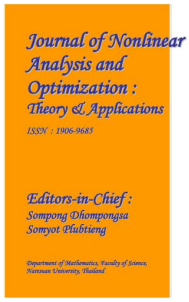
Journal of **N**onlinear **A**nalysis and **O**ptimization
Vol. 15, Issue. 1, No.15 : 2024
ISSN : **1906-9685**



A MULTI-PERSPECTIVE FRAUD DETECTION METHOD FOR MULTI-PARTICIPANT E-COMMERCE TRANSACTIONS

[1]Vadde Raymond Paul,[2]Mr A.D.Sivarama Kumar
[1]Student,[2]Assistant Professor
Department Of CSE
SVR Engineering College, Nandyal

ABSTRACT

Transaction security solutions have traditionally been centered on the identification and blocking of fraudulent transactions in e-commerce platforms. However, it is difficult to apprehend attackers based just on historical order information since e-commerce is hidden. Numerous efforts attempt to create technologies that stop fraud, but they do not take into account the changing behaviors of consumers from different angles. This makes it more difficult to identify fraudulent activity. In order to do this, this paper suggests a unique approach to fraud detection that combines process mining and machine learning models to track user activity in real time. Initially, we create a process model that includes the identification of user behaviors for the business-to-customer (B2C) e-commerce platform. Secondly, an approach to anomaly analysis that may be used to identify significant characteristics in event logs is described. Next, we input the collected features into a fraud behavior-detection classification model that is built on support vector machines (SVMs). Through the studies, we show how well our approach captures dynamic fraudulent activities in e-commerce platforms.

I. 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 worldwideeveryyear [4].ThedynamicanddistributednatureoftheInternet has madeanti-fraud systems inevitable to ensure the securityof online transactions. Existing fraud detection systems focusing ondetecting abnormaluser behaviours stillcharacterize vulnerabilities when mitigating emerging securitythreats. 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 ofthe 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 behaviours are recorded and analyzed in real-time, and historical data is transformed into controllable data. In addition, we incorporate a multi-perspective detection of abnormalbehaviours.

This project 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 informationabouteachactionembedded inacontrolflow model. Bymodelingandanalyzingthe business process ofthe 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 project 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) Auser behaviour detection method is proposed to perform comprehensive anomaly detection based on Petri nets.

3) An SVM modelis developed by embedding a multi perspective process mining into machine learning methods to automatically classify fraudulent behaviours. The rest of this project is organized as follows: Section 2 introduces the related work. Section 3 presents a modelanalysis 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 project along with outlining our future research directions.

II. LITERATURESURVEY

[1] P.Raoetal,Thee-commercesupplychainandenvironmentalsustainability:Anempirical investigation on the online retail sector,2021

In the rapidly expanding realm of ecommerce, particularly in the business to-consumer (B2C) online retail sector, the environmental consequences of this growth have been a subject of ambiguity in existing research. To address this gap, this study employs two conceptual models derived from literature to investigate the environmental impacts of e-commerce. Collecting 303 responses through a structured questionnaire from the Gulf Cooperation Council (GCC) countries, the studyvalidates and evaluates the proposed models, assessing the relevance ofeach construct and its underlying items.

[2]E.A.Ministering,andG.Manita,AnAnalysisoftheMostUsedMachineLearning Algorithms for Online Fraud Detection, 2019

The escalating complexity and transnational nature of illegal activities in online financial transactions have led to substantial financial losses for both customers and organizations. Countering this challenge, numerous techniques have been proposed for fraud prevention and detection in the online environment. However, each of these techniques exhibits distinct characteristics, advantages, and drawbacks, making it imperative to comprehensivelyreview and analyse the existing research in fraud detection. This paper employs a systematic quantitative literature review methodology to identify the algorithms used in fraud detection and analyses each algorithm based on specific criteria.

[3]WangyangYu;YadiWang;LuLiu;YushengAn;BoYuan;JohnPanneerselvam,AMultperspective Fraud Detection Method for Multiparticipant E-Commerce Transactions,2021

In the persistent challenge of detecting and preventing fraudulent transactions within e-commerce platforms, traditional security systems relying on historical order information often fall short, given the elusive nature of online activities. Recognizing the limitations of existing approaches that neglect dynamic user behaviours, this article proposes an

innovative fraud detection method that seamlessly integrates machine learning and process mining models for real-time monitoring. The methodologyunfolds inthree keystages. First,a business-to-customer (B2C) e-commerce platform is modelled, incorporating a robust framework for detecting user behaviours. This foundationalprocess aims to better understand and adapt to the dynamic nature of user interactions within the platform. Second, the article introduces a method for analysing abnormalities, leveraging event logs to extract essential features crucial for fraud detection. This step ensures a nuanced understanding of irregular patterns indicative of potentially fraudulent activities.

III. SYSTEM ANALYSIS AND DESIGN

EXISTINGSYSTEM

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]. Xuetong Niu et al. conducteda comparative studyoncredit card fraud detection methodsthat relyonmachine-learningalgorithms. Mostofthe machine-learning modelsperform 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 discoveringspecificabnormaluser behavioursto detect fraud. Thesupervised learningalgorithm is the most commonlyused 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 behavioural 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 multipledetectionmethodsfor comprehensivefrauddetection. Forexample, focusing on payment fraud applications, Dahee Choi et al. proposed a method by combining supervised andunsupervised learning [11]. Most ofthe machine learning based methods use historicaldata to analyze fraudulent transactions. They have not given enough emphasis to the transactional process flow and dynamic user behaviours. 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 modelto further detect, locate, and interpret the deviationbetweenthe established modeland 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 eventlog by establishing corresponding training and testing models for conformance checking [17]. Tools such as ProM, Disco and Heustic 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 theunderstanding 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 fraudat a much earlier stage due to the continuous monitoring nature of event logs [22].

DISADVANTAGES:

1) Fraud mode one - anorder is tempered bya malicious actor:The malicious actormaydeceive the victim merchant by sending a fake formal payment order order F Atothecashierserver.Themaliciousactorobtaine dtheorderitemsthatdonotmatchthe payment value by tampering with the order information, such as the total amount.

2) Fraud mode two - subcontract the order:The victimpaysthe maliciousactor'sorder instead of hisorder.Toachievetheirgoals,themaliciousacto rsimpersonatethedutiesofsellersandbuyers. The order information changes before and after the payment.

PROPOSEDSYSTEM

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 informationabouteachactionembedded inacontrolflow model. Bymodelingandanalyzingthe business process ofthe 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)Aconformancecheckingmethodbasedonproce ssminingisappliedinthefieldofe- 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 multiperspective process mining into machine learning methods to automatically classify fraudulent behaviors.

ADVANTAGES:

1) 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.

2) Byclicking ona givenaction, we canobtainthe matching informationbetweenthe modeland 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 learningmodels.

IV. SYSTEMARCHITECTURE

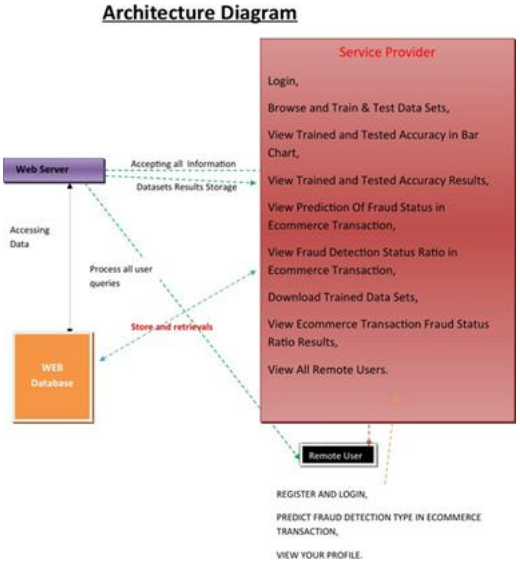


Fig-3.1ArchitectureDiagram

V. IMPLEMENTATION

Modules

ServiceProvider

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 E-commerce Transaction,View Fraud Detection Status Ratio in E-commerce Transaction,Download Trained Data Sets,View E-commerce Transaction Fraud Status Ratio Results,View All Remote Users

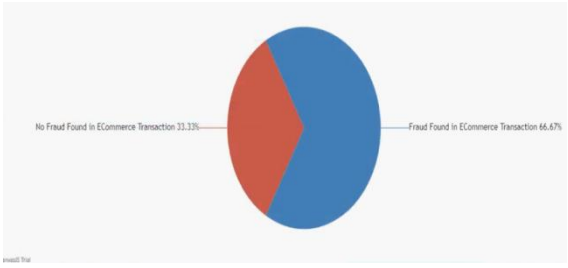
ViewandAuthorizeUsers

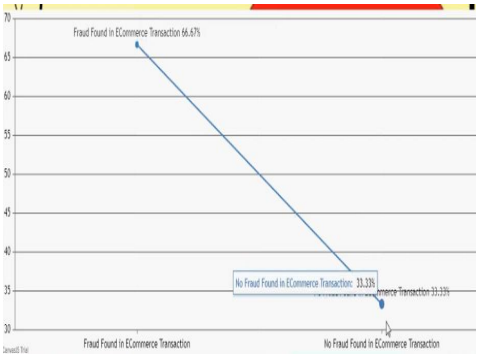
In this module, the admin can view the list of users who all registered. In this, the admin can view the user's details such as, user name, email, address and admin authorizes the users.

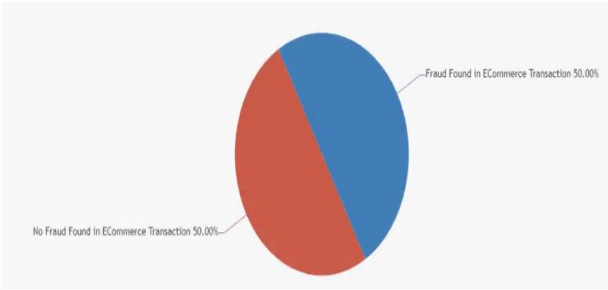
RemoteUser

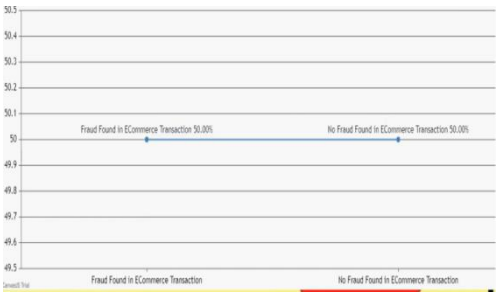
In this module, there are n numbers of users are present. User should register before doing any operations. Once user registers, their details will be stored to the database.After registration successful,hehastologinbyusingauthorizeduser nameandpassword.OnceLoginissuccessful user willdo some operations likeREGISTER AND LOGIN,PREDICT FRAUD DETECTION TYPE IN E-COMMERCE TRANSACTION, VIEWYOUR PROFILE.

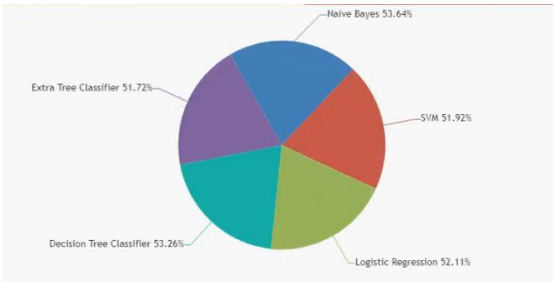
VI. SCREENSHOTS

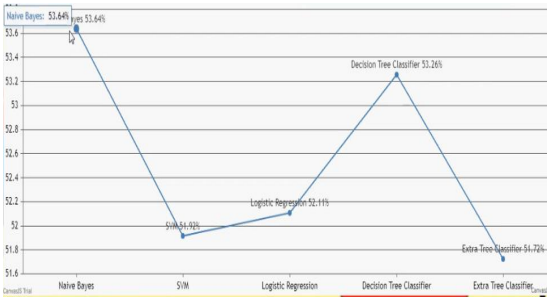


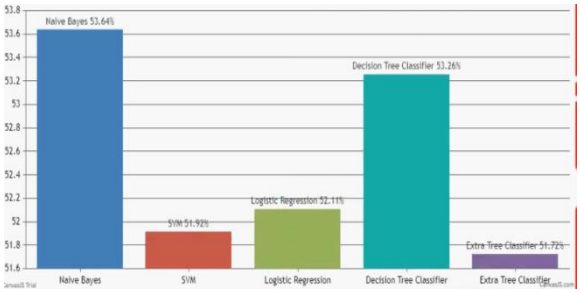












VIII. CONCLUSION

This project 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 Petrinets 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.

REFERENCES

1. R.A.Kuscu,Y.Cicekcisoy,andU.Bozoklu,ElectronicPayment Systems in Electronic Commerce.
2. M.Abdelrhim,andA.Elsayed, "TheEffectofCOVID-19Spreadon the e-commerce market: The case of the 5 largest e-commerce companies in the world."
3. P. Rao et al., "The e-commerce supply chain and environmental sustainability:Anempiricalinvestigationontheonlineretailsector." Cogent. Bus. Manag., vol. 8.
4. S.D.Dhobe,K.K.Tighare,andS.S.Dake, "Areviewonprevention of fraud in electronic payment gateway using secret code," Int. J. Res. Eng. Sci. Manag., vol. 3.
5. A.Abdallah,M.A.Maarof,andA.Zainal, "Frauddetectionsystem:A survey," J. Netw. Comput. Appl., vol. 68.
6. E.A.Minastireanu,andG.Mesnita,"An AnalysisoftheMostUsed Machine Learning Algorithms for Online Fraud Detection," Info. Econ., vol. 23, no. 1, 2019.
7. X.Niu,L.Wang,andX.Yang,"Acomparisonstudyofcreditcard fraud detection: Supervised versus unsupervised," arXiv preprint arXiv:vol.1904,no.10604,2019,doi:10.48550/arXiv.1904.10604.
8. L.Zhengetal., "Transaction Fraud Detection Based on Total Order RelationandBehaviorDiversity,"IEEE Trans.Computat.SocialSyst., vol. 5, no. 3, pp. 796-806, 2018.
9. Z.Li,G.Liu,andC.Jiang,"DeepRepresentationLearningWithFull Center Loss for Credit Card Fraud Detection," IEEE Trans. Computat.Social Syst.,vol.7,no.2,pp.569-579,2020.
10. I.M.Mary,andM.Priyadharsini,"Online TransactionFraud Detection System," in 2021 Int. Conf. Adv. C. Inno. Tech. Engr. (ICACITE), 2021, pp. 14-16.
11. D.Choi,andK.Lee,"Machinelearningbasedapproachtofinancial fraud detection process in mobile payment system," IT Conv. P. (INPRA), vol. 5, no. 4, pp. 12-24, 2017.
12. R.Sarnoetal.,"HybridAssociationRule LearningandProcess Mining for Fraud Detection," IAENG Int. J. C. Sci., vol. 42, no. 2, 2015.

13. J.J.Stoop,"Processminingand fraud detection-Acasestudyonthe theoretical and practical value of using process mining for the detectionoffraudulentbehavior intheprocurementprocess,"M.S. thesis, Netherlands, ENS: University of Twente, 2012.
14. M.Jansetal.,"Abusinessprocess miningapplicationforinternal transaction fraud mitigation," Expert Syst. Appl., vol. 38, no. 10, pp. 13351-13359, 2011.
15. C.Rinneretal.,"Processminingandconf ormancecheckingoflong 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,andX.Fang,"Confor manceChecking: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 historyusingconformancechecking,"in 201614thInt.Conf. ICT K. Eng. (ICT&KE), 2016, pp. 77-83.
18. M.D.Leoni,W.M.VanDerAalst,andB.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.