Application	Method	Reference	Code availability	Year
Transaction graph	Data (usage)	Homogeneous	Elliptic	Anti-money laundering	GNN	[18]	No	2019
Bank account graph	Data (money transfer)	Heterogeneous Multi-partite	CBank (private) CFD	Anti-money laundering	Non-GNN (FlowScope)	[29]	FlowScope	2020
User-transaction graph	Data (transactions)	Homogeneous	WeBank-small/-medium/-large (private) OTC Alpha Elliptic	Anti-money laundering	GNN (Diga)	[14]	No	2023
Transaction graph	Data (related transactions)	Homogeneous	Alipay data (private)	Anti-money laundering	GNN	[15]	No	2023
User-transaction graph	Data (transactions)	Dynamic Homogeneous	UnionPay data (private)	Anti-money laundering	GNN	[30]	No	2023
Transaction graph	Data (related transactions)	Homogeneous	Bitcoin transaction dataset	Anti-money laundering	GNN	[16]	No	2023
User-transaction graph	Data (transactions)	Homogeneous	AMLSim Elliptic	Anti-money laundering	GNN	[17]	No	2023
Transaction graphs	Data (relations)	Dynamic Heterogeneous	HI LI (small, medium, large)	Anti-money laundering	GNN (Multi-GNN)	[13]	Multi-GNN	2024
User login behavior graph	Data (relations)	Heterogeneous	Jingdong e-commerce (private)	Collective fraud	Non-GNN (statistic or other anomaly detection algorithms, HGsuspector)	[31]	No	2018
Transaction graph	Data (usage)	Heterogeneous	Vesta Sparkov	Credit card fraud detection	GNN (FIW-GNN)	[19]	No	2023
Transaction graph	Data (relations)	Heterogeneous	ELECTRONIC ARTS data (private)	Fraudulent transactions	Non-GNN (predefined meta-paths, HitFraud)	[32]	No	2017
Transaction-user graph	Data (usage)	Dynamic Heterogeneous Multimodal	Alipay data (private)	Fraudulent transactions	RNN	[11]	No	2019

Graph	Construction method	Graph type	Data	Application	Method	Reference	Code availability	Year
User-attribute graph	Data (relations)	Heterogeneous	Ant Credit Pay dataset (private)	Fraudulent transactions Fraudulent users	Non-GNN (predefined meta-paths, HACUD)	[33]	DGFraud	2019
Transaction graph	Data (usage)	Dynamic Homogeneous	Alipay data (private)	Fraudulent transactions	Non-GNN (sequence-based)	[34]	No	2019
User behavior sequence	Data (usage)	Dynamic	E-commerce company data from four countries (private)	Fraudulent transactions	Non-GNN (sequence-based, hierarchical, transfer learning)	[9]	No	2020
Transaction-attribute graph	Data (usage)	Heterogeneous	*eBay-small* (per request) *eBay-large/-xlarge* (private)	Fraudulent transactions	GNN (transformer)	[24]	xFraud	2021
Transaction graph	Data (rules)	Homogeneous	BTFSD (private)	Fraudulent transactions	GNN (knowledge-guided, graph, Know-GNN)	[3]	No	2021
Transaction graph	Data (rules)	Homogeneous	BTFSD (private) IEEE-CIS Fraud Detection YelpCHi	Fraudulent transactions	GNN (knowledge-guided, rules, KS-GNN)	[2]	No	2021
Intention-transaction graph	Data (usage)	Heterogeneous	Alibaba graph (private)	Fraudulent transactions	GNN (IHGAT)	[4]	No	2021
Transaction graph	Data (usage)	Heterogeneous Multimodal	eBay (private)	Fraudulent transactions	Bi-LSTM GPU-powered HDBSCAN clustering (FinDeepBehaviorCluster)	[6]	No	2021
Transaction-attribute graph	Data (usage)	Heterogeneous Dynamic	eBay (private)	Fraudulent transactions	GNN (BRIGHT)	[8]	No	2022
Transaction graph	Data (usage)	Heterogeneous Multimodal	eBay (private)	Fraudulent transactions	Bi-LSTM Transformer (BehaviorClustering)	[5]	No	2022
Transaction graph	Data (relations)	Dynamic Heterogeneous	PR01 (private) Orange Finance Company (upon request)	Fraudulent transactions	GNN (Transformer, STA-GT)	[23]	No	2023
Transaction graph	Data (usage)	Heterogeneous Multimodal	eBay (private)	Fraudulent transactions	Transformer (MMBT)	[12]	No	2024

Graph	Construction method	Graph type	Data	Application	Method	Reference	Code availability	Year
User-behavior graph Review graph Transaction graph	Data (relations, usage)	Heterogeneous Homogeneous	Reddit Weibo Amazon YelpChi Tolokers Questions T-Finance Elliptic DGraph-Fin T-Social	Graph anomaly detection	GNN (GADBench)	[21]	GADBench	2023
User review graph User-transaction graph	Data (homophily and heterophily edges)	Heterogeneous	YelpCHi Amazon T-Finance	Graph anomaly detection	GNN (spectral, SEC-GFD)	[22]	No	2024
Account graph	Data (usage)	Bipartite Dynamic	Amazon account activity data (private)	Risky account detection	GNN	[27]	No	2018
Device-account graph	Data (usage)	Heterogeneous	Alipay data (private)	Risky account detection	GNN (GEM)	[26]	GEM	2018
User-account graph	Data (usage)	Homogeneous	Pubmed BlogCatalog (no feature) BlogCatalog (128-dimension feature) PPI Alipay (private)	Risky account detection	GNN (breadth and depth, GeniePath)	[28]	GeniePath	2019
User-behavior graph	Data (relations)	Dynamic Homogeneous	Elliptic T-Finance T-Social YelpCHi Amazon	Suspicious account/ transaction	GNN (DGA-GNN)	[25]	DGA-GNN	2024

Table 1.
Summary of related works in fraud detection, sorted alphabetically first by the column Application and then by the column Year.

techniques in each study, and *Reference* provides citations for further reading. Finally, we survey the code availability and publication year in the last two columns.

3.1 Feature engineering

Feature engineering is a crucial step in improving fraud detection performance. E-commerce platforms extract meaningful features from textual descriptions, visual product images, and behavioral data such as browsing history and purchase frequency. For instance, fraudulent users can be detected by analyzing abnormal mouse trajectories [12], while suspicious accounts may be flagged based on IP address discrepancies and login patterns [27].

The choice of features influences the ability of the downstream models to distinguish fraudulent patterns from legitimate behaviors. Existing works employ a variety of feature engineering techniques tailored to the underlying data characteristics, graph structure of attributes, and anomaly detection tasks.

3.1.1 Feature extraction and graph construction

Fraud detection studies leverage different types of graphs, such as transaction graphs, user-transaction graphs, and account graphs. These graphs are constructed based on various criteria, including transaction relations [13], account behaviors [27], and financial interactions [16]. Feature extraction methods commonly include node embeddings, edge attributes, and temporal patterns, with several studies using predefined meta-paths [32, 33] to enhance feature representations.

3.1.2 Structural and relational features

To capture relational and structural dependencies, previous studies derive features based on node connectivity, degree distributions, and centrality measures. For instance, in anti-money laundering applications, Erik Altman et al. [13] incorporate multi-type relationships to better represent complex financial ecosystems. In credit card fraud detection, Yan et al. [19] extract statistical patterns from transaction sequences to identify suspicious activities.

3.1.3 Temporal and behavioral features

Dynamic features are increasingly adopted to model evolving fraudulent behaviors. Studies such as Cao et al., Tian et al., and Cheng et al. [23, 30, 34] analyze transaction sequences over time, leveraging time-based embeddings to improve detection accuracy. Sequence-based methods, including behavioral clustering [5] and hierarchical transfer learning [9], further enhance fraud detection by capturing sequential user activity patterns.

3.1.4 Multimodal and knowledge-guided features

To improve feature richness, several approaches integrate multimodal data sources. For instance, transaction-attribute graphs combine user behaviors with additional contextual information, such as transaction intentions [4]. Knowledge-guided techniques, such as rule-based graph construction [2, 3], embed domain knowledge into graph representations, improving interpretability and model robustness.

3.1.5 Graph neural networks and alternative approaches

While many recent approaches utilize GNN-based feature extraction [17, 21], non-GNN methods, such as statistical anomaly detection [31] and flow-based models [29], remain relevant in certain fraud detection scenarios. The choice of feature engineering techniques is often driven by the nature of the data, the computational complexity of graph models, and the need for explainability.

Overall, feature engineering in anomaly detection continues to evolve, with a growing emphasis on dynamic, multimodal, and knowledge-guided representations. Future work may focus on improving feature selection strategies and developing more interpretable representations for fraud detection applications, for instance, with the help of large language models.

3.2 Integration of multimodal data for fraud detection

E-commerce platforms integrate multiple data sources, such as transaction logs, clickstream data, image-based product verification, and external knowledge bases, to improve fraud detection capabilities. Behavioral sequence embeddings from user activity logs can reveal unusual navigation patterns [12], while product image analysis [37] and grounded knowledge bases [38] help detect counterfeit items and invalid connections. When combining these data sources, we have a holistic review of multiple sources that fraudsters can default. One example of combining multiple sources of input is the integration of sequence embeddings in fraud detection tasks.

Recent studies have explored various sequence embedding approaches for fraud detection, leveraging different techniques to enhance model performance and interpretability. For instance, Li et al. [11] proposed a time attention-based embedding method that incorporates dwell time to better capture user behavior patterns. Additionally, other works have focused on improving interpretability through intent-aware embeddings [4], multi-task learning for general behavior representation [6], and cross-domain feature embeddings [5]. These approaches collectively aim to enhance the accuracy and interpretability of fraud detection systems by capturing complex user behavior patterns and leveraging diverse data sources.

3.3 E-commerce companies as dataset contributors

In most of the contributions, e-commerce companies generate large-scale anonymized datasets, such as Amazon [2, 19, 25, 27], Alibaba [4, 11, 15, 21, 22, 26, 28, 33, 34], eBay [5, 6, 8, 12, 24], and Jingdong [31]. Due to privacy concerns, many datasets remain private or are available only upon request, limiting accessibility for broader research. As dataset availability significantly impacts research progress, future efforts may focus on developing more openly accessible (synthetic) benchmarks while ensuring data privacy and compliance with regulations.

4. Explainability and scalability in e-commerce fraud detection

4.1 Explainability and human-in-the-loop systems

Balancing automated detection with human expertise is essential. Explainable AI techniques [39], such as SHAP (Shapley Additive Explanations) and LIME (Local

Interpretable Model-Agnostic Explanations), help fraud analysts understand model decisions. Human-in-the-loop systems incorporate fraud investigators to review flagged transactions, reducing false positives and improving trust in AI-driven systems.

Understanding the rationale behind fraud detection predictions is crucial, particularly when interpreting why certain transactions are flagged as suspicious and how an algorithm contributes to this process. Typically, explainability methods can be divided into these categories [40]: rule-based [4–6], input-level [41–43], self-explanatory [44], and model-level explanations [45].

The importance of explainability extends to dynamic graphs, where fraud patterns evolve over time. Several works have focused on explaining temporal GNN models, including DGExplainer [46] for discrete-time graphs and TGNNExplainer [47] for continuous-time graphs. Given that financial fraud detection often relies on dynamic and heterogeneous graph structures, these techniques are crucial for identifying evolving fraudulent behaviors and providing justifications for decisions.

As the complexity of fraud detection models increases, improving interpretability remains a priority to ensure compliance with regulatory standards and foster trust in automated systems. Future research may focus on integrating human-in-the-loop feedback mechanisms with self-explainable models to enhance decision-making in real-world fraud detection applications.

4.2 Scalability and deployment challenges

Real-time fraud detection systems encounter notable obstacles in terms of scalability and deployment, especially when required to process millions of transactions every second. Ensuring scalability is vital for handling substantial financial datasets, including transaction graphs and patterns of user behavior, while maintaining rapid response times to detect fraudulent actions. Solutions like Apache Spark and PyTorch, along with cloud-based platforms, offer flexible computing resources to handle heavy traffic and facilitate effective anomaly detection. Nonetheless, the intensive computational demands of processing diverse and multimodal graphs continue to pose significant challenges.

Several studies have addressed scalability challenges by leveraging dynamic graph structures and efficient model architectures. For instance, transaction graphs from large-scale financial datasets [8, 34] require high-throughput processing to detect fraudulent behaviors in real-time. Dynamic graph models, such as those proposed by Huang et al. [48, 49], improve efficiency by capturing evolving patterns in streaming data. Additionally, optimizations like knowledge-guided rule embeddings [2] and behavior clustering techniques [5] help reduce processing overhead while maintaining detection accuracy.

Deploying fraud detection models introduces additional operational challenges, including latency constraints, regulatory compliance, and the need for continuous model retraining. E-commerce platforms must comply with data privacy regulations like GDPR and CCPA while ensuring secure transaction processing. Real-time fraud detection systems, such as those deployed by Alipay [30, 34] and eBay [8, 24], utilize dynamic and heterogeneous graph structures that require efficient processing pipelines.

Model retraining and adaptation are critical for maintaining the effectiveness of fraud detection systems. Fraud tactics continuously evolve, requiring models to be periodically updated with new labeled data. Dynamic graph-based approaches [8, 46]

and hybrid methods, such as rule-based embeddings [2] and behavior clustering techniques [5], enhance robustness by incorporating domain knowledge and real-time behavioral patterns. Federated learning and privacy-preserving techniques may offer solutions for training fraud detection models across multiple institutions while maintaining data confidentiality.

Future research should focus on hybrid solutions that combine distributed computing, graph compression, and lightweight neural architectures to improve scalability and real-time performance. Additionally, deployment strategies must prioritize computational efficiency, reduce bias in automated decisions, and integrate adaptive learning techniques to stay ahead of emerging fraudulent activities.

5. Future directions of fraud detection in e-commerce

5.1 Federated learning for fraud detection

Federated learning allows multiple e-commerce (sub-)platforms to collaboratively train fraud detection models without sharing raw data [50–52]. This decentralized learning approach improves data privacy while leveraging knowledge from different sources. By deploying federated learning, companies can strengthen fraud detection capabilities across multiple platforms without violating privacy regulations.

Recent studies have explored federated learning for fraud detection, particularly in handling diverse financial and transactional data. For instance, domain adaptation techniques [53] enhance the ability of federated models to generalize across different e-commerce environments, reducing performance degradation caused by distributional shifts. Cross-domain applications [54] further demonstrate the potential of federated learning in improving fraud detection across heterogeneous datasets, where transactional patterns may vary significantly between different platforms.

Handling multi-relational and heterogeneous data is another challenge in federated learning, particularly in fraud detection scenarios involving transaction graphs, user behavior networks, and account-device relationships. Federated approaches must efficiently aggregate knowledge while maintaining structural and relational integrity across multiple sources [53]. Adversarial learning and contrastive self-supervised techniques have been integrated into federated frameworks to enhance robustness against fraudulent adaptation [55].

However, federated learning in fraud detection also presents challenges such as communication overhead, non-IID (non-independent and identically distributed) data distributions, and adversarial attacks on decentralized models. Privacy-preserving techniques are important in mitigating risks associated with data leakage and model inversion attacks, such as secure multi-party computation and differential privacy. Future research may focus on optimizing federated aggregation strategies, developing adaptive fraud detection mechanisms for non-IID data, and improving the interpretability of federated fraud detection models to ensure regulatory compliance and trustworthiness.

5.2 Adversarial machine learning and fraudulent adaptation

Fraudsters continuously adapt to detection methods by leveraging adversarial techniques, such as generating synthetic transaction patterns to evade detection.

Techniques like adversarial training and anomaly-aware model regularization help defend against evolving fraudulent strategies.

Several studies have explored adversarial methods to enhance fraud detection and anomaly detection in dynamic and heterogeneous graph structures. For instance, adversarial graph-based models have been employed for anomaly detection in dynamic graphs [56], where evolving fraud tactics require adaptive learning techniques. In the context of fake news detection, adversarially trained GNNs, such as AA-HGNN [57] and DAGA-NN [58], improve robustness against misinformation-spreading strategies by capturing deceptive relationships in textual similarity and publisher networks.

Adversarial contrastive learning has also been explored for detecting fraudulent behaviors in claim-evidence graphs, as demonstrated in GETRAL [55], which enhances resilience against manipulation in misinformation detection. Additionally, adversarial defenses have been applied to both financial and e-commerce fraud detection. For example, ACD [59] integrates adversarial learning for anomaly detection in transaction graphs as anti-money laundering efforts. Similarly, adversarial techniques have been used to detect suspicious user behaviors in user-product and review networks, as seen in MO-GAA and PBAAD [60], which mitigate evasion attacks by fraudsters who manipulate online platforms.

Despite these advancements, adversarial attacks remain a significant challenge in fraud detection, particularly in continuously evolving environments. Future research may focus on developing more robust defenses, such as adaptive adversarial training, self-supervised anomaly-aware learning, and hybrid approaches that integrate knowledge graphs with adversarial robustness techniques. These methods can help improve the ability of fraud detection systems to counteract increasingly sophisticated fraudulent strategies while maintaining interpretability and scalability.

5.3 Reinforcement learning in fraud detection

Reinforcement learning (RL) has shown growing potential in addressing fraud detection challenges in dynamic fraud detection environments, particularly through RL integration with graph-based methods. Most of the contributions of RL-based methods have been developed for fraud detection domains such as fake reviews, fake news, and spam detection.

RL is used in GNN structures to select the optimal nodes, edges, and subgraphs. Dou et al. [61] introduce CARE-GNN, where RL is utilized to find the optimal amounts of neighbors to select in review graphs (e.g., Amazon, Yelp) for detecting fraud rings, while Yuan Gao et al. [62] employ RL to alleviate structural distribution shifts by aggregating homophilous neighbors. Recent advancements include REGAD [63], which uses RL to iteratively prune suspicious edges in product-purchase graphs, and RHGNN [64], which designs a reinforced neighbor selector for heterogeneous review-reviewer-product graphs while filtering out the camouflaged relationships.

RL has also been applied to competitive scenarios. Nash-Detect [65] models fraud detection as a minimax game between review spammers and spam detectors, and HP-KGAT [66] optimizes path-aware graph attention for fake news detection with subgraph reasoning. RL is appealing in unsupervised settings as the label scarcity is not the bottleneck of modeling. Typically, anomaly scores of nodes are computed, where a larger score means a higher abnormality. RAND [67] introduces RL-based neighborhood selection to amplify reliable signals in social and citation graphs, whereas RARE-GNN [68] learns anomaly-resistant GNNs without prior knowledge of ground truth in citation networks

like Cora, CiteSeer, and PubMed. Additionally, DiG-In-GNN [69] combines RL with contrastive learning on transaction graphs (e.g., T-Finance), and RoSGAS [70] integrates RL with self-supervised learning in a setting of multimodal social bot detection. Last but not least, RL is also used to address model interpretability in the literature. EXplainable Graph Neural Network (XGNN) [45] uses RL to explain Graph Convolutional Network (GCN) graph generation. These works collectively highlight the adaptability of RL in handling complex relational data, adversarial dynamics, and structural noise. However, challenges like computational overhead, reward design, and scalability remain.

Scalability challenges in real-time fraud detection—such as high latency in policy updates or computational bottlenecks during graph traversal—remain understudied. One possible solution is to utilize hierarchical reinforcement learning (HRL) frameworks where large graphs are divided into smaller subgraphs [71]. Another approach is to use lightweight deep-Q networks (DQN) with prioritized experience replay to speed up convergence [72]. Additionally, implementing edge computing solutions enables decentralized reinforcement learning inference [73]. Finally, distributed reinforcement learning approaches, such as federated graph RL [74], can improve scalability by distributing training across segmented graphs in parallel.

5.4 Large language models in fraud detection

The advent of large language models (LLMs), such as BERT [75], GPT-3 [76], and their successors have opened new opportunities for fraud detection in e-commerce. These models, pre-trained on vast corpora of text data, have demonstrated remarkable capabilities in understanding context, semantics, and even subtle patterns in unstructured data. Their application in fraud detection is particularly promising due to their ability to process and analyze multimodal data in a unified manner, including text, images, and transactional metadata.

One of the key strengths of LLMs lies in their ability to perform *contextual anomaly detection*. Unlike traditional models that rely on handcrafted features, LLMs can automatically infer complex relationships between entities (e.g., buyers, sellers, and items) and detect anomalies that deviate from normal patterns. For instance, LLMs can analyze product descriptions, reviews, and customer interactions to identify fraudulent listings or fake reviews with high precision [77–79].

Moreover, LLMs can be fine-tuned on domain-specific data to enhance their performance in fraud detection tasks. For example, fine-tuning BERT on e-commerce transaction data has been shown to improve the detection of fraudulent transactions by capturing subtle linguistic cues in transaction descriptions or customer communications [80]. Additionally, LLMs can be integrated with graph-based approaches to model relationships between entities, enabling the detection of sophisticated fraud schemes such as collusive fraud or money laundering.

However, challenges remain in deploying LLMs for fraud detection. The expenses associated with fine-tuning and inference, along with the requirement for extensive, high-quality labeled datasets, can be daunting. Furthermore, the interpretability of LLMs remains a concern, as their "black-box" nature makes it difficult to explain fraud detection decisions to stakeholders [81]. Future research should focus on developing more efficient and interpretable LLM architectures tailored for fraud detection, as well as exploring hybrid approaches that combine LLMs with traditional rule-based systems for enhanced robustness.

In conclusion, LLMs allow a transformative shift in fraud detection, which offers new capabilities for analyzing complex and multimodal data. As these models keep

advancing, they are expected to become integral to the upcoming generation of fraud detection systems, as long as issues concerning scalability, interpretability, and domain adaptation are resolved.

6. Conclusions

This chapter offers an extensive review of techniques for detecting anomalies aimed at preventing e-commerce fraud. We trace the progression from traditional rule-based systems to contemporary approaches that utilize machine learning and deep learning, emphasizing the significance of feature engineering, graph models, and the integration of multimodal data. Furthermore, we address scalability challenges, highlighting the need for real-time detection systems to handle millions of transactions per second with minimal delay and high precision. The importance of explainability and involving humans in the loop is underscored to ensure transparency and meet regulatory standards, thereby aiding fraud analysts in understanding model decisions comprehensively.

Emerging trends in fraud detection research include federated learning, adversarial learning, reinforcement learning, and the usage of large language models. Federated learning facilitates privacy-preserving collaboration between e-commerce platforms, allowing fraud detection models to generalize across different data sources without sharing raw information. Reinforcement learning allows fraud detection techniques to focus on informative nodes, edges, and/or subgraphs with enhanced past experiences from ground truth labels in a supervised setting or with dynamically learned policies in an unsupervised setting. Adversarial machine learning has become increasingly relevant as fraudsters develop sophisticated techniques to evade detection, requiring robust anomaly detection models that can resist adversarial attacks. Large language models allow new opportunities to efficiently integrate the existing pipelines on multimodal sources.

Despite these advancements, several challenges remain, including the need for adaptive learning strategies to handle evolving fraud patterns, efficient model deployment to optimize resource utilization in cloud-based environments, and scalable graph-based learning approaches to process large-scale transactional data. Future research may focus on integrating self-supervised learning for fraud detection, improving adversarial robustness in dynamic graph structures, and developing hybrid models that combine rule-based expertise with deep learning techniques.

Author details

Susie Xi Rao[1,2*†], Jiawei Jiang[3†], Zhichao Han[4] and Hang Yin[4]

1 Department of Management, Technology and Economics, ETH Zurich, Zurich, Switzerland

2 ETH AI Center, Zurich, Switzerland

3 Department of Computer Science, Wuhan University, Wuhan, China

4 eBay China, Shanghai, China

*Address all correspondence to: srao@ethz.ch

† These authors contributed equally.

IntechOpen

© 2025 The Author(s). Licensee IntechOpen. This chapter is distributed under the terms of the Creative Commons Attribution License (http://creativecommons.org/licenses/by/4.0), which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited. CC BY

References

[1] del Mar Roldán-García M, García-Nieto J, Aldana-Montes JF. Enhancing semantic consistency in anti-fraud rule-based expert systems. Expert Systems with Applications. 2017;**90**:332-343

[2] Rao Y, Ren X, Duan C, Mi X, Cheng J, Yu C, et al. Knowledge-guided fraud detection using semi-supervised graph neural network. In: Web Information Systems Engineering–WISE 2021: 22nd International Conference on Web Information Systems Engineering, WISE 2021; Melbourne, VIC, Australia; October 26–29, 2021, Proceedings, Part I 22. Berlin, Heidelberg: Springer-Verlag; 2021. pp. 385-393

[3] Rao Y, Mi X, Duan C, Ren X, Cheng J, Chen Y, et al. Know-GNN: An explainable knowledge-guided graph neural network for fraud detection. In: International Conference on Neural Information Processing. Cham, Switzerland: Springer International Publishing; 2021. pp. 159-167

[4] Liu C, Sun L, Ao X, Feng J, He Q, Yang H. Intention-aware heterogeneous graph attention networks for fraud transactions detection. In: Proceedings of the 27th ACM SIGKDD Conference on Knowledge Discovery & Data Mining. New York, NY, USA: Association for Computing Machinery; 2021. pp. 3280-3288

[5] Yin H, Zhang Z, Wang Z, Özyurt Y, Liang W, Dong W, et al. Behavioral graph fraud detection in e-commerce. In: 2022 IEEE International Conference on Data Mining Workshops (ICDMW). New York City, U.S.: IEEE; 2022. pp. 1-8

[6] Min W, Liang W, Yin H, Wang Z, Li M, Lal A. Explainable deep behavioral sequence clustering for transaction fraud detection. In: The AAAI-21 Workshop on Knowledge Discovery from Unstructured Data in Financial Services. Washington DC, USA: AAAI Publisher; 2021. Available from: https://aaai-kdf.github.io/kdf2021/accepted_papers

[7] Mutemi A, Bacao F. E-commerce fraud detection based on machine learning techniques: Systematic literature review. Big Data Mining and Analytics. 2024;**7**(2):419-444

[8] Lu M, Han Z, Rao SX, Zhang Z, Zhao Y, Shan Y, et al. BRIGHT-Graph neural networks in real-time fraud detection. In: Proceedings of the 31st ACM International Conference on Information & Knowledge Management. New York, NY, USA: Association for Computing Machinery; 2022. pp. 3342-3351

[9] Zhu Y, Xi D, Song B, Zhuang F, Chen S, Xi G, et al. Modeling users' behavior sequences with hierarchical explainable network for cross-domain fraud detection. In: Proceedings of The Web Conference 2020. New York, NY, USA: Association for Computing Machinery; 2020. pp. 928-938

[10] Zhang R, Zheng F, Min W. Sequential behavioral data processing using deep learning and the markov transition field in online fraud detection. arXiv preprint arXiv:1808.05329. 2018

[11] Li L, Liu Z, Chen C, Zhang Y-L, Zhou J, Li X. A time attention based fraud transaction detection framework. arXiv preprint arXiv:1912.11760. 2019

[12] Zhang Z, Yin H, Rao SX, Yan X, Wang Z, Liang W, et al. Identifying e-commerce fraud through user behavior data: Observations and insights. Data Science and Engineering. 2024;**10**:24-39,

[13] Altman E, Blanuša J, Von Niederhäusern L, Egressy B, Anghel A,

Atasu K. Realistic synthetic financial transactions for anti-money laundering models. Advances in Neural Information Processing Systems. 2024;**36**: 29851-29874

[14] Li X, Li Y, Mo X, Xiao H, Shen Y, Chen L. Diga: Guided diffusion model for graph recovery in anti-money laundering. In: Proceedings of the 29th ACM SIGKDD Conference on Knowledge Discovery and Data Mining. New York, NY, USA: Association for Computing Machinery; 2023. pp. 4404-4413

[15] Chai Z, Yang Y, Dan J, Tian S, Meng C, Wang W, et al. Towards learning to discover money laundering sub-network in massive transaction network. AAAI. 2023;**37**(12):14153-14160

[16] Hyun W, Lee J, Suh B. Anti-money laundering in cryptocurrency via multi-relational graph neural network. In: Pacific-Asia Conference on Knowledge Discovery and Data Mining. Berlin, Heidelberg: Springer-Verlag; 2023. pp. 118-130

[17] Karim MR, Hermsen F, Chala SA, de Perthuis P, Mandal A. Catch me if you can: Semi-supervised graph learning for spotting money laundering. arXiv preprint arXiv:2302.11880. 2023

[18] Weber M, Domeniconi G, Chen J, Weidele DKI, Bellei C, Robinson T, et al. Anti-money laundering in bitcoin: Experimenting with graph convolutional networks for financial forensics. arXiv preprint arXiv:1908.02591. 2019

[19] Yan K, Gao J, Matsypura D. FIW-GNN: A heterogeneous graph-based learning model for credit card fraud detection. In: 2023 IEEE 10th International Conference on Data Science and Advanced Analytics (DSAA). New York City, U.S.: IEEE; 2023. pp. 1-10

[20] Rao SX, Lanfranchi C, Zhang S, Han Z, Zhang Z, Min W, et al. Modelling graph dynamics in fraud detection with "attention". arXiv preprint arXiv: 2204.10614. 2022

[21] Tang J, Hua F, Gao Z, Zhao P, Li J. Gadbench: Revisiting and benchmarking supervised graph anomaly detection. arXiv preprint arXiv:2306.12251. 2023

[22] Fan X, Wang N, Wu H, Wen X, Zhao X, Wan H. Revisiting graph-based fraud detection in sight of heterophily and spectrum. Proceedings of the AAAI Conference on Artificial Intelligence. 2024;**38**:9214-9222

[23] Tian Y, Liu G, Wang J, Zhou M. Transaction fraud detection via an adaptive graph neural network. arXiv preprint arXiv:2307.05633. 2023

[24] Rao SX, Zhang S, Han Z, Zhang Z, Min W, Chen Z, et al. xFraud: Explainable fraud transaction detection. Proceedings of the VLDB Endowment. 2021;**15**:427-436

[25] Duan M, Zheng T, Gao Y, Wang G, Feng Z, Wang X. DGA-GNN: Dynamic grouping aggregation gnn for fraud detection. Proceedings of the AAAI Conference on Artificial Intelligence. 2024;**38**:11820-11828

[26] Liu Z, Chen C, Yang X, Zhou J, Li X, Song L. Heterogeneous graph neural networks for malicious account detection. In: Proceedings of the 27th ACM International Conference on Information and Knowledge Management. New York, NY, USA: Association for Computing Machinery; 2018. pp. 2077-2085

[27] Ma J, Zhang D, Wang Y, Zhang Y, Pozdnoukhov A. GraphRAD: A graph-based risky account detection system. In: KDD 2018 Workshop. New York, NY, USA: Association for Computing Machinery; 2018

[28] Liu Z, Chen C, Li L, Zhou J, Li X, Song L, et al. GeniePath: Graph neural networks with adaptive receptive paths. Proceedings of the AAAI Conference on Artificial Intelligence. 2019;**33**: 4424-4431

[29] Li X, Liu S, Li Z, Han X, Shi C, Hooi B, et al. Flowscope: Spotting money laundering based on graphs. Proceedings of the AAAI Conference on Artificial Intelligence. 2020;**34**:4731-4738

[30] Cheng D, Ye Y, Xiang S, Ma Z, Zhang Y, Jiang C. Anti-money laundering by group-aware deep graph learning. IEEE Transactions on Knowledge and Data Engineering. 2023; **35**(12):12444-12457

[31] Li X, Zhang W, Xi J, Zhu H. HGsuspector: Scalable collective fraud detection in heterogeneous graphs. In: KDD 2018 Workshop. New York, NY, USA: Association for Computing Machinery; 2018

[32] Cao B, Mao M, Viidu S, Yu S, Philip. HitFraud: "A broad learning approach for collective fraud detection in heterogeneous information networks". In: 2017 IEEE International Conference on Data Mining (ICDM). New York City, U.S.: IEEE; 2017. pp. 769-774

[33] Hu B, Zhang Z, Shi C, Zhou J, Li X, Qi Y. Cash-out user detection based on attributed heterogeneous information network with a hierarchical attention mechanism. Proceedings of the AAAI Conference on Artificial Intelligence. 2019;**33**:946-953

[34] Cao S, Yang XX, Chen C, Zhou J, Li X, Qi Y. TitAnt: Online real-time transaction fraud detection in Ant Financial. Proceedings of the VLDB Endowment. 2019;**12**(12):2082-2093

[35] Rao S, X, Han Z, Yin H, Jiang J, Zhang Z, Zhao Y, et al. Fraud detection at eBay. Emerging Markets Review. 2025. Special Issue: Multi-Source Data-Driven Financial Fraud Risk Analysis (Accepted subject to minor revision due on Mar 2, 2025). Available form: https://www.sciencedirect.com/science/article/pii/S1566014125000263

[36] Wang J, Zhang S, Xiao Y, Song R. A review on graph neural network methods in financial applications. arXiv preprint arXiv:2111.15367. 2021

[37] Tavares JPHE, da Silva Medeiros ML, Barbin DF. Near-infrared techniques for fraud detection in dairy products: A review. Journal of Food Science. 2022; **87**(5):1943-1960

[38] Attigeri G, Manohara Pai MM, Pai RM, Kulkarni R. Knowledge base ontology building for fraud detection using topic modeling. Procedia Computer Science. 2018;**135**:369-376

[39] Raufi B, Finnegan C, Longo L. A comparative analysis of shap, lime, anchors, and dice for interpreting a dense neural network in credit card fraud detection. In: World Conference on Explainable Artificial Intelligence. Cham, Swizterland: Springer Nature Switzerland; 2024. pp. 365-383

[40] Yuan H, Haiyang Y, Gui S, Ji S. Explainability in graph neural networks: A taxonomic survey. IEEE Transactions on Pattern Analysis and Machine Intelligence. 2022;**45**(5):5782-5799

[41] Ying Z, Bourgeois D, You J, Zitnik M, Leskovec J. GNNExplainer:

Generating explanations for graph neural networks. In: Advances in Neural Information Processing Systems. New York, US: Curran Associates, Inc; 2019. pp. 9244-9255

[42] Li X, Saude J, Reddy P, Veloso M. Classifying and Understanding Financial Data Using Graph Neural Network. Washington DC, USA: AAAI Publisher; 2020

[43] Huang Q, Yamada M, Tian Y, Singh D, Yin D, Chang Y. GraphLIME: Local interpretable model explanations for graph neural networks. arXiv preprint arXiv:2001.06216. 2020

[44] Zhang Z, Liu Q, Wang H, Chengqiang L, Lee C. ProtGNN: Towards self-explaining graph neural networks. Proceedings of the AAAI Conference on Artificial Intelligence. 2022;**36**:9127-9135

[45] Yuan H, Tang J, Hu X, Ji S. XGNN: Towards model-level explanations of graph neural networks. arXiv preprint arXiv:2006.02587. 2020

[46] Xie J, Liu Y, Shen Y. Explaining dynamic graph neural networks via relevance back-propagation. arXiv preprint arXiv:2207.11175. 2022

[47] Xia W, Lai M, Shan C, Zhang Y, Dai X, Li X, et al. Explaining temporal graph models through an explorer-navigator framework. In: The Eleventh International Conference on Learning Representations. OpenReview; 2023. Available form: https://openreview.net/

[48] Huang Q, Wang X, Rao SX, Han Z, Zhang Z, He Y, et al. Benchtemp: A general benchmark for evaluating temporal graph neural networks. In: 2024 IEEE 40th International Conference on Data Engineering (ICDE). New York City, U.S.: IEEE; 2024. pp. 4044-4057

[49] Huang Q, Yan X, Wang X, Rao SX, Han Z, Fu F, et al. Retrofitting temporal graph neural networks with transformer. arXiv preprint arXiv:2409.05477. 2024

[50] Yang W, Zhang Y, Ye K, Li L, Cheng-Zhong X. FFD: A federated learning based method for credit card fraud detection. In: Big Data–BigData 2019: 8th International Congress, Held as Part of the Services Conference Federation, SCF 2019; San Diego, CA, USA; June 25–30, 2019, Proceedings. Vol. 8. Cham, Switzerland: Springer International Publishing; 2019. pp. 18-32

[51] Myalil D, Rajan MA, Apte M, Lodha S. Robust collaborative fraudulent transaction detection using federated learning. In: 2021 20th IEEE International Conference on Machine Learning and Applications (ICMLA). New York City, U. S.: IEEE; 2021. pp. 373-378

[52] Ahmed A, A, Alabi O. Secure and scalable blockchain-based federated learning for cryptocurrency fraud detection: A systematic review. IEEE Access. 2024;**12**:102219-102241

[53] Peng H, Zhang Y, Sun H, Bai X, Li Y, Wang S. Domain-aware federated social bot detection with multi-relational graph neural networks. In: 2022 International Joint Conference on Neural Networks (IJCNN). New York City, U.S.: IEEE; 2022. pp. 1-8

[54] Wang Q, Pang G, Salehi M, Buntine W, Leckie C. Cross-domain graph anomaly detection via anomaly-aware contrastive alignment. Proceedings of the AAAI Conference on Artificial Intelligence. 2023;**37**:4676-4684

[55] Wu J, Xu W, Liu Q, Wu S, Wang L. Adversarial contrastive learning for evidence-aware fake news detection with graph neural networks. arXiv preprint arXiv:2210.05498. 2022

[56] Lou S, Zhang Q, Yang S, Tian Y, Tan Z, Luo M. GADY: Unsupervised anomaly detection on dynamic graphs. arXiv preprint arXiv:2310.16376. 2023

[57] Ren Y, Wang B, Zhang J, Chang Y. Adversarial active learning based heterogeneous graph neural network for fake news detection. In: 2020 IEEE International Conference on Data Mining (ICDM). New York City, U.S.: IEEE; 2020. pp. 452-461

[58] Yuan H, Zheng J, Ye Q, Qian Y, Zhang Y. Improving fake news detection with domain-adversarial and graph-attention neural network. Decision Support Systems. 2021;**151**:113633

[59] Wang L, Zhao H, Feng C, Liu W, Huang C, Santoni M, et al. Removing camouflage and revealing collusion: Leveraging gang-crime pattern in fraudster detection. In: Proceedings of the 29th ACM SIGKDD Conference on Knowledge Discovery and Data Mining. New York, NY, USA: Association for Computing Machinery; 2023. pp. 5104-5115

[60] Zheng X, Wu B, Zhang AX, Li W. Improving robustness of gnn-based anomaly detection by graph adversarial training. In: Proceedings of the 2024 Joint International Conference on Computational Linguistics, Language Resources and Evaluation (LREC-COLING 2024). Paris, France: ELRA (European Language Resources Association) and ICCL (International Committee on Computational Linguistics); 2024. pp. 8902-8912

[61] Dou Y, Liu Z, Sun L, Deng Y, Peng H, Yu PS. Enhancing graph neural network-based fraud detectors against camouflaged fraudsters. In: Proceedings of the 29th ACM International Conference on Information & Knowledge Management. New York, NY, USA: Association for Computing Machinery; 2020. pp. 315-324

[62] Gao Y, Wang X, He X, Liu Z, Feng H, Zhang Y. Alleviating structural distribution shift in graph anomaly detection. In: Proceedings of the Sixteenth ACM International Conference on Web Search and Data Mining. New York, NY, USA: Association for Computing Machinery; 2023. pp. 357-365

[63] Wang Z, Zhou S, Dong J, Yang C, Huang X, Zhao S. Graph anomaly detection with noisy labels by reinforcement learning. arXiv preprint arXiv:2407.05934. 2024

[64] Zhao J, Shao M, Tang H, Liu J, Du L, Wang H. RHGNN: Fake reviewer detection based on reinforced heterogeneous graph neural networks. Knowledge-Based Systems. 2023;**280**: 111029

[65] Dou Y, Ma G, Yu PS, Xie S. Robust spammer detection by Nash reinforcement learning. In: Proceedings of the 26th ACM SIGKDD International Conference on Knowledge Discovery & Data Mining. New York, NY, USA: Association for Computing Machinery; 2020. pp. 924-933

[66] Yang R, Wang X, Jin Y, Li C, Lian J, Xie X. Reinforcement subgraph reasoning for fake news detection. In: Proceedings of the 28th ACM SIGKDD Conference on Knowledge Discovery and Data Mining. New York, NY, USA: Association for Computing Machinery; 2022. pp. 2253-2262

[67] Bei Y, Zhou S, Tan Q, Hao X, Chen H, Li Z, et al. Reinforcement neighborhood selection for unsupervised graph anomaly detection. In: 2023 IEEE International Conference on Data Mining (ICDM). New York City, U.S.: IEEE; 2023. pp. 11-20

[68] Ding K, Shan X, Liu H. Towards anomaly-resistant graph neural networks via reinforcement learning. In: Proceedings of the 30th ACM International Conference on Information & Knowledge Management. New York, NY, USA: Association for Computing Machinery; 2021. pp. 2979-2983

[69] Zhang J, Zhengjia X, Lv D, Shi Z, Shen D, Jin J, et al. Dig-in-gnn: Discriminative feature guided gnn-based fraud detector against inconsistencies in multi-relation fraud graph. Proceedings of the AAAI Conference on Artificial Intelligence. 2024;**38**:9323-9331

[70] Yang Y, Yang R, Li Y, Cui K, Yang Z, Wang Y, et al. RoSGAS: Adaptive social bot detection with reinforced self-supervised gnn architecture search. ACM Transactions on the Web. 2023; **17**(3):1-31

[71] Pateria S, Subagdja B, Tan A-h, Quek C. Hierarchical reinforcement learning: A comprehensive survey. ACM Computing Surveys (CSUR). 2021;**54**(5): 1-35

[72] Pandey M, Kaur H, Echizen I. Enhancing location privacy through prioritized experience replay in deep Q-networks. In: 2024 IEEE International Conference on Systems, Man, and Cybernetics (SMC). New York City, U.S.: IEEE; 2024. pp. 354-360

[73] Yang N, Chen S, Zhang H, Berry R. Beyond the edge: An advanced exploration of reinforcement learning for mobile edge computing, its applications, and future research trajectories. IEEE Communications Surveys & Tutorials; 2024: pp. 1-50

[74] Liang X, Chen T, Hou Z, Zhang W, Hon C, Wang X, et al. Knowledge graph-based reinforcement federated learning for Chinese question and answering. IEEE Transactions on Computational Social Systems. 2023;**11**(1):1035-1045

[75] Devlin J, Chang M-W, Lee K, Toutanova K. Bert: Pre-training of deep bidirectional transformers for language understanding. arXiv preprint arXiv: 1810.04805. 2019

[76] Brown TB, Mann B, Ryder N, Subbiah M, Kaplan JD, Dhariwal P, et al. Language models are few-shot learners. arXiv preprint arXiv:2005.14165. 2020

[77] Iyer R, Maralapalle VC, Mahesh P, Patil D. 13 generative AI and LLM: Case study in e-commerce. In: Generative AI and LLMs: Natural Language Processing and Generative Adversarial Networks. Berlin/Boston: Walter de Gruyter GmbH; 2024. p. 253

[78] Roumeliotis KI, Tselikas ND, Nasiopoulos DK. LLMs in e-commerce: A comparative analysis of gpt and llama models in product review evaluation. Natural Language Processing Journal. 2024;**6**:100056

[79] Das R, Ahmed W, Sharma K, Hardey M, Dwivedi YK, Zhang Z, et al. Towards the development of an explainable e-commerce fake review index: An attribute analytics approach. European Journal of Operational Research. 2024;**317**(2):382-400

[80] Yang L, Ott M, Goyal N, Jingfei D, Joshi M, Chen D, et al. FinBERT: A pretrained language model for financial communications. arXiv preprint arXiv: 2006.08097. 2020

[81] Rudin C. Stop explaining black box machine learning models for high stakes decisions and use interpretable models instead. Nature Machine Intelligence. 2019;**1**(5):206-215