International Journal of Interdisciplinary Innovative Research & Development (IJIIRD)
ISSN: 2456-236X
Vol. **11** Special Issue **03** | **2026**

A Machine Learning - Based UPI Fraud Detection System

Mr. Shardul S. Sawant[1], Mr. Yash M. Kumbhar[2], Mr. Aaron A. Fernandes[3], Mr. Yash G. Chavan[4], Professor Poonam Kadam[5]

[1.2.3.4] *Student, Computer Engineering Department, Metropolitan Institute of Technology and Management Sindhudurg, Maharashtra, India*

[5]*Vice Principal, Computer Engineering Department, Metropolitan Institute of Technology and Management Sindhudurg, Maharashtra, India*

DOI: 10.5281/zenodo.20631258

ABSTRACT

The rapid growth of digital payment systems has dramatically changed the financial environment, especially after the introduction of the Unified Payments Interface (UPI) system. UPI allows users to make instant transactions directly from their bank accounts through mobile applications. It is one of the most popular digital payment systems used today in the country. However, with the advent of digital payment systems, fraudulent practices like phishing, identity theft, and illegal transactions have also been on the rise. In traditional rule-based systems used to detect fraudulent transactions, the ability to detect sophisticated patterns of fraud has been limited because the rules used to detect fraud cannot keep pace with the changing nature of online fraud. Machine learning has been considered a potential approach to detecting fraudulent transactions because patterns can be used to identify anomalies. The objective of the research paper is to propose a machine learning-based approach to detecting fraudulent transactions that occur through the UPI payment system. In order to achieve the objective of the research paper, the Random Forest classification algorithm along with the Synthetic Minority Oversampling Technique (SMOTE) can be used to develop the system that can identify different parameters associated with the transaction, like the amount of the transaction, the type of transaction, the time of the transaction, device information, and geographical information. This will help the system to identify whether the transaction is genuine or fraudulent. The dataset that will be used for this research contains approximately 100,000 transactions. In this dataset, the genuine transactions will be the majority class, while the fraudulent transactions will be a small percentage. For this purpose, the dataset will be pre-processed through various techniques such as feature scaling, categorical encoding, normalization, etc. The results of the experiment prove that the Random Forest model provides a high accuracy of 98.61% and a ROC-AUC score of 0.9756. The model can be used to predict the results through a web-based application built with the Streamlit library. The proposed system can be used to efficiently detect fraudulent UPI transactions. ***Keywords: - UPI Fraud Detection, Machine Learning, Random Forest, SMOTE, Digital Payments, Financial Fraud***

1. INTRODUCTION

1.1 Background of Digital Payment Systems

Digitalization of financial services has profoundly altered the manner in which monetary transactions take place. With the introduction of the Unified Payments Interface by the National Payments Corporation of India, the digital payment system has revolutionized the manner in which money transfer services take place between bank accounts through the help of a mobile device. The Unified Payments Interface has gained huge popularity due to the simplicity of use, the low transactional costs, and the ability to make instant transactions. Although the Unified Payments Interface offers numerous benefits to the users, the rapid development of the digital payment system has led to an increase in financial fraud. Financial fraud is the exploitation of loopholes in the digital payment system by cybercriminals through phishing, fraudulent links, fraudulent payment requests, and social

engineering attacks. Financial fraud not only causes financial loss to the users but also affects the trust level of the public with regard to the digital payment system.

1.2 Need for Fraud Detection Systems

Traditionally, fraud detection systems have used rule-based systems in which specific conditions have been applied to detect fraudulent transactions. Although rule-based systems can be used to identify simple patterns of fraud, they may not be effective when dealing with sophisticated and changing patterns of fraud. This is because machine learning can learn patterns from historical transactions and automatically identify suspicious transactions.

The aim of carrying out this research is to develop a machine learning-based fraud detection system that can accurately identify fraudulent transactions while minimizing false positives.

2. LITERATURE REVIEW

Financial fraud detection has been an active area of research for many years in the domain of data mining and machine learning. With the rapid increase in the number of digital financial transactions, researchers have tried to develop various computational techniques to effectively detect fraudulent transactions. Earlier, various fraud detection systems were based on the application of statistical techniques or rule-based methods. Various techniques like Logistic Regression and Decision Trees were applied to analyze the financial transaction data to detect fraudulent transactions. Though the techniques showed good performance for the structured dataset, they were not effective for handling imbalanced datasets where the fraudulent transactions were fewer. With the recent advancements in machine learning techniques, researchers have developed various sophisticated techniques to effectively handle high-dimensional datasets. Various ensemble techniques like Random Forest, Gradient Boosting, and Extreme Gradient Boosting (XGBoost) have been applied to the fraud detection problem. These techniques aggregate the output from various decision trees to effectively classify the fraudulent transactions. Random Forest has gained popularity for its effectiveness to handle both numerical and categorical features.

Another challenge with the fraud detection system is the problem of class imbalance. Generally, the number of legitimate transactions far exceeds the number of fraudulent transactions. Because of this, the machine learning model becomes biased towards the majority class. As a result, it becomes ineffective in detecting fraudulent transactions. To solve the problem of class imbalance, various methods have been proposed to resample the given set of data. Some of the methods include under sampling the majority class, oversampling the minority class, and a combination of both. One of the most commonly used methods to solve the problem of class imbalance is the Synthetic Minority Oversampling Technique.

In addition to the commonly used machine learning algorithms for solving the problem of fraud detection, researchers have also used the Artificial Neural Network (ANN) model and the Long Short-Term Memory (LSTM) network to solve the problem. These models can effectively learn the complex relationships between the variables in the dataset. However, they require a lot of computational power to solve the problem. As a result, the ensemble machine learning model known as the Random Forest model can be used to solve the problem.

3. PROBLEM STATEMENT

The rapid growth of digital payment systems has caused a substantial increase in the number of financial transactions that are being conducted through online platforms. Among the digital payment systems, the Unified Payments Interface (UPI) has emerged as one of the most popular digital payment systems that is being used in the country because of the speed and ease of use of the system. Millions of financial transactions are being conducted through the UPI system on a daily basis, which has made the digital payment system an integral part of the digital economy. However, the growing popularity of the digital payment system has made the UPI system the primary target of cybercriminals who seek to exploit the loopholes of the digital payment systems for the purpose of carrying out fraudulent financial transactions. Fraudulent activities that can occur with the implementation of the UPI system can occur through several means, including phishing attacks, unauthorized access to the payment systems, fake payment requests, and social engineering attacks. It is a highly complex task to identify fraudulent financial transactions because the nature of the fraud is always changing.

Conventional fraud detection mechanisms use rule-based systems, wherein the transactions are analysed based on predefined rules. However, such rule-based systems are incapable of detecting complex fraud patterns, as the fraud patterns may emerge in the future. Another major challenge that has been identified with fraud detection systems is the class imbalance problem that occurs within the dataset of financial transactions. In most cases, the number of valid transactions is larger compared to the number of fraudulent transactions. This has caused the machine learning model to be biased towards the majority class, which has, in turn, influenced the accuracy of the model in detecting fraudulent transactions. Additionally, the detection system should be able to process a large number of transactions in a short time period with high accuracy and low false positives. In general, the objective of the study is to develop a machine learning model that can accurately identify fraudulent transactions using the UPI payment mode, where the model works efficiently.

4. PROPOSED SYSTEM ARCHITECTURE

The proposed system architecture is composed of different components that handle transactional data and perform the fraud detection process through machine learning algorithms.

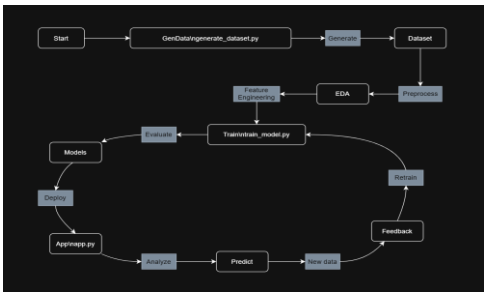

Fig-1: System Architecture Diagram

The proposed system starts by collecting transactional data that consists of different attributes regarding the behaviour of the users. The collected data is then fed into the preprocessing stage where missing values in the data are filled, categorical variables are encoded, and numerical variables are normalized.

The Synthetic Minority Oversampling Technique is used to handle the class imbalance problem in the dataset. Feature engineering methods are used to find the significant attributes affecting the behaviour of the transactions. Finally, the proposed system utilizes the Random Forest classifier to identify the fraudulent transactions in the dataset. The proposed system is implemented as a web application through the Streamlit library.

5. METHODOLOGY

The methodology employed for the current study includes various steps like data set preparation, data preprocessing, feature engineering, model training, and performance evaluation. The data set employed for the current study contains about 100,000 transactions, including legitimate and fraudulent UPI transactions. Each transaction includes various attributes like the characteristics of the transactions, the amount involved, the type of transaction, the time of the transaction, the devices employed, and the location.

The initial step employed in the methodology employed for the current study includes data preprocessing, which includes the transformation and cleaning of the data set to prepare it for the machine learning analysis. During this stage, the data set is prepared by employing appropriate techniques to handle the missing values and converting the data into numerical values using encoding techniques. The numerical values are normalized using the StandardScaler technique to provide equal weight to all the features employed during the machine learning model. Since the fraud detection dataset is highly imbalanced, the Synthetic Minority Oversampling Technique (SMOTE) will be used to balance the dataset. This will improve the learning capacity of the model to identify the patterns linked to the fraudulent transactions.

Once this dataset is balanced, it will be split into a training dataset and a testing dataset. It should be noted that the proportion of the training dataset to the testing dataset will be 80:20. While the training dataset will be used to train the machine learning model, the testing dataset will be used to test the performance of the machine learning model. A Random Forest classifier will be used as a primary model to train the machine learning model. This model is efficient in handling a huge volume of data.

Once the machine learning model is trained, it will be checked in terms of various parameters. The parameters in this case will include accuracy, precision, recall, F1 score, and ROC-AUC score. All these parameters will ensure a thorough analysis of the performance of the model in correctly predicting the fraudulent transactions while ensuring that no false positive prediction occurs.

5.1 Dataset Description

The dataset used in the present study consists of approximately 100,000 UPI transactions. These transactions include both legitimate and fraudulent transactions.

Table-1: Dataset Distribution

Category	Number of Transactions	Percentage
Legitimate Transactions	97,000	97%
Fraudulent Transactions	3,000	3%
Total Transactions	100,000	100%

5.2 Feature Description

Table-2: Transaction Feature Description

Feature Name	Description	Type
Transaction Amount	Amount transferred in UPI transaction	Numerical
Transaction Type	P2P / P2M / Others	Categorical
Transaction Time	Timestamp of transaction	Numerical
Device Type	Mobile / Desktop	Categorical
Location	User transaction location	Categorical
Is Fraud	Target variable (0 = Legit, 1 = Fraud)	Binary

5.3 Data Preprocessing

Data preprocessing involves handling missing values, categorical data encoding, and scaling numerical data with the StandardScaler. Data preprocessing is done to ensure that the data is in a state that can be used to train a machine learning model.

5.4 Model Training

For this research, the Random Forest algorithm will be used to train the model. This algorithm will be used because of its high accuracy in handling complex data sets. Data will be split into a training set and a test set in a ratio of 80:20.

5.5 Implementation

The proposed system for fraud detection will be developed using the Python programming language. The system will employ various libraries for machine learning, such as Scikit-learn, Pandas, and NumPy. The trained model of the random forest algorithm will be integrated into the web application using the Streamlit library. The web application enables users to upload the dataset of transactions, which is then processed by the system. The results of the prediction of the fraud are then presented to the user. The system includes additional visualizations of the statistics of the frauds detected and the risk analysis.

6. EXPERIMENTAL RESULTS

The experiment's outcomes verify the effectiveness of the proposed machine learning-based UPI fraud detection system. The Random Forest classifier is trained using the prepared dataset. The prepared dataset is employed to verify the effectiveness of the proposed model. The testing dataset was used to assess the effectiveness of the trained model in classifying the transactions.

Table-3: Model Performance Comparison

Model	Accuracy	ROC-AUC Score
Logistic Regression	97.84%	0.9521
Random Forest	98.61%	0.9756

The evaluation results indicate that the proposed model achieves an overall accuracy of 98.61%, demonstrating its strong ability to distinguish between legitimate and fraudulent transactions. In addition to accuracy, the model achieved a ROC-AUC score of 0.9756, which indicates excellent discriminative performance. The precision and recall values obtained for the fraud class show that the model is capable of identifying a significant portion of fraudulent transactions while maintaining a low false positive rate.

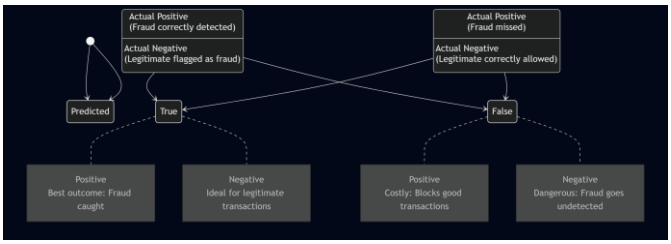

Fig-2: Confusion Matrix

In addition, the confusion matrix indicates the performance of the model, where the number of correct and incorrect classifications is indicated. In this case, the model is able to identify the majority of the legitimate transactions. Moreover, the model is able to identify a large number of the fraudulent transactions. This indicates that the Random Forest algorithm with SMOTE is a reliable model for detecting fraud transactions.

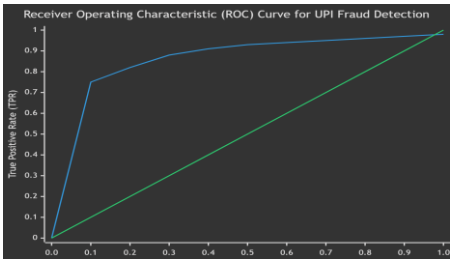

Fig-3: ROC Curve

7. CONCLUSION

This research paper proposed a machine learning-based system for detecting fraudulent UPI transactions by utilizing the Random Forest algorithm with the Synthetic Minority Oversampling Technique (SMOTE). The proposed system for detecting fraudulent transactions would be capable of analysing the attributes of the transactions to identify the pattern for fraudulent activities. In the experimental results, the proposed system in detecting fraudulent transactions showed a high level of accuracy by using the Random Forest algorithm with an accuracy level of 98.61%. Moreover, the ROC-AUC score of the proposed system was found to be 0.9756.

Moreover, the proposed system for detecting fraudulent transactions can be implemented by deploying the machine learning model through a web interface developed with the Streamlit library. Based on the experimental results, the proposed machine learning-based system for detecting fraudulent transactions can be concluded to be an efficient system for detecting fraudulent transactions to enhance the security of the digital payment system for UPI transactions. Apart from that, the proposed machine learning-based system to detect fraudulent transactions can be concluded to be an efficient system to detect fraudulent transactions to improve the security of the digital payment system for UPI transactions.

8. FUTURE SCOPE

Even though the proposed system in the case of fraud detection showed promising results, there are some opportunities that could be taken in the future to improve this system even more. One such opportunity is the proposed idea of using a system of real-time transaction monitoring systems that could detect fraudulent transactions instantly.

Another idea that could be taken into consideration is using more advanced techniques like Artificial Neural Networks, Long Short-Term Memory, and Deep Reinforcement Learning Models.

In addition to this, connecting the proposed system with banking APIs and payment gateways could also potentially allow real-time fraud detection in live systems. Continuously retraining the proposed model using updated data could also help improve this system in a better way.

9. REFERENCES

[1]. N. Dal Pozzolo, O. Caelen, Y. Le Borgne, S. Waterschoot and G. Bontempi, “Calibrating Probability with Undersampling for Unbalanced Classification,” *IEEE Symposium Series on Computational Intelligence*, pp. 159–166, 2015.

[2]. L. Breiman, "Random Forests," *Machine Learning*, vol. 45, no. 1, pp. 5–32, 2001.
[3]. N. V. Chawla, K. W. Bowyer, L. O. Hall and W. P. Kegelmeyer, "SMOTE: Synthetic Minority Over-Sampling Technique," *Journal of Artificial Intelligence Research*, vol. 16, pp. 321–357, 2002.
[4]. E. J. Ngai, Y. Hu, Y. Wong, Y. Chen and X. Sun, "The Application of Data Mining Techniques in Financial Fraud Detection: A Classification Framework and an Academic Review," *Decision Support Systems*, vol. 50, no. 3, pp. 559–569, 2011.
[5]. R. Bolton and D. Hand, "Statistical Fraud Detection: A Review," *Statistical Science*, vol. 17, no. 3, pp. 235–255, 2002.
[6]. S. Bhattacharyya, S. Jha, K. Tharakunnel and J. Westland, "Data Mining for Credit Card Fraud: A Comparative Study," *Decision Support Systems*, vol. 50, no. 3, pp. 602–613, 2011.
[7]. C. Phua, V. Lee, K. Smith and R. Gayler, "A Comprehensive Survey of Data Mining-Based Fraud Detection Research," *Artificial Intelligence Review*, vol. 34, no. 1, pp. 1–14, 2010.
[8]. V. Chandola, A. Banerjee and V. Kumar, "Anomaly Detection: A Survey," *ACM Computing Surveys*, vol. 41, no. 3, pp. 1–58, 2009.
[9]. T. Fawcett, "An Introduction to ROC Analysis," *Pattern Recognition Letters*, vol. 27, no. 8, pp. 861–874, 2006.
[10]. J. R. Quinlan, "Induction of Decision Trees," *Machine Learning*, vol. 1, pp. 81–106, 1986.
[11]. P. Chan and S. Stolfo, "Toward Scalable Learning with Non-Uniform Class and Cost Distributions: A Case Study in Credit Card Fraud Detection," *Proceedings of KDD*, pp. 164–168, 1998.
[12]. M. Zareapoor and P. Shamsolmoali, "Application of Credit Card Fraud Detection: Based on Bagging Ensemble Classifier," *Procedia Computer Science*, vol. 48, pp. 679–685, 2015.
[13]. S. Sahin and E. Duman, "Detecting Credit Card Fraud by ANN and Logistic Regression," *International Symposium on Innovations in Intelligent Systems and Applications*, pp. 315–319, 2011.
[14]. A. Bahnsen, D. Aouada, A. Stojanovic and B. Ottersten, "Feature Engineering Strategies for Credit Card Fraud Detection," *Expert Systems with Applications*, vol. 51, pp. 134–142, 2016.
[15]. I. Goodfellow, Y. Bengio and A. Courville, *Deep Learning*, MIT Press, 2016.
[16]. S. Jha, M. Guillen and J. Westland, "Employing Transaction Aggregation Strategy to Detect Credit Card Fraud," *Expert Systems with Applications*, vol. 39, no. 16, pp. 12650–12657, 2012.