International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

Digital Payment Fraud Detection Using Machine Learning

Ms. A. B. Lahari[1], K. Karthik Kumar[2], B. Neelima[3], K. Raghu[4], K. Pranay Varsh[5]

[1]Asst Professor, CSE, NSRIT
[2,3,4,5]Student, CSE, NSRIT

ABSTRACT

Digital payment, Fraud detection, machine learning, financial transactions, classification algorithms, data mining, cyber security, anomaly detection.

The fast development of digital payment systems has made finance much more convenient. However, the likelihood of fraudulent transactions is rising instead. Traditional rule-based fraud detection algorithms often fail to detect conventional fraud models. Fraud detection techniques. This paper will attempt to deal with this problem by proposing a machine learning-based solution to digital payment fraud detection. To categorize the transactions as legitimate and fraudulent, It reviews the previous transaction history and determines pertinent attributes such as the amount of the transactions, the frequency, and the preferred behaviours. There are many supervised machine learning algorithms that have been Implemented such as the Random Forest, Decision Tree, Support Vector Machine and the Logistic Regression.

1. INTRODUCTION:

Digital payment systems have changed the way we do things with money every day. We can use our phones to pay for things send money to people and buy things online without using a card. This has made it easier and faster to do transactions. A few years ago we could not have imagined that we could do so many things with money so quickly.

This change has some things about it. For one it is very convenient. We can pay for things from anywhere and at any time. It is also very efficient. We do not have to wait in line or go to a bank to do things with our money.. More people can use digital payment systems even if they do not have a lot of money or a bank account.

There is also a problem, with digital payment systems. Some people try to cheat and steal money from others. This is called payment fraud. It is not something that happens sometimes. It is a problem that is getting worse. As more people use payment systems it is easier for bad people to cheat and steal. They can use technology and tricks to get around the rules and take money from people.

The big question is how to tell if a transaction is real or fake. It is hard to do this because there are many transactions happening all the time.. Sometimes we do not have enough information to know if a transaction is real or not. Also people are always changing the way they use payment systems so it is hard to keep up. Digital payment systems are the focus of this study. We want to know how to stop payment fraud and make digital payment systems safer for everyone to use.

2. LITERATURE REVIEW

Digital payment technologies are becoming very rapid these days as the number of individuals using online banking, credit cards, debit cards and mobile payment applications continues to increase. This is because the risk of financial fraud is also on the rise as it becomes simpler to carry out transactions. In order to counter this researchers are developing systems that apply machine learning to detect fake transactions and safeguard financial networks. This part examines studies of applying machine learning to identify fraud in online payments.

P. Jeyachandran, Leveraging Machine Learning to detect Real-Time Fraud in Digital Payments, SSRN Working Paper, 2024.

Link: http://dx.doi.org/10.2139/ssrn.5076783 In the current paper, the author examines the topic of machine learning implementation in the context of fraudulent transaction detection as it occurs in digital payment systems a bit more closely. The main concept is to create smarter models by feeding them actual payment data in order to learn how to identify anything suspicious before it is too late. The paper takes along with it the important steps such as cleaning and preparing the data, extracting meaningful features and the last step is putting the trained models into action in a live payment setting.

L. Kumar, L. Kumar, "The use of machine learning algorithms to detect real-time fraud in digital payment systems: Leveraging the methods of the International Journal of Multidisciplinary Innovation and Research Methodology, vol. 3, no. 2, 2024.

Reference: https://ssrn.com/abstract=5052498 This article goes deep into explaining how machine learning algorithms can be implemented to identify and prevent fraud as it occurs in electronic payment systems. The author examines how such models can be trained and tuned to transaction data to predict with reasonable accuracy whether a piece of activity is legitimate or a piece of fraud. There are also some quite practical issues that the study addresses that are associated with such a system, including having to contend with uneven datasets, maintaining low response times, and ensuring that everything can withstand the increased workload as transaction volumes increase.

P. R. Kantheti and S. Bvuma, AI and Machine Learning in Fraud Detection: Securing Digital Payments and Economic Stability, International Journal of Scientific Research in Science and Technology, vol. 11, no. 3, pp. 974–982, 2024.

Link: https://doi.org/10.32628/IJSRST52310291 In the paper, the authors discuss the role that AI and machine learning increasingly have in ensuring the safety of digital payments and, therefore, the overall economic stability. They consider the way smart models can be incorporated into payment platforms to identify suspicious transactions early, reduce false alarms, and develop a more robust defence against financial fraud. Finally, the paper presents a strong argument as to how effective and well-structured fraud detection systems can save the daily user and the mega financial institutions against the ever-changing tricks of the cybercriminals.

3. METHODOLOGY

The digital payment fraud detection system is designed to find transactions in digital payment systems. It does this by following a series of steps. These steps include collecting data checking the data is correct getting the data ready using machine learning to predict if a transaction is fake putting everything together and making the system work.

This way the system can find transactions as they happen. It can do this because it looks at how people use the system and finds transactions that do not fit this pattern.

3.1 Collecting Data

The step is to collect data about digital transactions from places like online banking, mobile wallets and card payment systems. This data includes things like how much money was moved, when it was moved what kind of store it was moved to, where it was moved from and how the user normally acts. All this data is stored safely. Get ready to be looked at.

This step makes sure the system gets the data it needs to find transactions.

3.2 Checking and Preparing Data

After the data is collected it is checked to make sure it is real and complete. Any data that is not correct is a copy. Is broken is removed. This makes sure the data is quality. The data is also prepared by filling in missing information making sure all the transaction information is similar and changing words into numbers. This makes the data more reliable and ready to use.

It also helps get rid of information that is not needed and makes sure the system can find the important patterns in the transactions.

3.3 Using Machine Learning to Predict Fraud

InIn this step the system uses machine learning to decide if a transaction is real or fake. The system looks at things like how much money was moved, where it was moved from and how often the user makes transactions. It finds patterns that're like fake transactions.

The system can find transactions that're suspicious because they are different from what the user normally does. The machine learning models learn what fake transactions look like and use this to predict if a new transaction is suspicious.

The digital payment fraud detection system uses payment fraud detection to find fake transactions in digital payment systems. It does this by using machine learning to look at payment transactions and find patterns that are like fake transactions.

The digital payment fraud detection system is good at finding transactions because it uses digital payment fraud detection to look at the transactions and find patterns that are, like fake transactions.

3.4 Workflow and Deployment

The workflow puts together data input and preprocessing and prediction and result generation in one pipeline.When something is bought or sold it goes through a trained model to check if everything is okay.

The system then tells us if it's fraud or not and gives a score that shows how sure it is that it's fraud.The fraud detection model is put into a payment platform when its ready to use.

We use this platform all the time to check for fraud It watches all transactions to see if anything bad is happening.It tells the system if something suspicious is going on with the fraud detection model.

4. Result and Analysis:

5. LIMITATIONS AND STRENGTHS

Limitations:

- The system is reliant on the dataset on which the model is being trained.
- It could also not be able to identify all new or sophisticated fraud patterns.
- When other real-world data is used, the model accuracy could be reduced.
- The system may fail to handle transaction volumes that are very high.

Strengths:

- Identifies fraudulent transactions automatically.

- Aids in the decrease of financial fraud.
- Offers rapid analysis of transactions.
- Enhances digital payment systems security.

6. CONCLUSION:

This paper is going to study payment fraud detection.It is curious to know how methods are approached in transaction pattern and detection of fraud in digital payment.The paper also examines the shortcomings of rule-based systems in the detection of digital payment fraud. It verifies the ability of machine learning models to increase the accuracy of payment fraud detection.The aim is to minimize positive and adjust to new trends in digital payment fraud detection.The study follows a methodology to examine the results of the recent studies.It is not only about technical performance, but about the detection of payment fraud. It raises the question of the effectiveness of existing digital payment fraud detection systems in digital payment scenarios in the world.This paper seeks to learn about payment fraud detection, in the complex digital payment landscapes.It examines the state of digital payment detection fraud and the way it can be changed.The existing digital payment fraud detection systems are limited.The experiment is interested in whether machine learning can be used to enhance the detection of payment fraud..

7. Future Work:

The fraud detection system that we have can be made better. We can work on it to make it perform well handle a lot of work and be useful in the world. In the future we can add machine learning and deep learning techniques to help it find more complicated fraud patterns. We can also make it watch transactions in time for big payment platforms.We can also use cloud-based infrastructure and big data technologies to handle a lot of transactions. We can add security features like alerts and multi-factor authentication to make fraud prevention stronger.

Improvements :

We should use deep learning algorithms to detect fraud more accurately.
We should watch payment gateways in time.
We should put the system on cloud platforms so it can handle a lot of work.
We should add alerts, by SMS or email when we see transactions.
We should use data technologies to process a lot of transaction data.

References:

1. Jeyachandran, P. (2024). Leveraging Machine Learning for Real-Time Fraud Detection in Digital Payments. SSRN Working Paper. http://dx.doi.org/10.2139/ssrn.5076783 (SSRN)
2. Kumar, L. (2024). Leveraging Machine Learning Algorithms for Real-Time Fraud Detection in Digital Payment Systems. International Journal of Multidisciplinary Innovation and Research Methodology, 3(2). https://ssrn.com/abstract=5052498 (SSRN)
3. Kantheti, P. R., & Bvuma, S. (2024). AI and Machine Learning in Fraud Detection: Securing Digital Payments and Economic Stability. International Journal of Scientific Research in Science and Technology, 11(3), 974–982. https://doi.org/10.32628/IJSRST52310291 (Ijsrst)
4. Ali, A., Abd Razak, S., Othman, S. H., et al. (2022). Financial Fraud Detection Based on Machine Learning: A Systematic Literature Review. Applied Sciences, 12(19), 9637.

https://doi.org/10.3390/app12199637 (MDPI)

5. Alarfaj, F. K., Malik, I., Khan, H. U., et al. (2022). Credit Card Fraud Detection Using State-of-the-Art Machine Learning and Deep Learning Algorithms. IEEE Access, 10, 39700–39715. (Springer)
6. Lebichot, B., Verhelst, T., Le Borgne, Y.-A., He-Guelton, L., Oblé, F., & Bontempi, G. (2021). Deep learning techniques for fraud detection — reviewed in: Year-over-Year Developments in Financial Fraud Detection via Deep Learning. arXiv:2502.00201. (arXiv)
7. Bodepudi, A. (2021); Musiliudeen et al. (2024) — comparative study of ML models for fraud detection, cited in: Enhancing Fraud Detection in Credit Card Transactions: A Comparative Study of Machine Learning Models. Computational Economics. https://doi.org/10.1007/s10614-025-11071-3 (Springer)
8. Ahmad, H., Kasasbeh, B., Aldabaybah, B., & Rawashdeh, E. (2023). Class Balancing Framework for Credit Card Fraud Detection Based on Clustering and Similarity-Based Selection (SBS). International Journal of Information Technology, 15, 325–333. (MDPI)
9. Jemai, J., Zarrad, A., & Daud, A. (2024). Identifying Fraudulent Credit Card Transactions Using Ensemble Learning. IEEE Access, 12, 54893–54900. (MDPI)
10. Esenogho, E., Mienye, I. D., Swart, T. G., Aruleba, K., & Obaido, G. (2022). A Neural Network Ensemble with Feature Engineering for Improved Credit Card Fraud Detection. IEEE Access, 10. (Nature)
11. Cherif, A., Badhib, A., Ammar, H., Alshehri, S., Kalkatawi, M., & Imine, A. (2023). Credit Card Fraud Detection in the Era of Disruptive Technologies: A Systematic Review. Journal of King Saud University – Computer and Information Sciences, 35(1). (Eajournals)
12. Hilal, W., Gadsden, S. A., & Yawney, J. (2022). Financial Fraud: A Review of Anomaly Detection Techniques and Recent Advances. Expert Systems with Applications, 193. (Eajournals)
13. Al-Hashedi, K. G., & Magalingam, P. (2021). Financial Fraud Detection Applying Data Mining Techniques: A Comprehensive Review from 2009 to 2019. Computer Science Review, 40, 100402. (Sage Journals)
14. Deep learning credit card fraud detection paper noting that global payment card fraud losses totaled USD 33.83 billion in 2023: Yi, Z., et al. (2025). A Deep Learning Method of Credit Card Fraud Detection Based on Continuous-Coupled Neural Networks. Mathematics, 13(5), 819. https://doi.org/10.3390/math13050819 (MDPI)
15. Compagnino, A. A., et al. (2025). An Introduction to Machine Learning Methods for Fraud Detection. Applied Sciences,15(21),11787. https://doi.org/10.3390/app15211787 (MDPI)