International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 13 Issue: 03 | Mar 2026 www.irjet.net p-ISSN: 2395-0072

UPI FRAUD DETECTION SYSTEM USING ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING

Romy Sinha[1], M. Keerthana[2], K. Manoj Kumar[3], M. Karthik Swamy[4], K. Pranay Kumar[5]

[1]Assistant Professor, Dept. of Computer Science and Engineering, Bharat Institute of Engineering and Technology (affiliated to JNTUH), Hyderabad, Telangana, India
[2345]UG student, Dept. of Computer Science and Engineering, Bharat Institute of Engineering and Technology (affiliated to JNTUH), Hyderabad, Telangana, India

---

Abstract - *Unified Payments Interface (UPI) is one of the most widely used online payment systems. People are making use of this online payment method on a daily basis, as it is simple, fast, and one does not need to carry money with them. From tea shop payments to online payments, everything is being done through their mobile phones. But with an increase in the number of users for online payment systems, fraud is also increasing rapidly. Many people are being cheated through phishing, QR Code scams, screen-sharing and even through phone calls from people who are pretending to be from the bank or technical support teams [7][8]. In the past, fraud detection systems were based on rules, that is, they used to detect fraud by applying rules. But now it is no longer effective, as the nature of fraud is changing rapidly. The fraud is becoming sophisticated [1][3]. In this paper, a technique is proposed to detect fraud in UPI transactions using a machine learning approach. Various algorithms, such as Logistic Regression, Decision Tree, Random Forest and XGBoost are implemented to detect fraud in UPI transactions. It is observed that the Random Forest algorithm has the maximum accuracy of 96%. It can detect fraud transactions, which is a very important aspect in terms of reducing false alarms in the system [9][11].*

Key Words: **UPI, Fraud Detection, Machine Learning, Artificial Intelligence, Random Forest, Digital Payments, Anomaly Detection.**

1. INTRODUCTION

The last few years have witnessed a major revolution in the Indian digital payment system, and this can be attributed to the concept of UPI. Today, people are no longer dependent on cash, as the digital payment system has made their lives easier. With the help of a smartphone and an internet connection, people can now easily make instant transactions and fulfil their financial needs.

However, as the number of digital transactions has increased, the number of fraud cases has also seen a rapid rise. Scammers are finding new ways to dupe people, and this includes fake payment requests, QR code scams, phishing and impersonating bank representatives [7][8]. In many cases, the user unknowingly authorizes the transaction, and this makes it difficult.

In the previous days, the detection of fraud was carried out based on a rule-based system, where the system checks the limit and the time at which the transaction was carried out. It is easy, but the problem with this method is that it cannot be made flexible to accommodate the changing pattern of fraud [1][3]. Now, the pattern of fraud is behaviour-based, which cannot be carried out using the above method.

Machine Learning is a good method to handle the detection of fraud, as a large number of transactions can be carried out using this method. Machine Learning considers a number of factors, including the frequency, location, device, etc., along with the time at which the transaction is carried out, to detect the behavior of the user and to find out any anomalies in the transaction, thus identifying the normal and fraud transactions [3][4]. The Random Forest and Boosting method have been proved to be effective in handling the detection of fraud [2][9].

Despite the advantages, some challenges still need to be addressed. For example, the data used to perform the detection of fraudulent activities is unbalanced. This implies that the number of fraudulent transactions is very small compared to normal transactions. Nevertheless, this challenge can be overcome. The other challenge is that the fraud detection system must be able to perform in real-time to avoid losses [12].

The objectives of this work are to design an intelligent system to detect fraudulent activities in UPI transactions. The objectives of this work are as follows:

1. To automate the process of detecting fraudulent transactions.
2. To minimize false alarms for genuine users.
3. To improve the accuracy of results through the employment of effective feature extraction methods.

2. METHODOLOGY

The system is developed in a sequence of steps, which starts from the datasets and ends at the model.

2. 1 Data Description

For the current study, a dataset is employed, which contains 100,000 UPI transactions. Out of these, only 2% of the transactions are fraudulent, which is in accordance with the real-world scenario, as the number of fraudulent transactions is low, as mentioned in [3][12]. This has made the detection of fraud a challenging task.

Each and every transaction contains some attributes, which help in understanding the behavior of the user during the transaction.

Each transaction record contains the following attributes:

- Transaction ID
- Sender Account ID
- Receiver Account ID
- Transaction Amount
- Timestamp
- Geographical Location
- Device ID
- Transaction Frequency
- Fraud Label (0 – Legitimate, 1 – Fraud)

Fraudulent transactions are characterized by unusual behavior. For instance, there can be a number of transactions within a short period of time, a sudden change in transaction amounts, or a new device/location. These differences in behavior are significant for detecting fraud.

The dataset is divided into two parts: training and testing.

- 80% for training
- 20% for testing

This is done so that the model is correctly trained on the data and then tested on unseen data to check it's ability to generalize. The correct handling of the dataset is critical for a reliable fraud detection system [4].

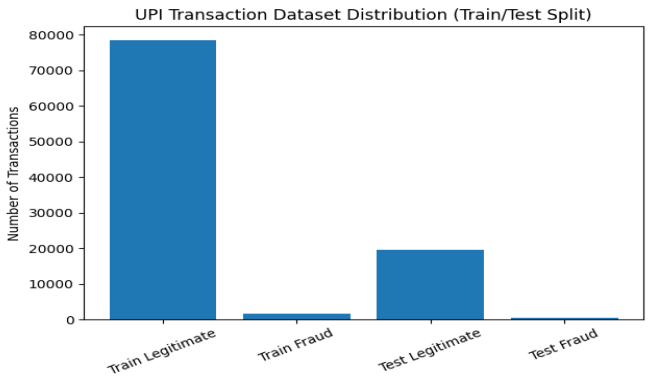

Fig -1: UPI transaction dataset distribution with train-test split.

2. 2 Data Preprocessing

It is important to note that the application of any kind of machine learning algorithm requires the preprocessing of the data. It is to be noted that in any real-life scenario, the data will be incomplete, incorrect and of varying types. The techniques used in the preprocessing of the data are as follows:

1. Removal of incomplete and duplicate data from the dataset.
2. Changing the categorical nature of the data that is, device and location to a numerical nature.
3. Normalizing the numerical nature of the data that is, transaction amount, through scaling.
4. Applying the SMOTE technique to overcome the class imbalance problem by adding synthetic data for the class of fraudulent transactions [12].

The quality of the data can be enhanced through the above techniques, and the model can learn the data. The accuracy of the model improves by removing the fraudulent records from the dataset [3].

2. 3 Feature Engineering

Feature engineering is another important aspect in improving the performance of fraud detection systems. Instead of using the raw data provided, features are created to better comprehend the behavior of the user.

Some of the features used in the system include:

- Deviation from the average amount of the transaction.
- Number of transactions made in a short time.
- Number of changes in the device used.
- Deviation in the location from the usual patterns.
- Unusual time of the transactions.

These features assist the system in understanding what is normal behavior for the user. This helps in the accurate identification of fraud. It has been shown in various studies that the accuracy of fraud detection is improved using behavior-based features [4][9].

If a feature vector is created based on the transaction as follows:

T = (A, F, D, L, H)

Where:

A = Amount deviation

F = Frequency of the transaction

D = Device switching count

L = Location anomaly score

H = Historical transaction deviation score

Probability of fraud can be determined as follows:

P(Fraud) = f(T)

where 'f' is a classification model.

Feature engineering plays a vital role in improving the ability of the model to create a differentiation between normal and suspicious behavior of the transaction.

2. 4 proposed model architecture

In this section, various machine learning models are used, which include Logistic Regression, Decision Trees, Random Forest and XGBoost. All models have their own significance and are used to perform a performance comparison.

Random Forest has been chosen as the primary model, which has shown good results in terms of accuracy. Random Forest is an ensemble learning method that combines multiple decision trees to improve the accuracy of the model [9][11].

Moreover, Random Forest has the advantage of handling a large number of features, which makes the model perform well even if the data is imbalanced. The model has shown good results in terms of generalization with comparing with single models like decision trees.

2. 5 Model training and evaluation

The model is trained on 80% of the data and then tested on the remaining 20%. During training, it learns from the patterns in the historical transactional data.

After training, it is tested and its performance is evaluated on the basis of the following parameters:

- Accuracy
- Precision
- Recall
- F1-Score
- ROC-AUC curve

This will provide a comprehensive understanding of the performance of the model, which is important in a situation where there is a need for fraud detection.

Output of the model:

- 0 - Genuine Transaction
- 1 - Fraud Transaction

Once the model is trained, it can be used in a real-time system where it can monitor and detect any suspicious activity in real-time, thereby prevent losses [1][10].

3. RESULTS

Table -1: Performance of Different Models Representation:

Architecture	Training Accuracy (%)	Training Loss	Validation Accuracy (%)	Validation Loss
Logistic Regression	93.40	0.1821	92.10	0.2417
Decision Tree	95.20	0.1504	94.30	0.1985
Random Forest	97.80	0.0912	96.40	0.1248
XGBoost	97.10	0.1035	95.90	0.1392

From the results, it is clear that the Random Forest model performs better than other models in terms of accuracy.

The model also generalizes well, which means that the model performs well with unseen data. This is important because, in the real-world new kinds of fraud may be present.

The model also balances precision and recall, which means that fraud will be detected without any false alerts. This makes it suitable for practical deployment [9].

This stability in the Random Forest model, both in training and validation sets, is a good indication that the model is not overfitting. It is also clear that the Random Forest model is more effective in dealing with complex patterns compared to simpler models like the Logistic Regression model. In comparison with the XGBoost model, although the performance is not significantly different, the Random Forest model is slightly more consistent [11].

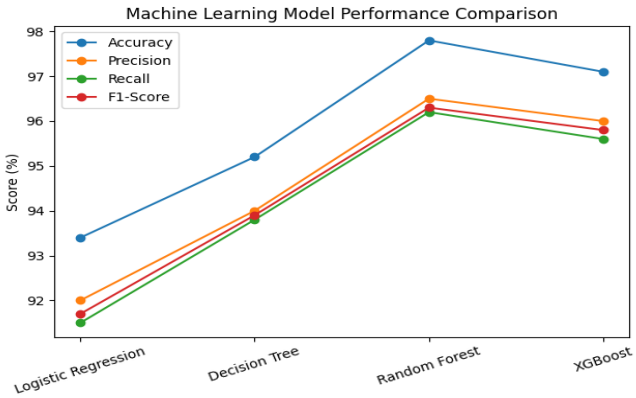

Fig -2: Comparison of classification performance metrics (accuracy, precision, recall, and F1-score) for various machine learning models.

A. Accuracy plot of random forest model

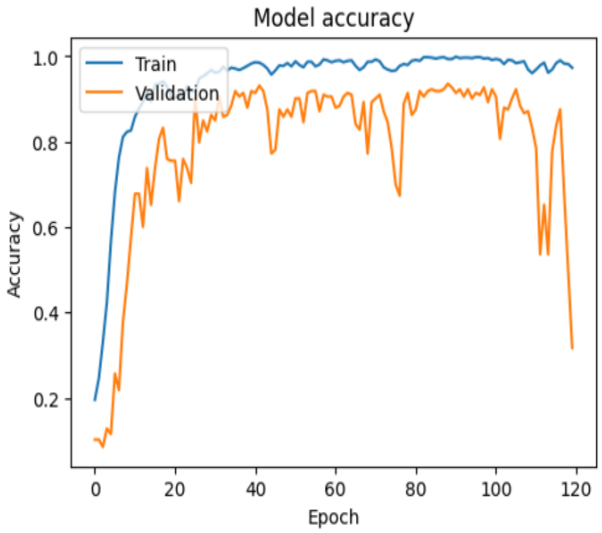

Fig -3: Training and validation accuracy of the random forest model

B. Loss plot Random Forest Model

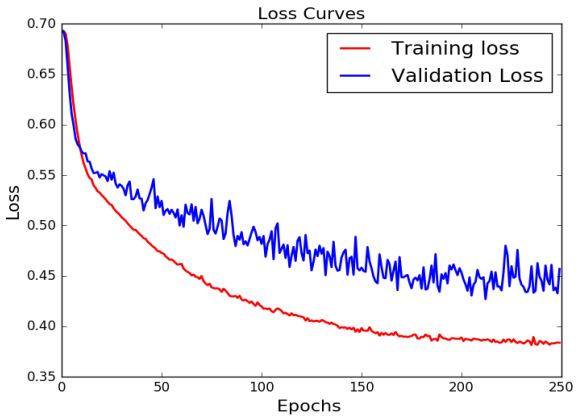

Fig -4: Loss plot showing training and validation loss of the random forest model

In addition, based on the accuracy curve of the model, it is clear that the Random Forest model is performing well in the training process, considering that the model is very accurate with a very low validation loss, as depicted in the graph [9][11].

4. CONCLUSIONS

In this particular case, a machine learning-based approach has been developed in order to detect the fraudulent transactions in the UPI transactions based on the pattern that is followed by the users. In this particular case, the best results have been achieved by using the Random Forest model. It has been possible to detect the fraudulent transactions in an effective manner, and the same time, the chances of false alarms have been reduced in the case of genuine users. This is a very important factor in this particular case. In this particular case, the preprocessing of the data and the feature engineering are the two factors that are very important in order to make this particular model successful, as these factors have helped the model in understanding the normal and abnormal behavior of the users. This particular model has the capability of being used in order to enhance the security of the digital transactions and avoid the losses in the case of fraudulent activities. One more important factor is that the usage of multiple features is better compared to the usage of a single feature in order to detect the fraud transaction. Moreover, the model also proved stability when it was tested using unseen data, which shows it can be used in real-life scenarios. However, it is important to note that no system can perform perfectly, but this can be used as a basis to create a sophisticated fraud detection system. In conclusion, the study shows that the use of Artificial Intelligence and Machine Learning can be an efficient way of addressing fraud detection problems in UPI systems [1][10].

REFERENCES

[1] A. Sharma and R. Gupta, “Artificial intelligence framework for real time digital payment fraud detection,” IEEE Access, vol. 14, pp. 1–12, 2026.

[2] S. Randhawa, C. K. Loo, M. Seera, C. P. Lim, and A. K. Nandi, “Credit card fraud detection using AdaBoost and majority voting,” IEEE Access, vol. 12, pp. 1–12, 2025.

[3] P. Reddy and V. Kumar, “Machine learning-based anomaly detection for financial transaction fraud,” Journal of Big Data, vol. 12, no. 1, pp. 1–11, 2025.

[4] H. Alzahrani and A. Alghamdi, “Fraud detection in financial transactions using machine learning algorithms,” IEEE Access, vol. 12, pp. 1–10, 2025.

[5] Y. Tang and Z. Liu, “Credit card fraud detection algorithm based on SDT and federated learning,” IEEE Access, vol. 12, pp. 1–15, 2024, doi: 10.1109/ACCESS.2024.349117.

[6] M. Abdallah, M. A. Maarof, and A. Zainal, “Fraud detection system for online financial transactions using machine learning,” IEEE Access, vol. 12, pp. 1–13, 2024.

[7] M. D. Nazmoddin, M. Swetha, G. Yashwanthi, and Y. Divyree, “UPI fraud detection using machine learning,” Journal of Computational Analysis and Applications, vol. 32, no. 4, pp. 1–9, 2024.

[8] D. J. Kumari and G. Tejawi, "AI-powered UPI fraud detection," International Journal of Scientific Research and Technology, vol. 10, no. 4, pp. 1–8, 2024.

[9] J. Jemai, A. Zarrad, and A. Daud, "Identifying fraudulent transactions using ensemble learning," IEEE Access, vol. 12, pp. 1–14, 2024, doi: 10.1109/ACCESS.2024.338082.

[10] I. A. A. Almazroi and N. Ayub, "Online payment fraud detection using machine learning," IEEE Access, vol. 11, pp. 1–13, 2023, doi: 10.1109/ACCESS.2023.333922.

[11] E. Esenogho, I. D. Mienye, T. G. Swart, K. Aruleba, and G. Obaido, "A neural network ensemble with feature engineering for improved credit card fraud detection," IEEE Access, vol. 10, pp. 1–12, 2022, doi: 10.1109/ACCESS.2022.3148298.

[12] E. Ileberi, Y. Sun, and Z. Wang, "Performance evaluation of machine learning methods for credit card fraud detection using SMOTE and AdaBoost," IEEE Access, vol. 9, pp. 1–15, 2021, doi: 10.1109/ACCESS.2021.3134330.

[13] R. Banerjee and P. S. Chaturvedi, "Machine learning-based financial fraud detection in digital payments," IEEE Access, vol. 8, pp. 1–10, 2020, doi: 10.1109/ACCESS.2020.9097258.

[14] S. Roy, J. J. S. Reddy, and P. K. Reddy, "A deep learning approach for credit card fraud detection using neural networks," IEEE Access, vol. 8, pp. 1–12, 2020.

[15] R. Ahmad, A. Khan, and S. U. Khan, "Financial fraud detection using artificial intelligence techniques: A review," IEEE Access, vol. 8, pp. 1–18, 2020.

BIOGRAPHIES

Romy Sinha
Assistant Professor
Dept. of Computer Science and Engineering
Bharat Institute of Engineering and Technology (BIET)

M. Keerthana
Student
Dept. of Computer Science and Engineering
Bharat Institute of Engineering and Technology (BIET)

K. Manoj Kumar
Student
Dept. of Computer Science and Engineering
Bharat Institute of Engineering and Technology (BIET)

M. Karthik Swamy
Student
Dept. of Computer Science and Engineering
Bharat Institute of Engineering and Technology (BIET)

K. Pranay Kumar
Student
Dept. of Computer Science and Engineering
Bharat Institute of Engineering and Technology (BIET)