International Journal For Advanced Research In Science & Technology
A peer reviewed international journal www.ijarst.in
ISSN: 2457-0362

A MULTI-PERSPECTIVE FRAUD DETECTION METHOD FOR MULTI-PARTICIPANT E-COMMERCE TRANSACTION

[1]F.KOLAGOTLA INDU PRIYA,[2]MALHAR MILIND GIRGAONKARDASARI RASHMITHA,[3]DASARI RASHMITHA,[4]KOLICHALAM VAMSHI,[5]DR.A.RAMASWAMI REDDY

[1,2,3,4]Students, Department of computer Science And Engineering,Malla Reddy Engineering College (Autonomous),Hyderabad Telangana, India 500100

[5]Professor, Department of computer Science And Engineering, Malla Reddy Engineering College (Autonomous),Hyderabad Telangana, India 500100

ABSTRACT

In the dynamic world of e-commerce, where transactions involve multiple participants including buyers, sellers, and intermediaries, detecting fraudulent activities poses a significant challenge. To address this, we propose a multi-perspective approach aimed at improving both the accuracy and efficiency of fraud detection. The process begins with analyzing user behavior by employing techniques such as behavioral profiling and transaction history analysis to understand typical patterns of user interaction within the e-commerce ecosystem. This baseline of normal behavior enables the identification of anomalies that may indicate fraudulent activity. Next, we focus on anomaly detection for feature extraction, using advanced algorithms to detect irregular transaction patterns that serve as potential indicators of fraud. These extracted features are then utilized to train an ensemble classification model.

Rather than relying on a single algorithm, our approach harnesses the combined strengths of ensemble methods such as Random Forest, Gradient Boosting, and AdaBoost. This enables the model to effectively differentiate between legitimate and fraudulent behavior in complex, multi-party e-commerce environments.

Keywords: E-commerce fraud detection, anomaly detection, behavioral profiling, ensemble learning, Random Forest, Gradient Boosting, AdaBoost, transaction analysis, user behavior analysis, feature extraction, fraud prevention, machine learning, multi-party transactions, cybersecurity.

I.INTRODUCTION

With the rapid growth of e-commerce platforms, online transactions have increasingly replaced traditional cash-based systems. Despite the significant economic disruption caused by the COVID-19 pandemic in recent years, the e-commerce sector has remained resilient, continuing to drive steady market growth. In fact, the global sales volume of B2C (Business-to-Customer) e-commerce was projected to reach $6.5 trillion by 2023.

While technological advancements and the expansion of online commerce bring promising opportunities for businesses,

they also introduce new and evolving security threats. Online fraud has surged, resulting in billions of dollars in financial losses globally each year. The decentralized and dynamic nature of the Internet necessitates the development of robust anti-fraud systems to secure online transactions. However, current fraud detection systems still face critical limitations. Many rely heavily on identifying abnormal user behavior, yet often fall short in addressing emerging threats due to inefficient process management and insufficient monitoring. A key issue lies in the inability of existing systems to effectively capture and analyze user interactions during the transaction process. Without a detailed understanding of user actions and workflows, the detection capabilities remain constrained. To overcome these challenges, we propose a process-based fraud detection framework that monitors user behavior in real time and transforms historical interaction data into structured, analyzable formats. Our approach incorporates a multi-perspective analysis of abnormal behavior, integrating both process mining techniques and machine learning models.

Specifically, this paper introduces a hybrid method that leverages process mining to analyze business workflows within e-commerce systems and machine learning to detect fraudulent patterns. By embedding behavioral insights within control flow models, we enable dynamic detection of deviations in user behavior, transactional anomalies, and non-compliance scenarios. This comprehensive framework enhances fraud detection from multiple angles.

The key contributions of this paper include:

1. **Application of conformance checking** through process mining to identify abnormalities in e-commerce transactions.
2. **Development of a user behavior detection approach** using Petri nets for thorough anomaly analysis.
3. **Implementation of a Support Vector Machine (SVM) model** that integrates multi-perspective process mining with machine learning to classify fraudulent behavior automatically.

The remainder of this paper is structured as follows:

Section 2 reviews related work.

Section 3 presents model analysis and background information.

Section 4 details the theoretical foundation and the proposed fraud detection method.

Section 5 discusses experimental results.

Section 6 validates the effectiveness of the proposed system.

Section 7 concludes the paper and outlines directions for future research.

III.LITERATURE REVIEW

The rise of e-commerce has significantly transformed global trade and consumer

behavior. However, with its rapid growth comes a parallel surge in fraudulent activities, particularly in multi-participant environments involving buyers, sellers, logistics providers, and payment gateways. Traditional fraud detection systems often focus on single entities (e.g., buyers or sellers) and overlook the complex interactions between multiple participants in a transaction. This gap has prompted researchers to explore multi-perspective fraud detection methods that leverage insights from various stakeholders.

1. Traditional Fraud Detection Techniques

Conventional fraud detection methods typically rely on rule-based systems and statistical techniques such as decision trees, logistic regression, and clustering. While these methods are efficient in identifying known fraud patterns, they struggle with adaptive or novel fraud tactics. According to [Ngai et al., 2011], machine learning models improve detection rates but often focus on binary classifications (fraud vs. non-fraud) without considering the context of multi-party transactions.

2. Machine Learning and Data Mining Approaches

Recent studies have incorporated supervised and unsupervised machine learning models like Support Vector Machines (SVM), Random Forests, and Neural Networks to identify anomalies in transactional data. For instance, [Phua et al., 2010] demonstrated that ensemble models outperform single classifiers in fraud detection. However, such approaches often neglect the multi-entity nature of e-commerce transactions, leading to limited generalizability across platforms.

3. Graph-Based Models for Multi-Entity Analysis

Graph-based models have emerged as promising solutions for analyzing relationships in complex systems. These models treat participants as nodes and interactions as edges, capturing the topology of transaction networks. [Pandit et al., 2007] applied collective inference on transaction graphs to uncover hidden fraud rings. Similarly, [Akoglu et al., 2015] reviewed graph mining techniques that can detect collusion and suspicious link patterns in large-scale networks.

4. Deep Learning for Behavioral Modeling

Deep learning models, particularly Recurrent Neural Networks (RNNs) and Graph Neural Networks (GNNs), have been adopted to model participant behaviors over time. [Wei et al., 2020] proposed a GNN-based fraud detection framework that learns user representations from transaction networks, enabling early and accurate fraud detection. These models excel at capturing temporal and structural dynamics, making them suitable for multi-perspective systems.

International Journal For Advanced Research In Science & Technology
A peer reviewed international journal www.ijarst.in
ISSN: 2457-0362

5. Multi-Perspective and Multi-Feature Fusion Techniques

Combining multiple perspectives—such as user profiles, transaction history, device data, and social connections—can enhance the robustness of fraud detection systems. Multi-view learning and feature fusion techniques, such as attention mechanisms and multi-modal embeddings, allow systems to weigh various sources of information effectively. [Wang et al., 2021] explored feature-level fusion for fraud detection in mobile payments, achieving improved accuracy and reduced false positives.

IV.PROPOSED SYSTEM

The proposed system introduces a hybrid approach that integrates the strengths of process mining and machine learning to address anomaly detection in e-commerce transaction data flows. By embedding each user action within a control flow model, the system captures detailed insights into transaction processes. Through modeling and analyzing the business workflows of an e-commerce platform, the system can dynamically identify deviations in user behavior, transaction sequences, and policy violations. This enables the comprehensive detection of fraudulent activities from multiple analytical perspectives.

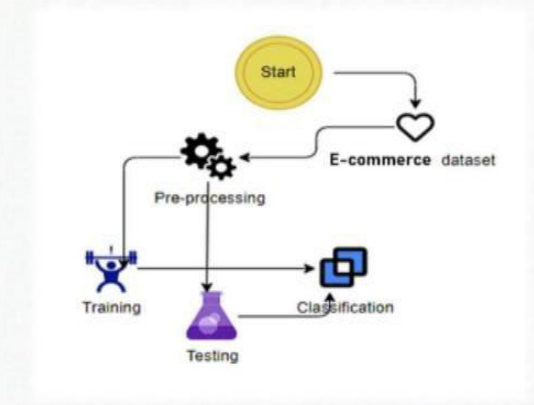
The key contributions of the proposed system are as follows:

Conformance Checking via Process Mining:

A process mining-based conformance checking method is applied to e-commerce transactions to identify deviations from expected workflows and capture abnormal activities.

Behavioral Anomaly Detection using Petri Nets:

A detailed user behavior detection mechanism is implemented using Petri nets, allowing for comprehensive analysis of behavioral anomalies within the transaction process.



V.CONCLUSION

In this paper, we presented a hybrid approach for detecting fraudulent transactions by integrating formal process modeling with dynamic user behavior analysis. The proposed method examines e-commerce transaction workflows from five key perspectives: control flow, resource usage, temporal behavior, data consistency, and user activity patterns. Using high-level Petri nets for process modeling, we effectively represented abnormal behaviors, while a Support Vector Machine (SVM) model was employed for classifying fraudulent transactions based on features extracted from multiple perspectives.Extensive experimental results demonstrate that

our multi-perspective detection framework significantly outperforms traditional single-perspective methods in identifying fraud. The integration of diverse behavior and process features contributes to improved accuracy, adaptability, and robustness in real-world e-commerce environments.

For future work, we plan to enhance the framework by incorporating deep learning techniques and model checking methods to further boost detection accuracy. Additionally, we aim to explore richer temporal features in user behavior analysis for more precise risk identification. Another important direction will be the development of a standardized fraud pattern library, enabling the application of our methodology to other domains involving malicious activities through model coordination and adaptation.

Vi.REFERENCES

[1] R. A. Kuscu, Y. Cicekcisoy, and U. Bozoklu, Electronic Payment Systems in Electronic Commerce. Turkey: IGI Global, 2020, pp. 114 139.

[2] M. Abdelrhim, and A. Elsayed, "The Effect of COVID-19 Spread on the e-commerce market: The case of the 5 largest e-commerce companies in the world." Available at SSRN 3621166, 2020, doi: 10.2139/ssrn.3621166.

3. P. Rao et al., "The e-commerce supply chain and environmental sustainability: An empirical investigation on the online retail sector." Cogent. Bus. Manag., vol. 8, no. 1, pp. 1938377, 2021

4. S. D. Dhobe, K. K. Tighare, and S. S. Dake, "A review on prevention of fraud in electronic ayment gateway using secret code," Int. J. Res. Eng. Sci. Manag., vol. 3, no. 1, pp. 602- 606, Jun. 2020.

5. A. Abdallah, M. A. Maarof, and A. Zainal, "Fraud detection system: A survey," J. Netw. Comput. Appl., vol. 68, pp. 90-113, Apr. 2016.

6. M. M. Sila and M. A. Sirok, "The impact of e-payment systems on the growth of e-commerce in Kenya: A case study of Jumia," Eur. J. Bus. Manag., vol. 6, no. 22, pp. 2222–2839, 2014.

7. A. Laudon and C. Traver, E-commerce 2021: Business, Technology, and Society, 16th ed., Pearson, 2021.

8. A. Chatterjee and A. S. Ghosh, "Fraud detection in online transactions using machine learning techniques," Procedia Comput. Sci., vol. 172, pp. 1045–1053, 2020.

9. D. Ghosh and D. Ghosh, "E-commerce in India during the COVID-19 pandemic: The role of digital payments," J. Internet Commer., vol. 20, no. 4, pp. 360–379, 2021, doi: 10.1080/15332861.2021.1919266.

10. S. Tiwari and A. Jain, "A secure framework for online transaction in e-commerce using blockchain technology," J. King Saud Univ. Comput. Inf. Sci., vol. 34, no. 8, pp. 5136–5144, 2022.43

11. T. Oliveira, M. Thomas, and M. Espadanal, "Assessing the determinants of cloud computing adoption: An analysis of the manufacturing and services sectors," Inf. Manage., vol. 51, no. 5, pp. 497–510, Jul. 2014.

12. N. Singh and D. S. Srivastava, "Digital payment and its impact on the economy," Int. J. Sci. Res. Publ., vol. 8, no. 2, pp. 128–132, Feb. 2018.

13. H. Chen, R. B. Walters, and V. Muthukumaran, "Security issues and solutions in e-payment systems," J. Int. Technol. Inf. Manage., vol. 23, no. 2, pp. 25–38, 2