International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 08 Issue: 05 | May - 2024 SJIF Rating: 8.448 ISSN: 2582-3930

A Multi-Perspective Fraud Detection Method for Multi-Participant E-Commerce Transactions

MRS.I.VASANTHA KUMARI, S.SAIDEEP, M.ABHISHEK, CH.ABHINAV, A.RAVITEJA

Abstract - In our paper, we talk about how tricky it is to catch fraud in e-commerce when lots of people are involved. Usually, fraud detectors look at individual transactions, but they miss the bigger picture of how buyers, sellers, and middlemen interact. So, we came up with a new way to spot fraud in these complex transactions.

Our method looks at transactions in different ways, like what's happening, how people are behaving, and who's connected to who. We use fancy computer programs and graphs to find subtle signs that something fishy might be going on.

We also added a feature where we learn from past fraud cases to get better at catching new ones. We tested our method on real e-commerce data, and it did a good job at finding fraud in all sorts of situations.

***Key Words*:** Fraud detection, E-commerce, Multiple participants, Buyer-seller interaction, Past fraud cases, Complex transactions.

INTRODUCTION

E-commerce has made buying and selling easier, but it's also made fraud a big problem, especially when multiple people are involved. Traditional ways of spotting fraud aren't always good at catching it in these complex situations. So, we came up with a new method to detect fraud in multi-person e-commerce deals.

Our method looks at transactions in different ways, like what's happening, how people are acting, and how transactions are connected. We use smart computer programs and graphs to find any signs that something might be fishy.

Instead of just looking at individual transactions, our method looks at everything: how people behave, how transactions are connected, and more. We use smart computer programs to find any signs that something's not right. We also made our method learn from past fraud cases, so it gets better at spotting new ones over time. We tested it on real e-commerce data, and it worked well at finding fraud in lots of different situations.

In conclusion, the evolution of e-commerce and the proliferation of online transactions present unparalleled opportunities for businesses. However, these advancements also bring forth new security challenges that demand innovative solutions. Our multi-perspective fraud detection method represents a significant step towards enhancing the security and resilience of multi-participant e-commerce transactions, ensuring a safe and trustworthy online environment for businesses and consumers alike. In the future, we'll keep improving our method to make e-commerce safer for everyone

RELATED WORK

Existing fraud detection method in e-commerce are broadly categorized into two main approaches: non-formal methods such as machine learning, and formal methods such as process mining.

Machine-learning-based methods leverage historical data to classify or predict future observations, aiming to identify potential risky transactions, both offline and online. Supervised learning algorithms are commonly used in online fraud monitoring due to their higher accuracy and coverage. Recent research has demonstrated the efficiency of machine learning methods in capturing fraudulent transactions in credit card applications. Fraudsters often adapt their behavioral patterns dynamically to evade detection methods. Support Vector Machines (SVM) have shown promise in classifying user behaviors under complex scenarios, particularly in online credit card fraud detection. Many researchers advocate combining multiple detection methods for comprehensive fraud detection.

However, most machine learning-based methods primarily rely on historical data to analyze fraudulent transactions and often overlook the transactional process flow and dynamic user behaviors. This limitation underscores the need for a more comprehensive approach.

On the other hand, process mining, a formal method, focuses on extracting knowledge from existing event logs in information systems to monitor and improve operational processes in business IT infrastructure. It specializes in comparing event logs with established models to detect, locate, and interpret deviations. Process mining can detect a large number of abnormal transactions not identifiable by traditional methods. Researchers have proposed process mining as an appropriate solution to mitigate fraud, incorporating internal affairs. For instance, conformance checks have been applied to monitor processes in medical settings, ensuring adherence to established workflows. Tools like Disco, and Heuristic Miner are commonly used for conformance checking in process mining.

Process mining is particularly effective in detecting fraud as it compares actual data against standard models to identify outliers. Despite its advantages, there is still a need to develop hybrid learning methods to improve detection accuracy. A multi-perspective anomaly detection method has been proposed to enhance understanding and development in this field, going beyond control flow perspectives to include time and resources.

In conclusion, while both machine learning and process mining offer valuable insights into fraud detection in e-commerce, there's a need for more dynamic and multi-perspective approaches to account for the evolving nature of fraudulent activities. Incorporating real-time analysis and considering various factors can enhance the effectiveness of fraud detection systems in safeguarding e-commerce transactions.

MODEL ANALYSIS

An e-commerce platform is a website where people can buy and sell things online. B2C (Business to Customer) platforms are very common, especially in China. These platforms use third-party payment systems to make sure transactions are fair for both buyers and sellers.

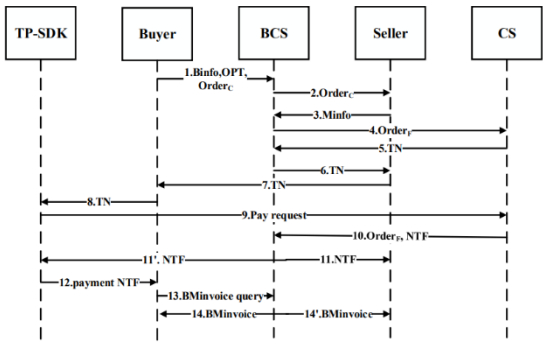


Fig.1. Interaction flow of the transaction process

1. The buyer logs in and chooses what they want to buy. The platform creates an order and sends it to the seller.

2. The seller decides if they want to accept the order. If they do, the platform creates a formal order with all the details.

3. Once the buyer pays, the payment system notifies both the platform and the seller.

4. The seller checks the payment and confirms the order.

5. The payment system creates a unique transaction number and sends it to the platform.

6. The seller gets the number and passes it to the buyer. The buyer confirms the payments and enters their password.

7. The payment system verifies everything and completes the payment.

To prevent fraud, someone might fake a payment order to get goods without paying the right amount.

A scammer might pretend to be a buyer or seller and trick the other person into paying for their order.

They could send a fake notification saying they paid, even though they didn't.
They might pay for a cheap order but try to get expensive items without paying for them.

By knowing these tricks, we can better protect ourselves from fraud when buying and selling online.

ANALYTICAL METHODS

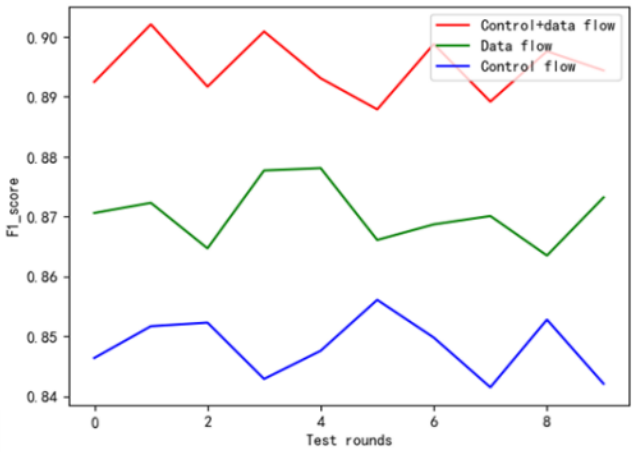
Fig.12(a) and 12(b) show the results of our fraud detection model using SVM. The blue curve represents the control flow index, the green curve shows the model score based on data flow, and the red curve indicates the score when both perspectives are combined.

From the figures, we can see that when we combine both control flow and data flow perspectives, we achieve a higher F1-score. This means that considering both perspectives together helps us detect user anomalies more effectively than when we only look at one type of data.

` TABLE-1

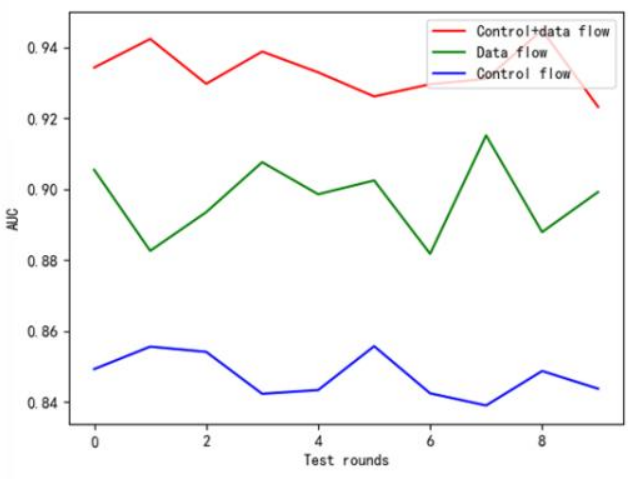
FRAUD DETECTION MODEL RESULTS BASED ON SVM

Perspectives	*Precision*	*Recall*	*F1-score*	*AUC*
Control+data flow	0.946	0.852	0.895	0.935
Data flow	0.912	0.837	0.871	0.892
Control flow	0.889	0.812	0.849	0.842



(a) F1-score statistics

We tested our fraud detection model in 50 rounds and found that when combining data flow and control flow features, the F1-score and AUC were higher compared to considering only one perspective. This means our model is better at detecting user anomalies when it uses information from both perspectives.



(b) AUC statistics

Fig. 2. F1-score and AUC statistics for three situations.

In summary, our model outperforms others by considering multiple perspectives, resulting in better detection of abnormal e-commerce users. Also, unlike deep learning methods, our model is interpretable and can describe transaction processes and structures.

CONCLUSIONS

This paper suggests a mix of techniques to catch fraudulent transactions by combining formal process modeling with dynamic user behaviors. We examined the e-commerce transaction process from five main angles: how the process flows, what resources are involved, how time plays a role, what data is used, and patterns in user behavior.

We used high-level Petri nets to model abnormal user behaviors and built an SVM model to detect fraudulent transactions. Our experiments showed that our method is good at spotting fraudulent activities. Overall, our multi-perspective approach performed better than looking at just one perspective.

In the future, we plan to incorporate deep learning and model checking methods for even better accuracy. We also want to add more time-related features to make risk identification more precise. Additionally, we aim to create a standard library of fraud modes and apply our method to other areas of malicious behavior by combining different models.

REFERENCES

[1] Electronic Payment Systems in Electronic Commerce by R. A. Kuscu, and U. Bozoklu,

[2] "The Effect of COVID-19 Spread on the e-commerce market: The case of the 5 largest e-commerce companies in the world." By M. Abdelrhim, and A. Elsayed.
[3] "The e-commerce supply chain and environmental sustainability: An empirical investigation on the online retail sector." by P. Rao et al.

[4] "A review on prevention of fraud in electronic payment gateway using secret code," by S. D. Dhobe, K. K. Tighare, and S. S. Dake.

[5] "Fraud detection system: A survey," J. Netw. Comput. Appl, by A. Abdallah, M. A. Maarof, and A. Zainal.

[6] "An Analysis of the Most Used Machine Learning Algorithms for Online Fraud Detection," by E. A. Minastireanu, and G. Mesnita.

[7] "A comparison study of credit card fraud detection: Supervised versus unsupervised," by L. Wang, and X. Yang.

[8] "Data-and resource-aware conformance checking of business processes," by M. D. Leoni, W. M. Van Der Aalst, and B. F. V. Dongen

[9] "A survey on fraud detection techniques in ecommerce," *Tech-Knowledge*, S. M. Najem, and S. M. Kadeem.

[10] "Anomaly detection in business process runtime behavior--challenges and limitations," K. Böhmer, and S. Rinderle-Ma [11] "Fraud detection on event logs using fuzzy association rule learning," K. D. Febriyanti, R. Sarno and Y. Effendi.

[12] "A framework of applying process mining for fraud scheme detection," T. Chiu, Y. Wang and M. Vasarhelyi.

[13] "Show Me the Money! Finding Flawed Implementations of Third-party In-app Payment in Android Apps," W. Yang et al.

[14] "Conformance Checking: Workflow of Hospitals and Workflow of Open-Source EMRs," E. Asare, L. Wang, and X. Fang .

[15] "Process mining on medical treatment history using conformance checking," W. Chomyat and W. Premchaiswadi.