Industrial Engineering Journal
ISSN: 0970-2555
Volume : 53, Issue 4, April : 2024

Fraud Detection In Banking System Using Machine Learning

Prof.Sneha Tirth, Viraj Bhalekar, Pranali Sakpal, Shramik Rathod, Siddhant Ladkat
Trinity College Of Engineering And Research, Pune-48, Maharashtra, India

❖ ABSTRACT

In today's world, online payment are mostly used making it easy for the fraudsters to cause fraud in banking. Various security techniques are involved in this. We conducted a comparative evaluation of existing machine learning methods designed for modeling imbalanced data and outlier detection.
The system is designed with a React on Frontend, a Node.js on Backend, and MongoDB as a database to store transactional history. Logistic Regression is employed as the primary machine learning model to classify transactions as fraudulent or legitimate. The system's architecture integrates machine learning models directly with the blockchain. This project aims to develop a comprehensive fraud detection system for banking transactions, credit card frauds and leveraging machine learning, blockchain technology, and secure cryptographic practices.

Keywords: Credit Card · Mobile payment · Fraud detection · Machine learning · Imbalanced data · Outlier detection

❖ I - INTRODUCTION

Now-a-days mobile payment has become one of the mainstream payment methods. Thousands of transactions are carried out on the online trading platform all the time.Personal property in the complex network environment has the risk of theft, which not only damages the interests of consumers, but Nowadays, the number of smartphones are increasing, due to this online payment systems are becoming more popular, which in turn attracts more fraudsters. For this extensive research is required for detection of fraud using machine learning techniques. In [3] The author has proposed the extra boost based framework for detection of fraud in financial transactions. For efficiency of this framework a comparative study of machine learning techniques of modelling and outlier detection was done.
In [3] The author has used various resources and methods like risk models, algorithms, human action, tools, web technology tools and business system in risk management. Now-a-days, online fraud detection is a difficult problem which requires a great understanding to deal with the large data set.
Therefore, the transaction fraud detection is one of the key and tools to solve the problem of network transaction fraud. That are the Since they are verification techniques, it is difficult to obtain the laws hidden behind the fraud transaction data. The big data technology and machine learning algorithm provide efficient detection from methods for transaction fraud detection [2].
In the rapidly evolving financial landscape, fraud detection systems are crucial for maintaining trust and security among users. There are three key stages where you should focus your ecommerce anti-fraud efforts. These are the signup, login, and transaction stages.
Ecommerce fraud includes any kind of malicious action designed to exploit online stores.
The most common attacks are related to fraudulent transactions, made with stolen credit card numbers.
This system aims to enhance security and efficiency in detecting fraudulent transactions by leveraging machine learning algorithms.
In response to this challenge, banks have been increasingly relying on advanced technological solutions, particularly machine learning and data analytics, to detect and prevent fraud. This report provides an overview of fraud detection in banking, highlighting the importance of proactive measures and the role of technology in combating fraudulent activities.

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 53, Issue 4, April : 2024

❖ II - OBJECTIVE

- We are not only detecting the fraud in transactions but we are blocking the whole transaction.
- We can also use Human Inteligence for better context and insights.
- Interpretability is needed so that all the people can use this system.
- We can prevent financial loss of users.
- Risk of non-compliance is reduced

Risk Assessment: Analyzing the data to identify potential risks, predict default probabilities, and enhance risk management strategies.

Fraud Detection: Using data analytics to detect unusual patterns and behaviors that could indicate fraudulent activities, helping banks prevent financial losses.

Customer Insights: Gaining a deeper understanding of customer behavior, preferences, and needs to improve customer experience and tailor services.

Operational Efficiency: Optimizing banking processes by analyzing data to identify bottlenecks, streamline operations, and reduce costs.

Credit Scoring: Developing predictive models to assess creditworthiness and determine appropriate lending terms for customers.

Detection of Fraudulent Transactions: The primary goal is to accurately detect fraudulent transactions, such as credit card fraud, insurance fraud, or online payment fraud. This involves identifying unusual patterns or anomalies in the data that may indicate fraudulent behavior.

Minimize False Positives: While detecting fraud is crucial, it's equally important to minimize false positives, where legitimate transactions are incorrectly flagged as fraudulent. Balancing accuracy with the reduction of false positives is a key objective.

Real-time Detection: In some cases, the system may need to operate in real-time, detecting fraud as transactions occur. This requires efficient algorithms and data processing.

Market Trends: Analyzing market data to understand current needs and technologies.

High Security: This application provides high security to users with no loss of data.

The system aims to leverage blockchain technology to enhance the security and transparency of transactions.

By integrating blockchain, the system can provide a tamper-proof ledger for transactions, making it more difficult for fraudsters to manipulate transaction data.

The addition of blockchain technology will require the implementation of advanced security measures, such as SHA-256 for hashing, AES for encryption, and crypto-js for securely performing transactions.

The primary goal is to accurately detect fraudulent transactions, such as credit card fraud, insurance fraud, or online payment fraud.

•

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 53, Issue 4, April : 2024

❖ III - LITERATURE SURVEY

1. **Fraud Detection using Machine Learning and Deep Learning (2019)**Many scammers steal the credit card' information for unauthorized purchases which causes fraudulent activities everyday.Various website and bank figure out fraudulent activities and stop them by using Machine learning & Deep learning.

2. **Predicting Mobile Money Transaction Fraud using Machine Learning Algorithms(2022)** [4] This study mainly focuses on the machine learning classifiers in online money transfer to predict the transactions whether they are accurate or not. The classifiers such as Random forest gives the best performance in terms of fraud detection also the techniques such as logistic regression are also used.

3. **Big Data Application the Banking Sector A Bibliometric Analysis Approch(2021) [7],[8]** This study focuses on the literature study on the applications of big data in the banking sector. They use a bibliometric analysis method. This approach describes all the research outputs, implementations streams and citation rates and research agenda.

4. **Online transaction fraud detection system based on machine learning(2023)** detection algorithm based on XGBoost. This algorithm constructs the XGBoost classifier with best parameters by using Hyperopt [7][8]transaction fraud detection system finally provides services in the form of Web. In order to ensure the detection accuracy, we built an online detection platform based on XGBoost model with Django framework.

5. **Fraud Detection in Banking Data by Machine Learning Techniques Banking** sector are best use now-a-days in online mode only making it easy for the fraudsters in order to avoid such fraud in banking various security techniques are involved. Machine learning can be de-facto in order to detect the fraud efficiently. Ml/DL can be utilize for fraud detection in better way for those attackers who surpasses basic cryptographic methods.The data received here are unbalanced data so to detect fraud in efficient way [1] has mentioned the ML/DL methods. Here Bayesian optimization methods are used to optimize the hyperparameters.

6. **An Amalgamated Novel IDS Model for Misbehaviour Detection using VeReMiNet** While using the machine methods the unbalanced data-sets need to be prepossessed where feature selection is wisely improve the efficiency of fraud detection. In [2] the author used the marine predator algorithm for feature selection algorithm which nature inspired meta-heuristic algorithm and follow the concept the marine creature prey and predator methods. This is one of the latest algorithm and now it is utilizing for machine learning feature selection.

7. **FRAUD DETECTION USING MACHINE LEARNING** Various machine learning algorithm are used to detect the fraud in financial transaction. To increase the precision in financial transaction of detecting fraud various strategies and algorithms are used.In [3] the author reviews research in addressing advantages and disadvantages

8. **Fraud Detection in Mobile Payment Systems using an XGBoost-based Framework** Nowadays, the number of smartphones are increasing, due to this online payment systems are becoming more popular, which in turn attracts more fraudsters. For this extensive research is required for detection of fraud using machine learning techniques. In [3] The author has proposed the extra boost based framework for detection of fraud in financial transactions. For efficiency of this framework a comparative study of machine learning techniques of modelling and outlier detection was done.

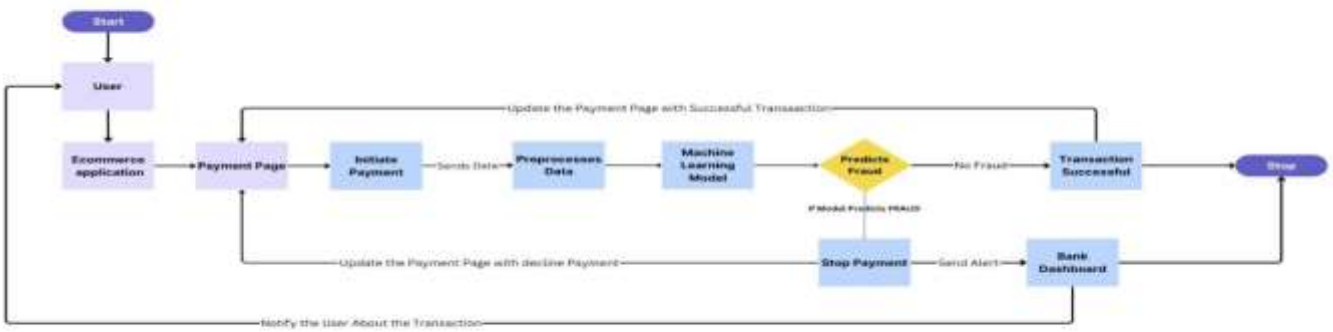
9. **Online payment fraud: from anomaly detection to risk management** In [3] The author has used various resources and methods like risk models, algorithms, human action, tools, web technology tools and business system in risk management. Now-a-days, online fraud detection is a difficult problem which requires a great understanding to deal with the large data set**.**

10. **The Impact of Big Data Analytics on the Banking Industry(2022)**[1] ,[2] in this paper, we propose an efficient approach for detecting on publicly available datasets and has used optimised algorithms LightGBM, XGBoost, CatBoost, and logistic regression individually.

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 53, Issue 4, April : 2024

❖ IV - PROPOSED METHODOLOGY

❖ Fraud Detection Model



Designing a fraud detection system for an e-commerce application using the technology stack which involves integrating machine learning models into the backend(Node) and creating a user-friendly frontend for monitoring and analysis.

MongoDB is used as the database to store transactional data securely. RESTful APIs are used to handle data communication between the React Native Frontend and the Database.

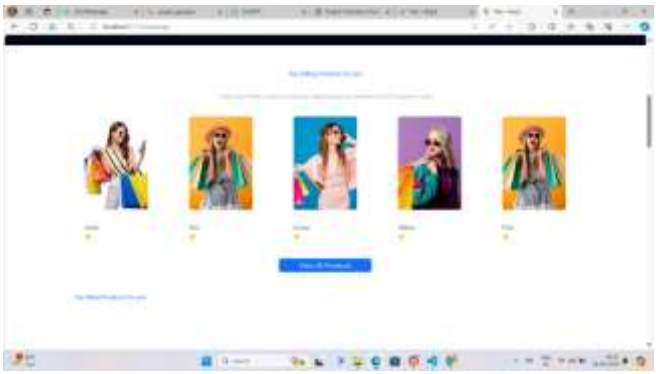
To enhance security, the system incorporates blockchain technology, which provides a decentralized and immutable ledger for transactions. This integration not only ensures the integrity and traceability of transactions but also serves as a robust foundation for fraud detection.

This methodology provides a high-level overview of how to implement a fraud detection system in a baking system using machine learning, React, Node.js, MongoDB, and blockchain technology.

❖ RESULT:-

➢ Homepage of the website where we can view multiple products

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 53, Issue 4, April : 2024



- Here the user can view all the products amd order them.

- In Product Details, after viewing all the details of the product, user can order the desired product by clicking on "Order Now" button.

- After clicking on Order Now, it will redirect you to the payment page where there are multiple options displayed for payment.

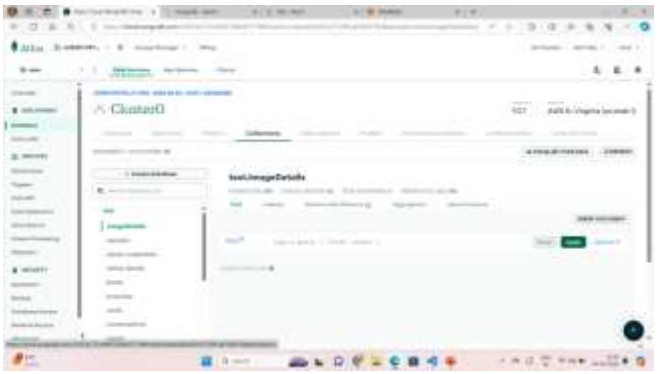
- We have redirected to "pay with visa" option which performs card payment and carries transactions and also identifies whether the transaction is legitimate or fraudulent.

- In this case, the system identifies that the fraud has occurred by displaying a popup message.

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 53, Issue 4, April : 2024

- By clicking on pay with metamask, it will redirect you to the connect to blockchain option. Here metamask acts as a payment gateway.

"Payment Successful" message is displayed on the screen after carrying out the transaction



- Here is the database to store the data, we have used MongoDB for the same, which is very secure and stores transaction history efficiently. Here the passwords are displayed in the encrypted form to avoid insecurity

❖ V. CONCLUSION

One of the leading frauds in the past few decades is Online Payment Fraud. In this research paper, we discussed and studied the concept of online payment fraud detection. It was seen that feature selection techniques are very important and can be implemented to attain lower false positive rate. We also implemented various machine learning algorithms like Logistic Regression, Random Forest for prediction. It is used for detecting if a particular transaction is fraudulent or not. A good fraud detection system should be accurate to predict if a given transaction is fraudulent or not. To improve the performance of the models, various techniques such as handling class imbalance, feature selection was used. Confusion matrix was used to evaluate the performance of our models, however we did not attain 0 False Positive and false negative score. It is important for a financial organization to attain 0 false positive and negative score as we discussed it impacts on the customer retention and costs lot of money for the refunds. More future works can be done on this research in order to attain the 0 false positive and negative score. Combination of models can be used to attain high accuracy in identifying the transactions as fraudulent and non-fraudulent

❖ VI. REFERENCES

[1] S. K. Hashemi, S. L. Mirtaheri and S. Greco, "Fraud Detection in Banking Data by Machine Learning Techniques," in IEEE Access, vol. 11, pp. 3034-3043, 2023, doi: 10.1109/ACCESS.2022.3232287.

[2] Saleha Saudagar, Rekha Ranawat, An Amalgamated Novel IDS Model for Misbehaviour Detection using VeReMiNet, Computer Standards & Interfaces, Volume 88, 2024, 103783, ISSN 0920-5489, https://doi.org/10.1016/j.csi.2023.103783

[3] Raghavan, Pradheepan & Gayar, Neamat. (2019). Fraud Detection using Machine Learning and Deep Learning.334-339. 10.1109/ICCIKE47802.2019.9004231.

[4] Hajek, PetrAbedin, Mohammad ZoynulSivarajah, Uthayasankar2023 2023/10/01Fraud Detection in Mobile Payment Systems using an XGBoost-based Framework Information Systems Frontiers 1572-9419

https://doi.org/10.1007/s10796-022-10346-6

[5] JOUR Vanini, Paolo Rossi, Sebastiano Zvizdic, Ermin Domenig, Thomas 2023 2023/03/13 Online payment fraud: from anomaly detection to risk management Financial Innovation https://doi.org/10.1186/s40854-023-00470-w.

[6] S. Saudagar and R. Ranawat, "Detecting Vehicular Networking Node Misbehaviour Using Machine Learning," 2023 International Conference for Advancement in Technology (ICONAT), Goa, India, 2023, pp. 1-3, doi: 10.1109/ICONAT57137.2023.10080114.

[7] Rahul More, et. al. International Journal of Engineering Research and Applications www.ijera.com ISSN: 2248-9622, Vol. 11, Issue 4, (Series-II) April 2021, pp. 01-05

[8] P. Raghavan and N. E. Gayar, "Fraud Detection using Machine Learning and Deep Learning," 2019 International Conference on Computational Intelligence and Knowledge Economy (ICCIKE), Dubai, United Arab Emirates, 2019, pp. 334-339, doi: 10.1109/ICCIKE47802.2019.9004231.

[9] S. Saudagar, M. Kulkarni, I. Raghvani, H. Hirkani, I. Bassan and P. Hole, "ML-based Java UI for Residence Predictor," 2023 International Conference on Intelligent Data Communication Technologies and Internet of Things (IDCIoT), Bengaluru, India, 2023, pp. 838-843, doi: 10.1109/IDCIoT56793.2023.10053480.

[10] Emmanuel Gbenga Dada, Joseph Stephen Bassi, Haruna Chiroma, Shafi'i Muhammad Abdulhamid, Adebayo Olusola Adetunmbi, Opeyemi Emmanuel Ajibuwa, Machine learning for email spam filtering: review, approaches and open research problems, Heliyon, Volume 5, Issue 6 2019, e01802, ISSN 2405-8440, https://doi.org/10.1016/j.heliyon.2019.e01802.

[11] R. Achary and C. J. Shelke, "Fraud Detection in Banking Transactions Using Machine Learning," 2023 International Conference on Intelligent and Innovative Technologies in Computing, Electrical and Electronics (IITCEE), Bengaluru, India, 2023, pp. 221-226, doi: 10.1109/IITCEE57236.2023.10091067.

[12] S. Saudagar, Ranawat, “Attack Detection and Classification for misbehaving Vehicles in Vehicular Networks using ML/DL”, accepted for publication in International journal on Recent and Innovation Trends in Computing and Communication, Vol 11 issue 9 Sept 2023.

[13] Ali, Abdulalem, Shukor Abd Razak, Siti Hajar Othman, Taiseer Abdalla Elfadil Eisa, Arafat Al-Dhaqm, Maged Nasser, Tusneem Elhassan, Hashim Elshafie, and Abdu Saif. 2022. "Financial Fraud Detection Based on Machine Learning: A Systematic Literature Review" Applied Sciences 12, no. 19: 9637. https://doi.org/10.3390/app12199637

[14] Ali, A.; Abd Razak, S.; Othman, S.H.; Eisa, T.A.E.; Al-Dhaqm, A.; Nasser, M.; Elhassan, T.; Elshafie, H.; Saif, A. Financial Fraud Detection Based on Machine Learning: A Systematic Literature Review. Appl. Sci. 2022, 12, 9637. https://doi.org/10.3390/app12199637.

[15] S. Saudagar, Dr. R. P. Mahajan, “Solving Vehicular ad hoc network issue using machine learning”, International journal of creative research and technology, Vol 9 Issue 4, April 2021.

[16] Ileberi, E., Sun, Y. & Wang, Z. A machine learning based credit card fraud detection using the GA algorithm for feature selection. J Big Data 9, 24 (2022). https://doi.org/10.1186/s40537-022-00573-8

.