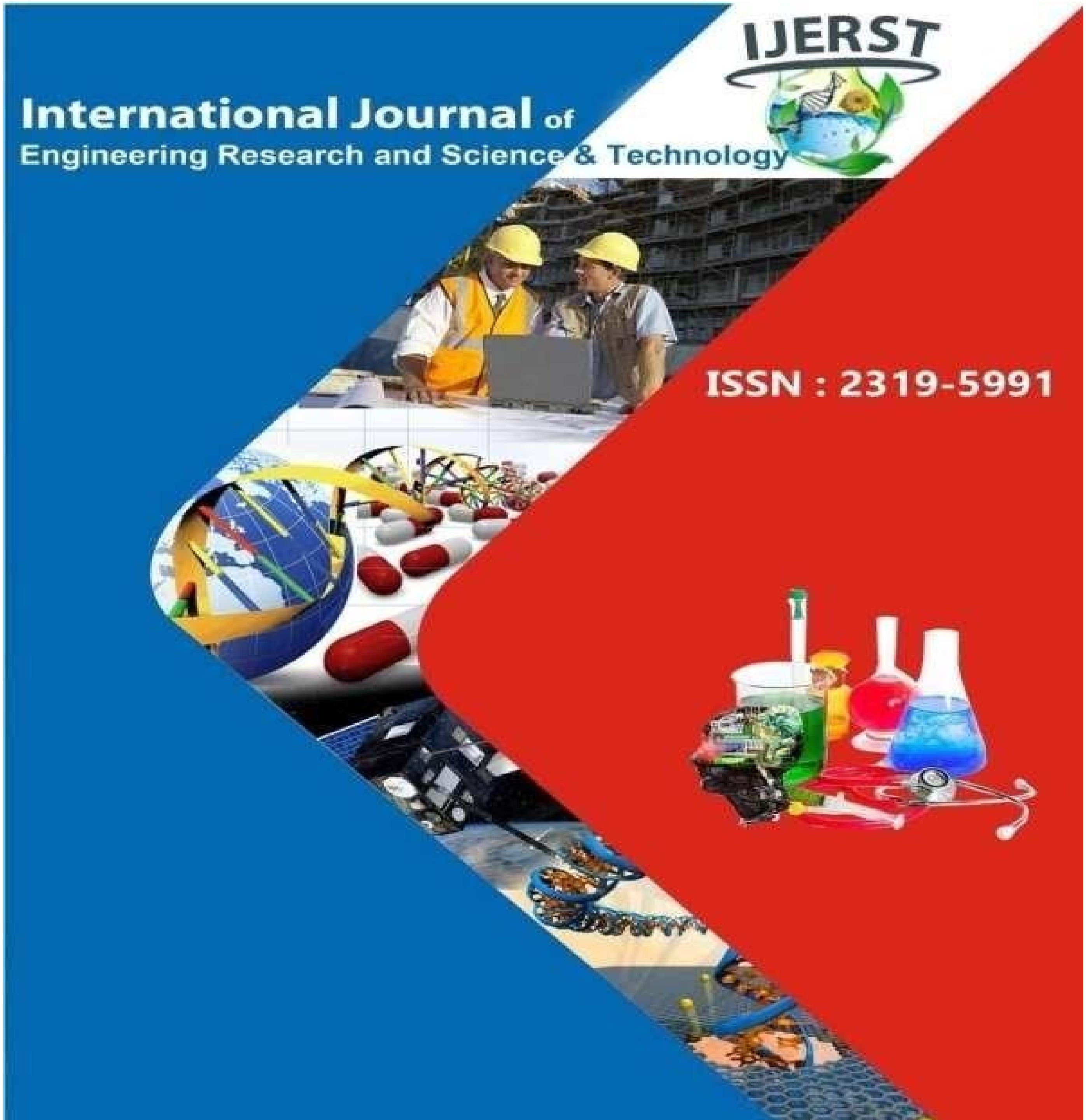
IJERST

International Journal of Engineering Research and Science & Technology



ISSN : 2319-5991

www.ijerst.com

Email: editor@ijerst.com or editor.ijerst@gmail.com

ISSN 2319-5991 www.ijerst.com
https://doi.org/10.62643/ijerst.2025.v21.i2.pp892-902
Vol. 21, Issue 2, 2025

ADAPTIVE FRAUD DETECTION IN MULTI-PARTICIPANT E-COMMERCE USING PROCESS MINING AND MACHINE LEARNING

[1]N. Swetha, MCA Student, Department of MCA
[2] CH Sri Lakshmi Prasanna, M.Tech, (Ph.D), Assistant Professor, Department of MCA
[12]Dr KV Subba Reddy Institute of Technology, Dupadu, Kurnool

ABSTRACT

Transaction security solutions have traditionally focused on identifying and stopping fraudulent transactions in e-commerce platforms. However, it is difficult to apprehend attackers using just the historical order information since e-commerce is hidden. Numerous studies attempt to create technologies that stop fraud, however they haven't taken into account consumers' changing behaviours from various angles. As a result, fraudulent activities are detected inefficiently. In order to do this, this study suggests a unique approach to fraud detection that combines process mining and machine learning models to track user behaviour in real time. We start by creating a process model for the B2C e-commerce platform that includes user behaviour detection. Second, a technique is described for examining anomalies in order to extract significant characteristics from event logs. A classification model based on Support Vector Machines (SVM) that can identify fraudulent activity is then fed the derived characteristics. Through the studies, we show how well our approach captures dynamic fraudulent behaviours in e-commerce platforms.

I. INTRODUCTION

A growing number of business transactions are now using web-based methods rather to the conventional cash-based method due to the growing popularity of e-commerce platforms [1]. While the COVID-19 pandemic has had a significant influence on the entity economy in recent years, e-commerce has been relatively unscathed, contributing to its sustained market expansion [2]. By 2023, it is anticipated that business-to-consumer (B2C) e-commerce sales would total 6.5 trillion USD [3].

In recent years, new security dangers have surfaced, despite the fact that the spread of contemporary technology and the rise of e-commerce provide improved chances for online firms. According to reports, the substantial rise in internet fraud cases costs billions of dollars annually on a global scale [4]. Anti-fraud solutions are now essential to ensuring the security of online transactions due to the Internet's dynamic and dispersed character. When addressing new security threats, vulnerabilities are still identified by current fraud detection systems that concentrate on identifying unusual user behaviour. The ineffective process management of current fraud detection technologies throughout the trading process is a significant problem. One of the main problems that need attention is the ineffective monitoring function [5]. Because process capture is lacking in the current work, the detection viewpoint is often insufficient. In order to do this, we suggest a process-based approach in which historical data is converted into controlled data and user behaviours are captured and examined in real-time. Furthermore, we integrate a multi-perspective approach for identifying anomalous behaviours.

In order to address anomaly detection in data flows, this study introduces a hybrid approach that offers information on every action incorporated in a control flow model, combining the benefits of process mining and machine learning models. This approach can dynamically detect changes in user behaviours, transaction processes, and noncompliance issues by modelling and analysing the e-commerce system's business process. It can also thoroughly analyse and identify fraudulent transactions from a variety of angles. The following is a list of this paper's significant contributions:

1) To identify the anomalies in e-commerce transactions, a conformance checking technique based on process mining is used.

2) To carry out thorough anomaly detection based on Petri nets, a user behaviour detection technique is suggested.

3) To automatically categorise fraudulent behaviours, an SVM model is created by integrating multi-perspective process mining into machine learning techniques. This is how the remainder of the paper is structured: The relevant work is introduced in Section 2. A background research and model analysis are presented in Section 3. The theoretical underpinnings and description of our suggested fraud detection technique are provided in Section 4. Our experiments' findings are shown and discussed in Section 5, and our suggested fraud detection technique is validated in Section 6. Our study is concluded in Section 7, which also outlines our future research plans.

II. LITERATURE REVIEW

"The effect of COVID-19 spread on the e-commerce market: The case of the 5 largest e-commerce companies in the world" ,

A. Elsayed and M. A. Elrhim,

In order to examine the impact of the COVID-19 pandemic on international e-commerce businesses, the top five global e-commerce businesses were selected based on their market value and revenue. These were as follows: German Zalando, Chinese Alibaba, Japanese Rakuten, American Amazon, and UK ASOS have all been calculating the daily "cumulative infections" and "cumulative deaths" to determine the corona virus prevalence. In addition to being measured by the values of "new corona virus cases" and "new corona virus deaths" per day, the dependent variable shows how the global e-commerce market has responded to the effects of the corona virus's spread and is calculated by the daily returns of e-commerce companies' stock to the international financial markets. This was implemented every day between March 15, 2020, and May 25, 2020.

The findings of the descriptive analysis of the e-commerce firms' returns shown that by figuring out the average daily returns, the companies are able to generate positive daily returns. According to the Beta Standardised

ISSN 2319-5991 www.ijerst.com

https://doi.org/10.62643/ijerst.2025.v21.i2.pp892-902

Vol. 21, Issue 2, 2025

Coefficients test, the aggregate model's results show the most significant independent variables and their effects on the returns of shares of international electronic trading companies. The first rank of the model was influenced by the variable "total deaths," followed by the second rank by the variable "total cases," and the third rank by the variable "new cases."

Depending on the country to which it belonged, the percentage of the effect of coronavirus spread varied from company to company. For example, the German company Zalando was the most influential variable "cumulative deaths," while the Chinese companies Alibaba and Rakuten were the most influential in their share price returns, and the American company Amazon and the United Kingdom company ASOS were "the cumulative cases of infection are the most influential and this is consistent with that they are the most affected countries of the coronavirus during the period of research." "The e-commerce supply chain and environmental sustainability: An empirical investigation on the online retail sector"

J. Chanchaichujit, V. Shukla, S. Jabeen, N. Vihari, S. Balasubramanian, and P. Rao

Although e-commerce has grown significantly in recent years, particularly in the business-to-consumer (B2C) online retail sector, it is unclear from prior studies what the good and negative environmental effects of e-commerce are. Two conceptual models were first created from the literature to comprehend the effects of e-commerce on the environment. The suggested models, together with the appropriateness and relevance of each concept and its underlying items, were then tested using 303 answers gathered from the GCC nations using a structured questionnaire. The hypothesised correlations between the constructs were then evaluated. According to Model 1's results, consumers' positive and negative environmental views towards e-commerce are shaped by green consumerism, and this in turn affects their behavioural intention to utilise e-commerce channels. With the addition of perceived utility and ease of use components, positive environmental attitudes in Model 2 no longer predicted behavioural intention because consumers valued e-commerce's usefulness and ease of use above its good environmental aspects. It's interesting to note that behavioural intention was still impacted by unfavourable environmental attitudes even when perceived utility and simplicity of use were present. While working to reduce or eliminate e-commerce's negative environmental effects, the research offers practitioners and policymakers important insights for promoting and utilising the positive environmental advantages of e-commerce. The study's conclusions are innovative since it is perhaps the first empirical effort to comprehend the environmental benefits and drawbacks of e-commerce as well as how it affects consumers' intentions to use it.

"A review on prevention of fraud in electronic payment gateway using secret code"

K. K. Tighare, S. S. Dake, and S. D. Dhobe

ISSN 2319-5991 www.ijerst.com

https://doi.org/10.62643/ijerst.2025.v21.i2.pp892-902

Vol. 21, Issue 2, 2025

Due in large part to the popularity of electronic commerce, or e-commerce, and online shops like Amazon.com, eBay, and AliExpress.com, the number of electronic transactions has increased dramatically in recent years. Credit cards are now the most widely used form of payment for both online and offline transactions. One of the main ethical problems with electronic payment gateways is fraud. In essence, fraud is the dishonest use of deceit to gain something for oneself and/or cause someone else to lose something. Additionally, we see a sharp rise in fraud instances, which cause billions of dollars' worth of damages annually on a global scale. As a result, it is crucial to avoid fraud and use strategies that may help with its identification and prevention. It is not unexpected that many fraud systems have significant limitations since it is difficult to prevent fraud in real time. The process of encoding a message or piece of information such that only those with permission may access it and those without permission cannot is known as encryption. Credit card numbers and other financial and personal data must be encrypted in this system in order to be used for online transactions. The system uses a secret code to minimise fraud. To prevent unauthorised users from using this secret code, it is kept in an encrypted manner. This paper's objective is to provide a thorough analysis of fraud prevention in electronic payment gateways.

"Fraud detection system: A survey" ,

M. A. Maarof, A. Zainal, and A. Abdallah

The majority of financial transactions may now be carried out via electronic commerce systems, including credit card, telecommunication, and health insurance systems, thanks to the rise in computer technology usage and the ongoing expansion of businesses. Regretfully, criminals and authorised users alike use these technologies. Additionally, fraudsters broke into the electronic commerce systems using a variety of methods. Electronic commerce systems cannot be sufficiently secured by fraud prevention systems (FPSs). To protect electronic commerce systems, however, FDSs and FPSs working together might be beneficial. The performance of FDSs is, however, hampered by a number of problems and difficulties, including concept drift, real-time detection assistance, skewed distribution, and massive data sets. The purpose of this survey article is to provide a thorough and methodical summary of these problems and difficulties that hinder FDS functioning. Credit cards, telecommunications, health insurance, auto insurance, and online auctions are the five electronic commerce platforms that we have chosen. A detailed introduction is given to the most common forms of fraud in such e-commerce platforms. Furthermore, cutting-edge FDSs techniques are methodically incorporated in a few e-commerce systems. Following that, a succinct overview of prospective future research trends and a conclusion are given.

"An examination of the most popular machine learning techniques for identifying online fraud

G. Mesnita and E.-A. Minastireanu,

Illegal acts pertaining to online financial transactions have become more intricate and international in nature in recent years, causing significant financial losses for both consumers and businesses. Numerous methods have been put forward to prevent and identify fraud in online settings. Nevertheless, each of these methods has unique traits, benefits, and drawbacks in addition to sharing the objective of detecting and stopping fraudulent online transactions. In light of this, this study examines the body of research on fraud detection in order to identify the algorithms that are used and evaluate each one according to certain standards. The systematic quantitative literature review approach was used to examine the research works in the area of fraud detection. A hierarchical typology is created based on the most popular machine-learning algorithms in scholarly publications and their attributes. Therefore, by integrating three selection criteria—accuracy, coverage, and costs—our research presents the best methods for detecting fraud in a novel approach.

III. SYSTEM ANALYSIS

EXISTING SYSTEM

In order to detect potentially harmful offline or online transactions, machine-learning-based techniques classify or forecast future observations based on previously acquired historical data [6]. A comparison of machine-learning algorithm-based credit card fraud detection techniques was carried out by Xuetong Niu et al. On the dataset of credit card transactions, the majority of machine-learning models exhibit good performance. Furthermore, following further pre-processing, including eliminating outliers, supervised models outperform unstructured models by a small margin [7].

The concept of identifying certain aberrant user behaviours to detect fraud is the basis for the widespread application layer deployment of credit card fraud detection. Because of its greater accuracy and scope, the supervised learning algorithm is the most often utilised learning technique in online fraud monitoring transactions. The machine learning approach may effectively detect fraudulent transactions in credit card applications, according to recent study in [8, 9].

In order to evade current fraud detection techniques, scammers often alter their behavioural patterns on the fly. SVM can reliably categorise user behaviours under complicated circumstances in online credit card fraud detection [10]. For thorough fraud detection, several researchers benefit from mixing different detection techniques. For instance, Dahee Choi et al. suggested a technique that combined supervised and unsupervised learning with an emphasis on payment fraud applications [11]. The majority of machine learning-based techniques analyse fraudulent transactions using previous data. The transactional process flow and dynamic user behaviours have not received enough attention. In order to monitor and enhance the operational process in company IT infrastructure, the second category of fraud detection techniques employs process mining, which focusses on gaining knowledge from current event logs in information systems [12]. In order to further identify, locate, and

https://doi.org/10.62643/ijerst.2025.v21.i2.pp892-902
Vol. 21, Issue 2, 2025

understand the discrepancy between the existing model and the actual event log, process mining focusses on comparing the event log with an established model [13].

Many anomalous transactions that are unknown to conventional techniques may be found via process mining. The new process mining technique was proposed by M. Jans et al. as a suitable way to prevent fraud involving internal affairs [14]. For instance, C Rinner et al. used conformance checks to track melanoma patients' progress [15]. Alignment and replay were used by Asare et al. to verify that the hospital workflow model and the electronic medical record log were in compliance [16]. By developing matching training and testing models for compliance checking, research has concentrated on tracking and assessing the order of activities taking place in the historical medical event record [17]. For conformity verification, tools like ProM, Disco, and Heustic miner are often used. One effective method for detecting fraud is process mining.

In particular, when identifying fraudulent user behaviour, it is critical to be dynamic and multi-perspective [18]. In order to find outliers, process mining assists in comparing the real data with the standard model. Even with current advancements in fraud detection, hybrid learning techniques must be developed to increase detection accuracy [19]. A multi-perspective anomaly detection approach that extends beyond the viewpoint of control flow, encompassing time and resources, is suggested in order to further the comprehension and advancement of process mining for anomaly identification [20]. Febriyanti et al. [21] suggested a hybrid approach combining association rules and process mining to identify certain suspicious aberrant behaviours, assuming that any discernible alterations in business processes were a sign of suspected fraud behaviour. Prior studies on the use of process mining to identify fraudulent transactions shown that, since event logs are continuously monitored, process mining can both identify fraudulent transactions and successfully stop audit fraud. [22].

Disadvantages

1) The manner of fraud 1. An order is tampered with by a bad actor: The bad actor can submit a phoney official payment order to trick the victim merchant. A to the server/cashier. By altering the order details, including the total cost, the malicious actor was able to receive the order products that do not match the payment value.

2) Subcontracting the order: The victim pays the malicious actor's order rather than his own. This is the second fraud method. The bad actors pose as customers and vendors in order to accomplish their objectives. Before and after the payment, the order details are updated.

PROPOSED SYSTEM

The suggested solution introduces a hybrid approach to anomaly detection in data flows, which gives details about every activity incorporated in a control flow model, combining the benefits of process mining and machine learning models. This approach can dynamically detect changes in

ISSN 2319-5991 www.ijerst.com
https://doi.org/10.62643/ijerst.2025.v21.i2.pp892-902
Vol. 21, Issue 2, 2025

user behaviours, transaction processes, and noncompliance issues by modelling and analysing the e-commerce system's business process. It can also thoroughly analyse and identify fraudulent transactions from a variety of angles. The following is a list of this paper's significant contributions:

1) To identify the anomalies in e-commerce transactions, a conformance checking technique based on process mining is used.

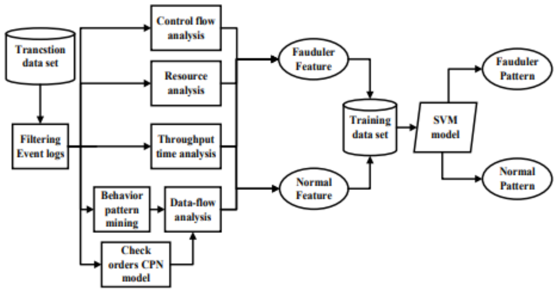
2) To carry out thorough anomaly detection based on Petri nets, a user behaviour detection technique is suggested.

3) To automatically categorise fraudulent behaviours, an SVM model is created by integrating multi-perspective process mining into machine learning techniques.

Advantages

- The event log and the DPN are compared and analysed using the plug-in Multi-Perspective Process Explorer and Conformance Checking to get a more lucid outcome. This method displays the outcome, with various colours denoting each action. For example, purple indicates a move on the model alone, grey indicates unseen actions, such as skipped actions, and green indicates a move on both the model and the log.
- We may get the information that matches the model and the event log in the data flow of each action by clicking on it. A mismatch is shown by the red-marked data. We identify these questionable anomalies and use them as the foundation for further machine learning model training.

SYSTEM ARCHITECTURE



IV. IMPLEMENTATION

Modules

Service Provider

The Service Provider must use a working user name and password to log in to this module. He may do many tasks after successfully logging in, including Train & Test Data Sets, See the Accuracy of Trained and Tested Datasets in a Bar Chart View Accuracy Results for Trained and Tested Datasets, Download Predicted Data Sets, View Cyber Attack Prediction Status Ratio, and View Cyber Attack Prediction Status See the results of the Cyber Attack Prediction Status Ratio. See Every Remote User.

View and Authorize Users

The administrator may see a list of all registered users in this module. Here, the administrator may see the user's information, like name, email, and address, and they can also grant the user permissions.

Remote User

International Journal of Engineering Research and Science & Technology

ISSN 2319-5991 www.ijerst.com

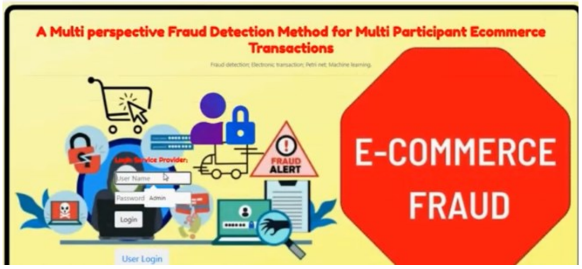
https://doi.org/10.62643/ijerst.2025.v21.i2.pp892-902

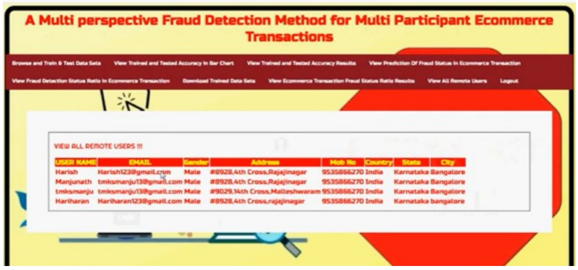
Vol. 21, Issue 2, 2025

A total of n users are present in this module. Before beginning any actions, the user needs register. Following registration, the user's information will be entered into the database. Following a successful registration, he must use his password and authorised user name to log in. Following a successful login, the user may do tasks including registering and logging in, predicting the status of cyberattacks, and seeing their profile.

V. RESULTS

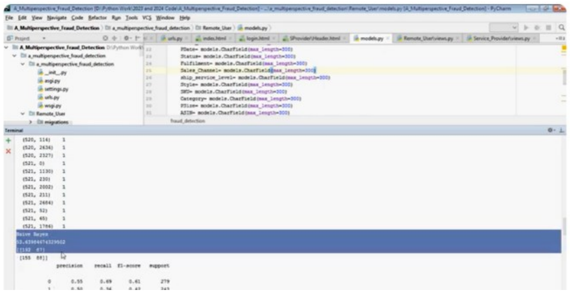
A Multi perspective Fraud Detection Method for Multi Participant Ecommerce Transactions
Home| Remote User| Service Provider
eCommerce Fraud


A Multi perspective Fraud Detection Method for Multi Participant Ecommerce Transactions
Fraud detection; Electronic transaction; Petri net; Machine learning.
Login Service Provider:
User Name
Password Admin
Login
User Login
FRAUD ALERT
E-COMMERCE FRAUD


A Multi perspective Fraud Detection Method for Multi Participant Ecommerce Transactions
Browse and Train & Test Data Sets
View Trained and Tested Accuracy in Bar Chart
View Trained and Tested Accuracy Results
View Prediction Of Fraud Status in Ecommerce Transaction
View Fraud Detection Status Ratio in Ecommerce Transaction
Download Trained Data Sets
View Ecommerce Transaction Fraud Status Ratio Results
View All Remote Users
Logout

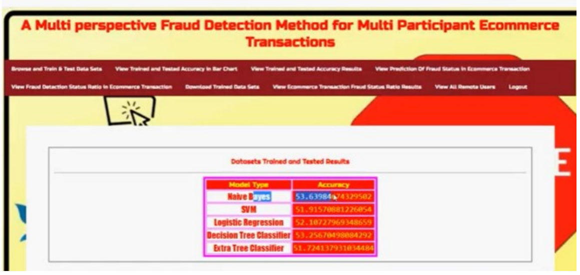
VIEW ALL REMOTE USERS !!!

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,Malleshwaram	9535866270	India	Karnataka	Bangalore
Hariharan	Hariharan123@gmail.com	Male	#8928,4th Cross,rajajinagar	9535866270	India	Karnataka	bangalore


A_Multiperspective_Fraud_Detection [D:\Python Work\2023 and 2024 Code\A_Multiperspective_Fraud_Detection] - ...\a_multiperspective_fraud_detection\Remote_User\models.py [A_Multiperspective_Fraud_Detection] - PyCharm
File Edit View Navigate Code Refactor Run Tools VCS Window Help
urls.py
index.html
login.html
SProvider\Header.html
models.py
Remote_User\views.py
Service_Provider\views.py
A_Multiperspective_Fraud_Detection
a_multiperspective_fraud_detection
__init__.py
asgi.py
settings.py
urls.py
wsgi.py
Remote_User
migrations
Terminal

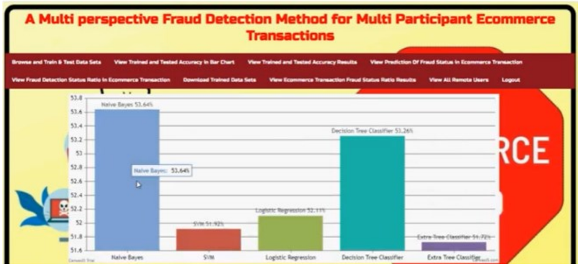
```
PDate= models.CharField(max_length=300)
Status= models.CharField(max_length=300)
Fulfilment= models.CharField(max_length=300)
Sales_Channel= models.CharField(max_length=300)
ship_service_level= models.CharField(max_length=300)
Style= models.CharField(max_length=300)
SKU= models.CharField(max_length=300)
Category= models.CharField(max_length=300)
PSize= models.CharField(max_length=300)
ASIN= models.CharField(max_length=300)
```

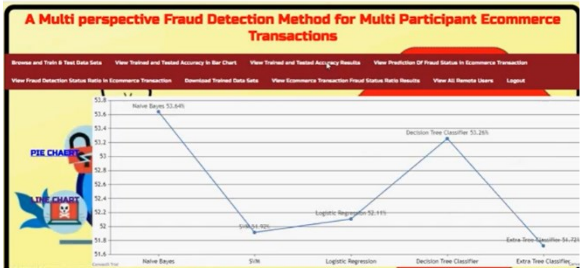
```
(520, 114)    1
(520, 2636)   1
(520, 2327)   1
(521, 0)      1
(521, 1130)   1
(521, 230)    1
(521, 2002)   1
(521, 211)    1
(521, 2684)   1
(521, 52)     1
(521, 65)     1
(521, 1786)   1
Naive Bayes
53.63984674329502
[[192  87]
 [155  88]]
              precision    recall  f1-score   support

           0       0.55      0.69      0.61       279
           1       0.50      0.36      0.42       243
```

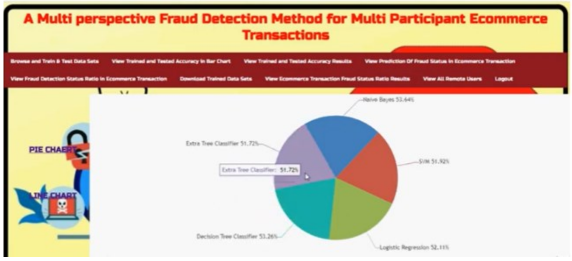

A Multi perspective Fraud Detection Method for Multi Participant Ecommerce Transactions
Browse and Train & Test Data Sets
View Trained and Tested Accuracy in Bar Chart
View Trained and Tested Accuracy Results
View Prediction Of Fraud Status in Ecommerce Transaction
View Fraud Detection Status Ratio in Ecommerce Transaction
Download Trained Data Sets
View Ecommerce Transaction Fraud Status Ratio Results
View All Remote Users
Logout

Datasets Trained and Tested Results

Model Type	Accuracy
Naive Bayes	53.63984674329502
SVM	51.91570881226054
Logistic Regression	52.10727969348659
Decision Tree Classifier	53.25670498084292
Extra Tree Classifier	51.724137931034484



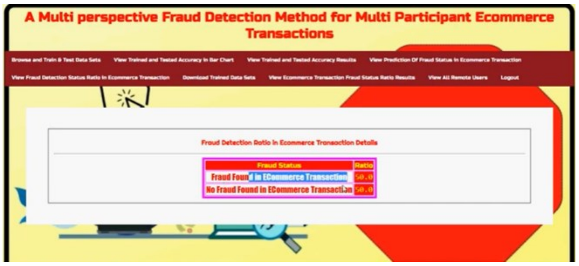




ISSN 2319-5991 www.ijerst.com

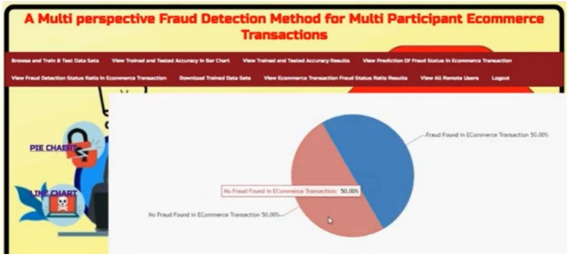
https://doi.org/10.62643/ijerst.2025.v21.i2.pp892-902

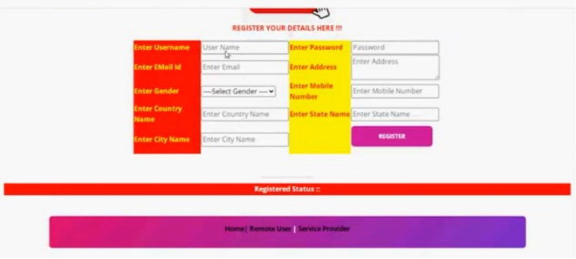
Vol. 21, Issue 2, 2025


A Multi perspective Fraud Detection Method for Multi Participant Ecommerce Transactions
Browse and Train & Test Data Sets
View Trained and Tested Accuracy in Bar Chart
View Trained and Tested Accuracy Results
View Prediction Of Fraud Status In Ecommerce Transaction
View Fraud Detection Status Ratio In Ecommerce Transaction
Download Trained Data Sets
View Ecommerce Transaction Fraud Status Ratio Results
View All Remote Users
Logout

Fraud Detection Ratio in Ecommerce Transaction Details

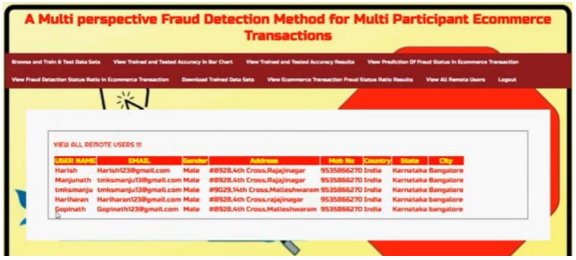
Fraud Status	Ratio
Fraud Found in ECommerce Transaction	50.0
No Fraud Found in ECommerce Transaction	50.0


A Multi perspective Fraud Detection Method for Multi Participant Ecommerce Transactions
Browse and Train & Test Data Sets
View Trained and Tested Accuracy in Bar Chart
View Trained and Tested Accuracy Results
View Prediction Of Fraud Status In Ecommerce Transaction
View Fraud Detection Status Ratio In Ecommerce Transaction
Download Trained Data Sets
View Ecommerce Transaction Fraud Status Ratio Results
View All Remote Users
Logout
PIE CHART
LINE CHART
Fraud Found in ECommerce Transaction 50.00%
No Fraud Found in ECommerce Transaction: 50.00%
No Fraud Found in ECommerce Transaction 50.00%


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 ::


A Multi perspective Fraud Detection Method for Multi Participant Ecommerce Transactions
Browse and Train & Test Data Sets
View Trained and Tested Accuracy in Bar Chart
View Trained and Tested Accuracy Results
View Prediction Of Fraud Status In Ecommerce Transaction
View Fraud Detection Status Ratio In Ecommerce Transaction
Download Trained Data Sets
View Ecommerce Transaction Fraud Status Ratio Results
View All Remote Users
Logout

VIEW ALL REMOTE USERS !!!

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,Malleshwaram	9535866270	India	Karnataka	Bangalore
Hariharan	Hariharan123@gmail.com	Male	#8928,4th Cross,rajajinagar	9535866270	India	Karnataka	bangalore
Gopinath	Gopinath123@gmail.com	Male	#8928,4th Cross,Malleshwaram	9535866270	India	Karnataka	bangalore

VI. CONCLUSION

This study combined formal process modelling with dynamic user behaviours to develop a hybrid approach for capturing fraudulent transactions. The five main viewpoints that we used to analyse the e-commerce transaction process were control flow, resource, time, data, and user behaviour patterns. This study developed an SVM model to identify fraudulent transactions and used high-level Petri nets as the foundation for process modelling to describe aberrant user behaviours. Our thorough testing demonstrated that the suggested approach is capable of successfully capturing fraudulent transactions and activities. Our suggested multi-perspective detection approach fared better overall than the single-perspective detection method. For increased accuracy, we would include relevant deep learning [38–42] and model verification techniques [43–45] into the suggested framework as part of our future work. To improve the accuracy of risk detection, it will also be necessary in the future to add additional temporal aspects to the behaviour patterns. Additionally, by coordinating the models, we will extend the suggested technique to additional areas of harmful behaviour and investigate the creation of a common fraud mode library.

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.

ISSN 2319-5991 www.ijerst.com
https://doi.org/10.62643/ijerst.2025.v21.i2.pp892-902
Vol. 21, Issue 2, 2025

[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] 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] 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.

[7] 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. [8] 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.

[9] 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.

[10] 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.

[11] 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.

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

[13] 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.

[14] 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

https://doi.org/10.62643/ijerst.2025.v21.i2.pp892-902

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.