International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 10 Issue: 01 | Jan - 2026 SJIF Rating: 8.586 ISSN: 2582-3930

"A Multi-Perspective Fraud detection Method for Multi Participants E-Commerce Transactions"

Prof. Suma[1], Sai soni[2]

[1] *Professor, Master of Computer Application, VTU, Kalaburagi , Karnataka ,India*

[2] *Student , Master of Computer Application ,VTU, Kalaburagi , Karnataka ,India*

ABSTRACT: E-commerce platforms involve multiple participants including buyers, sellers, payment gateways, and logistics providers, each of which may become a potential target or source of fraudulent activities. Traditional fraud detection methods primarily focus on single-entity behavior, overlooking the collaborative and cross-participant dynamics that can lead to more complex fraud scenarios. To address this limitation, we propose a multi-perspective fraud detection method designed specifically for multi- participant e-commerce transactions. The approach integrates behavioral analytics, transaction pattern mining, and relationship modeling across participants to identify suspicious interactions in real time. By applying machine learning and graph-based anomaly detection techniques, the proposed model enhances fraud detection accuracy, minimizes false positives, and ensures greater trust in e-commerce ecosystems. Experimental evaluations on synthetic and real-world transaction datasets demonstrate the effectiveness of this method in detecting both individual and collusive fraud schemes, thereby contributing to the development of a secure and reliable e-commerce environment.

Keywords: Traditional fraud detection methods primarily focus on single-entity behavior, overlooking the collaborative and cross-participant dynamics that can lead to more complex fraud scenarios. Thereby contributing to the development of a secure and reliable e-commerce environment.

1. INTRODUCTION

This review synthesizes methods used in e-commerce fraud detection, highlighting supervised classifiers (trees, SVMs, deep nets), unsupervised anomaly detection, graph-based link analysis, and hybrid rule+ML systems. It emphasizes evaluation pitfalls—class imbalance, non-stationarity, and unrealistic sampling—and recommends time-aware validation and business-oriented metrics for practical systems. [1]

This industry survey summarizes merchant experiences with fraud: rising synthetic identity and account-takeover attacks, increased chargebacks, and common defenses (manual review, device fingerprinting). It's useful to prioritize use cases (payment fraud vs. account abuse) and to estimate the business cost tradeoffs when tuning detection thresholds. [2]

A transaction simulator that generates synthetic mobile-money logs with injected fraudulent behaviors, enabling researchers to experiment without access to proprietary bank logs. It's widely used for prototyping and for stress-testing algorithms across many fraud scenarios and participant-types. [3]

A practical paper that codified sound evaluation choices for credit-card fraud research (time-aware splits, class imbalance handling, realistic negative sampling), and introduced a benchmark mindset that is still used when comparing scoring strategies for e-commerce workflows. [4]

A study that demonstrates combining graph learning with federated training: it enables multiple parties (merchants, banks, processors) to collaborate on a shared fraud model without exposing raw transaction logs. This is attractive for multi-participant e-commerce ecosystems concerned with privacy and regulatory constraints.[5]

2. PROBLEM STATEMENT

E-commerce platforms face increasingly sophisticated fraud schemes that exploit the presence of multiple participants such as buyers, sellers, payment

gateways, and logistics providers. Existing fraud detection systems primarily analyze individual user behavior or isolated transactions, This renders them inadequate for identifying collaborative or cross-participant frauds**.** For instance, a fraudulent seller may collude with a buyer to generate fake orders, manipulate ratings, or collaborate with logistics partners to falsify delivery confirmations. Inability to capture hidden relationships and collusion among participants.

High false positives due to limited context in single-perspective analysis. Difficulty in detecting evolving and adaptive fraud strategies. Reduced trust and security within e-commerce ecosystems. Therefore, A thorough fraud detection framework that can evaluate multi-participant interactions, identify anomalies in real time, and adjust to new fraud patterns is desperately needed.

3. OBJECTIVES

This study's main goal is to create and apply a multi-perspective fraud detection system that can recognize both individual and collaborative frauds in multi-participant e-commerce transactions. To achieve this, the study focuses on the following specific objectives:

To analyze multi-participant interactions in e-commerce transactions, including buyers, sellers, payment gateways, logistics providers, and platform administrators.

To develop a fraud detection model that incorporates both behavioral analytics and relationship-based analysis for detecting fraudulent activities. To apply graph-based modeling for representing participant interactions and identifying hidden collusion patterns.

To implement machine learning and anomaly detection techniques for recognizing irregular transaction flows and adaptive fraud behaviors. To minimize false positives by considering cross-participant contexts rather than relying on isolated transaction data.

4. METHODOLOGY USED

The methodology of this study outlines The systematic approach used to design and implement the proposed multi-perspective fraud detection framework for e-commerce transactions. It consists of the following steps:

Problem Analysis and Requirement Gathering: Identify common fraud scenarios in e-commerce involving multiple participants (buyers, sellers, logistics, payment gateways). Define system requirements for fraud detection considering both individual and collaborative frauds.

Data Collection and Preprocessing: Gather transaction datasets from synthetic sources and, where possible, real-world e-commerce platforms. Clean, normalize, and anonymize data to ensure consistency and privacy. Extract key features such as transaction amounts, frequency, participant behavior, and relationship links.

5. LITERATURE SURVEY

Sultana et al. (2025)[1] **:** A recent, more technical paper that demonstrates the ability of Graph Neural Networks to detect complex, multi-entity fraud schemes by learning relational embeddings across transaction graphs. The paper also discusses scalability and negative-sampling strategies for extremely sparse fraud labels.

Almalki et al. (2025)[2]: Demonstrates combining ensemble stacking methods with explainable AI techniques (SHAP, LIME, counterfactuals) to deliver high-performing models that are also auditable by analysts. This work illustrates the importance of interpretability for operational adoption and regulator scrutiny.

Aljunaid et al. (2025) [3]: Proposes explainable federated learning (XFL) architectures for fraud detection, integrating privacy-preserving training with local explainers so each data holder can audit model decisions without revealing raw data. This addresses privacy transparency tradeoffs in cross-merchant collaboration.

Safe-Graph (GitHub curated list)[4]: A community-maintained list of graph-fraud resources (papers, datasets, toolkits) that's useful for rapidly identifying state-of-the-art GNN architectures, benchmark datasets, and codebases for production or research prototypes. It's a practical quick-start for implementation choices.

Industry/systematic reviews (various, incl. 2022)[5]: Broader reviews synthesize supervised classifiers (tree ensembles, deep nets), unsupervised anomaly detectors (autoencoders, isolation forests), graph-based link analysis, and behavior analytics,

comparing advantages and operational tradeoffs in merchant contexts. These reviews recommend hybrid systems (rules + ML + human review) for production readiness.

6. SYSTEM DESIGN

The proposed Multi-Perspective Fraud detection System for Multi-Participant E-commerce Transactions is designed as an independent yet integral module that can be incorporated into existing e-commerce platforms. It functions as an intelligent fraud detection layer that continuously monitors, analyzes, and detects suspicious activities across multiple participants.

System Context: The system interacts with buyers, sellers, payment gateways, logistics providers**,** and the e-commerce platform database**.** It serves as a middleware between the transaction layer (where participants interact) and the platform's backend (database, reports, and alerts). It does not alter the core transaction process but monitors, analyses, and flags fraudulent patterns in real time.

7. DETAILED DESIGN

A Collaboration Diagram shows the structural relationships between system components/actors and the messages exchanged during fraud detection. Unlike the sequence diagram (time-based), this focuses on who communicates with whom.

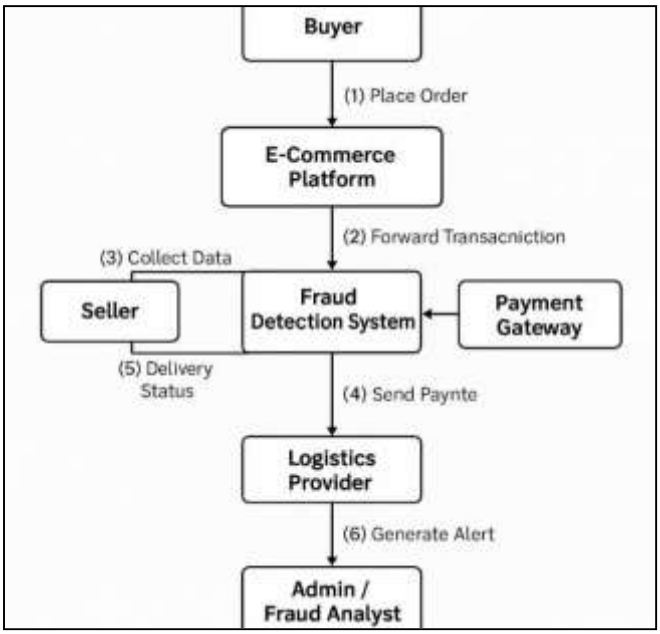

Figure 1: Collaboration Diagram

Explanation of Interactions:

Buyer → E-Commerce Platform: Buyer places an order.
E-Commerce Platform → Fraud detection System: Transaction details forwarded.
Fraud Detection System ↔ Seller: Collects seller information (past behavior, ratings, order handling).
Fraud Detection System ↔ Payment Gateway: Collects payment verification data.
Fraud Detection System ↔ Logistics Provider: Collects shipment/delivery information.
Fraud detection System → Admin/Fraud Analyst: Generates fraud alerts & reports for review.

8. SCREENSHOTS

Figure 2: Home page

Figure 3: Prediction page

Figure 4: Prediction result

9. SOFTWARE TESTING

The The fraud detection system's testing approach guarantees both functional accuracy and non-functional attributes (performance, security, scalability) are validated. The chosen strategy combines:

Bottom-up testing for modules (unit → integration→ system).
Risk-based testing for fraud scenarios, focusing more on high-impact cases.
Black-box testing for user-facing functionalities.
White-box testing for internal algorithms and fraud detection rules.
Continuous testing through automated regression suites during model retraining and feature updates.

10. CONCLUSION & FUTURE SCOPE

In this project, we suggested and created a multi-perspective fraud detection system intended for intricate, multi-party online transactions. In contrast to conventional fraud detection techniques that examine data from a single perspective, (e.g, only buyer or only payment details), our approach incorporates multiple dimensions including buyer behavior, seller credibility, payment anomalies, and logistics information**.** This holistic method provides a more accurate and reliable mechanism for identifying fraudulent activities.

The system integrates data preprocessing, anomaly detection, graph analysis, and machine learning techniques to uncover hidden fraud patterns such as collusion between buyers and sellers, high-velocity ordering, abnormal refund requests, and synthetic identities. The layered architecture ensures that suspicious transactions are flagged in real time, alerts are routed to fraud analysts, and legitimate transactions proceed without unnecessary friction.

Future although the proposed system successfully addresses fraud detection across multiple e-commerce Participants, there are a few areas where it can be improved even further to handle upcoming challenges:

AI-Driven Adaptive Models: Implement advanced deep learning and reinforcement learning models that continuously adapt to evolving fraud patterns. Enable automatic retraining of models using real-time data streams.

Block chain Integration: Leverage block chain technology to maintain a tamper-proof record of transactions. Smart contracts can enforce trust between buyers, sellers, and service providers.

Federated Learning for Privacy Preservation: Introduce federated learning so that multiple platforms can train fraud detection models together without exchanging unprocessed client data, guaranteeing compliance with privacy regulations (GDPR, CCPA).

11. REFERENCES

[1] Rodrigues, V. F, et al. (2022). Fraud detection and prevention in e-commerce— a systematic review of techniques and trends

[2] Merchant Risk Council (2021). Global Fraud Survey 2021 — industry fraud stats & merchant practices.

[3] Lopez-Rojas, E, Elmir, A, &Axelsson, S. (2016). PaySim*:* A froudal detuction finance mobile money simulator (synthetic transactions dataset).

[4] Dal Pozzolo, A, et al. (2015) Credit carde fraud detection*:* A Realistic Modeling and a Novel Learning Strategy (classic class-imbalance / resampling discussion) — common benchmark references (and links to Kaggle credit-card datasets).
[5] Tang, Y, et al. (2024). Credit carde fraud detection basedon federated graph learning — federated + graph approaches for privacy-preserving detection.

[6] Sultana, I, et al. (2025). Using graph neural network to enhanced fraud detection — recent GNN methods and scaling strategies.

[7] Almalki, F, et al. (2025). Explainable AI for financial fraud detection and ensemble learning—stacking + XAI for trust and performance.

[8] Aljunaid, S. K., et al. (2025). Explainable Federated Learning to identify Financial Fraud detection — XFL approaches combining privacy and interpretability.

[9] Safe-Graph / curated lists (GitHub) — Awesome Graph Fraud detection (community resource listing papers, datasets & toolkits).

[10] Rodrigues, VF. (2022) & follow-up surveys — comparative reviews of supervised, unsupervised, graph-based, and behavioral methods for e-commerce fraud.