




Optimization of Machine Learning Algorithms for Fraud Detection in Electronic Financial Transactions

^{1*} Rully Fildansyah

¹ Sanskara Karya Internasional

*correspondence e-mail: rollfil@gmail.com

Article Info	Abstract
<p>Keywords: Fraud Detection, Electronic Financial Transactions, Machine Learning Algorithm, Algorithm Optimization</p>	<p>Electronic financial transactions play a pivotal role in the modern financial ecosystem, but they also attract sophisticated fraudulent activities. This research delves into the optimization of machine learning algorithms for fraud detection in electronic financial transactions. The study demonstrates that algorithm optimization significantly enhances detection performance, as evidenced by improved accuracy, reduced false positives, increased recall, precision, and F1-score. The practical implications of these findings are substantial. Enhanced fraud detection algorithms contribute to heightened security for individuals and financial institutions. Reduced false positives streamline transaction verification processes, bolstering customer confidence and operational efficiency within financial institutions. Looking ahead, future research should explore more advanced techniques and algorithms for fraud detection, such as real-time data processing and deep learning. Additionally, policy, legal implications, and data privacy considerations should be integrated into developing more robust fraud detection solutions. Further studies on the impact of regulatory changes on fraud detection represent valuable avenues for future research. By continuously advancing technology and detection approaches, we can better safeguard electronic financial transactions in our ever-evolving digital landscape.</p>


This is an open access article under the CC-BY-SA license.

INTRODUCTION

Electronic financial transactions have become an integral part of our daily lives. The development of information and communication technology has changed the way we make payments, transfer funds, and access financial services (W. Zhang et al., 2023). This has brought convenience, efficiency, and comfort to both individual and business financial management. However, along with these advancements, there is a growing and intensifying threat in the form of electronic financial fraud (Herryani, 2023).

The context of fraud in electronic financial transactions is critical to understand and deal with. This fraud can take many forms, such as identity theft, credit card abuse, fraudulent transactions, phishing and more. Cybercriminals with

increasingly sophisticated methods and strategies continue to attempt to exploit loopholes in the electronic financial system.

The impact of e-finance fraud is devastating to individuals, financial institutions and the economy as a whole. Individuals can suffer significant financial losses, while financial institutions have to bear the cost of refunding funds and repairing their reputation. In addition, e-financial fraud can also threaten public confidence in the e-financial system as a whole (Satapathy, 2023).

The increasing rate of electronic financial crime has become an increasingly alarming phenomenon in this digital age. Such crimes not only include fraudulent acts of electronic financial transactions, but also include cyber-attacks targeting sensitive data and corporate funds. With the rapid development of technology, criminals are getting more sophisticated in carrying out their actions and finding new ways to undermine the integrity of electronic financial systems.

The relevance of machine learning algorithms in financial fraud is becoming increasingly important in addressing this challenge. The speed and complexity of electronic-based financial attacks make conventional methods of fraud detection less effective. Machine learning algorithms have the ability to process and analyze large volumes of data in real time, which is an essential requirement in identifying suspicious patterns and detecting fraud (Bonsu et al., 2023).

In addition, machine learning algorithms can continuously learn and adapt to new trends in electronic financial fraud (Sood & Kim, 2023). By using techniques such as historical data-driven learning, these algorithms can improve detection accuracy over time, thus keeping up with evolving criminals.

Dealing with the complexity and diversity of challenges in detecting fraud in electronic financial transactions is a top priority in efforts to maintain the security of the financial system in this digital era. Fraud perpetrators continue to evolve using increasingly sophisticated methods, requiring innovative approaches in identifying new and constantly changing fraud patterns. Processing high transaction volumes in real time, uncertainty in data, and collaboration-based fraud add to the complexity of creating an effective fraud detection system.

In this context, machine learning algorithms become a relevant and important option, as they are able to adapt to these changes and play a central role in protecting public trust and the integrity of the electronic financial system. With the right approach, research and development in this area can help address these challenges and make a significant contribution in reducing the threat of electronic financial fraud.

THEORETICAL FOUNDATION

Research Review on Basic Concepts of Electronic Financial Transactions

Electronic Financial Transactions (EFT) have become one of the essential elements in the transformation of the modern financial system. The basic concept of EFT involves the exchange of financial value through electronic media, which eliminates reliance on physical cash or conventional checks. EFT encompasses various forms of transactions, ranging from online payments, fund transfers between bank accounts, to the use of mobile payment applications (Murinde et al., 2022).

These diverse mediums allow consumers and businesses to execute transactions in a manner that best suits their needs. Transaction security is a critical cornerstone of the EFT concept. The development of encryption technology and security systems has become an integral part of protecting customer data and preventing fraudulent acts. However, security challenges such as personal data theft and electronic financial fraud continue to be a major concern, driving constant efforts to improve security systems (Mehrotra, 2023).

Authorization and authentication are critical steps in any EFT transaction (Aldboush & Ferdous, 2023). Through the use of PINs, passwords, fingerprint verification or other authentication methods, the system ensures that transactions are only made by authorized parties. This process provides an additional level of security for customers and minimizes the risk of unauthorized access. Payment processors or payment gateways act as intermediaries that connect merchants with customers in EFT transactions.

Fraud in Financial Transactions

Fraud in financial transactions has become a serious threat to individuals, businesses, and the economy as a whole. Financial fraud covers a wide range of forms, from identity theft, credit card abuse, to increasingly sophisticated acts of online fraud (Herryani, 2023). This phenomenon has detrimental effects, including significant financial losses, loss of customer trust, as well as additional operational costs incurred by financial institutions.

Research in this area has revealed that fraudsters continue to develop new methods to evade detection, use increasingly sophisticated technologies, and collaborate in complex networks. This points to the importance of ongoing efforts to identify new and rapidly changing fraud patterns.

Machine learning algorithms have emerged as an effective tool in detecting financial fraud. With the ability to analyze large volumes of data in real-time, these algorithms can identify suspicious behavior and trigger early warnings. However, challenges remain in processing high volumes of transactions and distinguishing between legitimate and suspicious activity (Sissodia et al., 2023).

Machine Learning Algorithms for Fraud Detection

Machine learning algorithms provide a robust approach in recognizing complex and rapidly changing fraud patterns. Through training models on historical transaction data, these algorithms can understand legitimate customer behavior and detect suspicious activity (Y. Zhang et al., 2023). Various types of machine learning algorithms have been used in fraud detection, including Decision Trees, Random Forests, Support Vector Machines, Neural Networks, and ensemble methods.

Each type of algorithm has its own advantages and disadvantages, and research continues to identify the most effective algorithms in various contexts. It is important to understand that machine learning algorithms not only require initial modeling, but also require continuous optimization. Algorithm parameters need to be adjusted and models need to be updated regularly to maintain their effectiveness in the face of increasingly sophisticated fraud (Prem, 2024). The selection of relevant features and feature engineering techniques are also key factors in improving algorithm performance.

The success of machine learning algorithms in fraud detection also depends on quality data. Complete, accurate and up-to-date electronic financial transaction data is essential to effectively train and test the model. Therefore, careful data processing, including preprocessing and data cleaning, is a critical early stage in the use of machine learning algorithms (Prem, 2024).

RESEARCH METHODS

Data Collection

In research on fraud detection in electronic financial transactions, collecting accurate and representative data from the right sources is a crucial first step. This data collection methodology aims to ensure that the data used in the research is of good quality and relevant for fraud detection analysis.

First, the source of electronic financial transaction data must be carefully selected. Commonly used data sources include banking transaction records, credit card data, e-commerce data, and mobile payment data. This data can be obtained

from financial institutions, payment service providers, or e-commerce businesses, depending on the research context.

Once the data sources have been selected, the data collection stage begins. In data collection, efforts are required to obtain a large enough and representative amount of transaction data for accurate analysis. This can involve the process of extracting data from multiple sources, merging data from multiple sources, or using existing historical data. Next, the data needs to be processed and properly labeled. The data needs to be processed to remove noise, fill in missing values, and undergo other preprocessing stages to ensure good data quality. Data labeling is also important to identify transactions that are fraudulent and legitimate transactions, thus providing a basis for training and testing fraud detection models.

RESULTS

Analysis of experimental results

In this study, we conducted experiments to compare the performance of machine learning algorithms in fraud detection in electronic financial transactions before and after the optimization process. The optimization process aims to improve the accuracy and efficiency of the algorithm in identifying fraud.

Before the optimization process, we used a machine learning algorithm that has been configured with default parameters. The initial results of the experiment showed an acceptable level of accuracy, but there was still room for improvement. The algorithm was able to identify some fraudulent actions, but also generated a number of false positives that required further verification.

After optimization, we adjusted the algorithm parameters, performed feature engineering, and improved data preprocessing. The result of this process was a significant improvement in the algorithm's performance. The accuracy rate of fraud detection increased notably, while the number of false positives was reduced.

Besides accuracy, we also observed other parameters such as precision, recall, and F1-score. The experimental results show that the optimized algorithm provides a better balance between precise fraud detection (recall) and misidentification minimization (precision).

In the analysis of the experimental results, we also compared the data processing time before and after optimization. The results show that although the optimized algorithm has better performance, the data processing time does not increase significantly, making it feasible to use in real-time applications.

Fraud detection results

The experimental results we obtained in this study reveal that the optimization process of the machine learning algorithm significantly improves the fraud detection capability in electronic financial transactions. In the comparison between the performance of the algorithm before and after optimization, some key aspects of the fraud detection results can be summarized as follows:

Fraud Detection Accuracy: After the optimization process, the accuracy of fraud detection has improved significantly. The optimized algorithm is able to correctly identify more fraudulent actions, reducing the risk of missed fraudulent transactions.

Reduction of False Positives: One of the most noticeable improvements is the significant reduction in the number of false positives. The optimized algorithm is able to minimize errors in classifying legitimate transactions as fraudulent, reducing the disruption and loss that additional verification may cause.

Higher Recall: Recall, which measures the extent to which the algorithm is able to detect actual fraudulent acts, also saw a significant improvement after optimization. The optimized algorithm was able to identify most of the fraudulent acts that occurred, providing better protection against fraudulent threats.

Improved Precision: Precision, which measures the extent to which actions identified as fraudulent by the algorithm are actually fraudulent, also showed a positive improvement. This indicates that the optimized algorithm tends to produce fewer errors in classifying legitimate transactions as fraudulent.

Higher F1-score: F1-score, which combines recall and precision, reflects the balance between correct detection of fraudulent acts and minimization of misidentification. The experimental results show a consistent improvement in F1-score after the optimization process.

Discussion

Implications of the findings for the security of electronic financial transactions:

The findings of this study have significant implications for the security of electronic financial transactions in the modern financial ecosystem. The experimental results showing improved performance of machine learning algorithms in detecting fraud have a positive impact on various aspects of electronic financial transaction security.

First, improved fraud detection accuracy means that security systems can be more effective in identifying potentially harmful fraudulent actions. This reduces

the risk of financial losses incurred by individuals and financial institutions due to fraud. Customers' trust in electronic financial systems is also enhanced as they feel that their transactions are better protected.

Secondly, the reduction of false positives has positive implications in reducing unnecessary disruptions to legitimate transactions. With a lower number of misidentifications, businesses and financial institutions can minimize manual intervention and additional time-consuming verification. This will increase efficiency in the transaction process and ensure a smoother customer experience.

Furthermore, improved recall and precision means that optimized machine learning algorithms can better recognize actual fraudulent acts and avoid errors in classifying legitimate transactions as fraudulent. This will help in reducing the risk to legitimate customers and increase the effectiveness in fighting fraud.

In the context of policy and regulation, these findings underscore the importance of investing in the development and maintenance of state-of-the-art fraud detection systems. The security of electronic financial transactions is critical to ensuring integrity and trust in the modern financial system. Regulators and supervisory agencies should take note of the results of this study in updating relevant security guidelines and requirements.

Advantages and disadvantages of the algorithms used

The machine learning algorithms used in electronic financial transaction fraud detection have advantages and disadvantages that need to be considered. The main advantage is its ability to identify complex and rapidly changing fraud patterns. They are capable of processing large volumes of data in real-time, enabling more accurate and rapid fraud detection. In addition, the algorithm can learn and adapt to new changes in fraud patterns without the need for reprogramming.

However, there are some drawbacks that need to be addressed. First, machine learning algorithms require initial modeling and a time-consuming training process. This can be an obstacle in applying the algorithm in emergency situations or when an instant reaction is required. Secondly, algorithms can be complex and require large computational resources, especially when used for processing very high volumes of transactions.

Furthermore, while algorithms can identify suspicious acts of fraud, they can also generate false positives, i.e. transactions that are wrongly classified as fraudulent. This can cause unnecessary disruption for customers and financial institutions. Algorithm accuracy can improve, but the risk of false positives needs to be carefully addressed.

Another drawback is that machine learning algorithms tend to be “black box,” meaning it is often difficult to explain in detail why a decision was made. This can be an obstacle in explaining to customers or authorities the reasoning behind an action or decision.

CONCLUSION

This research has revealed that optimization of machine learning algorithms in electronic financial transaction fraud detection can bring significant improvements in system performance. The experimental results show increased fraud detection accuracy, reduced false positives, improved recall and precision, and increased F1-score. This indicates that the optimized algorithm can be more effective in identifying actual fraudulent acts, while minimizing misidentification and interference with legitimate transactions.

Practical Implications

The practical implication of these findings is the increased security of electronic financial transactions for individuals and financial institutions. With more sophisticated and efficient algorithms in detecting fraud, the risk of financial loss due to fraudulent acts can be reduced. The reduction of false positives will also reduce the disruption and time required for transaction verification. This can increase customer confidence in the e-finance system and improve the operational efficiency of financial institutions.

Recommendations for Future Research

For future research, it is recommended to continue developing more sophisticated techniques and algorithms in fraud detection. Advances in real-time data processing and the use of technologies such as deep learning could be an interesting research area. In addition, it is important to consider policy, legal, and data privacy aspects in the development of better fraud detection solutions. Further study on the effect of regulatory changes on fraud detection can also be a valuable research topic. By continuously developing fraud detection technologies and approaches, we can better maintain the security of electronic financial transactions in the ever-evolving digital age.

REFERENCE

- Aldboush, H. H. H., & Ferdous, M. (2023). Building Trust in Fintech: An Analysis of Ethical and Privacy Considerations in the Intersection of Big Data, AI, and Customer Trust. *International Journal of Financial Studies*, 11(3), 90.

- Bonsu, M. O.-A., Roni, N., & Guo, Y. (2023). The Impact of Big Data on Accounting Practices: Empirical Evidence from Africa. In *Novel Financial Applications of Machine Learning and Deep Learning: Algorithms, Product Modeling, and Applications* (pp. 47–71). Springer.
- Herryani, M. R. T. R. (2023). Enhancing Legal Protection for Digital Transactions: Addressing Fraudulent QRIS System in Indonesia. *Rechtsidee*, 12(1), 10–21070.
- Mehrotra, A. (2023). FinTech driven financial inclusion-the hype and the reality of missed targets. *International Journal of Public Sector Performance Management*, 11(2), 165–176.
- Murinde, V., Rizopoulos, E., & Zachariadis, M. (2022). The impact of the FinTech revolution on the future of banking: Opportunities and risks. *International Review of Financial Analysis*, 81, 102103.
- Prem, P. S. (2024). Machine learning in employee performance evaluation: A HRM perspective. *International Journal of Science and Research Archive*, 11(1), 1573–1585.
- Satapathy, S. S. (2023). Interpretive Structural Modeling Approach To Effective Internal Control Practices for Prevention of Accounting Fraud in Small Businesses Using Micmac Analysis. *Interantional Journal of Scientific Research in Engineering and Management*, 07(03), 1–8. <https://doi.org/10.55041/ijrsrem18068>
- Sissodia, R., Rauthan, M. S., & Barthwal, V. (2023). Challenges in Various Applications Using IoT. In *Handbook of Research on Machine Learning-Enabled IoT for Smart Applications Across Industries* (pp. 1–17). IGI Global.
- Sood, S., & Kim, A. (2023). The Golden Age of the Big Data Audit: Agile Practices and Innovations for E-Commerce, Post-Quantum Cryptography, Psychosocial Hazards, Artificial Intelligence Algorithm Audits, and Deepfakes. *International Journal of Innovation and Economic Development*, 9(2), 7–23. <https://doi.org/10.18775/ijied.1849-7551-7020.2015.92.2001>
- Zhang, W., Siyal, S., Riaz, S., Ahmad, R., Hilmi, M. F., & Li, Z. (2023). Data Security, Customer Trust and Intention for Adoption of Fintech Services: An Empirical Analysis From Commercial Bank Users in Pakistan. *SAGE Open*, 13(3), 21582440231181388.
- Zhang, Y., Xu, L., & Lu, Z. (2023). Purchase Decision of GPPS: An Empirical Study Based on Machine Learning in China. *Cybernetics and Systems*, 54(1), 60–87.