ISSN: 2454-9940

INTERNATIONAL JOURNAL OF APPLIED SCIENCE ENGINEERING AND MANAGEMENT

E-Mail :
editor.ijasem@gmail.com
editor@ijasem.org

www.ijasem.org

INTERNATIONAL JOURNAL OF APPLIED SCIENCE ENGINEERING AND MANAGEMENT

ISSN2454-9940
www.ijasem.org
Vol 18, Issue.2 April 2024

A MULTI-PRESPECTIVE FRAUD DETECTION METHOD FOR MULTI-PARTICIPANT ECOOMERCE TRANSACTIONS

Gulla Rakesh [1], Ramsetty Sai Krishna [2],
Kurri Vamshikrishna [3], Dr. B.V.Krishnaveni[4]
[1,2,3] UG Student, Dept. of ECE, CMR Institute of Technology, Hyderabad
[4] Associate Professor, Dept. of ECE,
CMR Institute of Technology, Hyderabad

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

ITH 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

ISSN2454-9940
www.ijasem.org
Vol 18, Issue.2 April 2024

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 multiperspective 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 REVIEW

INNOVATIVE TOOLKIT FOR FORMING AN EPS PORTFOLIO FOR ELECTRONIC TRADING PLATFORMS

ISSN2454-9940
www.ijasem.org
Vol 18, Issue.2 April 2024

When companies enter the e-commerce market, choosing an electronic payment system that fits well with the way they do business is relevant and one of the main concerns. Realizing this, almost all stakeholders are studying the different types of electronic payment systems and the challenges associated with electronic payment systems and digital currency. This study is aimed at outlining innovative tools for forming a portfolio of electronic payment systems for modern trading platforms in the e-commerce market. Achieving this goal involves solving a number of tasks, in particular highlighting the features of the application of electronic payment systems and the criteria that form the basis of the formation of an effective electronic payment systems (EPS) portfolio. Within the framework of this study, multi-criteria optimization using fuzzy logic methods was applied as a decision-making method to help trading platforms make decisions regarding the evaluation of EPS efficiency and the formation and management of a portfolio of electronic payment systems among a wide range of possible options. The research results demonstrate the high effectiveness of fuzzy logic methods, in particular Fuzzy TOPSIS, to achieve the research goal. The conclusions and recommendations formed will be useful both from a theoretical and a practical point of view for representatives of e-commerce and the scientific society in order to develop the methodology for managing electronic payment systems.

Consumer Privacy Protection With the Growth of AI-Empowered Online Shopping Based on the Evolutionary Game Model

Social distancing due to the COVID-19 pandemic has driven some consumers to online shopping, and concerns about pandemic risks and personal hygiene have increased the demand for e-commerce. Providing personalized recommendations seems quite profitable for e-commerce platforms, and consumers also benefit from personalized content with the advancement of AI technologies. However, this possible win-win situation is marred by the increase in consumers' privacy concerns. Technical solutions have been widely studied to protect consumer privacy, while few analyses have been conducted from the perspective of psychological and behavioral implications. In this paper, an evolutionary game model of privacy protection between e-commerce platforms and consumers is established to determine the mechanisms by which various factors

ISSN2454-9940
www.ijasem.org
Vol 18, Issue.2 April 2024

exert influence, and evolutionary stable strategies are obtained from equilibrium points. Then, the strategy selections are simulated with MATLAB 2020 software. Based on the results, the following conclusions are drawn: (1) the application of AI technologies in e-commerce will fundamentally benefit consumers, which makes them actively share personal information with e-commerce platforms with incentives for generous rewards; (2) it is profitable for e-commerce platforms to conduct data mining by improving the ability to use AI technologies and making efforts to reduce technical costs; and (3) regulators should improve the level of supervision instead of imposing a large penalty to enhance consumer trust, which could effectively increase the profits of e-commerce platforms and protect consumers' privacy.

Impact of E-Commerce and Digital Marketing Adoption on the Financial and Sustainability Performance of MSMEs during the COVID-19 Pandemic: An Empirical Study

The COVID-19 pandemic has remarkably affected the business processes and performance of micro-, small-, and medium-sized enterprises (MSMEs) across the world. MSMEs have had to adopt and implement numerous strategies to sustain their businesses, and their financial and sustainability performance has been impacted by their choice of e-commerce (EC) platforms and digital marketing (DM) strategies. The objective of this research was to explore the effects of EC and DM platforms and strategies on facilitating MSMEs' financial and sustainability performance amid the devastating COVID-19 pandemic. This study gathered data from 212 MSMEs from three districts of Bangladesh. A partial least squares structural equation modeling (PLS-SEM) approach was undertaken, to test the hypothesized model. The findings revealed that e-commerce had a significant association with MSMEs' financial performance and sustainability amid the pandemic. It was also observed that digital marketing strategies had a substantial impact on MSMEs' financial performance. However, the linkage between DM strategies and MSMEs' sustainability was found to be insignificant. Furthermore, it was found that the financial performance of MSMEs mediated the relationship between e-commerce adoption and their sustainability performance. These findings contribute to the extant technology adoption literature, by exploring the role of e-commerce and digital marketing on

ISSN2454-9940
www.ijasem.org
Vol 18, Issue.2 April 2024

firms' financial outcomes amid a global pandemic. Managers and policymakers of small businesses can learn several things from this study, and understand how crucial digital commerce and digital marketing are to their success and long-term survival.

National Payment Switches and the Power of Cognitive Computing against Fintech Fraud

National Payment Switches (NPSs) and International Payment Switches (IPSs), including major players such as SWIFT, Mastercard, and CHIPS, have become vital to the financial infrastructure, facilitating secure and efficient transactions among local financial institutions. Nonetheless, the growing adoption of digital payments has heightened the risk of financial fraud. Consequently, NPSs, under the direct ownership of Central Banks (CBs), are increasingly adopting advanced technologies, such as cognitive computing, to bolster their fraud detection capabilities in their respective countries. This article delves into the role of cognitive computing in detecting financial fraud within NPSs. It examines the advantages of cognitive computing in recognising patterns of fraudulent behaviour and analysing vast amounts of data. Additionally, the study highlights the importance of focusing on how cognitive computing can augment traditional fraud detection methods, such as rule-based systems and data analytics.

Nineteen real-world cases from eighteen countries are analysed, exploring the cognitive computing tools employed by NPSs to identify fraudulent transactions. The challenges and limitations of implementing cognitive computing in fraud detection and potential solutions to address these issues are identified. The primary assumption that cognitive computing is crucial for detecting financial fraud in NPSs is substantiated. Its ability to analyse large datasets and pinpoint patterns of fraudulent behaviour proves invaluable for financial institutions seeking to protect themselves against financial fraud in a progressively digital world. The conclusions drawn from the overview of the cases aim to identify best practices, potentially trigger new benchmarking standards, and facilitate the development of integrated cross-border solutions to combat financial fraud on a global scale effectively. The purpose of this research is to examine the role of cognitive computing in detecting financial fraud within NPSs, identify its advantages, challenges and limitations, and provide real-world case examples.

ISSN2454-9940
www.ijasem.org
Vol 18, Issue.2 April 2024

Systemic Acquired Critique of Credit Card Deception Exposure through Machine Learning

A wide range of recent studies are focusing on current issues of financial fraud, especially concerning cybercrimes. The reason behind this is even with improved security, a great amount of money loss occurs every year due to credit card fraud. In recent days, ATM fraud has decreased, while credit card fraud has increased. This study examines articles from five foremost databases. The literature review is designed using extraction by database, keywords, year, articles, authors, and performance measures based on data used in previous research, future research directions and purpose of the article. This study identifies the crucial gaps which ultimately allow research opportunities in this fraud detection process by utilizing knowledge from the machine learning domain. Our findings prove that this research area has become most dominant in the last ten years. We accessed both supervised and unsupervised machine learning techniques to detect cybercrime and management techniques which provide evidence for the effectiveness of machine learning techniques to control cybercrime in the credit card industry. Results indicated that there is room for further research to obtain better results than existing ones on the basis of both quantitative and qualitative research analysis.

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]. Xuetong 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.

ISSN2454-9940
www.ijasem.org
Vol 18, Issue.2 April 2024

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].

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

ISSN2454-9940
www.ijasem.org
Vol 18, Issue.2 April 2024

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.

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

ISSN2454-9940
www.ijasem.org
Vol 18, Issue.2 April 2024

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, 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.

ISSN2454-9940
www.ijasem.org
Vol 18, Issue.2 April 2024

[9] Karne, R. K. ., & Sreeja, T. K. . (2023). PMLC- Predictions of Mobility and Transmission in a Lane-Based Cluster VANET Validated on Machine Learning. International Journal on Recent and Innovation Trends in Computing and Communication, 11(5s), 477–483. https://doi.org/10.17762/ijritcc.v11i5s.7109

[10] Radha Krishna Karne and Dr. T. K. Sreeja (2022), A Novel Approach for Dynamic Stable Clustering in VANET Using Deep Learning (LSTM) Model. IJEER 10(4), 1092-1098. DOI: 10.37391/IJEER.100454.

[11] Reddy, Kallem Niranjan, and Pappu Venkata Yasoda Jayasree. "Low Power Strain and Dimension Aware SRAM Cell Design Using a New Tunnel FET and Domino Independent Logic." International Journal of Intelligent Engineering & Systems 11, no. 4 (2018).

[12] Reddy, K. Niranjan, and P. V. Y. Jayasree. "Design of a Dual Doping Less Double Gate Tfet and Its Material Optimization Analysis on a 6t Sram Cells."

[13] Reddy, K. Niranjan, and P. V. Y. Jayasree. "Low power process, voltage, and temperature (PVT) variations aware improved tunnel FET on 6T SRAM cells." Sustainable Computing: Informatics and Systems 21 (2019): 143-153.

[14] Reddy, K. Niranjan, and P. V. Y. Jayasree. "Survey on improvement of PVT aware variations in tunnel FET on SRAM cells." In 2017 International Conference on Current Trends in Computer, Electrical, Electronics and Communication (CTCEEC), pp. 703-705. IEEE, 2017