# Transaction Fraud Detection Based on Total Order Relation and Behavior Diversity's Article Review

1st Shengyu Jia
*MATH 402W*
*Simon Fraser University*
Burnaby, British Columbian, Canada
sja102@sfu.ca

***Abstract*—This review examines the article ”Transaction Fraud Detection Based on Total Order Relation and Behavior Diversity,” which introduces a novel approach to enhancing online transaction fraud detection. The authors propose a methodology leveraging Total Order Relation (TOR) and Behavior Diversity (BD) for constructing detailed Behavior Profiles (BPs) of users, based on their transaction histories. This approach significantly diverges from traditional models by capturing the unique, dynamic transaction behaviors of users, offering improved fraud detection accuracy. Through rigorous empirical analysis, the study demonstrates the superiority of the proposed Order Model (OM) over existing methods. The review also highlights the article's contributions, limitations, and suggests directions for future research, emphasizing the integration of machine learning techniques and broader data analysis for further advancements in fraud detection technology.**

***Index Terms*—Behavior profile (BP), e-commerce security, fraud detection, online transaction, article review**

## I. Introduction

This paper ”Transaction Fraud Detection Based on Total Order Relation and Behavior Diversity”, (for future reference, the paper will simply be referred to as ”the paper”), begins by highlighting the significant growth in online transactions due to the popularization of online shopping platforms like Amazon, eBay, and Alibaba. It forecasts a staggering future market value and emphasizes the rising trend of card-not-present transactions, which, while facilitating online shopping, also escalate the risk of transaction fraud. This increase in fraud cases, significantly higher online than offline, underscores the urgent need for robust fraud detection methods. The introduction sets the stage for discussing the limitations of existing fraud detection models and introduces the novel approach proposed in the paper, which aims at enhancing the accuracy and reliability of fraud detection in the rapidly evolving e-commerce landscape.

## II. Article Content Overview

In the paper, the authors introduce a sophisticated approach to addressing online transaction fraud, a growing concern in the e-commerce domain. The core of their methodology lies in the creation of Behavior Profiles (BPs) from users' transaction records. This innovative approach departs from traditional models, like the Markov chain, by emphasizing the diversity of user behaviors rather than merely predicting the next transaction. The essence of their method involves analyzing transaction logs to extract patterns that signify normal user behavior, which are then used to identify transactions deviating significantly from established patterns, flagging them as potential fraud.

The paper meticulously outlines the process of constructing these Behavior Profiles, starting with the definition of transaction records and logs. Each transaction record is composed of multiple attribute values, forming the dataset for analysis. The Behavior Profile is essentially a distilled representation of a user's transaction history, capturing the uniqueness of their online shopping habits.

The authors argue that this approach not only enhances the detection of fraudulent activities by accounting for the behavioral diversity among users but also addresses the shortcomings of previous models which often oversimplify user behavior patterns. By focusing on the totality of a user's transactions, the model aims to provide a more accurate and dynamic method of fraud detection in the face of constantly evolving online fraud tactics.

## III. Methodology

The paper delves deeply into the mathematical models and algorithms developed for fraud detection. The authors propose a novel approach that leverages Total Order Relation (TOR) and Behavior Diversity (BD) to construct Behavior Profiles (BPs) of users based on their transaction history. This method stands out by not only capturing the sequence of transactions but also by considering the diversity in users' transaction behaviors to enhance detection accuracy.

The process begins with the definition of a transaction record, which consists of multiple attributes such as transaction time, location, amount, and type of goods purchased. These records are used to construct a user's transaction log, a comprehensive dataset reflecting their purchasing behavior over time. By analyzing these logs, the study introduces a new model that orders transaction attributes and classifies their values, enabling the construction of a Logical Graph of Behavior Profile (LGBP). This graph abstracts and covers all different transaction records, providing a structured way to analyze transaction patterns.

To quantify the behavior diversity, the study introduces path-based transition probabilities and a diversity coefficient.

These metrics are crucial for understanding the nuances in user behaviors, enabling the model to detect anomalies effectively. Additionally, a state transition probability matrix captures the temporal features of transactions, further enriching the behavior profiles.

The proposed fraud detection method operates by evaluating incoming transactions against these behavior profiles, using calculated acceptance degrees to ascertain their legitimacy. This approach not only targets the detection of fraudulent activities but also considers the concept drift problem, where users' behavior patterns may evolve over time.

## IV. Empirical Results

The empirical results section of the paper presents a comprehensive performance evaluation of the proposed fraud detection methodology. Through a series of experiments, the authors compare their Order Model (OM) against three other models: Srivastava's method (SM), which relies on Markov chains for behavior profiling, and two anomaly detection methods, one based on Bayesian learning (BL) and another on self-organizing maps (SOM). These comparisons are grounded on real transaction data from 70 users, with each dataset containing 70 transaction records from Taobao, a popular Chinese online shopping platform.

The study's evaluation metrics include True Positive Rate (TPR) and False Positive Rate (FPR), crucial for understanding a model's ability to correctly identify fraudulent transactions while minimizing false alarms. The results, illustrate that TPR increases alongside FPR, indicating a trade-off between detecting fraud and avoiding false positives. The optimal parameter settings, found through exhaustive experimentation, are $N = 40$ (number of transactions considered), $k = 8$ (the number of latest transactions for behavior profiling), and a detection threshold of 90

The comparison demonstrates that the Order Model outperforms other methods, especially in scenarios involving Behavior Diversity (BD). For users classified under high stability (HS), medium stability (MS), and low stability (LS), OM consistently delivered better detection rates compared to SM, BL, and SOM, with notable advantages in handling diverse behaviors across different user segments. This is attributed to OM's capability to capture the nuanced variations in user transaction patterns, a significant improvement over the static nature of Markov chains, and the generalization errors of BL and SOM.

Furthermore, the authors explore the concept of acceptance degrees and their mean ($\phi k$), a novel approach to quantifying the legitimacy of transactions. This method enables dynamic adjustment to users' changing behaviors, a common challenge in fraud detection known as concept drift.

The empirical analysis concludes that the proposed OM, with its focus on total order relation and behavior diversity, offers a robust and flexible framework for detecting online transaction fraud. It significantly reduces false positives while maintaining high detection accuracy, addressing the critical need for reliable security measures in the e-commerce domain.

## V. Evaluation and Critique

The paper presents a novel methodology that significantly advances the field of fraud detection by incorporating the diversity of user behaviors into the detection process. This approach addresses a critical gap in traditional models, which often fail to capture the dynamic nature of fraudulent activities in online transactions.

One of the strengths of this study is its innovative use of Total Order Relation (TOR) and Behavior Diversity (BD) to construct Behavior Profiles (BPs). This methodology allows for a more nuanced understanding of user behaviors, leading to improved detection rates of fraudulent transactions. The empirical results, as demonstrated through rigorous testing against other models, underscore the effectiveness of this approach. Specifically, the Order Model's superior performance across various user stability categories highlights its adaptability and precision in detecting fraud.

However, the study is not without limitations. While the authors meticulously detail the construction of BPs and the application of TOR and BD, there is a relative lack of discussion on the scalability of their model. As online transactions continue to grow exponentially, the computational efficiency of fraud detection systems becomes increasingly critical. Future research could benefit from exploring the implementation of this model in real-world scenarios, particularly in terms of processing time and resource utilization.

Despite the model's innovative approach, its scalability and real-time adaptability remain critical for widespread application. Future studies could focus on optimizing the computational efficiency to facilitate deployment in large-scale e-commerce platforms. Additionally, adapting the model to accommodate emerging fraud patterns will enhance its longevity and effectiveness in dynamic online environments.

Another area for potential improvement lies in the model's adaptability to new fraud tactics. The dynamic nature of online fraud requires continuous updates to detection models. The authors mention the challenge of concept drift but do not fully explore strategies for updating the model in response to evolving fraud patterns. Incorporating machine learning techniques could enhance the model's ability to learn from new data and adjust its detection mechanisms accordingly.

In conclusion, the article makes a valuable contribution to the field of transaction fraud detection. Its focus on behavior diversity and the application of TOR in constructing BPs offers a promising direction for future research. However, addressing the challenges of scalability and adaptability to new fraud tactics will be crucial for the practical application of this model. Further exploration of these areas could significantly enhance the model's effectiveness and applicability in protecting against transaction fraud in the ever-evolving landscape of online commerce.

## VI. Application and Impact

The application and impact of the paper are significant in the realm of e-commerce security. The proposed Order Model (OM) stands as a pivotal development in combating transaction fraud, an ever-persistent threat in the online shopping domain. By focusing on the behavioral diversity of users and the total order relation of transaction attributes, this model offers a more nuanced and effective approach to detecting fraudulent activities compared to conventional methods.

The OM's application extends beyond mere theoretical advancement; it presents a practical tool for online marketplaces and financial institutions to enhance their fraud detection capabilities. By integrating this model into their transaction processing systems, these entities can significantly reduce the incidence of fraud, thereby safeguarding consumer trust and financial integrity. The model's ability to adapt to changing user behaviors and detect nuanced fraudulent patterns offers a dynamic solution to a dynamic problem.

Furthermore, the impact of this study is multifaceted. For one, it contributes to the academic and practical understanding of fraud detection by introducing a novel methodology that can be further explored and optimized. Secondly, it addresses the financial losses associated with transaction fraud, which are substantial both for businesses and consumers. By reducing these losses, the OM indirectly contributes to the stability and growth of the e-commerce ecosystem.

The future direction suggested by the authors, including the incorporation of machine learning methods for the automatic classification of transaction attributes and considering additional data such as user comments, indicates a promising horizon for fraud detection technologies. These advancements could lead to even more sophisticated and autonomous systems, capable of preempting fraudulent transactions with greater accuracy and efficiency.

In conclusion, the application of the Order Model in online transaction fraud detection represents a significant step forward in securing e-commerce transactions. Its impact, both immediate and long-term, is poised to reshape the landscape of fraud detection strategies, making them more adaptive, efficient, and effective in the face of evolving threats.

## VII. Future Research Directions

The concluding section of the paper outlines several promising avenues for future research, suggesting a proactive approach to further enhance the fraud detection model. The authors express a specific interest in exploring machine learning techniques to automate the classification of transaction attributes. This direction aims to refine the model's capacity to more precisely characterize user behaviors, thus improving its predictive accuracy and adaptability to new and evolving fraud tactics.

Moreover, the paper hints at the potential expansion of the Behavior Profile (BP) model to incorporate additional data types, such as user comments. This suggests an interdisciplinary approach, merging textual analysis with transactional behavior analysis, to gain a more holistic view of user activities and potentially uncover subtle indicators of fraud.

Future research directions could benefit from integrating advanced machine learning techniques, such as convolutional neural networks (CNNs) for more nuanced classification of transaction attributes, and natural language processing (NLP) methods for analyzing user-generated content. These approaches could provide deeper insights into user behavior and fraud tactics, further refining the model's predictive accuracy.

These proposed directions not only underscore the article's contributions but also highlight the dynamic nature of fraud detection research, emphasizing the need for continuous innovation. The integration of machine learning and broader data analysis signifies a move towards more sophisticated, self-learning models capable of adjusting to the rapidly changing landscape of online transactions and fraud methods.

The future research directions outlined in the paper promise to address some of the current limitations, such as the scalability of the model and its ability to cope with concept drift. By incorporating machine learning and expanding the dataset for behavior analysis, the authors aim to enhance the model's responsiveness and effectiveness in real-world applications.

In summary, the proposed future research directions reflect a commitment to advancing the field of fraud detection through technological innovation and interdisciplinary approaches. This forward-looking perspective not only enhances the academic value of the study but also

## VIII. Conclusion

This review has systematically explored the significant contributions of ”Transaction Fraud Detection Based on Total Order Relation and Behavior Diversity” to the field of e-commerce security. Through innovative methodologies that leverage Total Order Relation (TOR) and Behavior Diversity (BD) to construct detailed Behavior Profiles (BPs) of users, this study presents a novel approach to detecting transaction fraud. The empirical results demonstrate the model's superior performance compared to existing methods, highlighting its potential to significantly reduce fraud in online transactions.

The evaluation and critique of the study acknowledged its innovative approach and the effectiveness of its methodology, while also pointing out areas for further research and development, such as scalability and adaptability to new fraud tactics. The suggested future research directions, including the integration of machine learning techniques and the expansion of data types for analysis, indicate a robust pathway for advancing the model's capabilities.

In conclusion, this paper stands as a pivotal contribution to fraud detection research, offering new perspectives and tools to combat the ever-evolving challenges of transaction fraud in e-commerce. Its implications for both theoretical research and practical applications are profound, setting the stage for future innovations in the field.

## References

[1] L. Zheng, G. Liu, C. Yan, and C. Jiang, ”Transaction Fraud Detection Based on Total Order Relation and Behavior Diversity,” in IEEE Transactions on Computational Social Systems, vol. 5, no. 3, pp. 796-805, September 2018, doi: 10.1109/TCSS.2018.2856910.

[2] Shengyu Jia (GitHub username: chief11712138), *”Fraud_Detection_Public,”* GitHub repository, 2024. [Online]. Available: https://github.com/chief11712138/Fraud_Detection_Public. [Accessed: Feb. 24, 2024].