



ISSN: 2321-2152

**IJMECE**

*International Journal of modern  
electronics and communication engineering*

E-Mail

[editor.ijmece@gmail.com](mailto:editor.ijmece@gmail.com)

[editor@ijmece.com](mailto:editor@ijmece.com)

[www.ijmece.com](http://www.ijmece.com)

# A Multi-perspective Fraud Detection Method for Multi-Participant E-commerce Transactions

<sup>1</sup>P. SRINIVASA REDDY, <sup>2</sup> KAGITHA AKHILA

<sup>1</sup>Associate Professor, S.V.K.P & Dr. k .S. Raju Arts & Science College(A),Penugonda, W. G. District, Andhra Pradesh, [psreddy1036@gmail.com](mailto:psreddy1036@gmail.com)

<sup>2</sup>PG Scholar, S.V.K.P & Dr .k. S. Raju Arts & Science College(A),Penugonda, W.G District, Andhra Pradesh, [akhilakagitha720@gmail.com](mailto:akhilakagitha720@gmail.com)

## ABSTRACT

Detection and prevention of fraudulent transactions in e-commerce platforms have always been the focus of transaction security systems. However, due to the concealment of e-commerce, it is not easy to capture attackers solely based on the historic order information. Many researches try to develop technologies to prevent the frauds, which have not considered the dynamic behaviors of users from multiple perspectives. This leads to an inefficient detection of fraudulent behaviors. To this end, this paper proposes a novel fraud detection method that integrates machine-learning and process mining models to monitor real-time user behaviors. First, we establish a process model concerning the B2C e-commerce platform, by incorporating the detection of user behaviors. Second, a method for analyzing abnormalities that can extract important features from event logs is presented. Then, we feed the extracted features to a Support Vector Machine (SVM) based classification model that can detect fraud behaviors. We demonstrate the effectiveness of our method in capturing dynamic fraudulent behaviors in e-commerce systems through the experiments.

## INTRODUCTION

WITH the increasing popularity of e-commerce platforms, more and more commercial transactions are now relying on web-based systems than the

traditional cash-based approach [1]. Although the entity economy is greatly impacted by the COVID-19 epidemic in recent years, e-commerce remains largely unaffected by the pandemic, whereby aiding a steady market growth [2]. The sales volume of B2C (Business to Customer) e-commerce is expected to reach 6.5 trillion dollars by 2023 [3].

Though the growth of e-commerce and the expansion of modern technologies offer better opportunities for online businesses, new security threats have emerged over the past few years. Reportedly, the significant increase in the number of online fraud cases costs billions of dollars worldwide every year [4]. The dynamic and distributed nature of the Internet has made anti-fraud systems inevitable to ensure the security of online transactions. Existing fraud detection systems focusing on detecting abnormal user behaviors still characterize vulnerabilities when mitigating emerging security threats. An important issue in existing fraud detection systems is their lack of efficient process management during the trading process. The imperfect monitoring function is one of the key issues that need attention [5]. The detection perspective is usually not enough due to the lack of process capture for the existing work. To this end, we propose a process-based method, where user behaviors are recorded and analyzed in real-time, and historical data is transformed into controllable data. In addition, we incorporate a multi-perspective detection of abnormal behaviors.

This paper combines the advantages of process mining and machine learning models by introducing a hybrid method to solve the anomaly detection in data flows, which provides information about each action embedded in a control flow model. By modeling and analyzing the business process of the e-commerce system, this method can dynamically detect changes in user behaviors, transaction processes, and noncompliance situations, and comprehensively

analyze and identify fraudulent transactions from multiple perspectives. Important contributions of this paper are listed as follows:

- 1) A conformance checking method based on process mining is applied in the field of e-commerce transactions to capture the abnormalities.
- 2) A user behavior detection method is proposed to perform comprehensive anomaly detection based on Petri nets.
- 3) An SVM model is developed by embedding a multi perspective process mining into machine learning methods to automatically classify fraudulent behaviors. The rest of this paper is organized as follows: Section 2 introduces the related work. Section 3 presents a model analysis and a background study. Section 4 forms the theoretical basis and describes our proposed fraud detection method. Section 5 presents and discusses the results of our experiments and Section 6 validates our proposed fraud detection method. Section 7 concludes our paper along with outlining our future research directions.

## LITERATURE SURVEY

### INTRODUCTION

The rise of e-commerce has brought significant convenience to consumers and businesses alike, but it has also led to an increase in fraudulent activities. Detecting and preventing fraud in this digital marketplace is crucial to maintaining trust and security. Traditional fraud detection methods, which often rely on single-dimensional approaches, are no longer sufficient to counter sophisticated fraud tactics. Consequently, a multi-perspective fraud detection method has emerged as a more effective solution. This approach integrates various techniques, including machine learning, rule-based systems, and anomaly detection, to analyze transactions from multiple angles. By considering different data sources and contextual information, it provides a more comprehensive understanding of fraudulent patterns. This literature survey delves into the various methodologies that constitute multi-perspective fraud

detection, examining their effectiveness, challenges, and the latest advancements in the field. Through a thorough review of current research, this survey underscores the necessity and benefits of adopting a multi-faceted approach to secure e-commerce transactions against fraud.

## **EXISTING SYSTEM**

The machine-learning-based methods learn from previously obtained historical data to perform classifications or predictions of future observations to identify potential risky offline or online transactions [6]. Xuotong Niu et al. conducted a comparative study on credit card fraud detection methods that rely on machine-learning algorithms. Most of the machine-learning models perform well on the dataset of credit card transactions. Moreover, supervised models perform slightly better than unsupervised models after additional pre-processing, such as removing outliers [7].

Credit card fraud detection is widely deployed at the application layer, which uses the idea of discovering specific abnormal user behaviors to detect fraud. The supervised learning algorithm is the most commonly used learning method in online fraud monitoring transactions, since it has higher accuracy and coverage. Recent research in [8, 9] has proved that the machine learning method can efficiently capture fraudulent transactions in credit card applications.

Fraudsters often change their behavioral pattern dynamically to overcome existing fraud detection methods. In online credit card fraud detection, SVM can classify user behaviors under complex scenarios and deliver reliable results [10]. Many researchers take the advantage of combining multiple detection methods for comprehensive fraud detection. For example, focusing on payment fraud applications, Dahee Choi et al. proposed a method by combining supervised and unsupervised learning [11]. Most of the machine learning based methods use

historical data to analyze fraudulent transactions. They have not given enough emphasis to the transactional process flow and dynamic user behaviors. The second type of fraud detection methods uses process mining, focusing on extracting knowledge from existing event logs in information systems for the purpose of monitoring and improving the operational process in business IT infrastructure [12]. Process mining specializes in comparing the event log with an established model to further detect, locate, and interpret the deviation between the established model and the actual event log [13].

Process mining can detect a large number of abnormal transactions, which are not known to be identifiable by traditional methods. M Jans et al. postulated the emerging process mining approach as an appropriate solution to mitigate against fraud incorporating internal affairs [14]. For example, C Rinner et al. applied conformance checks to monitor the process of melanoma patients [15]. Asare et al. applied alignment and replay to check the conformance of the electronic medical record log and the hospital workflow model [16]. Research has focused on monitoring and evaluating the sequence of processes occurring in the historical medical event log by establishing corresponding training and testing models for conformance checking [17]. Tools such as ProM, Disco and Heuristic miner are largely used for conformance checking. Process mining can be an efficient approach for fraud detection.

Especially, it is important to be dynamic and multi perspective when detecting fraudulent user behaviors [18]. Process mining helps to compare the actual data against the standard model to identify outliers. Despite existing progress in fraud detection, it is still necessary to develop hybrid learning methods to improve the accuracy of detection [19]. To promote the understanding and development of process mining for anomaly detection, a method of multi-perspective anomaly

detection is proposed that goes beyond the perspective of control flow including time and resources [20]. Febriyanti et al. [21] assumed any noticeable changes in business processes as a suspected fraud behavior and proposed a method to detect some suspicious abnormal behaviors using a hybrid method of association rules and process mining. Previous research on using process mining to detect fraudulent transactions showed that process mining is capable of detecting fraudulent transactions, and it can effectively prevent audit fraud at a much earlier stage due to the continuous monitoring nature of event logs [22].

#### Disadvantages

1) Fraud mode one - an order is tempered by a malicious actor: The malicious actor may deceive the victim merchant by sending a fake formal payment order order F

A to the cashier server. The malicious actor obtained the order items that do not match the payment value by tampering with the order information, such as the total amount.

2) Fraud mode two - subcontract the order: The victim pays the malicious actor's order instead of his order. To achieve their goals, the malicious actors impersonate the duties of sellers and buyers. The order information changes before and after the payment.

#### **PROPOSED SYSTEM**

The proposed system combines the advantages of process mining and machine learning models by introducing a hybrid method to solve the anomaly detection in data flows, which provides information about each action embedded in a control flow model. By modeling and analyzing the business process of the e-commerce system, this method can dynamically detect changes in user behaviors, transaction processes, and noncompliance situations, and comprehensively

analyze and identify fraudulent transactions from multiple perspectives. Important contributions of this paper are listed as follows:

- 1) A conformance checking method based on process mining is applied in the field of e-commerce transactions to capture the abnormalities.
- 2) A user behavior detection method is proposed to perform comprehensive anomaly detection based on Petri nets.
- 3) An SVM model is developed by embedding a multi perspective process mining into machine learning methods to automatically classify fraudulent behaviors.

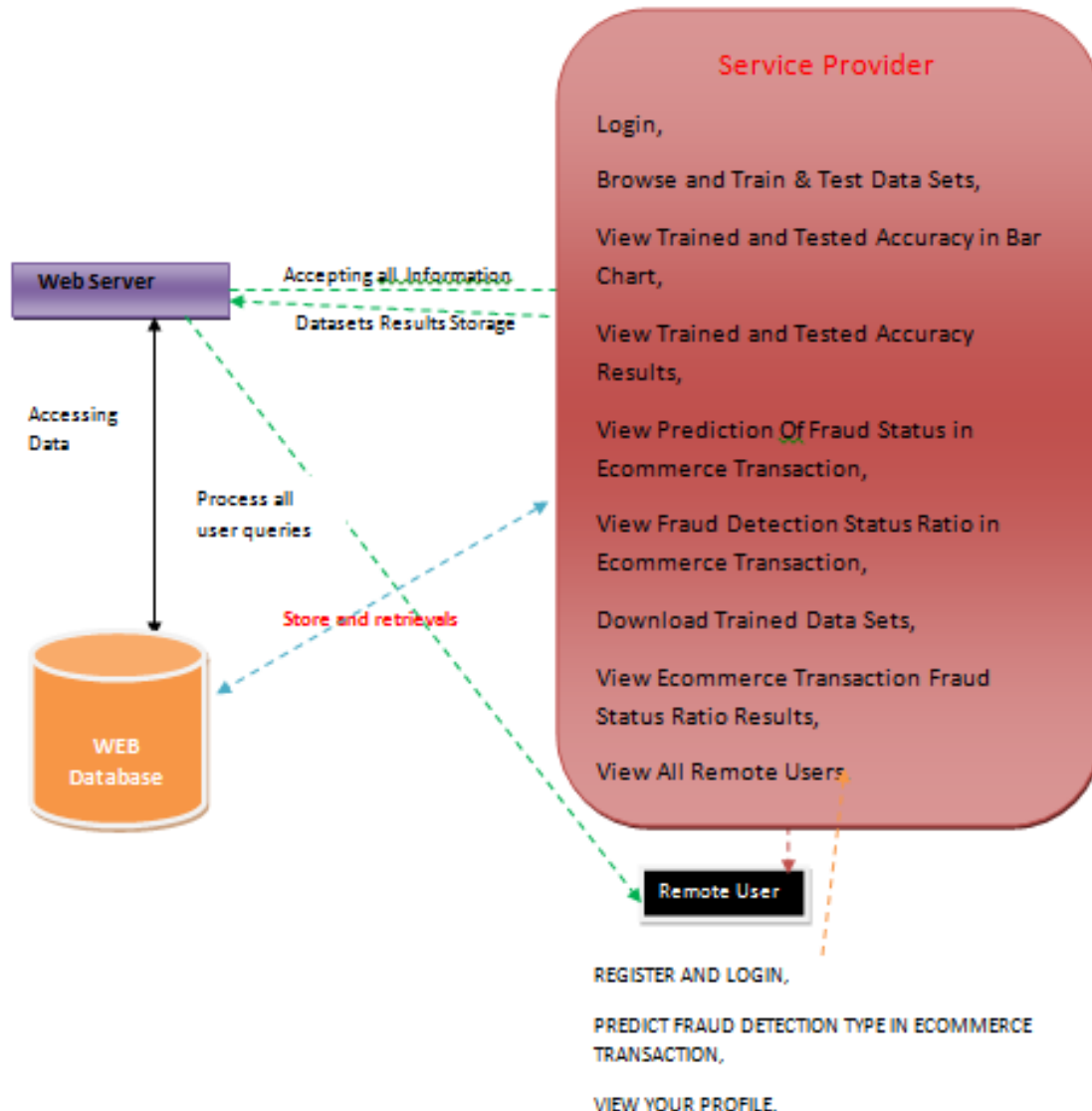
## **Advantages**

- To arrive at a clearer result, the plug-in Multi-Perspective Process Explorer and Conformance Checking are used to match and analyze the event log and the DPN. The result is shown in this system, where each action is represented with different colors. For instance, green represents the move both on model and log, purple means move on the model only, and grey represents invisible actions, that is, skipped actions.
- By clicking on a given action, we can obtain the matching information between the model and the event log in the data flow of each action. The data marked in red indicates a mismatch. We extract these suspicious anomalies and use them as the basis for subsequent training using machine learning models.

## **System Architecture**



## Architecture Diagram



## Modules

### **Service Provider**

In this module, the Service Provider has to login by using valid user name and password. After login successful he can do some operations such as 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

### **View and Authorize Users**

In this module, the admin can view the list of users who all registered. In this, the admin can view the user's details such as, user name, email, address and admin authorizes the users.

### **Remote User**

In this module, there are n numbers of users are present. User should register before doing any operations. Once user registers, their details will be stored to the database. After registration successful, he has to login by using authorized user name and password. Once Login is successful user will do some operations like REGISTER AND LOGIN, PREDICT FRAUD DETECTION TYPE IN ECOMMERCE TRANSACTION, VIEW YOUR PROFILE.

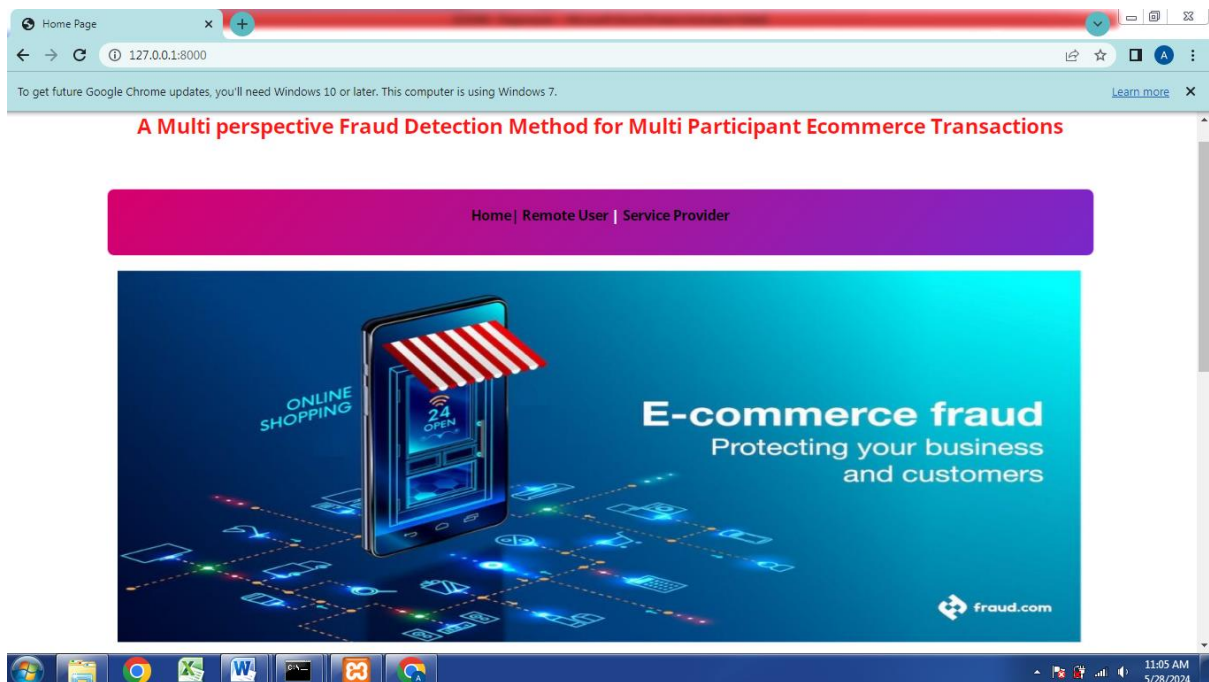
## **CONCLUSION**

This paper proposed a hybrid method to capture fraud transactions by integrating the formal process modeling and the dynamic user behaviors. We analyzed the e-commerce transaction process under five major perspectives: control flow perspective, resource perspective, time perspective, data perspective, and user behavior patterns. This paper utilized high-level Petri nets as the basis of process modeling to model the abnormal user behaviors and created an SVM model to perform fraudulent transaction detection. Our extensive experiments showed that the proposed method can effectively capture fraudulent transactions and

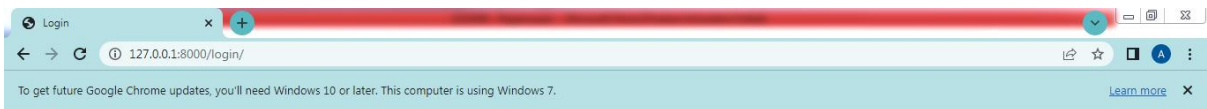
behaviors. The overall index of our proposed multi-perspective detection method outperformed the single-perspective detection method. As our future work, related deep learning [38-42] and model checking methods [43-45] would be incorporated in the proposed framework for higher accuracy. Additionally, it's also a future work to incorporate more time features to the behavior patterns so as to make the risk identification more accurate. Furthermore, we will conduct research on constructing a standard fraud mode library, and apply the proposed methodology to other malicious behavior areas by coordinating the models.

## Output screens

### HOME PAGE



### REMOTE USER



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



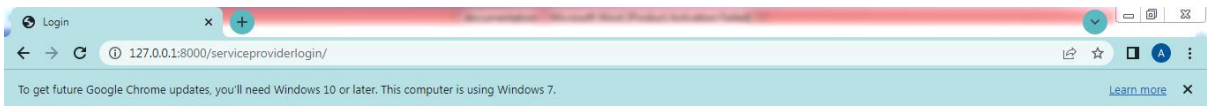
Login Using Your Account:

User Name

Password

LOGIN

Are You New User !!! REGISTER

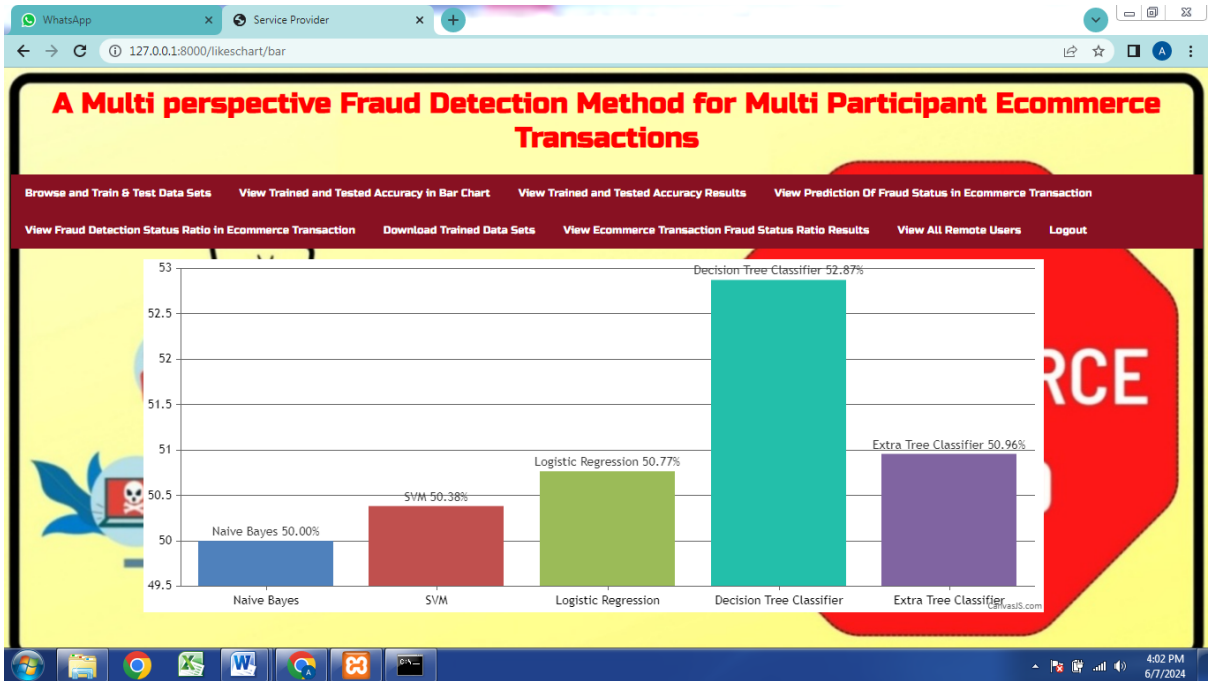


**A Multi perspective Fraud Detection Method for Multi Participant Ecommerce Transactions**

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



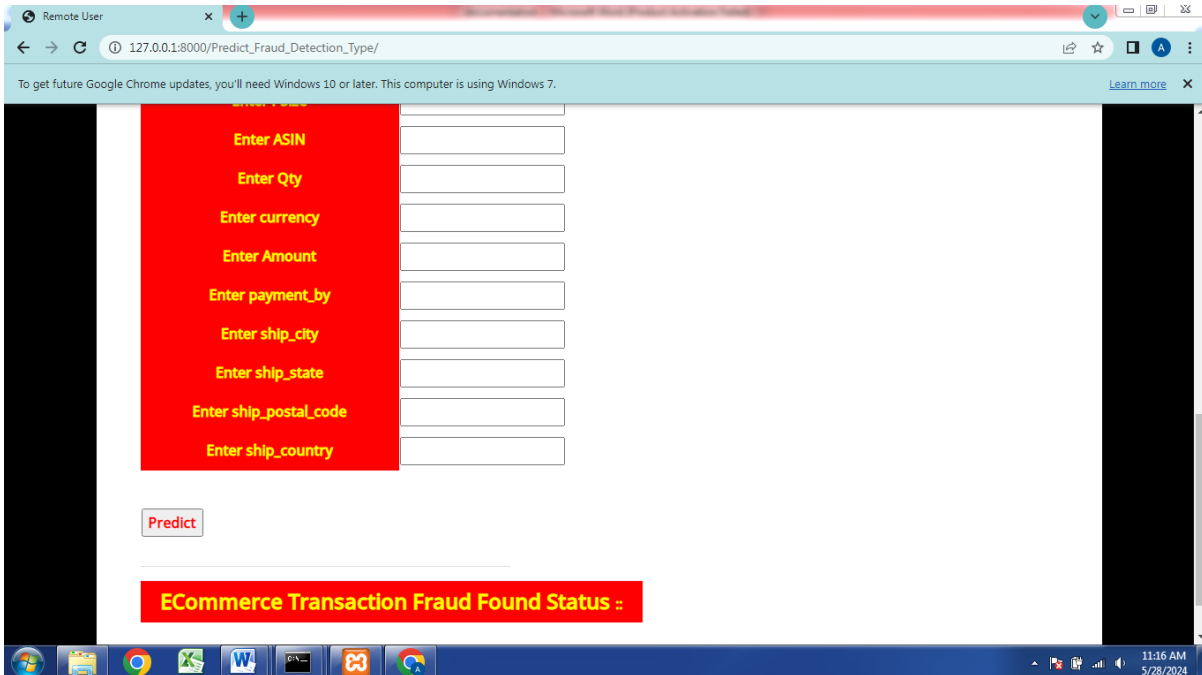
SERVICE PROVIDER



**PREDICTION OF FRAUD FOUND IN ECOMMERCE TRANSACTION STATUS!!!**

**ENTER DATASET DETAILS HERE !!!**

- Enter Order\_ID
- Enter PDate
- Enter Status
- Enter Fulfilment
- Enter Sales\_Channel
- Enter ship\_service\_level
- Enter Style
- Enter SKU
- Enter Category
- Enter PSize
- Enter ASIN



## PREDICTED THE OUTPUT

## REFERENCES

- [1] R. A. Kuscü, Y. Cicekcisoy, and U. Bozoklu, *Electronic Payment Systems in Electronic Commerce*. Turkey: IGI Global, 2020, pp. 114–139.
- [2] M. Abdelrhim, and A. Elsayed, “The Effect of COVID-19 Spread on the e-commerce market: The case of the 5 largest e-commerce companies in the world.” *Available at SSRN 3621166*, 2020, doi: 10.2139/ssrn.3621166.
- [3] P. Rao et al., “The e-commerce supply chain and environmental sustainability: An empirical investigation on the online retail sector.” *Cogent. Bus. Manag.*, vol. 8, no. 1, pp. 1938377, 2021.
- [4] S. D. Dhobe, K. K. Tighare, and S. S. Dake, “A review on prevention of fraud in electronic 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 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.

[24] W. Rui, S. Chen, X. Wang and S.Qadeer, “How to Shop for Free Online--Security Analysis of Cashier-as-a-Service Based Web Stores,” in *Proc. SSP*, Oakland, CA, USA, 2011, pp. 465-480.

[25] E. Ramezani, D. Fahland and W. Aalst, “Where did I misbehave? Diagnostic information in compliance checking,” in *BPM.*, Berlin, Germany, Springer, 2012, pp. 262-278.