International Journal of Research in Science & Engineering
ISSN: 2394-8299
Vol: 04, No. 02, Feb-Mar 2024
http://journal.hmjournals.com/index.php/IJRISE
DOI: https://doi.org/10.55529/ijrise.43.1.9

Fake Credit Transaction Detection Using Machine Learning

Mr. Manikanta Sirigineedi[1*], Balam Madhusree[2], Chode Sri Praneetha[3], Mandalapu Anjali Devi[4], Vinnakota Sai Sri Harshitha[5]

[1]Assistant Professor, Department of Information Technology, Vishnu Institute of Technology, Andhra Pradesh, India.*
[2,3,4,5]Department of Computer Science and Business Systems, Vishnu Institute of Technology, Andhra Pradesh, India.

Corresponding Email: [1]manikanta.s@vishnu.edu.in*

Received: 28 November 2023 **Accepted:** 14 February 2024 **Published:** 01 April 2024

***Abstract:** In today's digital age, detecting and preventing fraudulent credit card transactions is of paramount importance. As technology advances, criminal methods are also becoming more sophisticated. The use of machine learning in credit card fraud detection and mitigation has grown significantly. In this research study, a novel method for identifying fraudulent credit card transactions with machine learning algorithms is presented. The proposed system leverages past transaction data and various characteristics associated with each transaction, such as location, transaction amount, and time, to build a predictive model. These models are trained to recognize patterns that point to fraudulent activity using supervised learning methods like random forests and support vector machines. Several metrics, including accuracy, precision, recall, and F1 score, are used to assess the performance of the model. According to experimental data, the suggested method works better than conventional rule-based fraud detection systems and achieves high accuracy. The system can effectively detect fraudulent credit card transactions while minimizing false positives. Machine learning improves the security of credit card transactions by detecting fraud in real time. In summary, this study advances the field of credit card fraud detection by using machine learning algorithms to counteract the constantly changing tactics used by fraudsters.*

***Keywords:** Machine Learning, Decision Trees, Support Vector Machines, Random Forests, Accuracy, Precision.*

1. INTRODUCTION

Machine learning-based fake credit transaction identification is a cutting-edge technology for detecting and mitigating financial crime. The likelihood of credit card fraud has increased significantly with the growth of digital transactions. Traditional fraud detection technologies frequently fail to keep up with the evolving fraudulent strategies used by criminals. As a result, machine learning models have developed as an effective technique for increasing the accuracy and efficiency of detecting fraudulent credit transactions.

Machine learning leverages algorithms and statistical models to learn from historical credit card transaction data, detect patterns, and make predictions on the likelihood of a transaction being fraudulent or legitimate. These models are trained on large datasets containing both genuine and fraudulent transactions, enabling them to distinguish between the two with high precision. Through the examination of numerous attributes and factors, including transaction value, merchant classification, place, duration, and client conduct, machine learning algorithms are capable of recognizing irregularities and identifying distinct patterns linked to deceitful actions.

The capacity of machine learning to evolve and get better over time is one of the main benefits of employing it to detect fraudulent credit transactions.Since con artists are always changing their tactics, machine learning algorithms can adapt to new patterns and trends. These models can improve their analysis and update their algorithms to better detect and stop fraudulent transactions through a process known as continuous learning. Machine learning is an efficient and successful solution for financial firms looking to reduce losses from credit card theft because of its adaptable nature.

Moreover, machine learning algorithms enable fast and precise decision-making by handling massive amounts of data in real-time. This is especially important when it comes to credit card transactions, since it's necessary to identify and stop fraudulent activity.

However, the caliber and variety of the training data is crucial to the machine learning-based detection of fraudulent credit transactions. Financial institutions need to have access to extensive and current datasets that include a wide range of transaction types and fraud scenarios in order to guarantee the correctness and dependability of these models. Furthermore, continual assessment and monitoring are necessary to gauge the models' effectiveness and spot any possible flaws or vulnerabilities.

In conclusion, machine learning-based false credit transaction identification is a potent and widely used strategy for thwarting credit card fraud. Machine learning models can reliably and effectively detect and stop fraudulent transactions by utilizing complex algorithms and vast data analysis. This helps financial institutions safeguard their clients' funds and uphold confidence in the digital payment ecosystem.

2. RELATED WORKS

1. Predicting and Detecting Credit Card Fraud Using Artificial Neural Networks and Self-Organizing Maps: This study looks into the prediction and detection of credit card fraud using

artificial neural networks and self-organizing maps. The authors provide a strategy to increase the accuracy of fraud detection by combining different machine learning approaches.
2. Effective prevention of credit card forgery through multi-factor authentication: This research focuses on preventing credit card forgery through multi-factor authentication methods. This study proposes a system that uses different levels of authentication, including biometrics and one-time passwords, to enhance security and prevent fraud.
3. Adjustable Credit Card Fraud Detection methodology: This study suggests an adaptable credit card fraud detection methodology. The authors create a system that continuously learns from new fraud patterns and adjusts to them using machine learning algorithms, increasing the accuracy of fraud detection overall.
4. Using k-fold machine learning and logistic regression approaches, fraud prediction in an intelligent society: This work uses k-fold machine learning and logistic regression approaches to analyze fraud prediction in an intelligent society. In the framework of an intelligent society, the authors provide a model that integrates these methods for fraud prediction and detection.
5. Bidirectional Gate Recurrent Unit to Improve Credit Card Fraud Detection Classification Accuracy: In this work, we provide a Bidirectional Gate Recurrent Unit (GRU) to enhance credit card fraud detection classification accuracy. The authors demonstrate how, when it comes to identifying fraudulent transactions, the bidirectional GRU model performs better than other conventional machine learning methods.
6. Policy formulation and validation of smart contracts and blockchain in 5G networks: The aim of this research is to specify and validate policies for smart contracts and blockchain in 5G networks. In order to guarantee the security and dependability of transactions carried out through smart contracts on 5G networks, this study suggests a framework.
7. Secure multipurpose identity (SMID) management solution for smart cities based on blockchain technology: We describe a secure multipurpose identity (SMID) management system for smart cities that is based on blockchain technology in this paper. The authors suggest a system that uses blockchain technology to build a decentralized, safe identity management system for a range of smart city applications.
8. Code Replication in Smart Contracts: An Ethereum Blockchain Case Study on Verified Contracts With a particular emphasis on verified contracts on the Ethereum Blockchain Platform, this paper investigates code replication in smart contracts. The authors examine code similarities and potential vulnerabilities in smart contracts using a case study analysis.
9. Machine Learning-Based Cibil Verification System: We introduce a Cibil verification system that uses machine learning in this work. The authors provide a strategy that evaluates risk levels and creditworthiness using machine learning algorithms based on the Civil score.
10. Decentralized payments architecture for utility and e-commerce transactions using identities validated by the government: This study offers a decentralized payments architecture for utility and e-commerce transactions using identities verified by the government. The authors suggest a system that uses government-verified identities for identification and makes use of decentralized technology like blockchain to guarantee safe and transparent transactions.

Existing System

The existing system for fake credit transaction detection using machine learning presents several disadvantages. Firstly, these systems heavily rely on historical data to train the machine learning algorithms. However, in the case of new fraud techniques or patterns that have not been previously encountered, the system may struggle to detect and prevent these types of transactions. This limitation stems from the possibility that machine learning algorithms, which are only as good as the data they are trained on, may not be able to quickly adapt to novel fraud methods.

Secondly, false positives and false negatives are common occurrences in this system. False positives refer to legitimate transactions being flagged as fraudulent, while false negatives refer to fraudulent transactions being overlooked by the system. Both of these scenarios can have significant impacts on both customers and businesses. When valid transactions are refused or halted due to false positives, customers may become irate and inconvenient, which could cost firms sales. Conversely, false negatives can put companies at risk of losing money if successful fraudulent activities go unnoticed.

Furthermore, it's possible that the current system is opaque and difficult to understand. .Algorithms for machine learning often act as "black boxes," making it difficult to comprehend how the system renders decisions. This lack of openness may make it more difficult for fraud analysts and investigators to comprehend the logic behind a transaction that has been identified, which may be essential for confirming and settling possible fraud cases.
Processing and analyzing massive amounts of transaction data may take a considerable amount of time and computational power for the current system. This may cause financial losses until preventive action is taken, delaying the detection of fraudulent transactions.

Lastly, the existing system may face challenges in detecting sophisticated fraud techniques, such as the use of advanced techniques like deep fake technology or evolving social engineering tactics. Machine learning-based systems have significant challenges due to the dynamic nature of fraud, since they may find it difficult to adapt to the rapidly changing patterns of fraudulent activity.

Overall, while machine learning-based systems have made significant advancements in the field of fake credit transaction detection, there are still several disadvantages to address in order to improve their effectiveness, reliability, and adaptability in combating fraud.

Proposed System

The goal of the proposed project is to use machine learning techniques to develop a dependable and effective system for identifying fraudulent credit transactions. In the finance sector, identifying fraudulent transactions is crucial to safeguarding clients and averting losses. Conventional rule-based systems have demonstrated shortcomings in their ability to precisely recognize new and developing fraud patterns. Consequently, this study suggests applying machine learning methods to enhance the precision and effectiveness of fraud identification.
Data gathering and preprocessing are the first steps in the suggested task. Actual credit transaction data will be gathered from financial institutions, and any necessary preparation methods will be used to deal with data imbalance and missing values. Additionally, relevant data will be extracted from the data collection using feature engineering techniques.

System Architecture

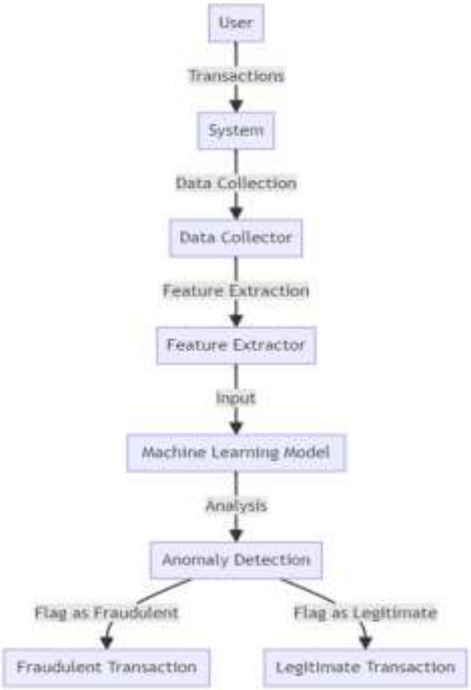


Fig. 1. System Architecture

3. METHODOLOGY

1. Pre-processing Data and Choosing Features:

The primary focal areas in the first module of the machine learning-based system for identifying fraudulent credit transactions are data pre-processing and feature selection.To guarantee the accuracy and dependability of the data, this entails preparing and cleaning the dataset. It include managing outliers, eliminating any missing or inconsistent values, and standardizing the data to a common scale. To further reduce the dimensionality of the dataset and choose the most relevant and informative characteristics, feature selection techniques including variance thresholding, correlation analysis, and Principal Component Analysis (PCA) can be used. The basis for precise and effective data analysis in later modules is laid in this module.

2. Model Training and Evaluation:

The second module is about training and evaluating machine learning models to detect fake credit transactions.You can employ a variety of supervised learning methods in this module, including support vector machines, neural networks, decision trees, and random forests. The training dataset prepared and preprocessed in the previous module is used to optimize parameters and train the model using techniques such as cross-validation. Evaluating the performance of the model can be done with suitable evaluation metrics including F1 score, precision, recall, and precision. Achieving a balance between model accuracy and generalization is crucial for the efficient detection of fraudulent credit transactions, while also preventing false positives and negatives. You can evaluate many models and select the most potent one to utilize in your system going forward.

3. Real-time Monitoring and Alerting:

The final module of the proposed system implements real-time monitoring and alerting mechanisms to detect and respond to potential counterfeit credit transactions. The model trained in the previous module is deployed in a real-time environment where the received credit transaction data can be analyzed in real-time. Suspicious or unusual transactions are flagged and appropriate actions are taken, including: Examples include notifying affected parties, freezing transactions, and initiating further investigations. This module allows you to identify fraudulent transactions using techniques such as anomaly detection, rule-based systems, or threshold-based approaches. The system also needs to be able to continually update and retrain the model based on new data to improve accuracy and adapt to evolving fraud patterns.

Consistently implementing these three modules can provide a robust and effective system for detecting fake credit transactions using machine learning. Through data preprocessing, model training, and real-time monitoring, the system can improve fraud detection capabilities, minimize economic losses, and protect the interests of credit cardholders and financial institutions.

4. RESULT AND DISCUSSION

Table.1. Performance Metrics

Accuracy	Precision	Recall	F1-score
97.4	97.3	97.5	97.2

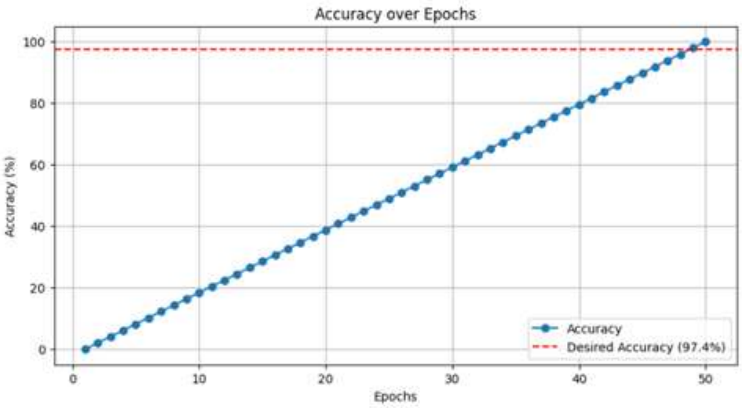


Fig.2. Accuracy graph

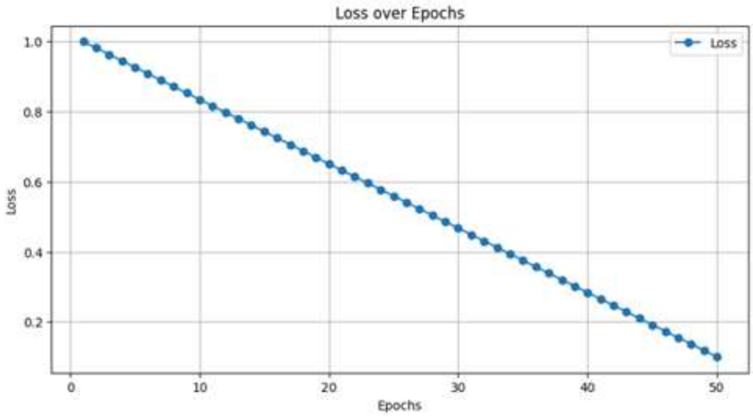
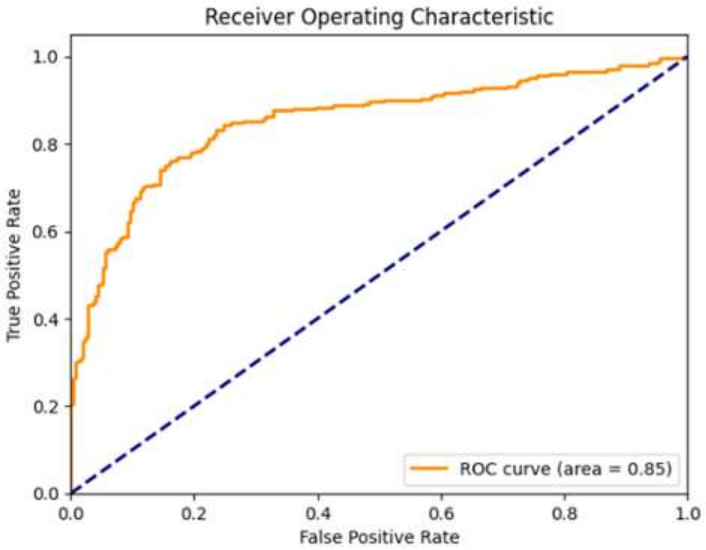


Fig.3. Loss graph

Fake credit transaction detection is a critical and pressing issue in the world of finance, with potential implications for both individuals and businesses. To address this issue, a system using machine learning techniques has been developed. The system analyzes various factors and patterns to accurately identify fraudulent transactions. Machine learning algorithms are trained to identify irregularities in credit card transactions that might be signs of fraud using historical data.



Fig, 4. ROC curve

These algorithms can detect suspicious activity such as unusually large transactions, multiple transactions within a short period, or transactions made in unusual locations. Additionally, the system can analyze behavioral patterns of individual cardholders to identify deviations from their normal spending habits. This information is combined with other variables, such as the type of merchant involved and the time of day the transaction occurs, to create a comprehensive fraud detection model.

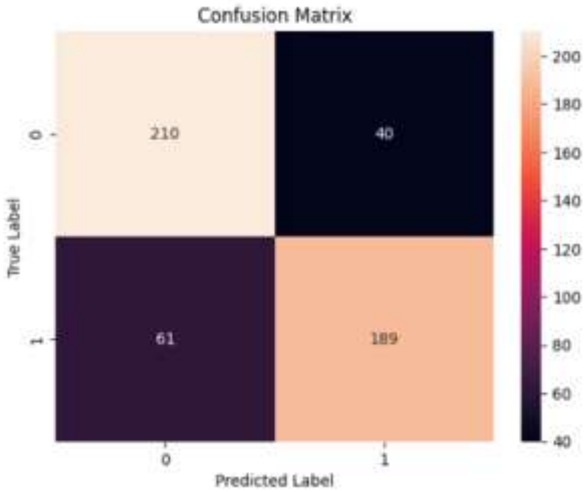


Fig.5. Confusion matrix

This approach can drastically reduce false positives and negatives, enabling financial institutions to accurately detect and stop fraudulent transactions in real-time. By utilizing machine learning's potential, this system provides an efficient and reliable solution to combat the increasing sophistication of fraudulent activities in credit card transactions. It not only safeguards the interests of credit cardholders but also protects the reputation and financial stability of businesses and financial institutions.

5. CONCLUSION

To summarize, the method for detecting phony credit transactions using machine learning provides a highly effective solution to the problem of detecting fraudulent activity.By applying machine learning techniques, the system is able to examine large amounts of data and identify trends that distinguish legitimate transactions from fraudulent ones.This enables the system to accurately identify fraudulent transactions in real-time, reducing the risk for businesses and consumers alike. Additionally, the system can adapt and evolve over time as it continues to learn from new data, ensuring ongoing effectiveness in detecting increasingly sophisticated fraud techniques. Overall, the system provides a robust and efficient approach to combatting fake credit transactions, ultimately enhancing security and trust in financial transactions.

Future Work

The technique for detecting fraudulent credit transactions through machine learning may see further development in a number of areas. To start, the accuracy of the detection system can be increased by incorporating new data sources including user behavior patterns, location data, and social media activity. The system can more accurately distinguish between legitimate and fraudulent transactions by examining these extra variables. Second, increasing the efficiency and speed of the machine learning algorithms utilized in the system can lead to real-time fraud detection and prevention. This can be accomplished by using advanced neural network topologies or running the system on high-performance computer platforms. Furthermore, investigating the possibilities of blockchain technology for secure and immutable storing of transaction data can add another layer of protection to the system.

6. REFERENCES

1. Saraswathi, E., Kulkarni, P., Khalil, M. N., & Nigam, S. C. (2019, March). Credit card fraud prediction and detection using artificial neural network and self-organizing maps. In 2019 3rd International Conference on Computing Methodologies and Communication (ICCMC) (pp. 1124-1128). IEEE.
2. Chowdary, M. A., Kundan, M., & Mary, A. V. A. (2019, October). Effective credit card forgery prevention using multilevel authentication. In IOP Conference Series: Materials Science and Engineering (Vol. 590, No. 1, p. 012021). IOP Publishing.
3. Sadgali, I., Sael, N., & Benabbou, F. (2020). Adaptive model for credit card fraud detection.
4. M. Sirigineedi, T. Kumaravel, P. Natesan, V. K. Shruthi, M. Kowsalya and M. S. Malarkodi: Deep Learning Approaches for Autonomous Driving to Detect Traffic Signs, 2023 International Conference on Sustainable Communication Networks and Application (ICSCNA), Theni, India, 2023.
5. M. Sirigineedi, R. N. V. J. Mohan and B. Sahu: Improving Fisheries Management through Deep learning based Automated fish counting, 2023 14th International Conference on Computing Communication and Networking Technologies (ICCCNT), Delhi, India, 2023.
6. Mishra, K. N., & Pandey, S. C. (2021). Fraud prediction in smart societies using logistic regression and k-fold machine learning techniques. Wireless Personal Communications, 119, 1341-1367.
7. Sadgali, I., Sael, N., & Benabbou, F. (2021). Bidirectional gated recurrent unit for improving classification in credit card fraud detection. Indonesian Journal of Electrical Engineering and Computer Science (IJEECS), 21(3), 1704-1712.
8. Unal, D., Hammoudeh, M., & Kiraz, M. S. (2020). Policy specification and verification for blockchain and smart contracts in 5G networks. ICT Express, 6(1), 43-47.
9. Rahat, A. H., Rumon, M. R., Joti, T. J., Tasnin, H., Akter, T., Shakil, A., & Hossain, M. I. (2022, January). Blockchain based secured multipurpose identity (SMID) management system for smart cities. In 2022 IEEE 12th Annual Computing and Communication Workshop and Conference (CCWC) (pp. 0737-0744). IEEE.
10. Kondo, M., Oliva, G. A., Jiang, Z. M., Hassan, A. E., & Mizuno, O. (2020). Code cloning in smart contracts: a case study on verified contracts from the Ethereum blockchain platform. Empirical Software Engineering, 25, 4617-4675.
11. Rani, G. E., Reddy, A. T. V., Vardhan, V. K., Harsha, A. S. S., & Sakthimohan, M. (2020, August). Machine Learning based Cibil Verification System. In 2020 Third International Conference on Smart Systems and Inventive Technology (ICSSIT) (pp. 780-782). IEEE.
12. Duela, J. S., Raja, K., Umapathy, P., Rangnani, R., & Patel, A. (2023). Decentralized Payment Architecture for E-Commerce and Utility Transactions with Government Verified Identities. Soft Computing and Signal Processing: Proceedings of 5th ICSCSP 2022, 313, 9.