Integrating Diverse Analytical Models for Enhanced Fraud Prevention in Collaborative E-Commerce Transactions

Neeli Sritha Rayal, Guduru Sreeja Reddy, Kamsali Lasya,
Gorle Sai Sree Varshini and Kota Lakshmi Prasana
Department of Computer Science and Engineering, Ravindra College of Engineering for Women, Kurnool 518002, Andhra Pradesh, India

Keywords: B2C e-Commerce, Support Vector Machine (SVM), Fraudulent Transactions, e-Commerce Platforms, Python, Django-ORM, Html, CSS, JavaScript. MySQL (WAMP Server).

Abstract: Traditional e-commerce transaction security systems have been designed to prevent and detect fraudulent transactions. Arresting the attackers only with the historical order information is difficult since e-commerce is hidden. There are many studies that aim to build technologies to prevent fraud, but they lack multi-angle perspectives on user behavioural evolution. Consequently, fraud detection is not very effective. To do so, this paper proposes a novel process-mining- and machine-learning-based model for user behaviour in real-time and its application in fraud detection. The user behaviour detection is the basis model on the B2C e-commerce platform. Second, an approach to identifying anomalies to derive meaningful aspects from event logs is proposed. The extracted features are then fed into a Support Vector Machine (SVM)-based classification model that identifies fraudulent activity. Through these experiments, we demonstrate the effectiveness of our proposed approach at capturing dynamic fraudulent behaviours in an e-commerce system.

1 INTRODUCTION

In recent years, new security threats have surfaced, despite the fact that the expansion of modern technologies and the growth of e-commerce present better opportunities for online businesses. According to reports, the substantial rise in online fraud cases costs billions of dollars annually on a global scale. Anti-fraud systems are now essential to ensuring the security of online transactions due to the Internet's dynamic and dispersed nature. When addressing new security threats, vulnerabilities are still identified by current fraud detection systems that concentrate on identifying unusual user behavior. The ineffective process management of current fraud detection systems during the trading process is a significant problem.

The monitoring function is one of the main problems that needs attention. Because process capture is missing from present work, the detection viewpoint is usually poor. To accomplish this, we propose a process perspective where historical big data is transformed into controllable data, and the process of user action is captured and scrutinized in real time. In addition, we combine a multi-perspective detection framework for detecting anomalous behaviours.

To overcome the limitations of the current procedure, this study proposes an innovative hybrid solution for anomaly detection on data flows based on all events in a control flow that incorporates both process mining and machine learning model benefits.

By analysing a model of an e-commerce system business process, this approach tries to dynamically detect changes in the users' behaviour, processes in the transaction, and noncompliance case. It can also analyse and detect fraudulent transactions from multiple dimensions.

2 EXISTING SYSTEM

The machine-learning-based techniques identify potentially risky offline or online transactions by classifying or predicting future observations based on previously acquired historical data. A comparison of machine-learning algorithm-based credit card fraud detection techniques was carried out by Xuetong Niu

Rayal, N. S., Reddy, G. S., Lasya, K., Varshini, G. S. S. and Prasana, K. L.
Integrating Diverse Analytical Models for Enhanced Fraud Prevention in Collaborative E-Commerce Transactions.
DOI: 10.5220/0013919200004919

In *Proceedings of the 1st International Conference on Research and Development in Information, Communication, and Computing Technologies (ICRDICCT'25 2025) - Volume 4*, pages 697-702
ISBN: 978-989-758-777-1

et al. On the dataset of credit card transactions, the majority of machine-learning models exhibit good performance. Furthermore, after further pre-processing, like eliminating outliers, supervised models outperform unsupervised models by a small margin.

The concept of identifying particular abnormal user behaviors to detect fraud is the basis for the widespread application layer deployment of credit card fraud detection. Because of its greater accuracy and coverage, the supervised learning algorithm is the most widely used learning technique in online fraud monitoring transactions. Recent studies have demonstrated the effectiveness of the machine learning approach in identifying fraudulent credit card transactions.

2.1 Drawbacks

1) Fraud mode one: A malicious actor modifies an order: The malicious actor may trick the victim merchant by posing as the cashier server and sending a phony formal payment order, order F A. By altering the order details, including the total amount, the malicious actor was able to obtain the order items that do not match the payment value.
2) The mode of fraud Second, the order is subcontracted: The victim pays the malicious actor's order rather than his own. The bad actors pose as buyers and sellers in order to accomplish their objectives. Before and after the payment, the order details are updated.

3 PROPOSED SYSTEM

The suggested system introduces a hybrid approach to anomaly detection in data flows, which gives details about every action embedded in a control flow model, combining the benefits of process mining and machine learning models. By simulating and examining the business process of the e-commerce system, this approach can thoroughly examine and identify fraudulent transactions from a variety of angles, as well as dynamically detect changes in user behaviors, transaction processes, and noncompliance situations. The following is a list of this paper's significant contributions:

1) To identify the anomalies in e-commerce transactions, a conformance checking technique based on process mining is used.
2) To carry out thorough anomaly detection based on Petri nets, a user behavior detection technique is suggested.
3) To automatically classify fraudulent behaviors, an SVM model is created by integrating multi-perspective process mining into machine learning techniques.

3.1 Advantages

The event log and the DPN are compared and analyzed using the plug-in Multi-Perspective Process Explorer and Conformance Checking to produce a more lucid outcome. This system displays the outcome, with various colors denoting each action. For example, purple indicates a move on the model only, grey indicates invisible actions, or skipped actions, and green indicates a move on both the model and the log. We can get the information that matches the model and the event log in the dataflow of each action by clicking on it. A mismatch is indicated by the red-marked data. We identify these questionable anomalies and utilize them as the foundation for further machine learning model training.

4 PRELIMINARY INVESTIGATION

The primary approach to project development begins with the idea of creating a mail-enabled platform for a small business that makes sending and receiving messages simple and convenient. It includes an address book, search engine, and some fun games. The first activity, or preliminary investigation, starts after it has been approved by the organization and our project guide.

There are three components to the activity:

- Request Clarification
- Feasibility Study
- Request Approval

4.1 Request Clarification

Once the project request has passed through an investigation and has been granted approval by the organization and project guide, the next step is to analyse the project request to determine exactly what the system requires. Thus, our project is primarily meant for those users of the company whose systems can be connected by LAN. These days, with men

constantly on the go, everything should be ready-made. Hence, its-development of the corresponding portal was based on the existing wide usage of the internet in daily life.

4.2 Request Approval

Not every project that is asked for is good or feasible. Some organizations receive excessive project requests by client users that make only a small percent that are acted on. Figure 2 shows the service provided. Such desirable and feasible projects, however, should be scheduled. When you approve a project request, you estimate its cost, priority, completion time and staffing needs; that information is then used to determine where the project request should fall on any project lists. In reality, development work can consider to begin after obtaining approval of the above listed factors. Figure 1 shows the Architecture diagram.

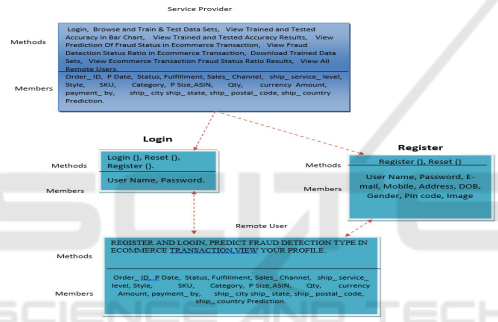

Figure 1: Architecture diagram.

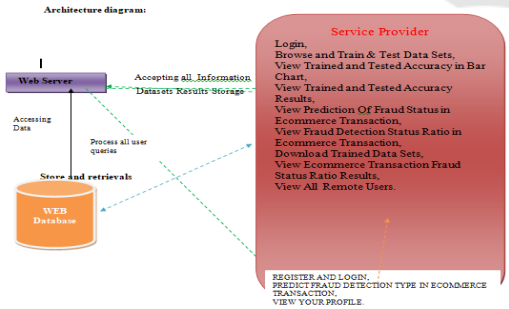

Figure 2: Service provided.

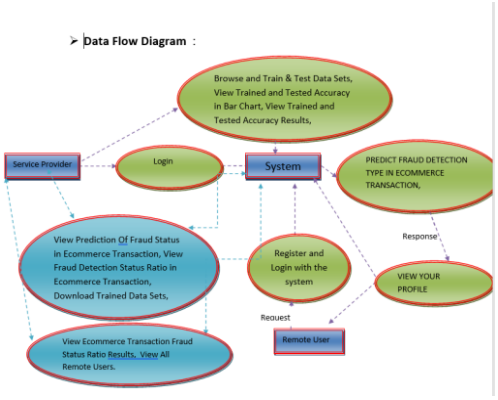

Figure 3: Data flow diagram.

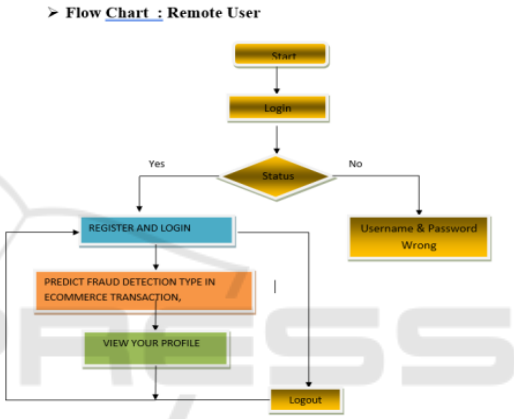

Figure 4: Remote user.

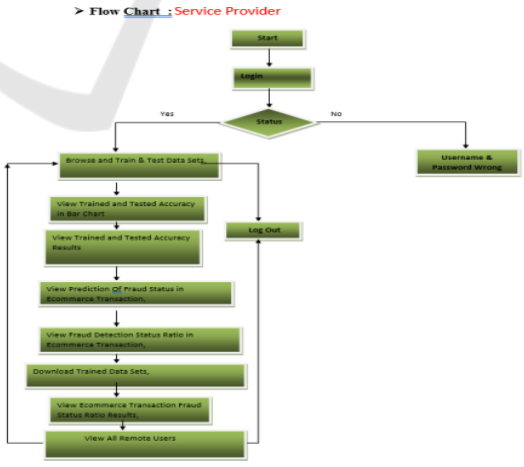

Figure 5: Service provider.

Figure 3 show the Data flow diagram which the below Figure 4 shows the Remote user and the Figure 5 illustrate the Service provider for the Request Approval.

5 IMPLEMENTATION METHODOLOGY

5.1 Service Provider

The Service Provider must log in to this module using a working user name and password. After successfully logging in, he can do various activities such as browsing and training and testing data sets. View Results of Trained & Tested Accuracy, View Trained & Tested Accuracy in Bar Chart, View the Fraud Detection Status Ratio in E-Commerce Transactions, View the Fraud prediction of Fraud Status in E-Commerce Transactions, Get Trained Data Sets Here E-Commerce Transactions + All Remote Users: Fraud Status Ratio Results

5.2 View and Authorize Users

This module allows the administrator to view a list of all registered users. There, the admin can view user details, such as name, email, and address, and also is able to assign users permission.

5.3 Remote User

This module consists of n present users. The user must register before conducting any operation. The data of the user would be stored in the database after registration. After a successful registration, he is to login using his password and authenticated user name. No after successful login user will able to REGISTER AND LOGIN, PREDICT FRAUD DETECTION TYPE IN ECOMMERCE TRANSACTION, VIEW YOUR PROFILE.

6 PYTHONS

Python is a high-level, interpreted, interactive and object-oriented scripting language. Python was designed to be readable. It has fewer syntactical constructions than other languages, and often uses English words as keywords while other languages use punctuation.

- Python is Interpreted: Python is processed at runtime by the interpreter. You do not need to compile your program before you can run it. Similar to PHP and PERL.

You are like Interactive Python: You could sit in front of a Python prompt and work straight though interpreter making your programs.

- Python is OOP: Python is defined as an object-oriented programming, which allows to encapsulate code into objects. Python is Great.

7 RESULTS

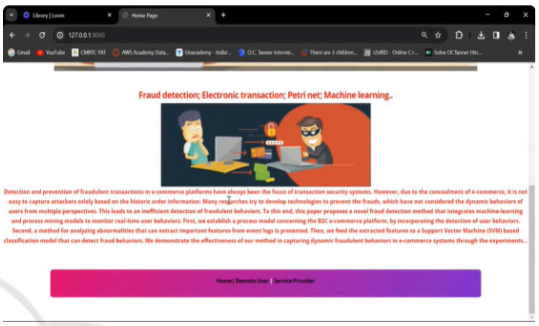

Figure 6: Run project software.

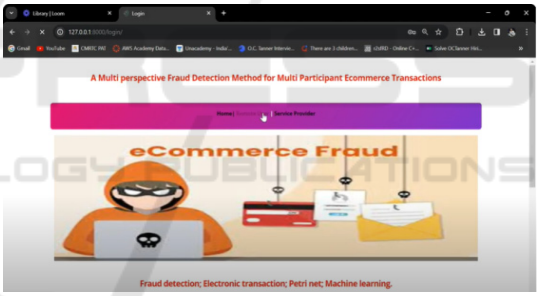

Figure 7: Open dashboard.

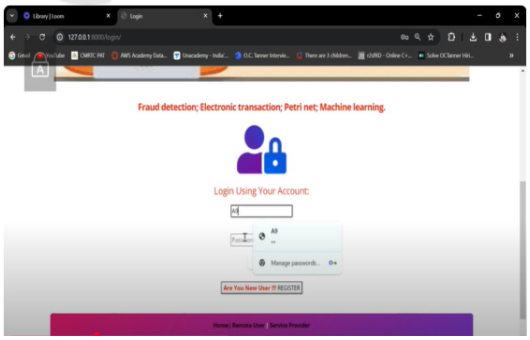

Figure 8: Login registration form.

Figure 6 shows the run project software and Figure 7 shows the open dashboard. Figure 8 illustrate the Login registration form. Figure 9 shows the view profile details.

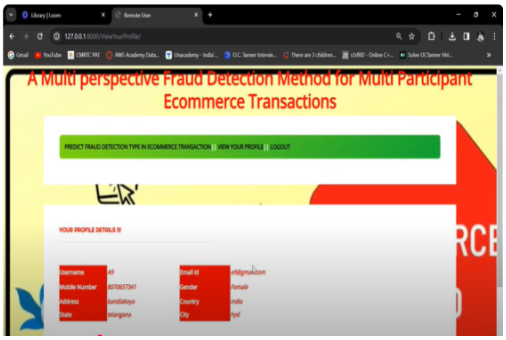

Figure 9: View profile details.

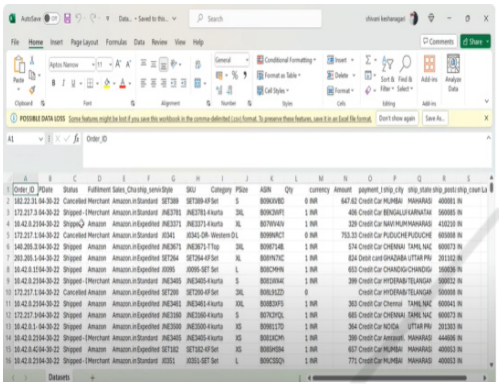

Figure 10: Datasets in CSV format.

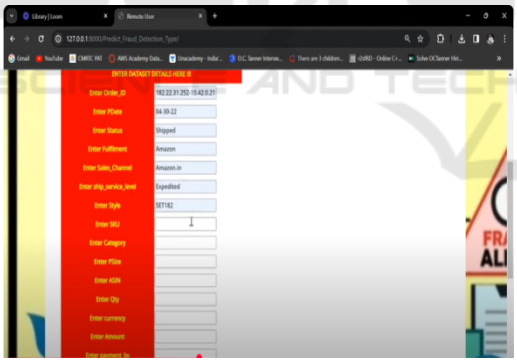

Figure 11: Enter datasets.

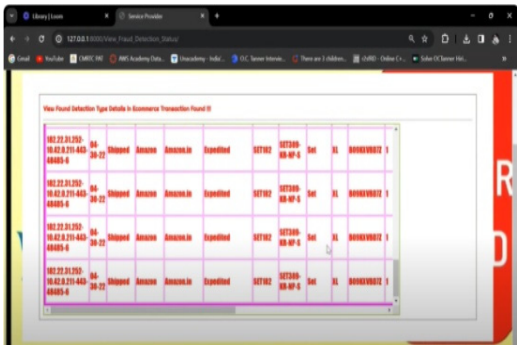

Figure 12: View result analysis.

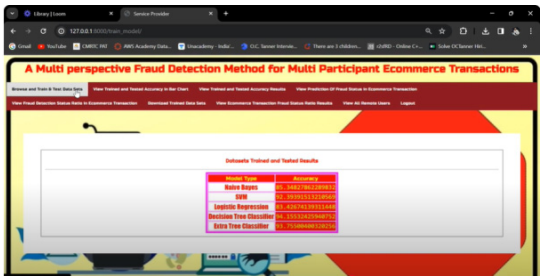

Figure 13: View predicted fraud transaction type.

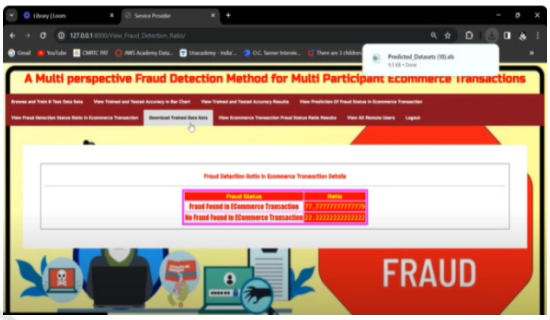

Figure 14: Fraud detection ratio in economics transaction details.

Figure 10 shows the datasets in CSV format and Figure 11 shows the enter datasets. Figure 12 and 13 shows the view result analysis and view predicted fraud transaction type. Figure 14 illustrate the Fraud detection ratio in Economics Transaction details.

8 CONCLUSIONS

In this study, a hybrid approach is proposed through employing formal process modelling, along with dynamic user behaviour to capture fraudulent transactions. We also examined the e-commerce transaction process based on five perspectives that we established: the control flow, the resource, the time, the data, and user behaviour patterns. In this study, a support vector machine (SVM) model was built to carry out fraud transaction detection, while high-level Petri nets were employed as a basis for process modelling to observe abnormalities in user behaviours. The robust testing that retrained by ourselves in against that the proposed method is able to accurately detect fraud in the transactions and actions. A: The multi-perspective detection method we proposed summed up better than the single-perspective detection method. In future work, we will use model checking techniques and similar deep learning within our proposed framework to enhance the precision. Also extending the behaviour patterns

with more time features will be needed in the future for improving the accuracy of risk identification. Furthermore, coordinate the model, apply the proposed methodology to more areas of malicious behaviour, and study the construction of a standard

REFERENCES

A. Abdallah, M. A. Maarof, and A. Zainal, "Fraud detection system: Asurvey," J. Netw. Comput. Appl., vol. 68, pp. 90-113, Apr. 2016.

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.

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.

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.

E. Asare, L. Wang, and X. Fang, "Conformance Checking:

I. M. Mary, and M. Priyadarshini, "Online Transaction Fraud Detection System," in 2021 Int. Conf. Adv. C. Inno. Tech. Engr. (ICACITE), 2021, pp. 14-16.

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.

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.

M. Jans et al., "A business process mining application for internaltransaction fraud mitigation," Expert Syst. Appl., vol. 38, no. 10, pp.13351-13359, 2011.

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.

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.

P. Rao et al., "The e-commerce supply chain and environmental sustainability: An empirical investigati on on the online retail sector. "Cogent. Bus. Manag., vol. 8, no. 1, pp. 1938377, 2021.

R. Sarno et al., "Hybrid Association Rule Learning and Process Mining for Fraud Detection," IAENG Int. J. C. Sci., vol. 42, no. 2,2015.

R. A. Kuscu, Y. Cicekcisoy, and U. Bozoklu, Electronic PaymentSystems in Electronic Commerce. Turkey: IGI Global, 2020, pp. 114–139.

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.

W. Chomyat and W. Premchaiswadi, "Process mining on medicaltreatment history using conformance checking, " in 2016 14th Int. Conf.ICT K. Eng. (ICT&KE), 2016, pp. 77-83.

Workflow of Hospitals and Workflow of Open-Source EMRs," IEEE Access, vol.8, pp. 139546-139566, 2020.

X. Niu, L. Wang, and X. Yang, "A comparison study of credit card fraud detection: Supervised versus unsupervised," arXiv preprintarXiv: vol. 1904, no. 10604, 2019, doi: 10.48550/arXiv.1904.10604.

Z. Li, G. Liu, and C. Jiang, "Deep Representation Learning withFull Center Loss for Credit Card Fraud Detection," IEEE Trans. Computat. Social Syst., vol. 7, no. 2, pp. 569-579, 2020.