

UPI Fraud Detection Using Machine Learning

Gayatri Dayanand Navare, Payal Subhash Rathod, Vedashri Keshavrao Dhane, Jayesh Ashok Dhumal, Prof. Swati Gaikwad

Dept. of Computer Science & Engineering (AI & ML) Bharat College of Engineering Badlapur, India - 421503

Abstract - The rapid growth of the Unified Payments Interface (UPI) has transformed digital payments in India by enabling fast, secure, and real-time money transfers. However, the increasing use of UPI has also led to a rise in fraudulent activities such as phishing attacks, fake applications, social engineering, and unauthorized access to accounts [4]. The system analyzes transaction details such as transaction amount, frequency, and user behavior to identify suspicious or abnormal activities. Machine learning algorithms including Random Forest, Logistic Regression, and XGBoost are used to classify transactions as legitimate or fraudulent [2],[10]. The proposed model also includes an alert system that notifies users or authorities when suspicious transactions are detected. This approach helps in early detection of fraud, reduces financial losses, and improves user trust in digital payment systems [4],[8]. The system is scalable and can be integrated into existing UPI platforms to make digital transactions safer and more reliable.

Keywords - UPI, Fraud Detection, Machine Learning, Random Forest, XGBoost, Digital Payment Security, Transaction Analysis.

1. INTRODUCTION

Digital payment systems have grown rapidly in India, especially with the introduction of the Unified Payments Interface (UPI). UPI allows users to transfer money instantly using mobile devices, making digital transactions fast, simple, and convenient. However, the increasing use of UPI has also led to a rise in fraudulent activities such as phishing, fake transactions, and unauthorized account access [4].

This project proposes a fraud detection system called UPI Fraud Detection, which uses Machine Learning to analyze UPI transaction data. Machine learning algorithms such as Random Forest and XGBoost are used to classify transactions as genuine or fraudulent [2], [10].

The main objectives of this project are:

- To analyze UPI transaction data and detect abnormal patterns [8].
- To apply machine learning algorithms for predicting fraudulent transactions [4].
- To evaluate the performance of the model using metrics such as accuracy, precision, recall, and F1-score [10].

The expected outcome of this system is early detection of fraud and improved security for digital transactions, which

will help reduce financial losses and increase user trust in digital payment platforms [4], [8].

2. LITERATURE REVIEW

- N. K. Kanakaraju and S. S. Sreedhar (2023) used Random Forest and SVM for behavioral fraud detection in UPI transaction metadata and achieved high accuracy in identifying known fraud patterns. However, the model mainly focused on known fraud behaviors.
- A. Dhoke and N. Jaiswal (2019) applied Logistic Regression and Random Forest for financial fraud classification and found Random Forest to be more effective in handling class imbalance. However, the study focused on credit card fraud rather than UPI-specific fraud.
- S. Gupta and B. Giri (2020) used NLP techniques to identify phishing triggers in digital communication channels, improving the detection of social engineering tactics. However, the study did not directly address transaction-level UPI fraud.
- P. Kumar and R. Singh (2020) studied QR phishing (Quishing) using Computer Vision and URL Analysis, emphasizing the need for automated QR verification in mobile apps. However, the study focused mainly on QR-related threats.
- NPCI Guidelines (2024) defined rule-based UPI safety measures, including the ₹1 lakh transaction limit, to improve regulatory safety. However, these guidelines do not provide machine learning-based fraud prediction.

3. SYSTEM ARCHITECTURE

The proposed system architecture for UPI fraud detection begins with collecting transaction details such as amount, time, UPI ID, device, and location. The collected data undergoes preprocessing steps including cleaning, encoding, and normalization to prepare it for analysis

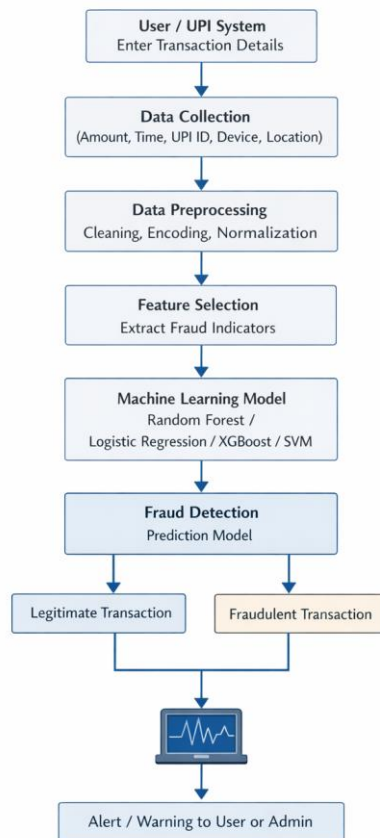


Fig. 1. System Architecture of UPI Fraud Detection

A. Core Components

- 1) Transaction Data collection: The system collects important transaction details such as transaction amount, time, user ID, device information, and transaction frequency. These parameters are used as input features for fraud detection [10].
- 2) Machine Learning Analysis The collected transaction data is processed using machine learning algorithms such as **Random Forest** to analyze patterns and classify transactions as legitimate or fraudulent [4], [10].
- 3) QR Code and Integrity Verification: The system analyzes QR code images using an image processing pipeline that includes grayscale conversion and binarization. This helps verify the authenticity of the transaction environment and detect high-risk QR codes.
- 4) SMS Phishing Detection & Reporting: The SMS analysis module scans message text using pattern matching techniques to detect suspicious keywords such as OTP or KYC. The system then compiles the results and generates a report for the user [5].

B. Environment Management

Although not visible in the source code logic, the deployment environment relies on specific Python structures identified in the project directory:

The system is developed using the **Python programming language** with libraries such as **NumPy, Pandas, Scikit-learn, and image processing tools** for data analysis, machine learning implementation, and QR code processing [2], [5].

4. METHODOLOGY AND IMPLEMENTATION

- 1) The implementation of the UPI Fraud Detection system is divided into three distinct modules: UPI Transaction Integrity, QR Code Analysis, and SMS Phishing Detection.
- 2) Model Training: A dataset containing 6 key features (UPI length, special characters, suspicious keywords, amount, device mismatch, and location mismatch) was used to train a Random Forest model [4], [10].
- 3) In this phase, a hybrid logic mechanism was implemented to enhance the efficiency and reliability of the fraud detection system. A pre-processing filter was developed to intercept any transaction exceeding **100,000 INR**, which is beyond the standard transaction limit defined for most UPI transactions. This rule-based filtering mechanism ensures that transactions violating predefined logical constraints are immediately flagged without being processed by the machine learning model [4]. By applying this preliminary validation step, the system reduces unnecessary computational overhead and improves the overall performance of the model.
- 4) Vision & NLP integration.
- 5) Implementation of OpenCV for image preprocessing and PyZbar for QR decoding. The SMS module was built using keyword-frequency [5].
- 6) D. Security Correlation: Establishing a dependency where the check_app_integrity function is triggered by the analyze_QR_code result.

5. ALGORITHMS

The system relies on specific algorithmic logic for data processing:

Random Forest Classifier

Random Forest is an ensemble learning algorithm that builds multiple decision trees and combines their results to improve prediction accuracy. It is used to analyze the six-feature transaction vector and classify transactions as legitimate or fraudulent while reducing overfitting [4], [10].

Aho-Corasick / Pattern Matching

The Aho-Corasick algorithm is used in the SMS analysis module to detect suspicious keywords such as "KYC", "OTP", and "Blocked". This helps identify potential phishing or fraudulent messages quickly [5].

Image Processing Pipeline

The image processing pipeline processes QR code images by applying grayscale conversion and binarization. These steps improve the accuracy of QR code decoding even in low-light or unclear scanning conditions. These preprocessing steps improve the accuracy of QR code decoding, especially under challenging conditions such as low-light environments or blurred scans. The processed image is then decoded to extract transaction information, which can be further analyzed for potential fraud.

6. TECHNOLOGIES USED

- **Python 3.10+** : The primary programming language for backend logic.
- **Flask** : A micro-web framework used for routing and session management.
- **Scikit-learn** : For implementing the Machine Learning pipeline and model serialization.
- **OpenCV-Python** : To handle image processing tasks for the QR scanner.
- **PyZbar** : For decoding the data encoded within the QR symbols.
- **FPDF** : For generating professional, encoded-safe PDF security reports.
- **Jinja2** : The templating engine used to render dynamic HTML content.

7. MODULES AND WORKFLOW

- 1) **Dashboard Module:** The Dashboard module acts as the main interface of the system and provides an overview of the project functionalities. It serves as the entry point for users to access different modules and monitor system operations
- 2) **UPI Transaction QR Integrity Module:** This module collects transaction-related metadata such as transaction amount, user details, and device information to calculate the risk probability. It also scans QR code images and verifies the environment trust level; if a QR code is detected as **high risk [4], [10]**.
- 3) **SMS Module:** A sandbox where users can paste SMS text to check for phishing indicators [5].
- 4) **Report Generation Module:** Collects all "Session Results" and compiles them into a downloadable PDF for the user's records.

1) DATA FLOW DIAGRAM (DFD)

1) Level 1:

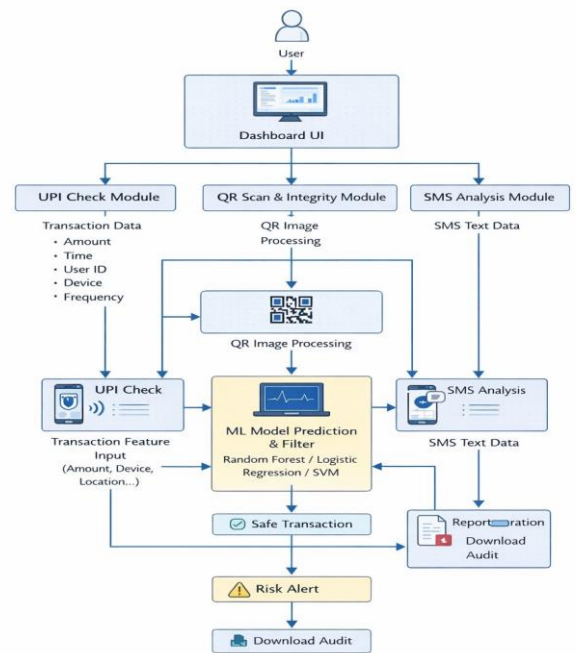
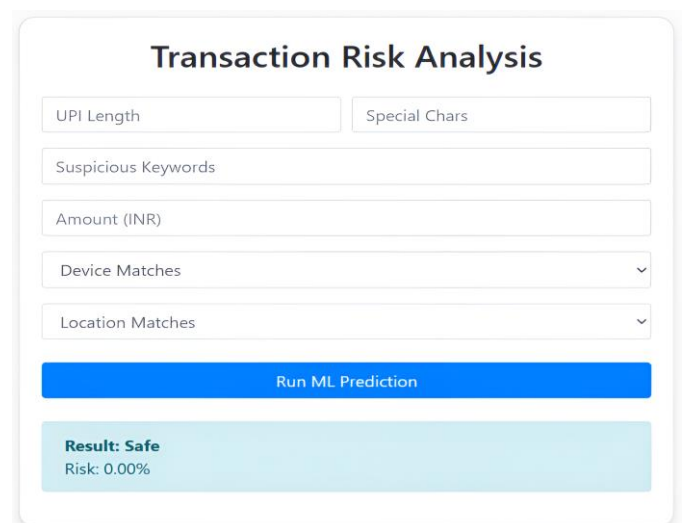
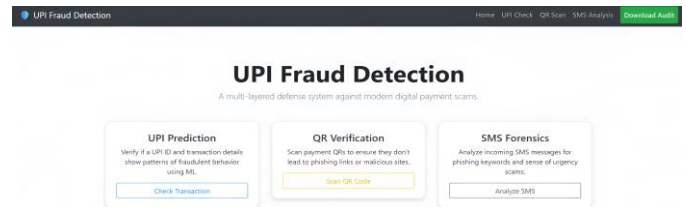


Fig. 2. DFD of UPI Fraud Detection.

8. RESULTS AND OUTPUT



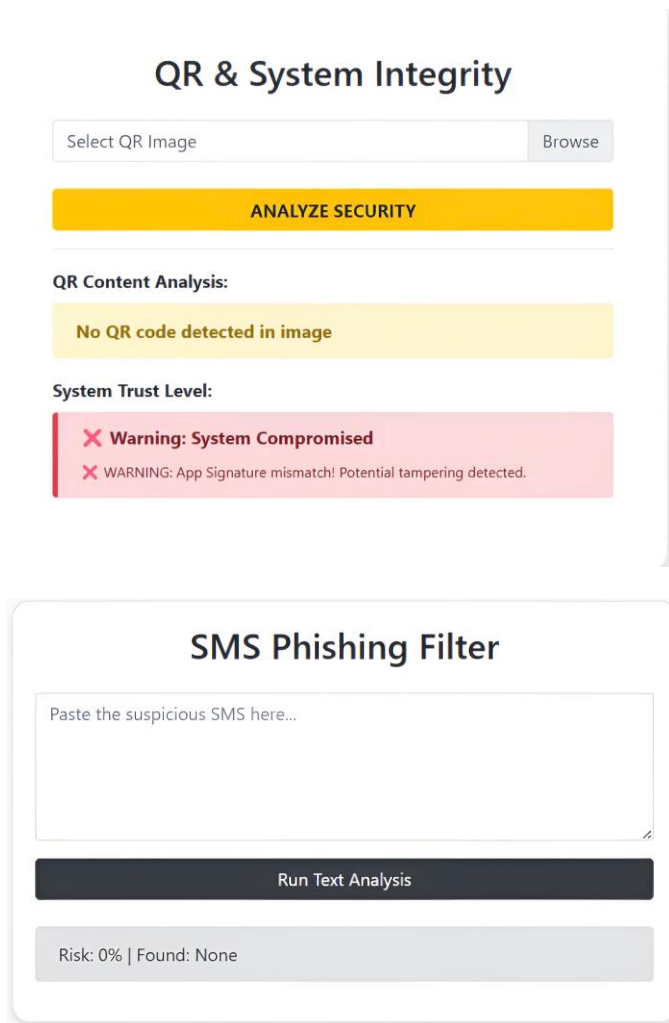


Fig. 3. Outputs & Results

9. FUTURE SCOPE

Deep Learning (LSTM): To analyze the sequence of user transactions to find "low-and-slow" fraud patterns- vide automated forecasting and trend analysis on the uploaded data [7].

Voice Phishing (Vishing) Detection: Adding a module to record and analyze audio calls for fraudulent speech patterns.

Blockchain Ledger: Storing the "Fraudulent UPI IDs" on a private blockchain to prevent scammers from deleting their history.

10. CONCLUSIONS

This project successfully demonstrates that a Hybrid Approach is the most effective way to secure UPI transactions. By combining the "Intelligence" of Machine Learning with the "Strictness" of Banking Rules, we have created a system that is both smart and compliant [4], [10]. The inclusion of QR and SMS analysis modules ensures that

the user is protected from the entire lifecycle of a modern digital payment scam [5].

ACKNOWLEDGEMENT (Optional)

The author would like to express their sincere gratitude to Prof. Swati Gaikwad (Project Coordinator) for her invaluable guidance, continuous encouragement, and technical support throughout the development of the UPI Fraud Detection system. We also extend our thanks to Prof. Vijaylakshmi Tadkal (Head of Department, Computer Science & Engineering - AI & ML) for providing the necessary academic resources and laboratory facilities at Bharat College of Engineering, Badlapur.

Finally, we thank the University of Mumbai for providing the curriculum platform that motivated this research work.

REFERENCES

1. N. K. Kanakaraju and S. S. Sreedhar, "Fraud Detection in UPI Transactions using Machine Learning Algorithms," in Proc. 7th IEEE Int. Conf. on Computing Methodologies and Communication (ICCMC), 2023, pp. 452-457. doi: 10.1109/ICCMC56507.2023.10128542
2. Dhoke and N. Jaiswal, "A Comparative Study of Machine Learning Algorithms for Credit Card Fraud Detection," Int. J. Comput. Appl., vol. 182, no. 48, pp. 24-29, Jan. 2019. Available: <https://www.ijcaonline.org/archives/volume182/number48/dhoke-2019-ijca-918641.pdf>
3. S. Gupta and B. Giri, "A Review of Phishing Detection Techniques based on Machine Learning," Int. J. Adv. Res. Comput. Sci., vol. 11, no. 2, pp. 112-118, Mar. 2020. Available: <http://www.ijarcs.info/index.php/Ijarcs/article/view/6565>
4. P. Kumar and R. Singh, "QR Code Security: A Survey of Phishing and Malicious Attacks," J. Inf. Secur. Appl., vol. 51, p. 102443, Apr. 2020. doi: 10.1016/j.jisa.2020.102443
5. National Payments Corporation of India (NPCI), "UPI Product Statistics and Safety Awareness Guidelines," 2024. [Online]. Available: <https://www.npci.org.in/what-we-do/upi/product-statistics>

BIOGRAPHIES**Gayatri Navare**

Currently pursuing Bachelor of Engineering in Computer Science (AIML) from Bharat College Of Engineering, Maharashtra, India. Interested in Data Analyst, MIS Analyst, Business Analyst, Dashboard Analyst as well as Python Programming, Artificial Intelligence and Machine Learning.

**Payal Rathod**

Currently pursuing Bachelor of Engineering in Computer Science (AIML) from Bharat College Of Engineering, Maharashtra, India. Interested in Cyber Security and Ethical Hacking as well as Python Programming and Artificial Intelligence.

**Vedashri Dhane**

Currently pursuing Bachelor of Engineering in Computer Science (AIML) from Bharat College Of Engineering, Maharashtra, India. Interested in Cybersecurity, Data Analysis and Power BI Dashboard and Networking.

**Jayesh Dhumal**

Currently pursuing Bachelor of Engineering in Computer Science (AIML) from Bharat College Of Engineering, Maharashtra, India. Interested in Artificial Intelligence, Machine Learning and as well as skillful in Data Analysis.