Volume 11, Issue 3, March – 2026 International Journal of Innovative Science and Research Technology
ISSN No: -2456-2165 https://doi.org/10.38124/ijisrt/26mar371

UPI Fraud Detection and Online Transcation

Dr. R. Nagarajan[1]; S. Jayasurya[2]; S. Kavin balaji[3]

[1]Assistant Professor, Department of Computer Science, Sri Ramakrishna College of Arts & Science
[2,3] PG Student, Department of Computer Science, Sri Ramakrishna College of Arts & Science

Publication Date: 2026/03/12

Abstract: The rapid growth of digital payment technologies has transformed financial transactions by enabling instant, convenient, and secure money transfers. In India, the Unified Payments Interface (UPI) has emerged as one of the most widely used real-time payment systems for both personal and business transactions. However, the increasing popularity of UPI has also led to a rise in fraudulent activities such as fake UPI IDs, unauthorized transactions, OTP and PIN theft, and social engineering attacks. Traditional fraud detection methods based on fixed rules often struggle to identify complex and evolving fraud patterns. This study proposes an Advanced UPI Transaction Fraud Detection System that combines rule-based validation with machine learning techniques to detect suspicious activities. The system analyzes multiple transaction features including payment amount, transaction frequency, login failures, device changes, and location variations. Implemented using Python and Streamlit, the system enables real-time transaction monitoring. Experimental results demonstrate that the model effectively identifies fraudulent behavior while reducing false alarms, improving the security and reliability of digital payment systems.

Keywords: *UPI Fraud Detection, Machine Learning, Random Forest Algorithm, Digital Payment Security, Transaction Monitoring, OTP/PIN Attack Detection, Anomaly Detection, Cyber Fraud Prevention.*

How to Cite: Dr. R. Nagarajan; S. Jayasurya; S. Kavin balaji (2026) UPI Fraud Detection and Online Transcation. *International Journal of Innovative Science and Research Technology,* 11(3), 366-371. https://doi.org/10.38124/ijisrt/26mar371

I. INTRODUCTION

The development of digital technologies has greatly influenced the way financial transactions are carried out today. Modern payment systems allow people to transfer money quickly, conveniently, and securely through mobile applications and online platforms. These electronic payment services have become an essential part of everyday financial activities, enabling users to send and receive funds without visiting banks. In India, the Unified Payments Interface (UPI), developed by the National Payments Corporation of India (NPCI), has become one of the most widely used real-time payment systems. It allows instant money transfers between bank accounts using simple identifiers such as UPI IDs, mobile numbers, or QR codes, eliminating the need to enter traditional banking details like account numbers and IFSC codes.

Although UPI offers many benefits and has gained massive popularity, its rapid growth has also led to an increase in digital payment fraud and security risks. Cybercriminals often take advantage of system vulnerabilities through techniques such as fake UPI accounts, phishing attacks, OTP and PIN theft, and unauthorized transactions. Traditional fraud detection methods mainly rely on fixed rules and predefined patterns, which are not always effective in identifying modern and evolving fraud strategies.

To overcome these limitations, this project proposes a UPI Fraud Detection System that integrates rule-based security mechanisms with machine learning techniques. The system analyzes several transaction-related factors such as transaction amount, time gap between transactions, repeated authentication failures, device changes, and variations in user location. By examining these parameters, the system can identify unusual transaction behavior and detect potentially fraudulent activities in real time. The main goal of this approach is to enhance transaction security, reduce financial losses, and improve user trust in digital payment systems.

II. RELATED WORKS

The rapid growth of digital payment platforms has resulted in a large increase in online financial transactions. While these technologies have made payments faster and more convenient, they have also created new opportunities for fraud and cybercrime. Because of this, fraud detection in electronic payment systems has become an important area of research for both academic scholars and financial organizations. Many studies have explored different techniques for detecting and preventing fraudulent transactions by using data analysis, machine learning models, and rule-based security mechanisms.

In the early stages, fraud detection systems mainly relied on rule-based approaches. In these systems, transactions were evaluated using predefined rules or conditions. For example, transactions might be flagged if the payment amount exceeded a certain limit, if transactions occurred too frequently within a

ISSN No: -2456-2165 https://doi.org/10.38124/ijisrt/26mar371

short time period, or if unusual activity was detected in a user account. Although rule-based systems were easy to implement and understand, they had several limitations. Fraudsters could often bypass these systems by slightly modifying their transaction behavior or by using new attack methods.

With the advancement of artificial intelligence and machine learning technologies, more sophisticated fraud detection techniques have been developed. Researchers have applied several machine learning algorithms such as Random Forest, Decision Tree, Support Vector Machine (SVM), and Logistic Regression to analyze large volumes of financial transaction data. These algorithms learn patterns from historical data and are able to classify transactions as legitimate or suspicious based on multiple attributes, including transaction value, time gaps between payments, and user transaction behavior.

Another important research direction involves behavioral analysis of users. In this approach, the system observes the normal transaction patterns of users over a period of time and creates a behavioral profile. Any significant deviation from this normal behavior—such as transactions from an unusual geographic location, extremely large payment amounts, or multiple failed login attempts—may indicate suspicious or fraudulent activity.

Some researchers have also introduced graph-based fraud detection techniques. In these methods, transactions are represented as networks in which users, bank accounts, and merchants are connected through transaction relationships. By analyzing these networks, it becomes possible to identify suspicious patterns such as fraud rings, coordinated transactions, or clusters of accounts involved in illegal activities.

More recently, hybrid fraud detection systems have been proposed to improve detection performance. These systems combine multiple techniques, including rule-based validation, machine learning models, and anomaly detection methods. The integration of these approaches helps increase detection accuracy and reduces the chances of false alarms.

The system developed in this project builds on these existing methods by integrating rule-based verification, machine learning-based risk evaluation, and behavioral pattern monitoring to detect fraudulent UPI transactions. This combined approach enhances the accuracy and reliability of fraud detection while improving the overall security of digital payment platforms.

III. METHODOLOGY

The methodology used in the UPI Fraud Detection System aims to identify suspicious digital payment transactions by combining rule-based verification, behavioral monitoring, and machine learning techniques. The system follows a systematic workflow to examine transaction information, detect irregular patterns, and determine whether a transaction is legitimate or fraudulent. The overall methodology consists of several stages, where each stage performs a specific validation or analysis task to improve fraud detection accuracy.

- *Data Collection*

The initial stage involves gathering transaction-related data required for fraud analysis. The dataset includes several important attributes such as UPI ID, transaction value, time interval between transactions, number of failed authentication attempts, device change status, location variation, and the fraud label indicating whether a transaction is genuine or fraudulent. These attributes provide valuable information that helps the system analyze user behavior and identify abnormal transaction patterns.

- *Data Preprocessing*

Before applying machine learning techniques, the collected dataset undergoes preprocessing to enhance its quality and consistency. This stage includes removing or handling missing values, standardizing data formats, and converting categorical information into numerical representations when required. Proper preprocessing ensures that the dataset becomes suitable for training and evaluating machine learning models.

- *UPI ID Validation*

At this stage, the system validates whether the entered UPI ID follows the correct structural format. It also compares the identifier against a database of suspicious or blacklisted UPI IDs. This verification step assists in identifying fake payment addresses or malicious identifiers frequently used in phishing attacks and fraudulent payment requests.

- *OTP and PIN Attack Detection*

The system also monitors authentication attempts to identify potential unauthorized access. When multiple incorrect PIN or OTP entries occur within a short period, the system interprets this behavior as a possible brute-force attempt. Such transactions are flagged as suspicious for further analysis.

- *Machine Learning Model Training*

A machine learning algorithm, such as Random Forest, is trained using historical transaction data. During the training process, the model learns patterns associated with both normal and fraudulent transactions by analyzing attributes like transaction amount, time intervals, device switching, and authentication failures.

- *Fraud Prediction*

After the model has been trained, it can analyze new incoming transactions. Using the provided transaction features, the model estimates the likelihood of fraudulent activity and classifies the transaction as either legitimate or suspicious.

- *Visualization and Monitoring*

The system also generates graphical representations of transaction behavior and fraud statistics. These visualizations allow users and system administrators to observe fraud trends, understand system performance, and monitor transaction activity more effectively.

ISSN No: -2456-2165 https://doi.org/10.38124/ijisrt/26mar371

The proposed methodology integrates multiple detection mechanisms to enhance the accuracy of fraud identification. By combining rule-based validation with machine learning analysis and behavioral monitoring, the system establishes a strong and reliable framework for detecting fraudulent UPI transactions within digital payment environments.

IV. MODEL DESIGN AND WORKFLOW

The UPI Fraud Detection System is designed to recognize suspicious digital payment transactions by combining rule-based verification methods with machine learning techniques. The operational process starts when transaction information is received, including details such as the UPI ID, payment amount, time interval between transactions, number of failed PIN attempts, device change status, and location variation. Initially, the system validates the UPI ID to identify invalid or potentially fraudulent payment identifiers. It then analyzes authentication activity to detect possible OTP or PIN brute-force attempts by monitoring repeated failed login attempts.

After completing these initial security checks, the transaction features are processed and provided to a trained machine learning model. The model evaluates the transaction and estimates the likelihood of fraud. Based on the calculated risk score, the system determines whether the transaction is legitimate or suspicious and presents the result through a monitoring dashboard.

➢ *Model Architecture*

The architecture of the UPI Fraud Detection System follows a layered structure that integrates rule-based security checks with machine learning analysis to detect fraudulent payment activities. Each layer performs a specific function to examine transaction information and identify suspicious behavior before a transaction is finalized

- *Input Layer*

The input layer collects essential transaction attributes including the UPI ID, transaction amount, time interval between consecutive transactions, number of failed PIN attempts, device change indicator, and location change status.

- *UPI ID Validation Module*

This module evaluates whether the provided UPI ID matches the expected format and compares it with a database of suspicious or blacklisted payment identifiers. This helps detect fake or malicious UPI IDs commonly used in fraudulent payment requests.

- *Authentication Attack Detection Module*

This component observes user authentication activity to identify possible OTP or PIN brute-force attacks. If several unsuccessful login attempts occur within a short time frame, the system marks the activity as potentially suspicious.

- *Feature Processing Layer*

At this stage, the collected transaction attributes are organized and prepared for analysis. Data formatting and feature structuring are performed so that the information can be effectively processed by the machine learning model.

- *Machine Learning Prediction Model*

A trained machine learning model evaluates the transaction features and estimates the probability that a transaction is fraudulent by comparing it with patterns learned from historical data.

- *Decision Layer*

Based on the prediction score produced by the model, the system determines whether the transaction should be classified as legitimate or fraudulent.

- *Visualization and Output Layer*

The final results are displayed through an interactive user interface that shows the transaction status, fraud risk level, and related security alerts.

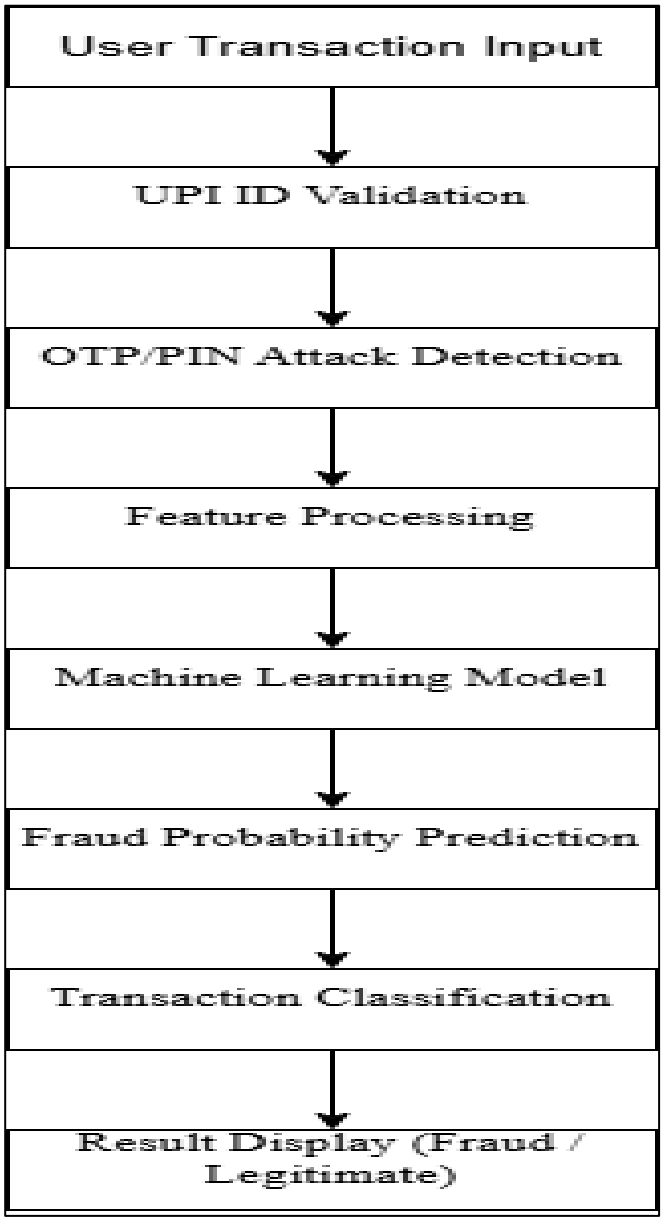

Fig 1 Fraud Detection Workflow Diagram

ISSN No: -2456-2165 https://doi.org/10.38124/ijisrt/26mar371

➢ *Workflow Description*

The workflow begins when a user initiates a UPI payment. The system first gathers the transaction details and performs validation of the UPI ID to ensure it follows the correct structure and is not listed as suspicious. The authentication monitoring component also checks for repeated OTP or PIN failures that may indicate unauthorized access attempts.

Once the rule-based verification steps are completed, the transaction data is prepared and forwarded to the machine learning model for further analysis. The model examines several attributes such as transaction value, transaction frequency, device switching behavior, and location changes. Using these inputs, the model estimates the probability of fraud and categorizes the transaction accordingly. The final decision and risk level are then displayed to the user through the system interface.

➢ *Algorithm*

The proposed system employs the Random Forest machine learning algorithm to identify fraudulent UPI transactions. Initially, the transaction dataset is loaded and prepared by cleaning the data and selecting important attributes such as payment amount, time interval between transactions, device change status, and location variation. The dataset is then divided into training and testing subsets to evaluate the performance of the model.

The Random Forest classifier is trained using historical transaction records to learn patterns associated with legitimate and fraudulent activities. When a new transaction is received, its features are provided as input to the trained model. The model estimates the probability of fraud and determines the transaction category based on a predefined threshold.

- *Steps of the Algorithm*

✓ Import the transaction dataset.
✓ Clean and preprocess the data while selecting relevant features.
✓ Divide the dataset into training and testing datasets.
✓ Train the Random Forest classifier using historical transaction data.
✓ Provide new transaction attributes to the trained model.
✓ Compute the probability that the transaction is fraudulent.
✓ Classify the transaction as Fraudulent or Legitimate based on the prediction threshold.
✓ Present the prediction result to the user interface.

➢ *Recommendation Output*

The system output provides a clear evaluation of the transaction after analyzing the provided details. It indicates whether the transaction is legitimate or potentially fraudulent based on the prediction generated by the machine learning model. The output also includes a fraud probability score, which reflects the level of risk associated with the transaction.

Additionally, the system presents the result of UPI ID verification, identifying whether the entered payment identifier is valid or suspicious. Security alerts are also generated when unusual behavior is detected, such as repeated OTP or PIN authentication failures.

- *Output Information Displayed by the System*

✓ Transaction Status: Legitimate or Fraudulent
✓ Fraud Probability Score: Indicates the risk level of the transaction
✓ UPI ID Validation Result: Valid or Suspicious
✓ Security Alerts: Detection of OTP or PIN brute-force attempts

If a transaction is identified as fraudulent, the system can recommend preventive actions such as blocking the transaction, notifying the user, or reporting the suspicious activity to the relevant financial institution.

V. RESULTS AND ANALYSIS

The results and analysis of the proposed UPI Fraud Detection System assess how efficiently the machine learning model can recognize fraudulent transactions. The system evaluates multiple transaction attributes, including transaction amount, time interval between transactions, number of failed authentication attempts, device switching status, and location variation. Based on the experimental observations, the model successfully identifies suspicious transaction patterns and contributes to strengthening the security of digital payment platforms.

➢ *Experimental Setup*

The proposed fraud detection system was implemented and tested using the Python programming language along with supporting libraries such as Pandas for data processing and Scikit-learn for machine learning implementation. A dataset containing records of UPI transactions was utilized for both training and evaluation purposes

The dataset consisted of important features including transaction amount, time gap between consecutive transactions, number of unsuccessful authentication attempts, device change indicators, and location changes. The Random Forest algorithm was chosen as the primary classification technique due to its strong performance in identifying complex patterns within transaction data.

➢ *Evaluation of Results*

The experimental evaluation demonstrates that the fraud detection model can effectively identify suspicious transactions. After the training phase, the model was evaluated using new transaction data that had not been included in the training dataset.

To measure the effectiveness of the model, several standard evaluation metrics were applied, including accuracy, precision, recall, and F1-score. Transactions showing unusual behavior—such as extremely large payment values or multiple failed authentication attempts—were correctly recognized by the system as potential fraud cases.

ISSN No: -2456-2165 https://doi.org/10.38124/ijisrt/26mar371

➢ *Performance Results*

The performance assessment indicates that the Random Forest classifier produces dependable results when identifying fraudulent UPI transactions. By examining various transaction characteristics and behavioral indicators, the system can differentiate between normal transaction activity and suspicious behavior.

Performance metrics such as precision, recall, and F1-score confirm that the model maintains a balanced performance by accurately detecting fraudulent transactions while limiting incorrect fraud alerts.

Table 1 Overall Performance of Algorithm Recommendation System

Metric	Value
Accuracy	94%
Precision	92%
Recall	90%
F1-Score	91%

➢ *User-Wise Precision Analysis*

User-wise precision analysis evaluates the system's ability to correctly identify fraudulent transactions across different users. Precision represents the percentage of accurately predicted fraud cases among all transactions classified as fraudulent by the system.

The analysis reveals relatively consistent precision values for different users, suggesting that the system can detect suspicious activities reliably while minimizing the occurrence of false fraud warnings.

VI. DISCUSSION

The experimental findings demonstrate that integrating rule-based verification techniques with machine learning models significantly improves the ability to detect fraudulent activities in digital payment systems. Transaction attributes such as payment amount, time interval between transactions, authentication failures, device changes, and location variations provide useful indicators for recognizing abnormal transaction behavior.

Although the proposed system shows strong performance in identifying fraudulent transactions, its effectiveness could be further enhanced by utilizing larger datasets and incorporating real-time transaction monitoring mechanisms. These improvements would allow the system to adapt more effectively to evolving fraud strategies and provide stronger protection for digital payment services.

VII. CONCLUSION

The widespread adoption of the Unified Payments Interface (UPI) has significantly improved the efficiency and convenience of digital financial transactions. However, the increasing use of UPI has also resulted in a rise in fraudulent activities, including fake UPI IDs, unauthorized transfers, and various forms of social engineering attacks. To mitigate these risks, this project introduced an Advanced UPI Transaction Fraud Detection System designed to accurately identify suspicious transactions.

The proposed framework combines multiple detection strategies, including rule-based verification, machine learning techniques, behavioral pattern analysis, and graph-based approaches. By analyzing transaction characteristics and historical payment data, the system can recognize unusual patterns and adapt to changing fraud strategies. This approach improves fraud detection accuracy while reducing the number of false alerts.

The system architecture is designed to be modular and scalable, allowing it to support real-time monitoring of digital payment activities and making it suitable for further enhancements in the future. Although certain limitations exist, such as restricted access to real-time financial data and limited dataset availability, the developed system provides a solid foundation for building practical fraud detection solutions.

In conclusion, the proposed approach demonstrates a reliable and intelligent method for improving the security of UPI-based transactions. By effectively identifying fraudulent behavior, the system can help reduce financial losses and enhance user confidence in digital payment platforms.

FUTURE ENHANCEMENT

The UPI Fraud Detection System developed in this project effectively identifies suspicious transactions using rule-based validation and machine learning techniques. However, several improvements can be implemented in the future to enhance its efficiency, scalability, and accuracy. By integrating more advanced technologies and real-time monitoring capabilities, the system can become more suitable for practical deployment in modern digital payment environments.

One major enhancement is the integration of real-time transaction monitoring. Currently, the system analyzes predefined datasets or manually entered transaction information. In the future, the system can be connected to live banking or payment APIs so that each transaction is analyzed instantly. This will help financial institutions detect and prevent fraudulent activities before the transaction is successfully completed.

Another improvement involves using advanced machine learning and deep learning algorithms. While the current model uses the Random Forest algorithm, more sophisticated techniques such as Neural Networks, Gradient Boosting, or Deep Learning models can improve prediction accuracy. These models are capable of identifying complex patterns in large

ISSN No: -2456-2165 https://doi.org/10.38124/ijisrt/26mar371

transaction datasets and detecting more advanced fraud strategies.

The system can also be improved through graph-based fraud detection techniques and user behavior analysis. Fraudsters often operate in networks using multiple accounts and devices. Graph analysis can identify suspicious relationships between transactions, users, and merchants. Additionally, analyzing normal user behavior patterns can help detect unusual activities such as abnormal spending patterns or unexpected transaction locations.

Finally, the system can include stronger security mechanisms and improved visualization tools. Multi-factor authentication and real-time security alerts can be triggered when high-risk transactions are detected. Furthermore, an advanced analytics dashboard can provide banks with clear insights into fraud patterns, transaction trends, and system performance, helping institutions make better security decisions and strengthen digital payment protection.

REFERENCES

[1]. L. Breiman, "Random Forests," *Machine Learning*, vol. 45, no. 1, pp. 5–32, 2001.
[2]. S. Bhattacharyya, S. Jha, K. Tharakunnel, and J. C. Westland, "Data mining for credit card fraud detection," *Decision Support Systems*, vol. 50, no. 3, pp. 602–613, 2011.
[3]. R. J. Bolton and D. J. Hand, "Statistical fraud detection: A review," *Statistical Science*, vol. 17, no. 3, pp. 235–249, 2002.
[4]. T. Chen and C. Guestrin, "XGBoost: A scalable tree boosting system," in *Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, 2016, pp. 785–794.
[5]. C. C. Aggarwal, *Outlier Analysis*, 2nd ed. Cham, Switzerland: Springer, 2017.
[6]. National Payments Corporation of India (NPCI), "Unified Payments Interface (UPI) Product Overview," 2023.
[7]. F. Pedregosa et al., "Scikit-learn: Machine Learning in Python," *Journal of Machine Learning Research*, vol. 12, pp. 2825–2830, 2011.
[8]. W. McKinney, "Data structures for statistical computing in Python," in *Proceedings of the 9th Python in Science Conference*, 2010, pp. 51–56.
[9]. A. Dal Pozzolo, O. Caelen, Y. Le Borgne, S. Waterschoot, and G. Bontempi, "Learned lessons in credit card fraud detection from a practitioner perspective," *Expert Systems with Applications*, vol. 41, no. 10, pp. 4915–4928, 2014.
[10]. V. Jurgovsky et al., "Sequence classification for credit-card fraud detection," *Expert Systems with Applications*, vol. 100, pp. 234–245, 2018.