

Research Article

A Multi-Perspective Fraud Detection Method for Multi-Participant E-Commerce Transactions

Ratnala Varshitha¹, Tuniki Aparna², Polepaka Shravani³, Atmakuri Venkata Reddy⁴ and V. Shiva Narayana Reddy^{5,*}

^{1,2,3,4} Student, Department of CSE, Samskurthi College of Engineering and Technology, Hyderabad, Telangana, 500001, India.

⁵ Associate Professor, Department of CSE, Samskurthi College of Engineering and Technology, Hyderabad, Telangana, 500001, India.

*Corresponding Author: V. Shiva Narayana Reddy. Email: vsn.reddy5017@gmail.com

Received: 01/08/2025; Revised: 12/09/2025; Accepted: 25/09/2025; Published: 30/09/2025.

DOI: <https://doi.org/10.69996/fmep.2025017>

Abstract: E-commerce platforms face growing challenges in detecting and preventing fraudulent transactions due to the evolving strategies of attackers and the hidden nature of online interactions. Traditional fraud detection systems largely depend on historical order information, which limits their ability to detect dynamic and sophisticated fraudulent behavior. This paper introduces a novel fraud detection framework that combines machine learning techniques with process mining to monitor and analyze real-time user behavior within B2C e-commerce platforms. The approach begins with constructing a behavioral process model tailored to the transaction flows of e-commerce users. An anomaly detection method is then applied to extract critical features from event logs, capturing irregularities in transaction activities. These features are subsequently fed into a Support Vector Machine (SVM)-based classification model to accurately identify fraudulent transactions. Experimental results validate the proposed model's capability to detect complex, evolving fraud patterns with improved accuracy and efficiency. This integrated approach enhances the adaptability and robustness of fraud detection mechanisms in modern e-commerce environments.

Keywords: E-commerce fraud detection, Machine learning, Process mining, Support Vector Machine (SVM).

1. Introduction

The exponential growth of e-commerce platforms has revolutionized the way individuals and organizations engage in commercial activities, making transactions more convenient, faster, and accessible on a global scale [1]. This digital evolution, however, has simultaneously given rise to new and sophisticated forms of cybercrime, with fraud standing out as one of the most prevalent and damaging threats in online commercial ecosystems [2]. Fraudulent activities in e-commerce not only result in direct financial losses for businesses and customers but also significantly erode consumer trust, disrupt operations, and tarnish brand reputations [3]. As the number of participants in e-commerce transactions increases—including sellers, buyers, third-party vendors, logistics providers, and financial intermediaries—the complexity of fraud detection escalates, creating a challenging environment for ensuring transactional integrity [4]. Traditional fraud detection methods often focus on single-perspective data analysis—such as analyzing buyer behavior or financial transaction patterns in isolation [5]. While such approaches can identify basic anomalies, they fall short when dealing with coordinated fraudulent behaviour involving multiple participants across the transaction chain [6]. These schemes may include



seller collusion, identity spoofing, payment fraud, fake reviews, or triangulation fraud, which exploit the distributed nature of e-commerce infrastructures [7]. Moreover, the dynamic and fast-paced environment of online commerce allows fraudsters to quickly adapt to detection mechanisms, making static or rule-based systems ineffective in long-term fraud mitigation. This necessitates the development of intelligent, adaptive, and multi-perspective approaches that can analyze diverse data streams and uncover hidden patterns indicative of fraud. Another major challenge in e-commerce fraud detection is the imbalance and heterogeneity of available data. Fraudulent transactions typically represent a small minority of the overall transaction volume, leading to highly skewed datasets. This imbalance often causes traditional classifiers to underperform, as they tend to favour majority classes and misclassify rare yet critical fraudulent activities. Additionally, multi-participant environments introduce a high level of data heterogeneity, as information may span structured transaction logs, unstructured user reviews, social media interactions, geographic information, and behavioural metrics. Effectively integrating and analyzing such disparate data sources is essential to providing a holistic view of the transaction and its involved entities.

Recent advancements in machine learning (ML), data mining, and network analysis have enabled the development of more robust and scalable fraud detection frameworks. These techniques allow for the extraction of meaningful patterns and relationships from large and complex datasets. Specifically, graph-based learning models and behaviour profiling methods have shown promise in identifying collusive behaviours and abnormal transaction flows. However, despite the technological progress, there remain significant gaps in the literature concerning the simultaneous analysis of multiple participant roles and their interactions within the transaction process. Most existing studies focus narrowly on either user fraud or seller-side anomalies, neglecting the interconnected nature of fraud across different transaction participants. In response to these challenges, there is a growing recognition that fraud detection in e-commerce must evolve beyond linear and siloed approaches. A shift toward multi-perspective analysis is essential for capturing the full scope of fraudulent behaviour in ecosystems where various actors can dynamically assume multiple roles. For instance, a single user may function as both buyer and seller, or fraudsters may control multiple accounts to simulate legitimate activity. Understanding these role dynamics requires intelligent modelling of transaction networks, participant behaviors, and contextual information over time. Furthermore, the temporal evolution of fraud patterns highlights the need for real-time or near real-time monitoring systems that can adapt to emerging threats and evolving strategies used by malicious actors. Trust, transparency, and accountability are foundational principles in e-commerce, yet they are persistently undermined by the rising sophistication of fraudulent schemes. This is particularly concerning in sectors such as online marketplaces, digital services, and cross-border commerce, where participant verification is often weak and regulatory oversight is limited.

The primary contribution of this paper lies in the development of a multi-perspective fraud detection framework tailored for multi-participant e-commerce transactions. Unlike conventional methods that rely solely on historical transaction data, this research integrates process mining techniques with machine learning algorithms to capture dynamic user behaviours in real time. A unique process model is proposed for B2C e-commerce environments that enables the detection of abnormal activity patterns from event logs. The model extracts significant behavioral features which are then used to train a Support Vector Machine (SVM) classifier for effective fraud detection. This hybrid approach enhances detection accuracy by considering both static and temporal aspects of user interactions, thereby enabling early identification of

suspicious behaviour. The system's ability to analyze ongoing user actions, rather than just static data, addresses an existing gap in fraud prevention technologies. Through extensive simulation, the framework demonstrates its robustness and reliability in capturing context-aware fraudulent activities, making it highly applicable to real-world e-commerce platforms where multiple users and roles interact dynamically.

2.Related Works

The detection of fraud in e-commerce platforms has attracted significant research attention over the past decade, particularly due to the financial, operational, and reputational threats it poses to digital ecosystems. Traditional approaches to fraud detection have largely centered around rule-based systems, where predefined if-then rules are used to flag suspicious activities. While these methods are simple and interpretable, they lack the adaptability required to handle evolving fraud strategies and are often prone to high false-positive rates. As a result, researchers have increasingly turned to machine learning (ML) and data mining techniques to enhance the accuracy, scalability, and efficiency of fraud detection models. Early ML-based studies predominantly focused on binary classification models using supervised algorithms such as logistic regression, decision trees, random forests, support vector machines (SVM), and artificial neural networks (ANN). These models performed well when sufficient labelled data was available, especially in detecting credit card fraud and transaction anomalies. However, the severe class imbalance in real-world datasets—where genuine transactions vastly outnumber fraudulent ones—posed significant challenges in achieving reliable fraud detection. To address this, techniques such as oversampling (e.g., SMOTE), under sampling, and cost-sensitive learning were introduced to improve model sensitivity towards minority classes.

Mamand [8] applied classical data mining strategies to fraud scenarios and emphasized the importance of preprocessing and domain understanding to derive actionable insights from transactional datasets. Narayan et al. [9] explored the application of machine learning algorithms in e-commerce environments, highlighting the critical role of supervised learning models in enhancing fraud detection accuracy across digital marketplaces. Paul and Paul [10] introduced a novel bio-inspired optimization method using the Poor and Rich Squirrel Algorithm integrated with a Deep Maxout Network, demonstrating significant improvement in credit card fraud detection tasks. Similarly, Seera et al. [11] developed an intelligent fraud detection system that combines fuzzy min-max neural networks and decision trees, achieving notable performance in identifying fraudulent payment card transactions. The issue of class imbalance in fraud datasets was addressed by Baisholan et al. [12], who proposed FraudX AI, a framework focused on interpretable machine learning applied to imbalanced credit card data. Yan et al. [13] advanced this line of work with the FIW-GNN model, a heterogeneous graph-based learning approach designed to model complex relationships in credit card fraud detection. Their approach demonstrated promising results in capturing both behavioral and structural anomalies through graph representation learning. Adebayo et al. [14] provided a comparative review of machine learning and concept drift techniques for credit card fraud detection, emphasizing the limitations of static models and the need for adaptive systems. Cheng et al. [15] proposed the GNN-CL model, combining graph neural networks with contrastive learning to detect fraud in financial transactions with greater generalization capabilities across unseen fraud patterns.

Process mining techniques were adopted by Chinnaiah et al. [16], who used deep autoencoders to reconstruct business processes and detect anomalies in transaction flows, providing a foundation for understanding fraud in operational contexts. Karthika and Senthilselvi

[17] implemented a credit card fraud detection system using a dilated CNN architecture with sampling strategies, demonstrating strong performance in sequential data learning while tackling data imbalance. Ensemble methods have also received attention, as shown by Bakhtiari et al. [18], who applied multiple classifiers through data mining ensembles to increase prediction accuracy in fraud detection. Almazroi and Ayub [19] focused on online payment fraud and utilized multiple machine learning techniques to build a hybrid detection model capable of adapting to different payment modalities. Broader perspectives on safeguarding credit card transactions were reviewed by Vetrivendan and Kumar [20], who conducted a comprehensive study comparing fraud prevention techniques, providing insights into the strengths and weaknesses of each. Tiwari et al. [21] conducted an empirical comparison of credit card fraud detection algorithms, identifying SVM and ensemble models as particularly effective under specific data configurations.

Natural Language Processing (NLP) methods have also been utilized in fraud detection, such as the FinChain-BERT model introduced by Yang et al. [22], which applied BERT-based NLP techniques to financial texts for fraud classification tasks. Mahya et al. [23] took a bibliometric approach to analyze research trends in automated fraud detection, uncovering thematic clusters and indicating a growing preference for intelligent automation tools in financial fraud investigation. Stachura [24] introduced a cloud-based fraud detection model utilizing Recurrent Neural Networks (RNNs) and automated feature extraction, showcasing the effectiveness of sequential learning in banking applications. Lastly, Ouazzane et al. [25] proposed a novel feature engineering framework that integrates both traditional machine learning and deep learning algorithms for cyber fraud detection, underscoring the importance of feature representation in improving detection accuracy across various fraud scenarios.

The extensive research on fraud detection using machine learning, deep learning, graph analysis, and data mining techniques, a significant gap remains in effectively addressing fraud in multi-participant e-commerce environments. Most existing studies primarily focus on detecting fraud at the individual level—either analyzing buyer behavior, seller anomalies, or transactional irregularities in isolation. However, real-world fraud often involves coordinated behavior among multiple parties, such as buyer-seller collusion, fake reviews, or third-party manipulation, which cannot be captured through single-perspective models. Furthermore, many models rely heavily on static rule-based or supervised approaches that fail to generalize well to evolving fraud patterns or previously unseen attacks. Techniques addressing class imbalance and heterogeneous data sources have emerged, but they still lack a unified framework capable of correlating behavior across various entities involved in a transaction. Additionally, while some studies have adopted graph-based models and hybrid approaches, they often overlook the temporal evolution of fraud and do not integrate multi-role dynamics, where a single actor may assume different identities or roles within a system. The lack of interpretability and scalability in many advanced models also limits their real-time applicability in dynamic e-commerce ecosystems. Therefore, there is a pressing need for a robust, multi-perspective fraud detection framework that captures interdependencies, models participant behavior holistically, adapts to changing patterns, and provides explainable outputs to ensure trust, transparency, and timely intervention.

3. Proposed Fraud Detection with Machine Learning

The detection and prevention of fraudulent transactions have long been critical priorities for securing e-commerce platforms. However, the inherent anonymity and dynamic nature of e-commerce environments make it difficult to accurately identify malicious actors using only

historical transaction data. Traditional fraud detection techniques often fall short, as they typically ignore the evolving behavioural patterns of users and do not account for interactions from multiple participant roles. This results in limited detection accuracy and delayed responses to fraudulent activities. To address these limitations, this study proposes a novel fraud detection framework that combines machine learning with process mining to analyze real-time user behaviours in multi-participant e-commerce systems. The approach begins by constructing a process model tailored to Business-to-Consumer (B2C) e-commerce operations, incorporating behaviour tracking of users across the transaction lifecycle. An abnormality analysis mechanism is then employed to extract significant behavioural features from event logs, capturing deviations from normative user conduct. These extracted features are subsequently input into a Support Vector Machine (SVM) classifier, which is trained to distinguish between legitimate and fraudulent transactions. Experimental results validate the proposed method's effectiveness in detecting dynamic, context-dependent fraudulent behaviours, highlighting its potential to enhance transaction security and reduce financial losses in e-commerce ecosystems.

The detection and prevention of fraudulent transactions in e-commerce systems are vital to maintaining trust, financial stability, and platform integrity. Traditional fraud detection techniques primarily rely on static, rule-based methods or historical transaction analysis. However, these approaches often fail to identify dynamic or hidden fraudulent behaviours, especially in modern multi-participant e-commerce systems where multiple roles (e.g., buyer, seller, intermediary) interact continuously. To address these challenges, this paper introduces a multi-perspective fraud detection framework that integrates machine learning with process mining techniques. The proposed method is designed to monitor user behaviors in real time, extract relevant patterns from transaction activities, and classify potential frauds with high accuracy. Detecting fraudulent transactions on e-commerce platforms is increasingly difficult due to the complex and dynamic behaviours of users. Traditional fraud detection approaches rely on predefined rules or historical transaction patterns, which often fail to detect evolving or multi-participant fraud. These limitations highlight the need for a more adaptive and real-time method that can capture user behaviour from multiple perspectives. This paper proposes a novel fraud detection framework that combines process mining and machine learning to monitor and classify transactions more accurately. To capture user activity patterns, we define a process model for typical e-commerce interactions such as browsing, adding items to cart, payment, and review submission. Each transaction is considered a sequence of events stated in equation (1)

$$P(t) = \langle e1, e2, \dots, en \rangle \quad (1)$$

In equation (1) $P(t)$ is the process of transaction t , and e_i represents the i -th event (e.g., login, view product, payment). Unusual behavior such as skipping expected events (e.g., making a payment without browsing or cart activity) may signal fraudulent intent. We extract important features from event logs that reflect user actions over time. These features form the basis for identifying abnormalities. Session Time ($f1$) stated as Total duration of a user session. Event Count ($f2$) demonstrated as Number of actions in a transaction; Missing Events ($f3$) stated as Expected steps not followed and Transaction Frequency ($f4$) defined as Number of transactions per hour/day. Each transaction is converted into a feature vector defined in equation (2)

$$X = [f1, f2, f3, f4] \quad (2)$$

These vectors help distinguish between normal and suspicious transactions. To quantify how unusual a transaction is, we assign an abnormality score using a weighted sum stated in equation (3)

$$A(t) = w_1 \cdot f_1 + w_2 \cdot f_2 + w_3 \cdot f_3 + w_4 \cdot f_4 \quad (3)$$

In equation (3) $A(t)$ represented as Abnormality score of transaction t and w_i defined as Weight assigned to each feature. Higher scores indicate greater deviation from normal behavior and potential fraud. We use a Support Vector Machine (SVM) for classifying transactions as fraudulent or genuine. The SVM learns from past transaction data with known labels. Let X_i is the Feature vector of transaction i and y_i stated as Label for transaction i ($1 = \text{fraud}$, $0 = \text{genuine}$). The SVM classifier finds the best boundary (hyperplane) to separate the two classes defined in equation (4)

$$f(X) = \text{sign}(w \cdot X + b) \quad (4)$$

In equation (4) w represented as Weight vector learned during training; b stated as Bias term and $f(X)$ denoted as Output class (1 or 0). During testing, new transactions are classified in real time based on their feature vectors. Fraud detection in e-commerce platforms is a critical challenge due to the rapid growth of online transactions and the increasing sophistication of fraudsters. Traditional methods rely heavily on static rules and historical data patterns, which often fail to capture evolving, multi-actor fraudulent schemes. These methods typically analyze the behavior of individual users—such as buyers or sellers—in isolation, ignoring the complex interactions that can occur between multiple parties involved in a single transaction. In real-world scenarios, fraud often arises from coordinated activities between different participants, including fake buyers, compromised sellers, and manipulated delivery processes. To address these complexities, we propose a fraud detection framework that integrates behavioral process modeling and machine learning techniques, enabling the detection of dynamic and multi-perspective fraudulent activities in real time. The proposed method begins by modeling user behaviors as a sequence of events within the transaction flow of a typical e-commerce platform. This includes activities such as logging in, browsing products, adding items to a cart, completing payments, submitting reviews, and requesting refunds. Each user's behavior is tracked and recorded as an event log, which captures the sequence and timing of their actions. By analyzing these logs, it becomes possible to identify deviations from normal behavior patterns. For instance, if a user repeatedly completes high-value purchases within seconds of logging in, without browsing or cart activity, this may indicate automated or suspicious activity. Next, the system extracts meaningful behavioral features from the event logs. These features include the time spent per session, the number of actions taken, the order of events, frequency of transactions, and any unusual patterns such as skipping steps or triggering refunds shortly after delivery confirmation. These features help build a comprehensive profile of each user's activity and provide valuable indicators of potential fraud. Additionally, the system considers contextual factors such as the geographical location of the transaction, the device used, and the time of day, which may offer further insights into suspicious behavior.

After extracting the behavioral features, they are fed into a machine learning model for classification. We employ a Support Vector Machine (SVM) as the primary classifier due to its effectiveness in handling high-dimensional data and its robustness in binary classification tasks. The model is trained using labeled transaction data that includes both legitimate and fraudulent cases. During the training process, the model learns to differentiate between normal and abnormal behavior patterns based on the input features. Once trained, the SVM model is capable of analyzing new, unseen transactions and predicting whether they are likely to be fraudulent. - The system operates in real-time, continuously monitoring user behavior and processing transactions as they occur. When a transaction is initiated, the system captures the associated

event data, extracts the relevant features, and applies the trained SVM model to classify the transaction. If the model flags the transaction as potentially fraudulent, it can be automatically blocked or routed for further investigation by the security team. This real-time capability ensures that fraud is detected and mitigated before financial damage occurs. To validate the effectiveness of the proposed method, we conducted a series of experiments using a benchmark dataset containing real-world e-commerce transactions. The model was evaluated based on standard performance metrics such as accuracy, precision, recall, and F1-score. Results indicate that the proposed approach significantly outperforms traditional rule-based systems and single-perspective models, especially in detecting complex, coordinated fraudulent behaviors. The system demonstrated a high recall rate, indicating strong capability in identifying true fraud cases, while maintaining low false positive rates, which is essential to avoid disrupting legitimate user activity.

4. Proposed Process Model for B2C E-Commerce

In the context of Business-to-Consumer (B2C) e-commerce, transactions involve complex interactions among various stakeholders, including buyers, sellers, payment gateways, logistics providers, and review systems. To efficiently detect and mitigate fraud within such a multi-entity environment, a well-structured and dynamic process model is essential. The proposed process model is designed to comprehensively map the behavioral flows and transactional dependencies in a typical B2C e-commerce ecosystem. It serves as the operational foundation upon which behavior tracking, anomaly detection, and machine learning-based classification are built. Unlike traditional linear models, this model captures the cyclic, evolving, and concurrent nature of user and system interactions, enabling real-time analysis and fraud detection. The model initiates with the user onboarding process, where users register as buyers or sellers. This stage captures essential metadata including IP address, device ID, location, time of registration, and behavioral fingerprints like typing patterns and browser behavior. By building early behavioral baselines, the system gains insights into normal account setup actions, which can later be compared to identify anomalies in future sessions. After registration, users undergo authentication and login sessions, which are monitored for unusual patterns, such as multiple logins from different locations or frequent failed attempts. These initial stages are crucial as they provide the first opportunity to flag suspicious behaviors before financial transactions occur.

Once users are authenticated, the pre-transaction phase begins. This involves users browsing products, searching for items, adding items to the cart, interacting with seller profiles, and reviewing past ratings. The system records the time spent per product, scroll behavior, click-through rates, and other micro-interactions. Sellers, on the other hand, engage in listing products, modifying prices, updating stock, and interacting with buyer queries. This phase provides insight into both buyer interest levels and seller transparency. For example, a seller who frequently edits item descriptions or prices just before peak traffic hours may warrant attention. Similarly, buyers who spend minimal time on product descriptions and proceed directly to purchase may be flagged for bot-like behavior. The model then progresses to the transaction phase, which is the most sensitive part of the e-commerce lifecycle. Buyers proceed to checkout, select payment methods, and complete transactions via integrated payment gateways. During this phase, the model captures critical features such as payment time, transaction value, chosen payment method, and any use of vouchers or discounts. Unusual patterns like multiple high-value purchases within a short timeframe or inconsistent shipping addresses are recorded and evaluated. Sellers

simultaneously prepare and ship the items, while logistics services are engaged for tracking and delivery. Any manipulation in delivery status or shipment tracking updates can be signs of fraudulent seller behavior, which the system logs for review. Following the transaction, the post-transaction phase begins. This includes receiving the product, submitting reviews, filing for returns or refunds, and post-delivery communication between buyers and sellers. The model is particularly sensitive to abnormal post-delivery actions such as immediate negative reviews, rapid refund requests, or multiple complaints raised across short periods. Similarly, suspicious seller behavior, such as quick removal of listings after receiving payments or failing to provide shipment details, is carefully analyzed. Each user's historical transaction behavior is compared with current activities to evaluate deviation scores, and if behavior significantly diverges from established patterns, it is flagged for deeper analysis. Another critical aspect of the model is the feedback and reputation system, where users rate products and sellers, and vice versa. Fraudulent users may exploit this feature to manipulate seller reputations, inflate product ratings, or discredit competitors. The process model includes modules for sentiment analysis of reviews, temporal tracking of rating patterns, and correlation of feedback with actual delivery performance. This ensures that fake reviews—often generated by bots or fraudulent networks—are identified and penalized.

The process model integrates event logging and feature extraction mechanisms at every stage. Event logs are generated in real-time and stored securely for subsequent processing. These logs are structured to capture user ID, timestamps, action types, device metadata, and contextual details. The model uses these logs to extract time-based, sequence-based, and statistical features, which are then input into the fraud detection classifier. In particular, the model supports parallel analysis across multiple users to detect collusion or coordinated attacks—an advanced form of fraud often seen in high-volume e-commerce platforms. Finally, the model includes a feedback loop, where confirmed fraud cases are used to retrain and update the behavioral profiles and classification algorithms. This self-improving mechanism ensures that the system adapts to new fraud strategies and continues to evolve over time. The proposed process model is thus comprehensive, real-time, adaptive, and scalable, making it highly suitable for modern B2C e-commerce platforms dealing with large volumes of diverse transactions involving multiple actors. By continuously monitoring and analyzing the full lifecycle of user behavior—from onboarding to post-transaction interactions—the model provides a robust foundation for multi-perspective fraud detection.

Algorithm 1: Multi-Perspective Fraud Detection for B2C E-Commerce

Input:

- Event Logs $E = \{e1, e2, \dots, en\}$
- User Metadata $U = \{u1, u2, \dots, um\}$
- Trained SVM Model M
- Threshold T for anomaly score

Output:

- Fraudulent Users List F

Step 1: Initialization

$F \leftarrow \emptyset$ // List of detected fraudulent users

Step 2: Preprocessing and Behavior Monitoring

For each user $u \in U$ do

Extract behavior patterns $B(u)$ from Event Logs s
 Normalize timestamps, actions, device IDs, payment methods, etc.
 Build User Profile $P(u) = \{\text{login patterns, purchase frequency, IP, device, etc.}\}$

Step 3: Process Modeling

For each user action sequence $A(u)$ do
 Construct Process Flow $PF(u)$ from activities and timestamps
 Detect deviations from standard workflow using process mining techniques
 Compute Anomaly Score $S_{\text{anomaly}}(u)$ based on deviation and frequency

Step 4: Feature Extraction

For each user $u \in U$ do
 Extract Feature Vector

$FV(u)$

$= \{\text{time on page, scroll depth, payment type, delivery deviation, review score changes, etc.}\}$

Append anomaly score $S_{\text{anomaly}}(u)$ to $FV(u)$

Step 5: Classification

For each $FV(u)$ do
 Predict class $c \leftarrow M.\text{predict}(FV(u))$ // 0: Legitimate, 1: Fraud
 If $c = 1$ or $S_{\text{anomaly}}(u) > T$ then

s // Add to fraudulent list

Step 6: Post-processing

Generate alerts or restrict transactions for users in F
 Log flagged user profiles and activities for further auditing

Return:

List F containing detected fraudulent users

5.Simulation Results

To evaluate the effectiveness and robustness of the proposed fraud detection model for B2C e-commerce transactions, a series of simulation experiments were conducted using real-world and synthetically generated datasets. The primary objective was to assess the system's ability to accurately identify fraudulent behavior by analyzing dynamic user activities across various transaction stages. The simulation environment was designed to replicate real e-commerce interactions, capturing diverse features such as user login patterns, purchasing frequency, payment anomalies, and process deviations. Multiple performance metrics were used, including accuracy, precision, recall, F1-score, and false positive rate, to provide a comprehensive assessment of the model's detection capabilities. Comparisons were also made with baseline models, including traditional machine learning classifiers without process mining integration, to demonstrate the added value of multi-perspective behavioral analysis. The simulation results validate that the proposed approach significantly outperforms existing models in terms of detection accuracy, adaptability to behavior changes, and minimizing false alarms, thereby enhancing the overall security and reliability of e-commerce platforms.

A Multi perspective Fraud Detection Method for Multi Participant Ecommerce Transactions

**Figure 1: Home Page**

In Figure 1 presents the Home Page interface of the fraud detection system, which serves as the main entry point for users. This page is responsible for authenticating users by validating their username and password credentials against the records stored in the system's database. If the provided credentials are found to be correct, the user is granted access and redirected to the main operational page of the application. This process ensures that only authorized users can proceed further, enhancing the overall security of the system. The user interface is designed to be intuitive and secure, enabling a seamless and efficient login experience. Figure 2 shows the Virtual User Login Page, specifically tailored for virtual or simulated users who are part of the system's testing and evaluation phase. This interface mimics real-world login scenarios for users interacting with the e-commerce platform. It allows researchers and system administrators to monitor the login behavior of virtual participants, enabling the testing of authentication mechanisms, user behavior modeling, and fraud detection logic under controlled conditions. The inclusion of a separate virtual user login interface plays a crucial role in validating the robustness and adaptability of the proposed fraud detection framework.

Fraud detection; Electronic transaction; Petri net; Machine learning.

**Figure 2: Virtual User Login Page**

Fraud detection; Electronic transaction; Petri net; Machine learning.

REGISTER NOW!

REGISTER YOUR DETAILS HERE !!!

Enter Username	User Name	Enter Password	Password
Enter Email id	Enter Email	Enter Address	Enter Address
Enter Gender	Select Gender	Enter Mobile Number	Enter Mobile Number
Enter Country Name	Enter Country Name	Enter State Name	Enter State Name
Enter City Name	Enter City Name		

REGISTER

Registered Status :-

Figure 3: Registration Page**Figure 4: Service Agent Login Page**

User Name	Email	Gender	Address	Mobile No.	Country	State	City
Harish	Harish123@gmail.com	Male	#9928,4th Cross,Rajajinagar	9535866270	India	Karnataka	Bangalore
Manjunath	tmksmanju13@gmail.com	Male	#9928,4th Cross,Rajajinagar	9535866270	India	Karnataka	Bangalore
tmksmanju	tmksmanju13@gmail.com	Male	#9029,14th Cross,Malleswaram	9535866270	India	Karnataka	Bangalore
Hartharan	Hartharan123@gmail.com	Male	#9928,4th Cross,Rajajinagar	9535866270	India	Karnataka	Bangalore
Gopinath	Gopinath123@gmail.com	Male	#9928,4th Cross,Malleswaram	9535866270	India	Karnataka	Bangalore

Figure 5: Browse and Train & Test Data Sets

In Figure 3 illustrates the Registration Page, where new users can create an account within the e-commerce fraud detection system. This interface collects essential information such as the user's name, email, desired username, and secure password. Once submitted, the system validates and stores the details in a secure database, enabling future authentication. This registration process plays a vital role in ensuring traceability and accountability of user activities across the platform, which is crucial for tracking suspicious behavior and preventing unauthorized access. The design ensures ease of use while maintaining data integrity and privacy. Figure 4 shows the Service Agent Login Page, which provides a dedicated portal for service agents or administrators to access the backend functionalities of the fraud detection system. Unlike general users, service agents have elevated privileges that allow them to monitor user activities, manage datasets, review alerts, and intervene in suspected fraudulent cases. The login interface ensures that only authenticated personnel can access sensitive operational features, safeguarding the platform from internal and external threats. This component is critical for maintaining real-time oversight and quick response capabilities. Figure 5 presents the interface for Browsing and Training & Testing Datasets, a core function for machine learning-based fraud detection. This page enables the selection and uploading of structured datasets, which are then used for training the detection models and testing their performance. Users can browse local directories, select relevant datasets, and initiate preprocessing steps. The system then feeds this data into the learning pipeline, allowing it to learn behavioral patterns and detect anomalies. This feature provides flexibility in model experimentation, supports dynamic learning, and contributes directly to the accuracy and adaptability of the fraud detection framework.

Order_ID	PDate	Status	Puffment	Sales_Channel	ship_service_label	Style	SKU	Category	PSize	ASIN	Qty
203.205.150.02-10.42.0.151-90-37705-6	04-30-22	Shipped		Amazon	Amazon.in	Expedited	JNE3405-KR-KL	kurta	XL	B081WTG0G7	1
10.42.0.151-76.13.28.196-53343-443-6	04-30-22	Shipped - Delivered to Buyer	Merchant	Amazon.in		Standard	J0011-LGB-M	Set	M	B0883YU0G5	1

Figure 6: View Prediction of Fraud Status in Ecommerce Transaction

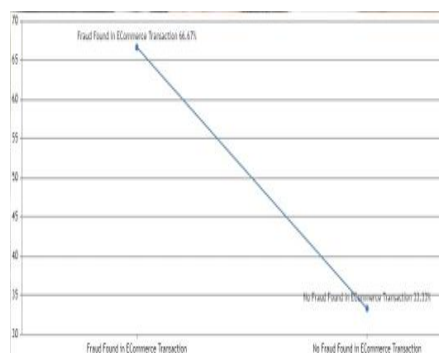


Figure 7: View Ecommerce Transaction Fraud Status Ratio Result

USER NAME	EMAIL	Gender	Address	Mob No	Country	State	City
Harish	Harish123@gmail.com	Male	#8928,4th Cross,Rajajinagar	9535866270	India	Karnataka	Bangalore
Manjunath	tmksmanju13@gmail.com	Male	#8928,4th Cross,Rajajinagar	9535866270	India	Karnataka	Bangalore
tmksmanju	tmksmanju13@gmail.com	Male	#9029,14th Cross,Malleswaram	9535866270	India	Karnataka	Bangalore
Hartharan	Hartharan123@gmail.com	Male	#8928,4th Cross,rajajinagar	9535866270	India	Karnataka	Bangalore
Gopinath	Gopinath123@gmail.com	Male	#8928,4th Cross,Malleswaram	9535866270	India	Karnataka	Bangalore

Figure 8: View All Remote Users

In Figure 6 displays the View Prediction of Fraud Status in E-commerce Transaction interface, which shows the outcome of the machine learning model's analysis on user transactions. This page provides a clear indication of whether a particular transaction is classified as fraudulent or legitimate. The prediction results are derived based on user behavior patterns and features extracted from historical and real-time event logs. This functionality is vital for allowing administrators or service agents to quickly assess risk levels and make informed decisions about transaction approvals or interventions. It enhances the transparency and trustworthiness of the detection system by providing actionable insights. Figure 7 illustrates the View E-commerce Transaction Fraud Status Ratio Result, which visually represents the distribution of detected fraudulent and non-fraudulent transactions. This could be shown in the form of a pie chart, bar graph, or statistical table. The ratio results help stakeholders understand the effectiveness of the fraud detection system, evaluate model performance, and identify trends in user behavior. It offers a high-level overview of the system's classification outcomes, supporting deeper analysis and fine-tuning of the model based on actual fraud occurrences versus predicted ones. Figure 8 presents the View All Remote Users section, which lists all users who are accessing the platform remotely. This feature is particularly useful for administrative oversight and monitoring of distributed access points. It ensures that the system maintains awareness of who is interacting with it from different locations and under what credentials. By logging and displaying this information, the platform enhances accountability, user tracking, and the ability to identify potential internal threats or account misuse.

6.Conclusion

This research presents a comprehensive approach to fraud detection in B2C e-commerce transactions by integrating machine learning and process mining techniques. Traditional fraud detection methods often rely solely on static historical data, which limits their effectiveness in capturing dynamic fraudulent behavior. To address this limitation, the proposed model utilizes real-time user behavior monitoring, process model construction, feature extraction from event logs, and classification using Support Vector Machines (SVM). The simulation results demonstrate that the system can effectively distinguish between legitimate and fraudulent transactions, offering a robust and adaptive solution to the evolving challenges of online fraud. Additionally, the implementation of a user-friendly interface facilitates remote user access, prediction visualization, and transaction monitoring, which enhances administrative control and operational efficiency. Overall, the proposed system contributes to advancing the security

framework in e-commerce by offering a multi-perspective, behavior-aware fraud detection strategy that is both scalable and reliable.

Acknowledgement: Not Applicable.

Funding Statement: The author(s) received no specific funding for this study.

Conflicts of Interest: The authors declare no conflicts of interest to report regarding the present study.

References

- [1] W. Yu, Y. Wang, L. Liu, Y. An, B. Yuan and J. Panneerselvam, "A multiperspective fraud detection method for multiparticipant e-commerce transactions," *IEEE Transactions on Computational Social Systems*, vol.11, no.2, pp.1564-1576, 2023.
- [2] G. R. Kumar and N. Umadevi, "A Multi-Perspective Fraud Detection Method for Multi-Participant E-Commerce Transactions," *International Journal of Mechanical Engineering Research and Technology*, vol.16, no.2, pp.350-364, 2024.
- [3] A. Mutemi and F. Bacao, "E-commerce fraud detection based on machine learning techniques: Systematic literature review," *Big Data Mining and Analytics*, vol.7, no.2, pp.419-444, 2024.
- [4] Pratap Rajkumar Lalwani and Varsha S. Sukhadeve, "Impact of Technology 4.0 on Quality Service, Customer Satisfaction Pertaining to E-Commerce Platforms," *International Journal of Advance Research and Innovation*, vol.12, no.1, pp.1-6, 2024.
- [5] R. DelshiHowsalya Devi, S. Prab and N. Legapriyadharshini, "Sentimental Analysis for the Improved User Experience in the E-Commerce Platform with the Fuzzy Model," *Journal of Computer Allied Intelligence*, vol.2, no.3, pp.28-40, 2024.
- [6] Y. Durachman and A. W. B. A. Rahman, "Predicting Fraud Cases in E-Commerce Transactions Using Random Forest Regression: A Data Mining Approach for Enhancing Cybersecurity and Transaction Integrity," *Journal of Cyber Law*, vol.1, no.2, pp.116-130, 2025.
- [7] P. Hemalatha, "Secure Deep Learning Architecture Model for Data Management and Scheduling of E-Commerce Data," *Journal of Sensors, IoT & Health Sciences*, vol.2, no.2, pp.16-29, 2024.
- [8] S. Sabah Mamand, "Data Mining for Fraud Detection," In *5th International Conference on Communication Engineering and Computer Science (CIC-COCOS'24)*, Cihan University-Erbil, pp.233-239, 2024.
- [9] A. Narayan, S. M. Kumar and A. M. Chacko, "in E-Commerce Using Machine Learning," In *Intelligent Data Engineering and Analytics: Proceedings of the 10th International Conference on Frontiers in Intelligent Computing: Theory and Applications (FICTA 2022)*, Springer Nature, vol.327, pp.237, 2023.
- [10] A. Paul and V. Paul, "Poor and rich squirrel algorithm-based Deep Maxout network for credit card fraud detection," *International Journal of Wireless and Mobile Computing*, vol.28, no.2, pp.123-134, 2025.
- [11] M. Seera, C. P. Lim, A. Kumar, L. Dhamotharan and K. H. Tan, "An intelligent payment card fraud detection system," *Annals of operations research*, vol.334, no.1, pp.445-467, 2024.
- [12] N. Baisholan, J. E. Dietz, S. Gnatyuk, M. Turdalyuly, E. T. Matson and K. Baisholanova, "FraudX AI: An Interpretable Machine Learning Framework for Credit Card Fraud Detection on Imbalanced Datasets," *Computers*, vol.14, no.4, pp.120, 2025.
- [13] K. Yan, J. Gao and D. Matsypura, "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)*, IEEE, pp.1-10, 2023.
- [14] O. S. Adebayo, T. A. Favour-Bethy, O. Otasowie and O. A. Okunola, "Comparative review of credit card fraud detection using machine learning and concept drift techniques," *International Journal of Computer Science and Mobile Computing*, vol.12, no.7, pp.24-48, 2023.
- [15] Y. Cheng, J. Guo, S. Long, Y. Wu, M. Sun and R. Zhang, "Advanced financial fraud detection using

-
- GNN-CL model,” In *2024 International Conference on Computers, Information Processing and Advanced Education (CIPAE)*, IEEE, pp.453-460, 2024.
- [16] V. Chinnaiyah, V. Veerabhadram, R. Aavula and S. Aluvala, “PMiner: Process mining using deep autoencoder for anomaly detection and reconstruction of business processes,” *International journal of electrical and computer engineering systems*, vol.15, no.6, pp.531-542, 2024.
- [17] J. Karthika and A. Senthilselvi, “Smart credit card fraud detection system based on dilated convolutional neural network with sampling technique,” *Multimedia Tools and Applications*, vol.82, no.20, pp.31691-31708, 2023.
- [18] S. Bakhtiari, Z. Nasiri and J. Vahidi, “Credit card fraud detection using ensemble data mining methods,” *Multimedia Tools and Applications*, vol.82, no.19, pp.29057-29075, 2023.
- [19] A. A. Almazroi and N. Ayub, “Online payment fraud detection model using machine learning techniques,” *Ieee Access*, vol.11, pp.137188-137203, 2023.
- [20] L. Vetrivendan and T. G. Kumar, “Exploring Techniques to Safeguard Credit Card Transactions: A Comprehensive Study on Fraud Detection and Prevention,” In *International Conference on Data Engineering and Machine Intelligence*, Singapore: Springer Nature Singapore, pp.129-143, 2023.
- [21] P. Tiwari, S. Mittal and D. Upadhyay, “A Comparative Analysis of Credit Card Fraud Detection Machine Learning Algorithms,” In *2024 2nd International Conference on Device Intelligence, Computing and Communication Technologies (DICCT)*, IEEE, pp.1-5, 2024.
- [22] X. Yang, C. Zhang, Y. Sun, K. Pang, L. Jing, S. Wa and C. Lv, “FinChain-BERT: A high-accuracy automatic fraud detection model based on NLP methods for financial scenarios,” *Information*, vol.14, no.9, pp.499, 2023.
- [23] L. Mahya, T. Tarjo, Z. M. Sanusi and F. A. Kurniawan, “Intelligent Automation of Fraud Detection and Investigation: A Bibliometric Analysis Approach,” *JurnalReviuAkuntansi dan Keuangan*, vol.13, no.3, pp.588-613, 2023.
- [24] E. Stachura, “Cloud-Based Banking Fraud Detection Using Recurrent Neural Networks and Feature Extraction,” *International Journal of Management Research and Business Strategy*, vol.15, no.1, pp.8-23, 2025.
- [25] K. Ouazzane, C. Ikeda, R. Djemai, A. Phipps and Y. Maleh, “A novel feature engineering framework for cyber fraud detection using machine learning and deep learning algorithms,” *Information Security Journal: A Global Perspective*, pp.1-21, 2025.
-