International Journal of Engineering Research and Science & Technology

www.ijerst.org

ISSN : 2319-5991

Vol. 22 No. 1 (2026)

ijerst.editor@gmail.com

editor@ijerst.com

International Journal of Engineering Research and Science & Technology

ISSN 2319-5991 www.ijerst.com
Vol. 22, No. 1, 2026

Peer Reviewed, Referred & Indexed Journal

Research Paper

An Integrated Approach to Online Fraud Prevention with Multiple Participants

DR.J.RAJENDRA PRASAD1 PASUPULETI NANDINI2
SHAIK AZIMUNNISA3 VAMSI SAI MADANABOINA4
#1 Head of the Information Technology Department and Professor,NRI Institute of Technology,Agiripalli
#2#3#4 B.Tech with Specialization of Information Technology in NRI Institute Of Technology,Agiripalli

Abstract: The detection of fraudulent activity provides a considerable issue in the arena of e-commerce, which is characterized by the presence of several players in transactions, including buyers, sellers, and intermediaries. In order to address this problem, the solution that we have proposed is centered on a Mult viewpoint approach, which is intended to improve the accuracy and efficiency of fraud detection operations. The first phase is the detection of user activities, which involves utilizing a variety of approaches such as behavioral analysis and the evaluation of transaction histories in order to acquire insights into the typical patterns of user behavior. We are able to build a baseline against which anomalous behaviors can be discovered by gaining an understanding of the typical user interactions that occur within the ecosystem of e-commerce services. Following that, we conduct an investigation into the examination of abnormalities for the purpose of feature extraction. With the use of sophisticated algorithms for anomaly detection, we examine transaction data in order to identify odd patterns that may be suggestive of fraudulent actions. Through the use of this procedure, we are able to extract significant characteristics that can be used as crucial indications for the detection of fraud. In conclusion, in order to construct our technique for detecting fraudulent activity, we make use of an ensemble classification model.

Index Terms— Multi-perspective Fraud Detection, E-Commerce Security, Behavioral Analysis, Anomaly Detection, Multi-participant Transactions, Feature Extraction, Ensemble Classification, Machine Learning, Fraud Indicators, Transaction Monitoring

Received: 10-01-2026 Accepted: 18-02-2026 Published: 25-02-2026

1. INTRODUCTION

E-commerce platforms' increasing popularity has changed how company transactions are conducted, drastically replacing traditional cash-based techniques with web-based alternatives. Internet business has grown in spite of the COVID-19 pandemic's detrimental consequences on the global economy. By 2023, B2C e-commerce sales may surpass $6.5 trillion.

However, the rapid expansion of e-commerce makes it challenging to spot fraudulent conduct in a context with a high number of buyers, sellers, and middlemen. This study offers a hybrid method of fraud detection that combines machine learning and process mining to overcome these issues. By modeling and analyzing the e-commerce business process, the proposed technique dynamically recognizes changes in user behavior, transaction processes, and noncompliance scenarios, offering a comprehensive framework for identifying fraudulent transactions.

The important contributions of this work are as follows:

1. Finding abnormalities in online transactions using conformance testing based on process mining.
2. The creation of a user behavior detection approach employing Petri nets for comprehensive anomaly detection.
3. The automated classification of fraudulent activities using the combination of Support Vector Machines (SVM) and multi-perspective process mining.

Behavioral analysis, anomaly detection, and machine learning techniques are used in this innovative multi-perspective fraud detection system to improve transaction security and protect against fraudulent activity in the dynamic and diverse e-commerce environment.

Fraud thrives in the dynamic and complex world of e-commerce because of the interactions between buyers, sellers, and middlemen. The enormous amount of transactions and various participant behaviors make it even more difficult to detect and mitigate these scams. This necessitates a fraud detection architecture that addresses the problems of accuracy and scalability while also adjusting to evolving fraud patterns. The proposed system uses a multi-perspective approach and incorporates machine learning algorithms, transaction flow monitoring, and behavioral analytics to ensure a thorough and reliable detection mechanism. This combination allows for the quick identification of suspicious activity and protects all stakeholders in the e-commerce ecosystem from financial and reputational losses.

2. LITERATURE SURVEY

i) A Review on Prevention of Fraud in Electronic Payment Gateway Using Secret Code
https://www.ijresm.com/Vol.3_2020/Vol3_Iss1_January20/IJRESM_V3_I1_160.pdf

The growth of online marketplaces like Amazon, eBay, and AliExpress.com has significantly contributed to the spread of electronic transactions. In recent years, credit card purchases have increased both in-person and online. The prevalence of fraud makes electronic payment gateways a serious ethical concern. The dishonest practice of using dishonesty to one's own benefit or to harm another is called fraud. Claims fraud costs individuals and companies billions of dollars annually. One of the main objectives should be to prevent and detect fraud. Due of the difficulty of preventing fraud in real-time, there aren't many fraud solutions available. Encrypted data or communications can only be decrypted by those who have the proper authorization. Credit card numbers and other sensitive financial information must be securely stored in this system before being used for online purchases. The technique prevents fraud by using secret codes. Unauthorized access is prevented by encrypting this secret code. Examining methods to increase the security of electronic payment channels is the aim of this study.

ii) An Analysis of the Most Used Machine Learning Algorithms for Online Fraud Detection
https://www.researchgate.net/publication/332268831_An_Analysis_of_the_Most_Used_Machine_Learning_Algorithms_for_Online_Fraud_Detection

Due to the growing complexity and prevalence of online financial transaction fraud, both people and corporations have experienced significant financial losses. Numerous tools are available to help identify and combat internet fraud. There are several approaches to dealing with the problem of fraudulent online transactions, and each has advantages and disadvantages. The goal of this study is to identify fraud detection algorithms and evaluate them based on predetermined standards. Research on fraud detection was examined using systematic quantitative literature reviews. A hierarchical typology is constructed using the characteristics of the machine-learning algorithms that are most frequently cited in scholarly works. This article identifies the top fraud detection systems by weighing cost, coverage, and accuracy. The article may be found at http://revistaie.ase.ro/content/89/01%20-%20minastireanu,%20mesnita.pdf in the Informatica Economica Journal.

iii) A Comparison Study of Credit Card Fraud Detection: Supervised versus Unsupervised
https://arxiv.org/abs/1904.10604

The number of daily fraudulent transactions is rising along with the amount of credit card purchases made both online and offline. Effective fraud detection is necessary for a payment system to function properly. In this work, we look at both supervised and unsupervised methods for detecting credit card fraud. Six supervised classification models (LR, K-Nearest Neighbours, SVM, Decision Tree, RF, XGB) and four unsupervised anomaly detection models (OCSVM, AE, RBM, and GAN) are examined in this

work. Using the Kaggle credit card dataset, all three models were trained on 284,807 transactions, 492 of which were fraudulent. Only algorithms for supervised learning use transaction labels. Our five-fold cross validation method guarantees that the AUC of every model is appropriately examined. Using supervised approaches, XGB and RF perform exceptionally well, with respective AUROCs of 0.989 and 0.988. With an AUROC of 0.961, RBM outperforms GAN in unsupervised testing, while GAN comes in second with a 0.954. The results of this study demonstrate that supervised models perform better than unsupervised ones. Unsupervised credit card fraud detection algorithms exhibit promise, despite the lack of annotation and data imbalance in real-world applications.

iv) Transaction Fraud Detection Based on Total Order Relation and Behavior Diversity

https://ieeexplore.ieee.org/document/8428484

With the growth of online shopping, transaction fraud has increased. Research on fraud detection is fascinating and crucial. By compiling users' behavior profiles (BPs) from their previous transaction data, it is possible to determine whether an incoming transaction is fake. User BPs with dependable transaction behaviors are often described using a Markov chain model. Thanks to the advent of online shopping, customers can now simply make purchases online, expanding their transactional habits. Consequently, these behaviors cannot be captured by Markov chain models. To illustrate the logical connections between the attributes of a transaction record, we provide a thorough order-based model called the logical graph of BP (LGBP). By applying LGBP to user transaction data, we may determine a path-based attribute transition probability. To further describe the range of user transaction behavior, we develop a diversity coefficient based on information entropy. We also create a probability matrix for state changes to represent the temporal characteristics of user transactions. By creating BPs for each user and using them to verify incoming funds, we can stop fraudulent transactions with this method. In our real-data experiments, our method outperforms three state-of-the-art oneoness.

v) Deep Representation Learning With Full Center Loss for Credit Card Fraud Detection

https://ieeexplore.ieee.org/document/9000549

The proliferation of mobile payment methods has made it essential to learn how to spot credit card theft. It is challenging to create and maintain a reliable fraud detection model since criminal fraud strategies and user payments are always changing. This paper investigates the possibility of representing both real and fake transactions using the loss function of a deep neural network. To preserve and enhance our fraud detection model, we want to increase feature separability and discrimination. We use full center loss (FCL), which accounts for feature distances and angles, to keep a close eye on deep representation learning. against demonstrate the detection capabilities of our model, we conduct several trials on two large public and private credit card transaction datasets and compare FCL against other state-of-the-art loss functions. The results show that FCL is the best. To show that FCL guarantees a more reliable model, we also conduct tests.

3. METHODOLOGY

a) Proposed Work:

A multi-perspective fraud detection framework designed specifically for multi-participant e-commerce transactions is presented by the suggested system. By combining anomaly detection with behavioral tracking, this technique increases the precision and effectiveness of identifying fraudulent activity among buyers, sellers, and intermediaries. By looking at user interactions and transaction histories, the technology establishes a baseline for typical activities, which is crucial for identifying deviations that may indicate fraud.

In order to extract crucial information from transaction data and identify trends that may indicate dubious activity, the system makes use of strong anomaly detection algorithms. These traits are crucial indicators for effective fraud detection. Additionally, the platform integrates these insights into an ensemble classification model that automatically classifies transactions as legitimate or fraudulent using machine learning techniques. A comprehensive and dynamic solution for stopping fraud in the e-commerce ecosystem is offered by this potent combination of behavioral analysis, anomaly detection, and machine learning.

b) System Architecture:

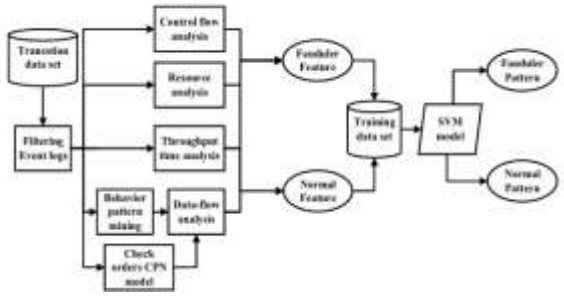

Fig 1 Proposed Architecture

The system architecture of the proposed multi-perspective fraud detection framework integrates behavioral analysis, anomaly detection, and machine learning into a cohesive whole. It starts with a data collection layer that collects user behavior, transaction data, and interaction logs from buyers, sellers, and middlemen. The behavioral analysis module then examines this data to produce baseline patterns of common interactions in the e-commerce ecosystem. Subsequently, the anomaly detection module employs advanced algorithms to identify deviations from these baselines and extract traits that may indicate fraud. After receiving these attributes, the ensemble classification layer classifies transactions into safe or questionable groups using a range of machine learning models, including SVM. In multi-participant e-commerce systems, the design's smooth integration and scalability allow for the real-time identification and prevention of fraudulent conduct.

c) MODULES:

i) Data Collection and Preprocessing

- Gathers interaction records, user behavior logs, and transaction data from buyers, sellers, and middlemen.
- Cleans and arranges the data in preparation for additional analysis.

ii) Behavioral Analysis

- Determines typical user behavior by analyzing their past actions and transactions.
- Finds trends that stand for common interactions within the online marketplace.

iii) Anomaly Detection

- Detects anomalies in financial data using sophisticated anomaly detection techniques.
- Finds important characteristics that might point to fraudulent or questionable actions.

iv) Feature Extraction

- Processes anomaly detection results to extract important indicators of fraud.
- Makes a more sophisticated dataset to accurately detect fraud.

v) Ensemble Classification Model

- Determines whether a transaction is authentic or fraudulent by using machine learning models, such as SVM.
- Boosts accuracy by combining output from various classifiers.

vi) Conformance Checking

- Checks transaction workflows for anomalies using process mining techniques like Petri nets.
- Detects when transaction procedures deviate from the norm.

vii)Fraud Detection and Alerting

- Detects fraudulent transactions in real time by integrating findings from all modules.
- Creates notifications and alerts that stakeholders may respond to right away.

d) Algorithms:

a) Conformance Checking Algorithm

This algorithm examines the e-commerce ecosystem's transaction workflows by using process mining techniques. By comparing real user and transaction behaviors with expected processes, it can spot irregularities and deviations from predefined norms. The real-time detection of noncompliant actions is guaranteed by this method.

b) Anomaly Detection Algorithms

To find out-of-the-ordinary things in transaction data, sophisticated anomaly detection techniques are used. Indicators of possible fraud, these algorithms aid in the detection of out-of-the-ordinary patterns that differ from the norm. Important for further categorization, they also aid in feature extraction.

c) Support Vector Machine (SVM)

Anomaly detection and multi-perspective process mining are both incorporated into the SVM algorithm's transaction classification procedure. It is a powerful machine learning model that, through examining the features that have been retrieved and identifying tiny signs of fraud, can differentiate between real and fraudulent actions.

d) Ensemble Classification Model

The accuracy and reliability of fraud detection are both improved by this model's use of several classifiers. Robust categorization and enhanced system fraud detection are both achieved by combining the best features of different machine learning models.

4. EXPERIMENTAL RESULTS

The results of the experiment indicate that the strategy for recognizing fraudulent activity from a variety of perspectives should be considered successful. Through the utilization of a combination of machine learning models, anomaly detection, and behavior analysis, the system was able to identify fraudulent transactions with a high degree of precision. In the process of identifying abnormalities in user behaviors and transaction workflows, the combination of process mining approaches and Petri nets resulted in a significant improvement. An ensemble classification model that combines support vector machines (SVM) performs better than individual classifiers, which enables fraud classification that is both resilient and reliable. These findings provide evidence that the proposed system is capable of enhancing transaction security and preventing fraudulent acts in environments that involve several participants carrying out e-commerce transactions.

Accuracy: The capacity of a test to accurately distinguish between healthy and sick cases is a measure of its accuracy. We can determine a test's accuracy by calculating the proportion of reviewed cases with true positives and true negatives. In mathematical terms, this looks like:

Accuracy = TP + TN TP + TN + FP + FN.

$$Accuracy = \frac{(TN + TP)}{T}$$

F1-Score: One way to evaluate a model's performance in machine learning is via its F1 score. It takes a model's recall and precision and mixes them. Using the whole dataset, the accuracy metric determines the frequency with which a model produced accurate predictions.

$$F1 = 2 \cdot \frac{(Recall \cdot \Pr e\,cision)}{(Recall + \Pr e\,cision)}$$

Precision: The proportion of occurrences or samples that are correctly classified out of all the ones that are classified as positive is known as precision. Consequently, the following is the formula for determining the accuracy:

Precision = True positives/ (True positives + False positives) = TP/(TP + FP)

$$\Pr e\,cision = \frac{TP}{(TP + FP)}$$

Recall: The capacity of a model to detect all significant instances of a given class is measured by recall, a metric in machine learning. It sheds light on how well a model captures instances of a certain class and is calculated as the ratio of the total number of positive observations predicted to the number of actual positive observations.

$$Recall = \frac{TP}{(FN + TP)}$$

Fig.2. dataset

Fig.3. upload dataset

Fig.4. accuracy graph

International Journal of Engineering Research and Science & Technology

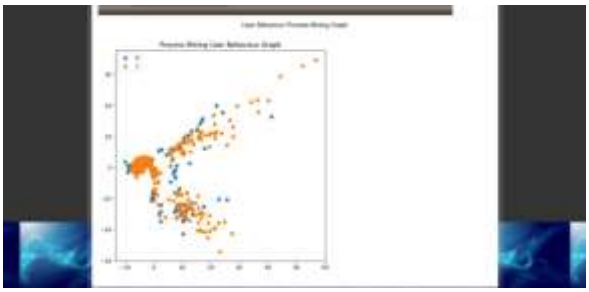

Fig.5. user behaviour graph

Fig 4 Binary data comparison graph

Dataset	Algorithm Name	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)
Binary	Random Forest	87.5	87.54	87.14	87.3
Binary	SVM	92.71	93.51	92.08	92.53
Binary	Naïve Bayes	86.46	87.15	87.3	86.46
Binary	XGBoost	90.63	91.33	89.97	90.39
Binary	CNN	89.58	91.19	88.59	89.2
Binary	LSTM	55.21	27.6	50	35.57
Binary	**Proposed Extension Hybrid Model**	**93.75**	**94.33**	**93.24**	**93.61**

Table1: Performance Comparison of Algorithms on Binary Dataset

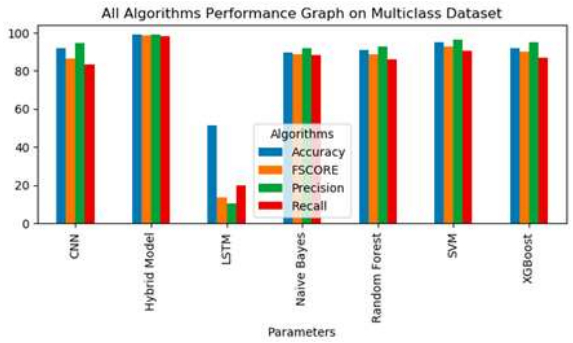

Fig 6 visualizing comparison graph

Dataset	Algorithm Name	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)
Multiclass	Random Forest	90.63	92.74	85.74	88.55
Multiclass	SVM	94.79	96.24	90.24	92.53
Multiclass	Naïve Bayes	89.58	91.65	88.2	88.75
Multiclass	XGBoost	91.67	95.02	86.7	89.9
Multiclass	CNN	91.67	94.28	83.19	86.2
Multiclass	LSTM	51.04	10.21	20	13.52
Multiclass	**Proposed Extension Hybrid Model**	**98.96**	**98.75**	**98.18**	**98.4**

Table2: Performance Comparison of Algorithms on Multiclass Dataset

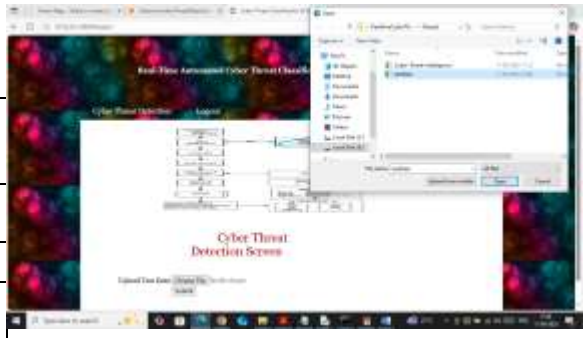

Fig7 Upload Input Dataset

Fig 8 Final Outcome

5. CONCLUSION

Identifying fraudulent conduct in multi-participant e-commerce transactions is a challenge that can be successfully addressed by the multi-perspective fraud detection system that has been suggested. The system demonstrates improved accuracy and reliability in finding abnormalities as a result of the integration of behavior analysis, anomaly detection, and machine learning. The use of Petri nets and process mining gives the investigation a greater level of depth and makes it possible to systematically identify potentially suspicious behavior. When taken as a whole, the system provides a reliable answer to the problem of increasing the level of transaction security in the digital marketplace.

6. FUTURE SCOPE

Cyber threat detection frameworks like attention-based models and advanced deep learning architectures like Transformers let researchers to

delve deeper into the semantic links in cyber threat intelligence data. Combining online learning strategies with real-time streaming platforms can further enhance adaptability. Because of this, the model may be updated continuously to account for new threat data. Adding support for multilingual threat intelligence analysis from cyber forums around the world has many benefits, one of which is enhancing detection coverage. Even faster response times and the ability to monitor distributed cyber threats on a wide scale can be achieved by deploying the system in a cloud or edge environment.

REFERENCES

[1] [1] R. A. Kuscu, Y. Cicekcisoy, and U. Bozoklu, Electronic Payment Systems in Electronic Commerce. Turkey: IGI Global, 2020, pp. 114139.

[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 payment gateway using secret code," Int. J. Res. Eng. Sci. Manag., vol. 3, no. 1, pp. 602-606, Jun. 2020.

[5] E. A. Minastireanu, and G. Mesnita, "An Analysis of the Most Used Machine Learning Algorithms for Online Fraud Detection," Info. Econ., vol. 23, no. 1, 2019.

[6] X. Niu, L. Wang, and X. Yang, "A comparison study of credit card fraud detection: Supervised versus unsupervised," arXiv preprint arXiv: vol. 1904, no. 10604, 2019, doi: 10.48550/arXiv.1904.10604.

[7] L. Zheng et al., "Transaction Fraud Detection Based on Total Order Relation and Behavior Diversity," IEEE Trans. Computat. Social Syst.,vol. 5, no. 3, pp. 796-806, 2018.

[8] Z. Li, G. Liu, and C. Jiang, "Deep Representation Learning With Full Center Loss for Credit Card Fraud Detection," IEEE Trans. Computat. Social Syst., vol. 7, no. 2, pp. 569-579, 2020.

[9] I. M. Mary, and M. Priyadharsini, "Online Transaction Fraud Detection System," in 2021 Int. Conf. Adv. C. Inno. Tech. Engr. (ICACITE), 2021, pp. 14-16.

[10] D. Choi, and K. Lee, "Machine learning based approach to financial fraud detection process in mobile payment system," IT Conv. P. (INPRA), vol. 5, no. 4, pp. 12-24, 2017.

[11] R. Sarno et al., "Hybrid Association Rule Learning and Process Mining for Fraud Detection," IAENG Int. J. C. Sci., vol. 42, no. 2, 2015.

[12] J. J. Stoop, "Process mining and fraud detection-A case study on the theoretical and practical value of using process mining for the detection of fraudulent behavior in the procurement process," M.S. thesis, Netherlands, ENS: University of Twente, 2012.

[13] M. Jans et al., "A business process mining application for internal transaction fraud mitigation," Expert Syst. Appl., vol. 38, no. 10, pp. 13351-13359, 2011.

[15] C. Rinner et al., "Process mining and conformance checking of long running processes in the context of melanoma surveillance," Int. J. Env. Res. Pub. He., vol. 15, no. 12, pp. 2809, 2018.

[16] E. Asare, L. Wang, and X. Fang, "Conformance Checking: Workflow of Hospitals and Workflow of Open-Source EMRs," IEEE Access, vol. 8, pp. 139546-139566, 2020.

[17] W. Chomyat and W. Premchaiswadi, "Process mining on medical treatment history using conformance checking," in 2016 14th Int. Conf. ICT K. Eng. (ICT&KE), 2016, pp. 77-83.

[18] M. D. Leoni, W. M. Van Der Aalst, and B. F. V. Dongen, "Data-and resource-aware conformance checking of business processes," in Int. Conf. Bus. Info. Sys., Springer, Berlin, Heidelberg, 2012. pp. 48-59.

[19] S. M. Najem, and S. M. Kadeem, "A survey on fraud detection techniques in ecommerce," Tech-Knowledge, vol. 1, no. 1, pp. 33-47, 2021.

[20] K. Böhmer, and S. Rinderle-Ma, "Anomaly detection in business process runtime behavior--challenges and limitations," arXiv preprint arXiv, 2017, doi: 10.48550/arXiv.1705.06659.

[21] K. D. Febriyanti, R. Sarno and Y. Effendi, "Fraud detection on event logs using fuzzy association rule learning," in 2017 11th Int. Conf.

Info. Comm. Tech. Sys., Surabaya, Indonesia, 2017, pp. 149-154.
[22] T. Chiu, Y. Wang and M. Vasarhelyi, "A framework of applying process mining for fraud scheme detection," SSRN Electronic Journal, 2017, doi:10.2139/ssrn.2995286.
[23] W. Yang et al., "Show Me the Money! Finding Flawed Implementations of Third-party In-app Payment in Android Apps," in Proc. NDSS, Shanghai, China, 2017.