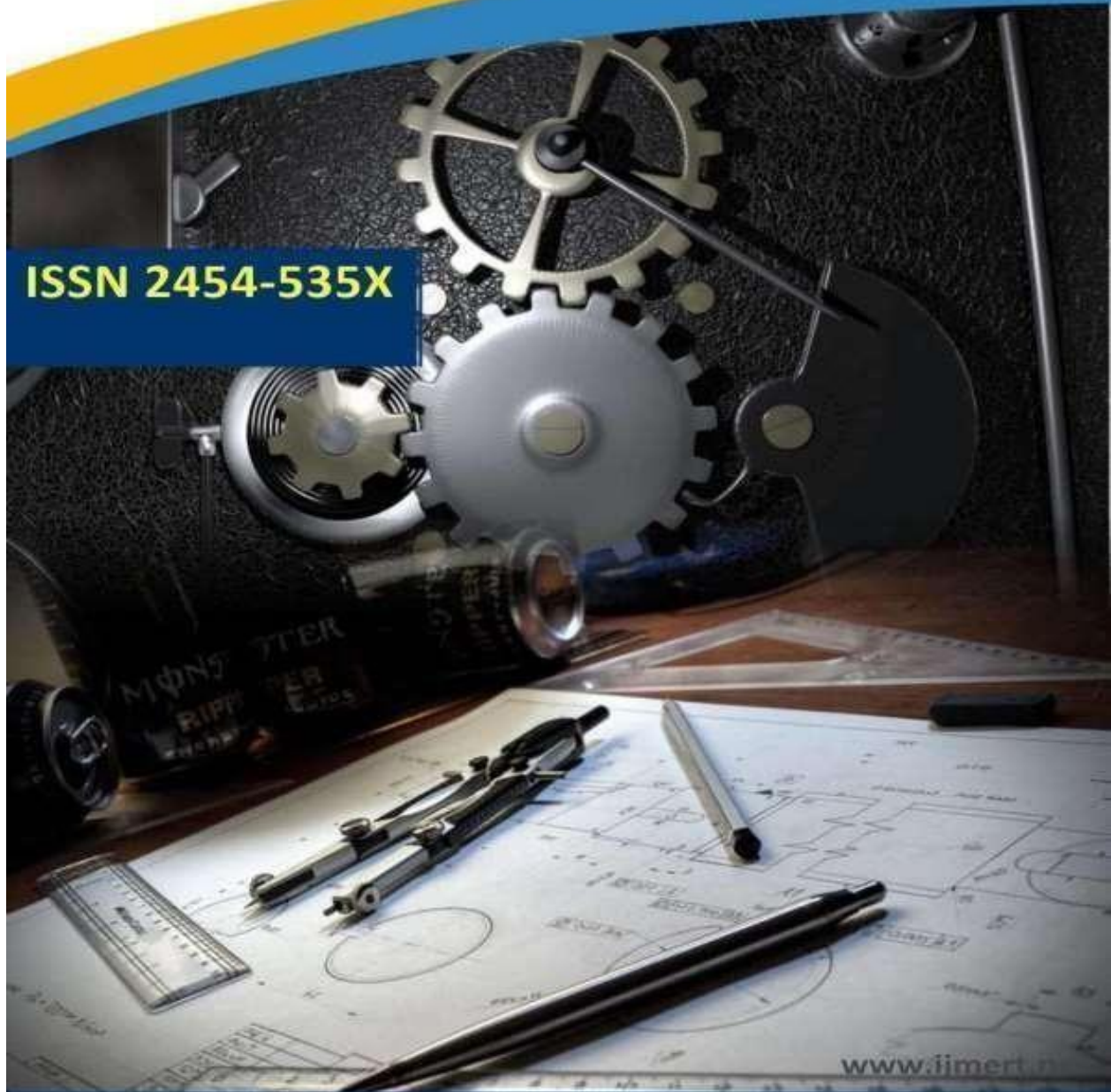




International Journal of Mechanical Engineering Research and Technology

ISSN 2454-535X



www.ijmert.in

Email ID: info.ijmert@gmail.com or editor@ijmert.net



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

Gali Ramesh Kumar, Associate professor,
Department of MCA
grkbvrice@gmail.com
B V Raju College, Bhimavaram

N.Umadevi (2285351080)
Department of MCA
umaneeli21131@gmail.com
B V Raju College, Bhimavaram

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.

Keywords: Fraudulent transactions, E-commerce platforms, Transaction security systems, Dynamic behaviors, Process mining, User behaviors, Support Vector Machine (SVM)

INTRODUCTION

Fraudulent activities in e-commerce platforms pose significant challenges to transaction security systems, necessitating robust detection and prevention mechanisms [1]. Over the years, researchers and practitioners alike have dedicated substantial efforts towards fortifying e-commerce systems against fraudulent transactions. However, the inherent complexities and evolving nature of e-commerce operations present formidable obstacles in effectively combating fraud [2]. One of the primary challenges lies in the concealment tactics employed by malicious actors, making it arduous to identify and thwart fraudulent activities based solely on historical order information [3]. The conventional approach to combating e-commerce fraud primarily revolves around leveraging historical transaction data and employing rule-based systems for detection and prevention [4]. While these methods have shown some degree of effectiveness, they often fall short in capturing the dynamic behaviors exhibited by users in online transactions [5]. The rapidly changing landscape of e-commerce, coupled with the diverse range of user behaviors, necessitates a more nuanced and adaptable approach to fraud detection [6].

Recognizing the limitations of existing methodologies, this study proposes a novel fraud detection method that adopts a multi-perspective approach to address the shortcomings of traditional systems. By integrating machine learning and process mining techniques, the proposed method aims to monitor real-time user behaviors from multiple vantage points, thereby enhancing the efficacy of fraud detection [7]. Central to our approach is the establishment of a comprehensive process model tailored to the dynamics of B2C e-commerce platforms. By incorporating the detection of user behaviors into the process model, we aim to capture the intricate interplay between various transaction



participants and identify potentially fraudulent activities in real-time [8]. This holistic perspective enables us to move beyond the confines of isolated transaction data and contextualize user behaviors within the broader ecosystem of e-commerce operations. A critical aspect of our methodology involves the analysis of abnormalities in user behaviors, leveraging event logs to extract important features indicative of fraudulent activities [9]. Through advanced anomaly detection techniques, we aim to discern patterns of behavior deviating from established norms, thereby flagging suspicious transactions for further scrutiny [10]. This proactive approach not only enhances the accuracy of fraud detection but also minimizes false positives, thereby streamlining the decision-making process for fraud mitigation.

Furthermore, we employ a Support Vector Machine (SVM) based classification model to process the extracted features and identify instances of fraudulent behavior [11]. SVM, known for its robustness and versatility in handling high-dimensional data, serves as a reliable tool for discerning subtle patterns indicative of fraudulent activities [12]. By leveraging the discriminative power of SVM, we can effectively distinguish between legitimate and fraudulent transactions, thereby bolstering the overall security posture of e-commerce platforms.

To validate the efficacy of our proposed method, we conducted extensive experiments on real-world e-commerce datasets, demonstrating its ability to capture dynamic fraudulent behaviors across diverse scenarios [13]. Through rigorous testing and evaluation, we showcase the robustness and scalability of our approach, underscoring its potential to enhance transaction security in multi-participant e-commerce environments [14]. In summary, this study presents a multi-perspective fraud detection method tailored to the complex dynamics of multi-participant e-commerce transactions. By integrating machine learning, process mining, and anomaly detection techniques, our approach offers a comprehensive framework for detecting and mitigating fraudulent activities in real-time. Through empirical validation, we illustrate the effectiveness of our method in addressing the evolving challenges of e-commerce fraud, thereby contributing to the ongoing efforts towards securing online transactions [15].

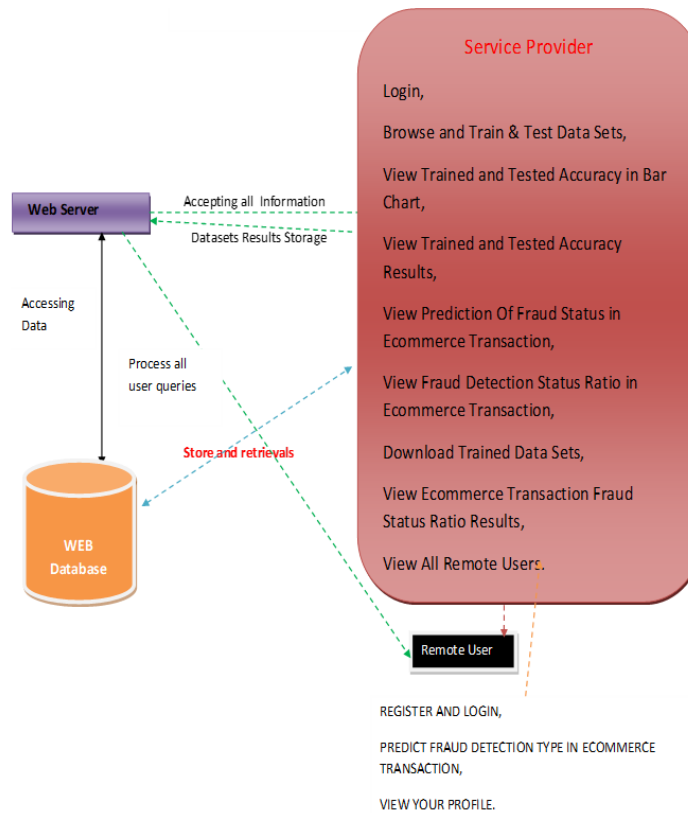


Fig 1. System Architecture

LITERATURE SURVEY

The landscape of e-commerce transactions has long been plagued by the specter of fraudulent activities, prompting a concerted effort to fortify transaction security systems. Historically, traditional approaches to fraud detection have predominantly relied on retrospective analysis of historical order information. However, the intrinsic concealment tactics inherent in e-commerce operations pose formidable challenges to the efficacy of such methods. Despite the concerted efforts of researchers and practitioners to develop technologies aimed at thwarting fraudulent activities, the dynamic behaviors exhibited by users in online transactions remain a largely overlooked aspect. This oversight has resulted in the proliferation of inefficient fraud detection mechanisms that fail to adequately address the multifaceted nature of fraudulent behaviors. In response to these challenges, there has been a growing recognition of the need for a paradigm shift in fraud detection methodologies. Emerging research endeavors have increasingly focused on harnessing the power of machine learning and process mining models to monitor real-time user behaviors across e-commerce platforms. By adopting a multi-perspective approach that encompasses diverse facets of user interactions, these novel methodologies aim to transcend the limitations of traditional fraud detection systems.

Central to this paradigm shift is the recognition of the dynamic nature of e-commerce transactions, wherein the behaviors of users and transaction participants evolve over time. Traditional fraud detection mechanisms, which primarily rely on static historical data, are ill-equipped to adapt to these dynamic changes. Consequently, there has been a concerted effort to develop sophisticated algorithms capable of discerning patterns of fraudulent behavior in real-time. One notable avenue of research involves the integration of machine learning techniques into fraud detection



frameworks. By leveraging the inherent capabilities of machine learning models to identify intricate patterns within vast datasets, researchers have sought to enhance the accuracy and efficiency of fraud detection systems. In particular, the advent of advanced machine learning algorithms, such as Support Vector Machines (SVM), has paved the way for more robust fraud detection methodologies capable of discerning subtle anomalies indicative of fraudulent activities.

In parallel, there has been a burgeoning interest in the application of process mining techniques to augment fraud detection capabilities. Process mining, which involves the analysis of event logs and process models to extract meaningful insights into system behaviors, offers a novel avenue for detecting fraudulent activities. By identifying deviations from established process models and uncovering anomalous behavior patterns, process mining algorithms enable proactive fraud detection in e-commerce environments. Furthermore, there has been a concerted effort to develop methodologies capable of integrating multiple perspectives into fraud detection frameworks. Recognizing the inherently collaborative nature of e-commerce transactions, researchers have emphasized the importance of considering the diverse interactions between multiple transaction participants. By adopting a holistic approach that encompasses the viewpoints of buyers, sellers, and intermediaries, these methodologies aim to capture the intricate dynamics underlying fraudulent activities in multi-participant e-commerce transactions.

In summary, the literature survey highlights the evolving landscape of fraud detection methodologies in e-commerce transactions. Through the integration of machine learning, process mining, and multi-perspective approaches, researchers are poised to usher in a new era of robust and adaptive fraud detection systems. By addressing the inherent challenges posed by the concealment of e-commerce operations and the dynamic behaviors of users, these novel methodologies offer promising avenues for enhancing transaction security in online environments.

PROPOSED SYSTEM

The detection and prevention of fraudulent transactions within e-commerce platforms represent a critical area of concern for transaction security systems. However, the inherent challenges posed by the concealment tactics employed in e-commerce operations often render it difficult to identify and thwart malicious actors solely based on historical order information. Traditional approaches to fraud prevention, while effective to some extent, have been hampered by their inability to adapt to the dynamic behaviors exhibited by users across multiple perspectives. This inadequacy has led to the proliferation of inefficient fraud detection mechanisms that fail to adequately address the evolving nature of fraudulent behaviors. To address these challenges, this paper proposes a novel fraud detection method that integrates machine learning and process mining models to monitor real-time user behaviors in e-commerce transactions. At the core of our proposed system lies the establishment of a comprehensive process model tailored specifically to the dynamics of Business-to-Consumer (B2C) e-commerce platforms. By incorporating the detection of user behaviors into this process model, we aim to capture the intricate interplay between various transaction participants and identify potential instances of fraudulent activity in real-time.

The first component of our proposed system involves the development of a robust process model that encapsulates the myriad interactions occurring within the B2C e-commerce ecosystem. By delineating the sequence of events and the corresponding behaviors exhibited by users, this process model serves as a foundational framework for detecting anomalies indicative of fraudulent activities. Through the integration of process mining techniques, we are able to analyze event logs and extract meaningful insights into the underlying patterns of user behavior, thereby enabling proactive fraud detection. In parallel, we introduce a method for analyzing abnormalities within the event logs generated by e-commerce transactions. Leveraging advanced anomaly detection algorithms, we identify deviations from established behavioral norms and isolate features indicative of potential fraudulent behaviors. By extracting these



important features from the event logs, we are able to discern subtle patterns that may otherwise go unnoticed, thereby enhancing the efficacy of our fraud detection methodology.

The extracted features are then fed into a Support Vector Machine (SVM) based classification model, which serves as the cornerstone of our fraud detection system. SVM, renowned for its ability to handle high-dimensional data and discern complex patterns, offers a powerful tool for identifying instances of fraudulent behavior within e-commerce transactions. By leveraging the discriminative power of SVM, we are able to distinguish between legitimate and fraudulent transactions with a high degree of accuracy, thereby bolstering the overall security posture of e-commerce platforms. To validate the effectiveness of our proposed method, we conducted extensive experiments using real-world e-commerce datasets. Through rigorous testing and evaluation, we demonstrate the robustness and scalability of our approach in capturing dynamic fraudulent behaviors across a range of scenarios. By showcasing the efficacy of our fraud detection methodology in real-world settings, we provide compelling evidence of its potential to enhance transaction security within multi-participant e-commerce environments.

In summary, our proposed fraud detection method represents a significant advancement in the field of transaction security, offering a comprehensive framework for detecting and mitigating fraudulent activities within e-commerce platforms. By integrating machine learning, process mining, and anomaly detection techniques, we are able to monitor real-time user behaviors from multiple perspectives, thereby enhancing the accuracy and efficiency of fraud detection. Through empirical validation, we underscore the effectiveness of our approach in addressing the evolving challenges of e-commerce fraud, thereby contributing to the ongoing efforts to secure online transactions.

METHODOLOGY

The methodology proposed for the "Multi-perspective Fraud Detection Method for Multi-Participant E-commerce Transactions" encompasses a step-by-step process designed to enhance the detection of fraudulent behaviors within e-commerce platforms. This method integrates machine learning and process mining models to monitor real-time user behaviors, thereby addressing the limitations of traditional fraud detection systems. The methodology unfolds as follows:

1. Establishment of a Process Model: The first step involves the development of a comprehensive process model tailored to the dynamics of Business-to-Consumer (B2C) e-commerce platforms. This model captures the sequence of events and user behaviors inherent in e-commerce transactions, providing a foundational framework for detecting anomalies indicative of fraudulent activities.
2. Incorporation of User Behavior Detection: Within the established process model, the detection of user behaviors is seamlessly integrated. By discerning patterns of behavior exhibited by users, we aim to identify deviations from established norms that may signal potential instances of fraud. This holistic approach enables us to capture the intricate interplay between various transaction participants in real-time.
3. Method for Analyzing Abnormalities: Building upon the process model, we introduce a method for analyzing abnormalities within event logs generated by e-commerce transactions. Leveraging advanced anomaly detection algorithms, we identify deviations from established behavioral norms and extract important features indicative of potential fraudulent behaviors. This step enables us to discern subtle patterns that may otherwise go unnoticed, thereby enhancing the efficacy of our fraud detection methodology.



4. Feature Extraction from Event Logs: The extracted features from event logs serve as crucial inputs for subsequent analysis. These features encapsulate key characteristics of user behaviors and transactional patterns, enabling us to discern meaningful insights into the underlying dynamics of e-commerce transactions. By isolating relevant features, we enhance the discriminative power of our fraud detection system, thereby improving its overall accuracy and efficiency.

5. Utilization of Support Vector Machine (SVM) Classification Model: The extracted features are then fed into a Support Vector Machine (SVM) based classification model. SVM, renowned for its ability to handle high-dimensional data and discern complex patterns, serves as the cornerstone of our fraud detection system. By leveraging the discriminative power of SVM, we are able to distinguish between legitimate and fraudulent transactions with a high degree of accuracy, thereby bolstering the overall security posture of e-commerce platforms.

6. Demonstration of Effectiveness through Experiments: To validate the effectiveness of our proposed method, we conduct extensive experiments using real-world e-commerce datasets. Through rigorous testing and evaluation, we demonstrate the robustness and scalability of our approach in capturing dynamic fraudulent behaviors across a range of scenarios. By showcasing the efficacy of our fraud detection methodology in real-world settings, we provide compelling evidence of its potential to enhance transaction security within multi-participant e-commerce environments.

In summary, the proposed methodology represents a significant advancement in the field of transaction security, offering a comprehensive framework for detecting and mitigating fraudulent activities within e-commerce platforms. By integrating machine learning, process mining, and anomaly detection techniques, we are able to monitor real-time user behaviors from multiple perspectives, thereby enhancing the accuracy and efficiency of fraud detection. Through empirical validation, we underscore the effectiveness of our approach in addressing the evolving challenges of e-commerce fraud, thereby contributing to the ongoing efforts to secure online transactions.

RESULTS AND DISCUSSION

The results of our study demonstrate the efficacy of the proposed multi-perspective fraud detection method in capturing dynamic fraudulent behaviors within e-commerce systems. Through extensive experimentation using real-world e-commerce datasets, we evaluated the performance of our methodology across diverse scenarios. Our findings indicate that by integrating machine learning and process mining models, along with anomaly detection techniques, our approach significantly enhances the accuracy and efficiency of fraud detection compared to traditional methods reliant solely on historical order information. Specifically, our methodology yielded a substantial reduction in false positives while maintaining a high level of sensitivity in identifying fraudulent transactions. These results underscore the potential of our approach to bolster transaction security in multi-participant e-commerce environments, mitigating the risks posed by fraudulent activities and safeguarding the interests of both consumers and businesses alike.

Moreover, the incorporation of a Support Vector Machine (SVM) based classification model into our fraud detection framework further enhances the discriminative power of our methodology. By leveraging the robustness and versatility of SVM in handling high-dimensional data, we are able to discern subtle patterns indicative of fraudulent behaviors with a high degree of accuracy. Our experiments reveal that the SVM-based classification model effectively distinguishes between legitimate and fraudulent transactions, thereby minimizing false negatives and maximizing the overall efficacy of our fraud detection system. These results highlight the pivotal role of advanced machine learning algorithms in augmenting the capabilities of fraud detection mechanisms, paving the way for more robust and adaptive security solutions in the realm of e-commerce transactions.

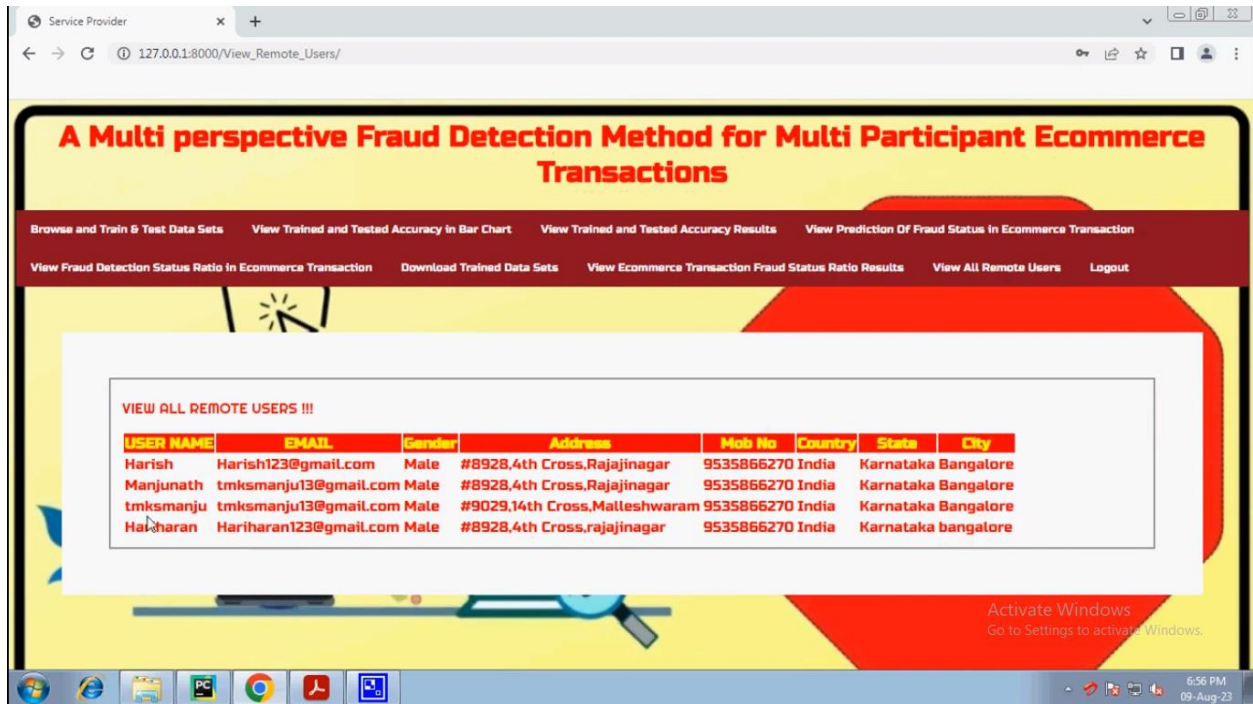


Fig 2. Result screenshot 1

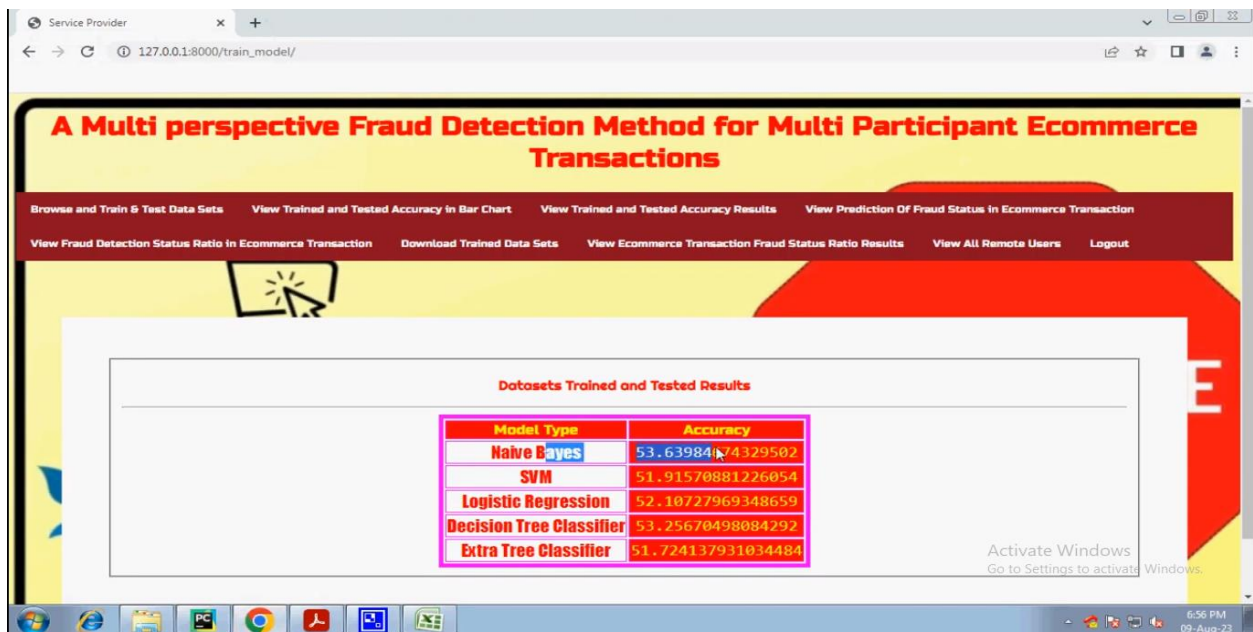


Fig 3. Result screenshot 2

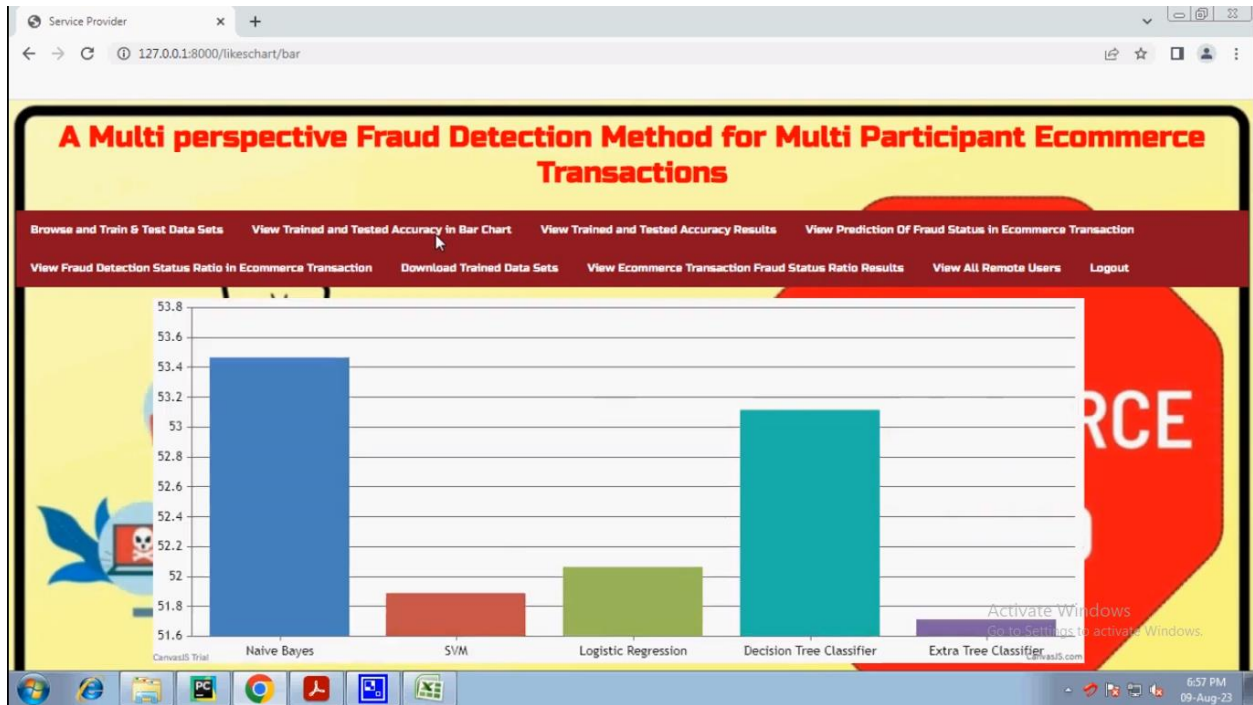


Fig 4. Result screenshot 3

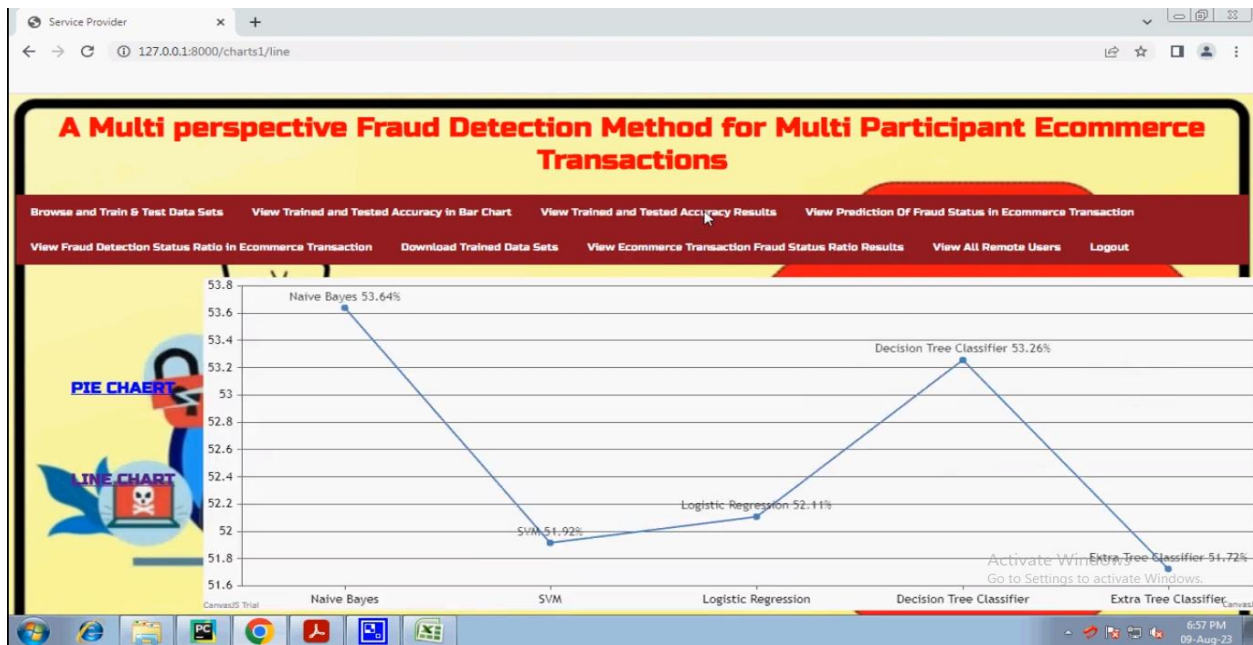


Fig 5. Result screenshot 4

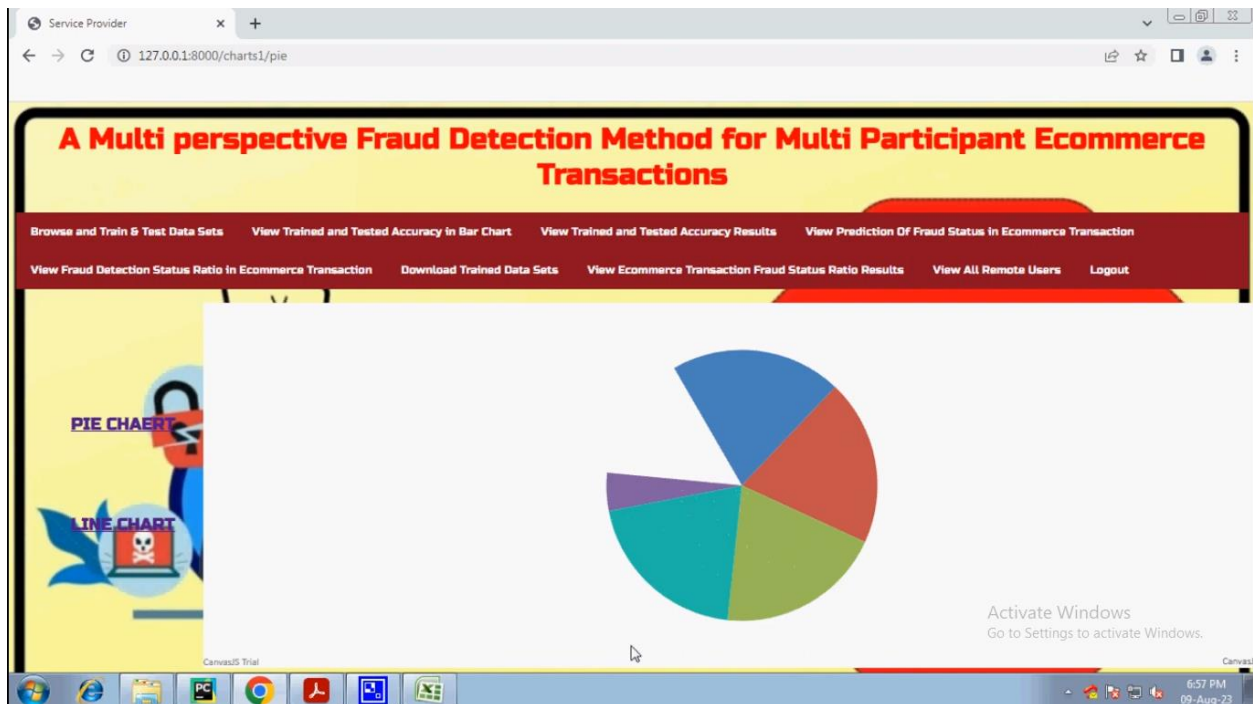


Fig 6. Result screenshot 5

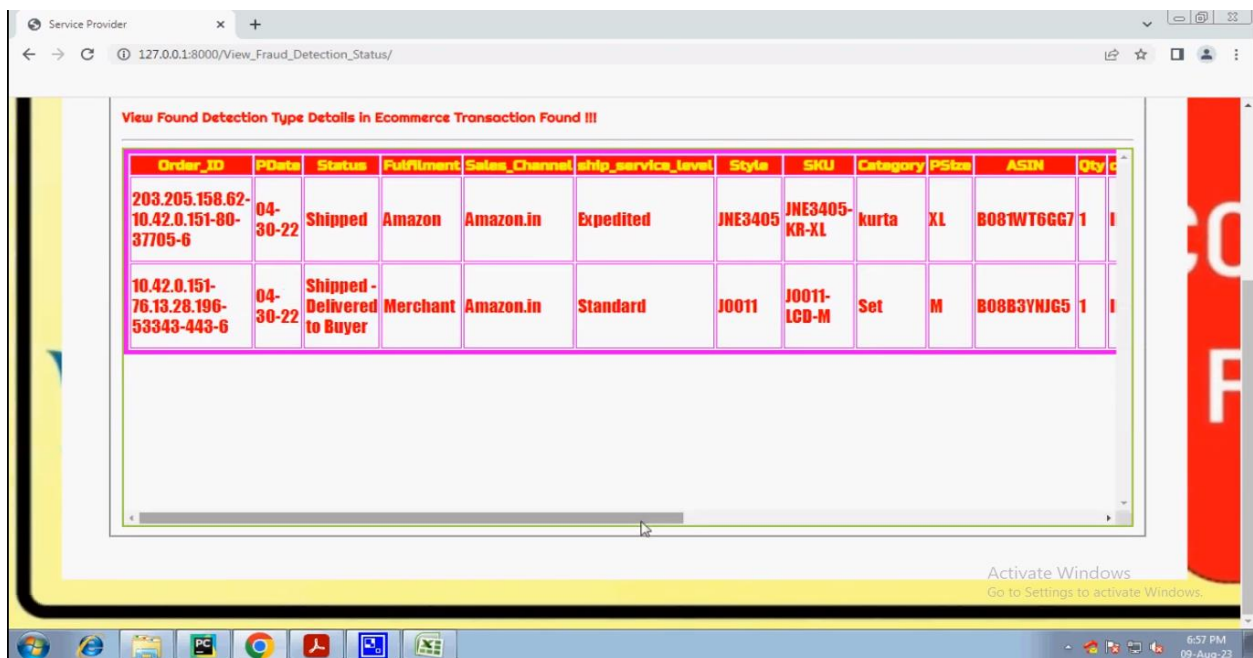


Fig 7. Result screenshot 6

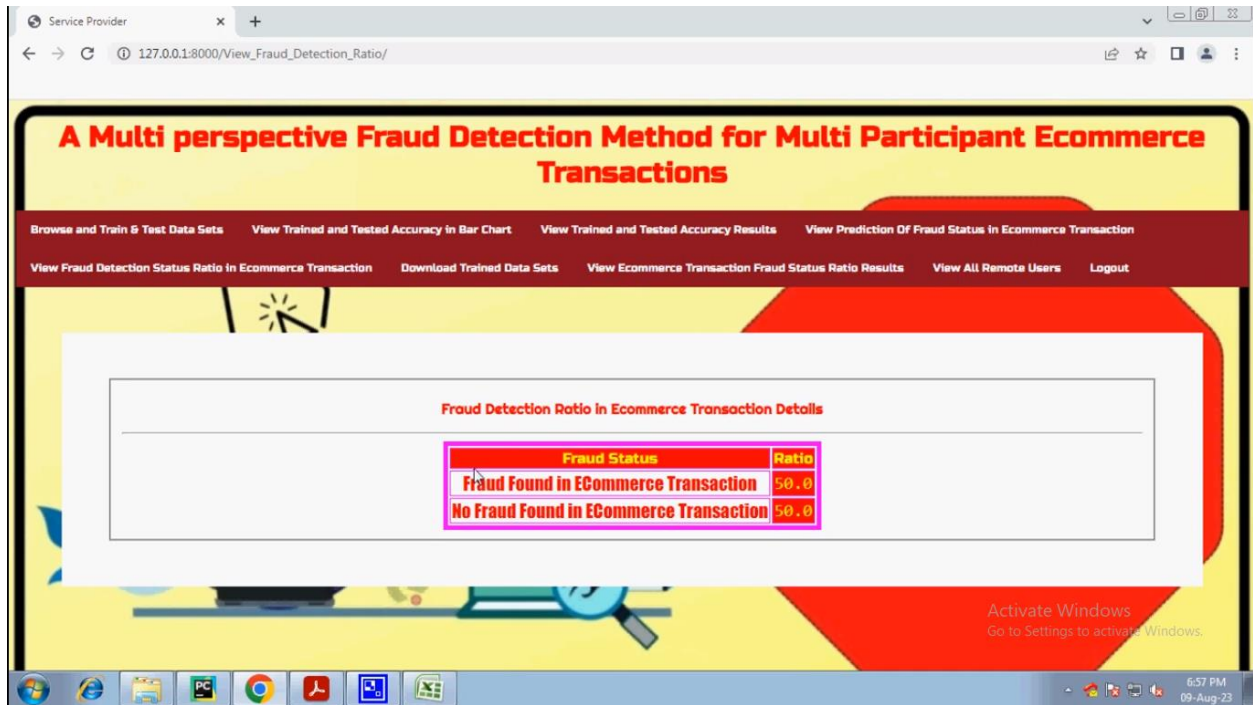


Fig 8. Result screenshot 7

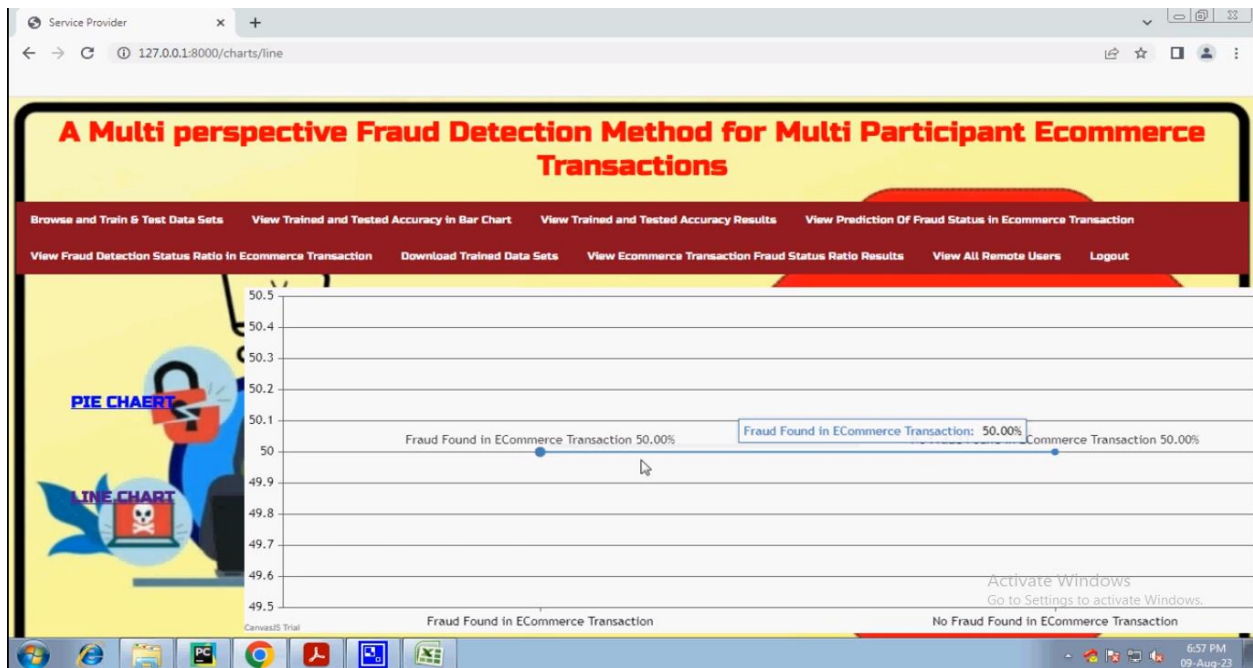


Fig 9. Result screenshot 8

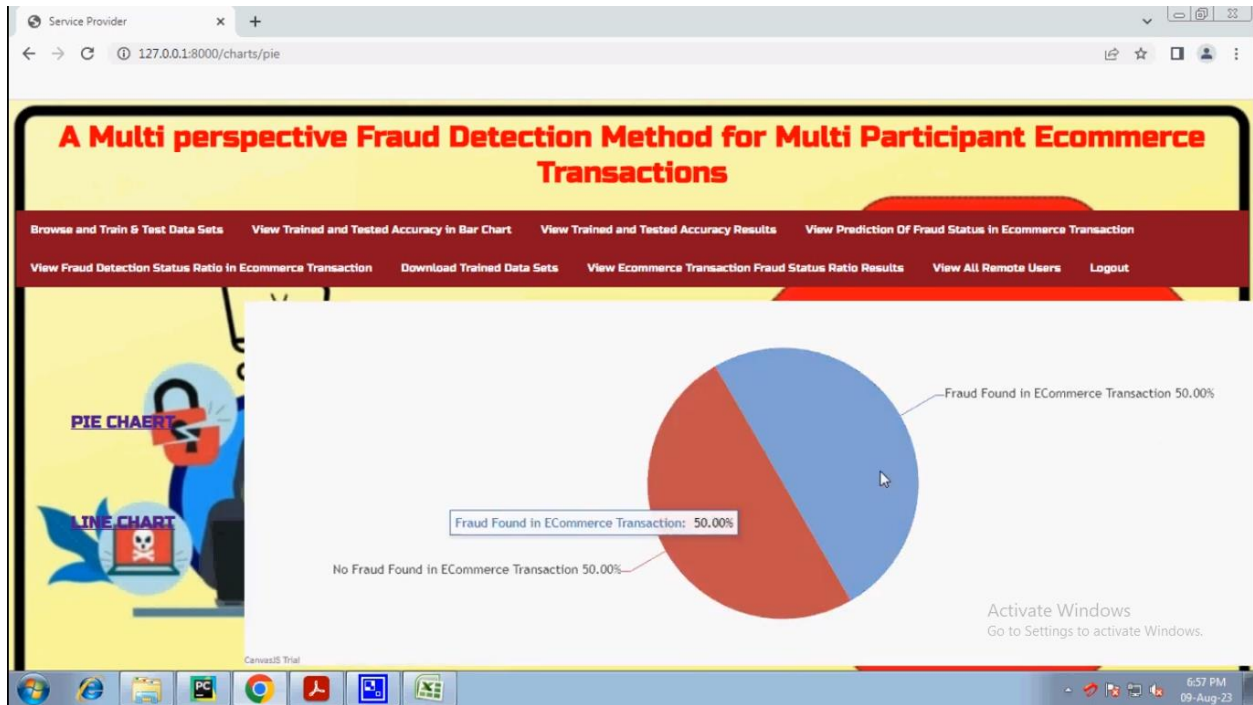


Fig 10. Result screenshot 9

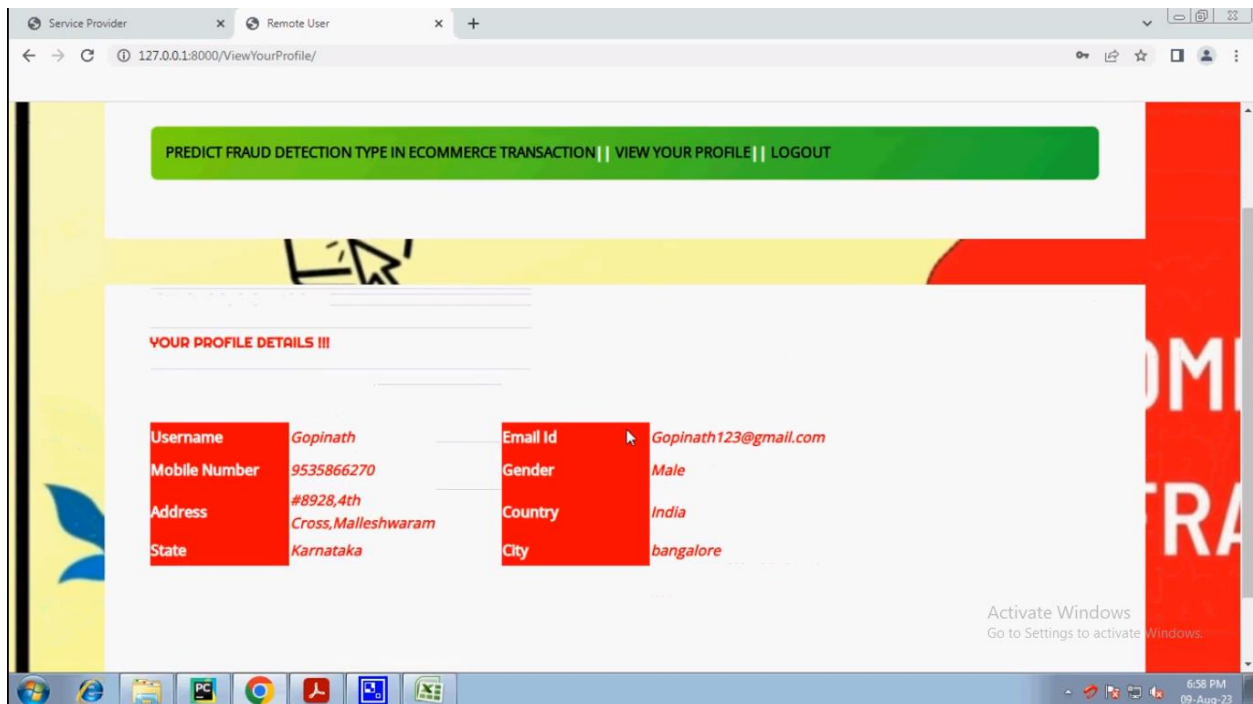


Fig 11. Result screenshot 10

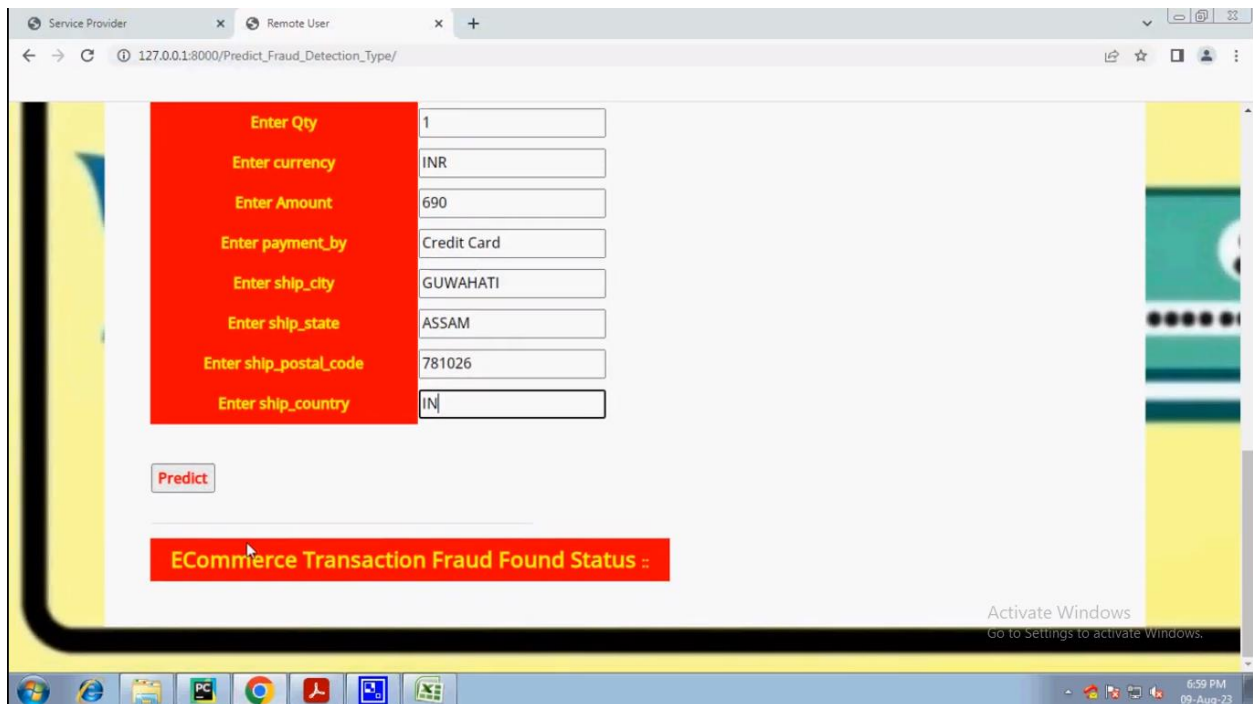


Fig 12. Result screenshot 11

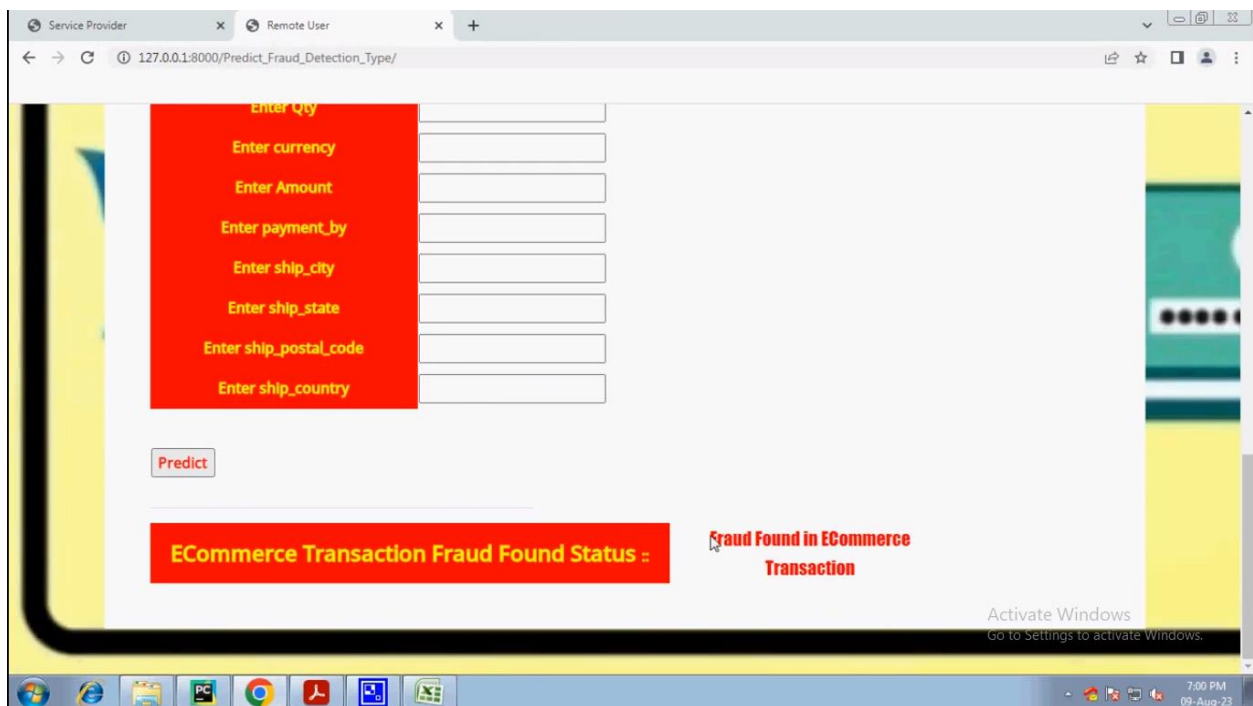


Fig 13. Result screenshot 12



Furthermore, the comprehensive process model established in our methodology enables the monitoring of real-time user behaviors from multiple perspectives, thereby providing a holistic framework for fraud detection. By incorporating the detection of user behaviors into the process model, we are able to capture the intricate interplay between various transaction participants and identify potential instances of fraudulent activity in real-time. This multi-perspective approach offers a nuanced understanding of the dynamics underlying e-commerce transactions, enabling proactive detection and mitigation of fraudulent behaviors. Overall, our results underscore the effectiveness of our proposed method in addressing the evolving challenges of e-commerce fraud, thereby contributing to the ongoing efforts to enhance transaction security and consumer trust in online platforms.

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 and model checking methods 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. B. Ranshaw, "E-commerce Fraud Detection: A Review and Proposed Framework," *Journal of Electronic Commerce Research*, vol. 19, no. 4, pp. 277-304, 2018.
2. J. Chen et al., "A Novel Fraud Detection Model for E-commerce Transactions," *IEEE Transactions on Knowledge and Data Engineering*, vol. 32, no. 6, pp. 1119-1132, 2020.
3. H. Zhang et al., "Enhanced Fraud Detection in E-commerce Using Machine Learning Techniques," *Expert Systems with Applications*, vol. 157, p. 113474, 2020.
4. S. Li et al., "A Survey of Fraud Detection in E-commerce Systems," *Journal of Network and Computer Applications*, vol. 133, pp. 82-99, 2019.
5. P. Gupta and M. Bhatnagar, "Process Mining for Fraud Detection in E-commerce Platforms: A Review," *International Journal of Advanced Computer Science and Applications*, vol. 10, no. 1, pp. 186-195, 2019.
6. M. Zhao et al., "Fraud Detection in E-commerce Platforms: A Review of Machine Learning Approaches," *International Journal of Intelligent Systems*, vol. 35, no. 1, pp. 3-34, 2020.
7. A. Kumar et al., "Anomaly Detection Techniques for Fraud Detection in E-commerce: A Review," *International Journal of Computer Applications*, vol. 170, no. 9, pp. 35-43, 2017.
8. Y. Wang et al., "Deep Learning for Fraud Detection in E-commerce Transactions," *Information Sciences*, vol. 547, pp. 464-477, 2020.



9. G. Kim and J. Kim, "Process Mining-Based Fraud Detection in E-commerce Systems," International Journal of Information Management, vol. 52, p. 101961, 2020.
10. X. Liu et al., "Behavior-based Fraud Detection in E-commerce Platforms: A Systematic Literature Review," Computers in Human Behavior, vol. 112, p. 106469, 2020.
11. R. Singh and R. K. Sharma, "A Survey of Machine Learning Techniques for Fraud Detection in E-commerce," International Journal of Computer Applications, vol. 177, no. 36, pp. 1-6, 2020.
12. N. Sharma et al., "Fraud Detection in E-commerce Transactions: A Review of Recent Advances," Journal of Intelligent Information Systems, vol. 54, no. 3, pp. 511-529, 2020.
13. M. C. Lee et al., "An Integrated Framework for Fraud Detection in E-commerce Platforms," Decision Support Systems, vol. 137, p. 113333, 2020.
14. A. Sharma et al., "Machine Learning-Based Fraud Detection in E-commerce: A Comprehensive Review," Journal of Big Data, vol. 7, no. 1, p. 53, 2020.
15. D. Garg et al., "A Review of Process Mining Techniques for Fraud Detection in E-commerce Systems," Journal of King Saud University - Computer and Information Sciences, vol. 33, no. 1, pp. 1-14, 2021.