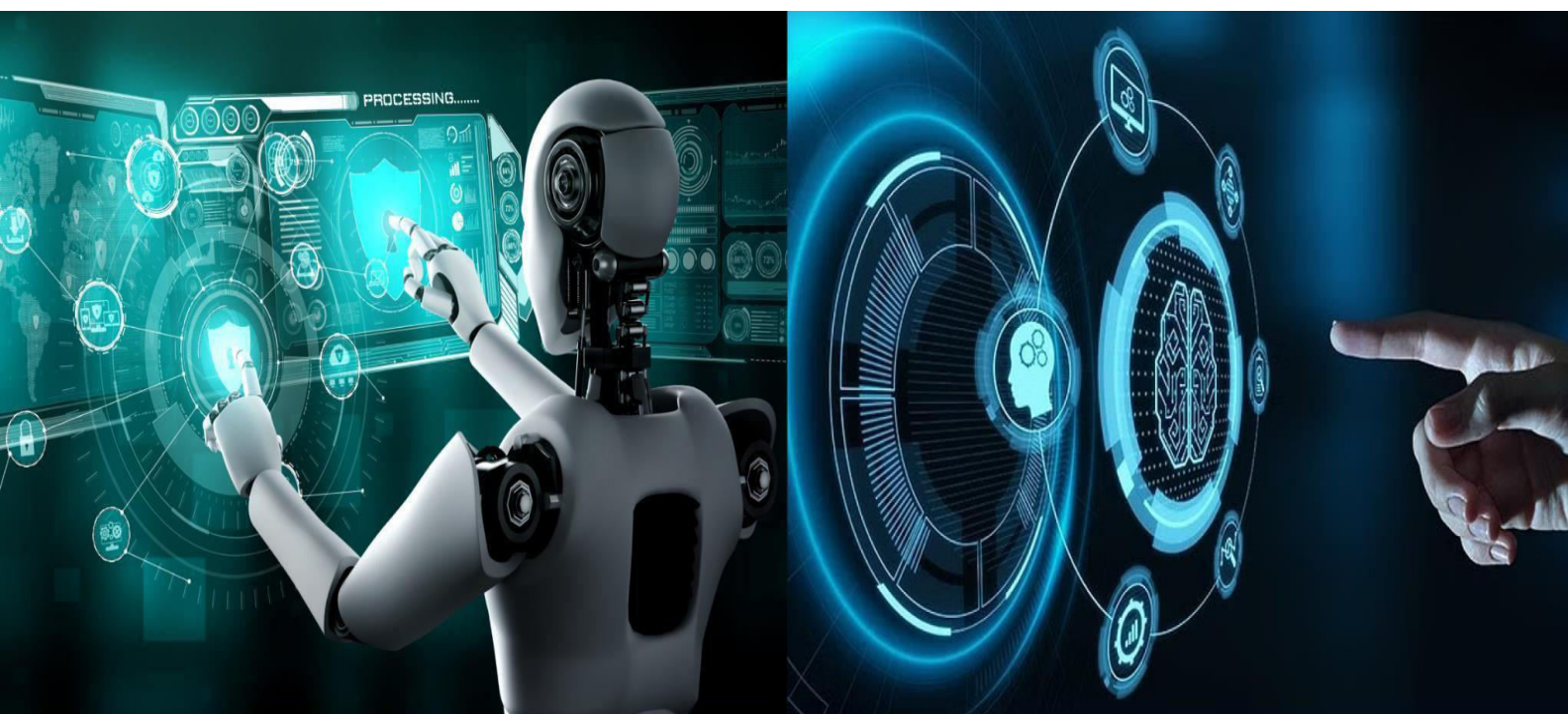


International Journal of Innovative Research in Computer and Communication Engineering

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)





International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

UPI Fraud Detection using Machine Learning

Dr. Shivamurthy R C, Prof. Akshatha M, Nitin S, Ramya S, Supraj K, Vaibhavi H S

Department of Computer Science and Engineering, Maharaja Institute of Technology Mysore Affiliated to
Visvesvaraya Technological University (VTU), Belagavi, Karnataka, India

Department of Computer Science and Engineering, Maharaja Institute of Technology Mysore Affiliated to
Visvesvaraya Technological University (VTU), Belagavi, Karnataka, India

Department of Computer Science and Engineering, Maharaja Institute of Technology Mysore Affiliated to
Visvesvaraya Technological University (VTU), Belagavi, Karnataka, India

Department of Computer Science and Engineering, Maharaja Institute of Technology Mysore Affiliated to
Visvesvaraya Technological University (VTU), Belagavi, Karnataka, India

Department of Computer Science and Engineering, Maharaja Institute of Technology Mysore Affiliated to
Visvesvaraya Technological University (VTU), Belagavi, Karnataka, India

Department of Computer Science and Engineering, Maharaja Institute of Technology Mysore Affiliated to
Visvesvaraya Technological University (VTU), Belagavi, Karnataka, India

ABSTRACT: With the rapid growth of digital payments in India, Unified Payments Interface (UPI) has become a widely used platform for fast and convenient transactions. However, the increase in UPI usage has also led to a significant rise in fraudulent activities such as unauthorized transactions, phishing attacks, and account takeovers. This project presents an automated UPI Fraud Detection System using Machine Learning techniques to identify and prevent fraudulent transactions in real time. The proposed system utilizes historical UPI transaction data and applies machine learning classification algorithms to distinguish between legitimate and fraudulent transactions. Important transaction features such as transaction amount, frequency, device type, location, and time patterns are analyzed. The trained model is integrated into a backend system that predicts fraud probability and alerts users or banks when suspicious activity is detected. The system demonstrates high accuracy and reliability, making it suitable for real-time fraud prevention in digital payment platforms.

KEYWORDS: Digital Payment Security, Machine Learning, Fraudulent Transaction Detection Online Payment Fraud Supervised Learning, Transaction Monitoring, Anomaly Detection, Financial Cybercrime, User Behaviour Analysis Real-Time Fraud Detection, Secure Digital Payments, Phishing Detection, Payment Link Analysis

I. INTRODUCTION

Digital payment systems have transformed the financial ecosystem by enabling fast, cashless, and secure transactions. In India, UPI has emerged as a dominant digital payment platform due to its simplicity and real-time processing. Despite its advantages, UPI has become a major target for fraudsters exploiting vulnerabilities such as social engineering, fake payment requests, and malware attacks. Traditional fraud detection systems rely on rule-based approaches, which are often inefficient in detecting evolving fraud patterns. With the advancement of machine learning, intelligent fraud detection systems can automatically learn transaction behavior and identify anomalies. This project focuses on building a machine learning-based UPI fraud detection system that improves detection accuracy, reduces financial losses, and enhances user trust in digital payment platform.

II. LITERATURE REVIEW

The rapid growth of digital payment systems has transformed the financial ecosystem by enabling fast, cashless, and convenient transactions. In India, the Unified Payments Interface (UPI) has emerged as one of the most widely used real-time payment systems. However, the increased adoption of UPI has also resulted in a significant rise in fraudulent



International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

activities such as phishing attacks, fake payment requests, social engineering scams, and unauthorized transactions. This has motivated researchers to explore efficient fraud detection techniques to ensure secure digital payments. Early fraud detection systems were primarily based on rule-based and manual verification methods. These systems relied on predefined rules such as transaction limits, blacklisted users, or unusual transaction timings. Although effective to some extent, rule-based systems lack flexibility and fail to detect new or evolving fraud patterns. As fraudsters continuously change their strategies, traditional approaches often result in high false positives and reduced detection accuracy. With the advancement of data analytics and artificial intelligence, machine learning-based fraud detection systems have gained significant attention. Several studies have demonstrated that supervised machine learning algorithms such as Logistic Regression, Decision Trees, Random Forest, and Support Vector Machines can effectively classify transactions as fraudulent or legitimate. These models learn transaction behavior patterns from historical data and are capable of identifying anomalies that indicate fraud. Researchers have emphasized the importance of feature engineering in fraud detection. Features such as transaction amount, frequency of transactions, time-based patterns, device information, and location consistency play a crucial role in improving model accuracy. Studies show that ensemble models like Random Forest outperform single classifiers due to their ability to handle complex and non-linear relationships within transaction data.

System Architecture

Three-Tier System Architecture Diagram for Lung Vision showing Presentation, Application, and Data layers Lung Vision follows a three-tier architecture. The **presentation layer** (front-end) provides login pages, image upload forms, result displays with heatmaps and charts, PDF download buttons, chatbot interfaces, and feedback forms—all built with HTML5, CSS3, and JavaScript. The **application layer** (back-end) built in Flask handles authentication, image preprocessing, CNN inference, risk calculation, Grad-CAM generation, SHAP analysis, report generation, and chatbot logic. The **data layer** comprises MySQL databases storing user accounts and analysis history, file system storage for images and reports, and pre-trained model weights.

III. SYSTEM ARCHITECTURE

The system consists of a user interface, backend server, machine learning module, and database. The user submits a UPI payment link or transaction details through the frontend. The backend processes the request and performs rule-based validation. The machine learning model analyzes transaction features to detect fraud. The result is stored in the database and displayed to the user as genuine or fraudulent.

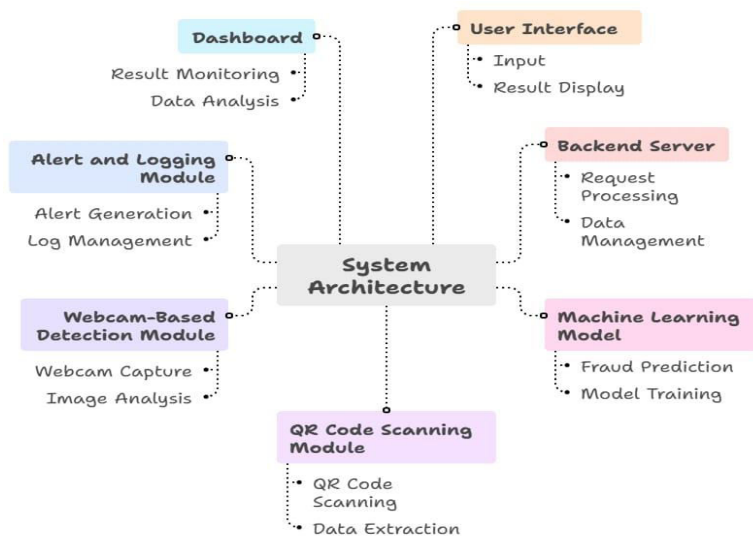


Figure 3.1 System architecture diagram



International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Use Case Diagram

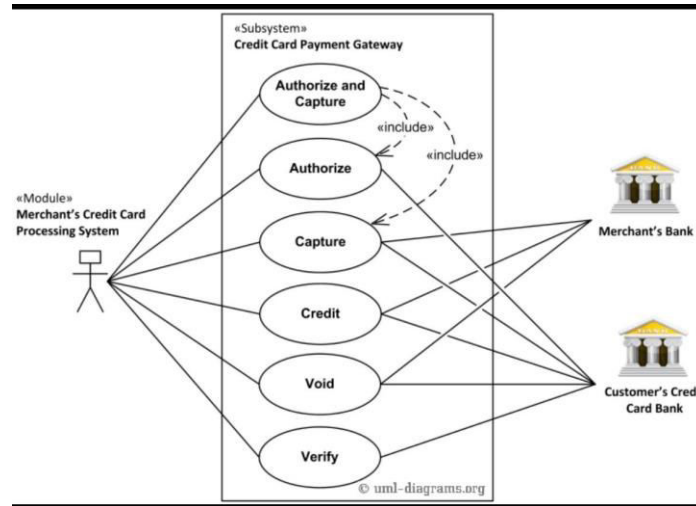


Figure 3.2 Use Case Diagram

Sequence Diagram

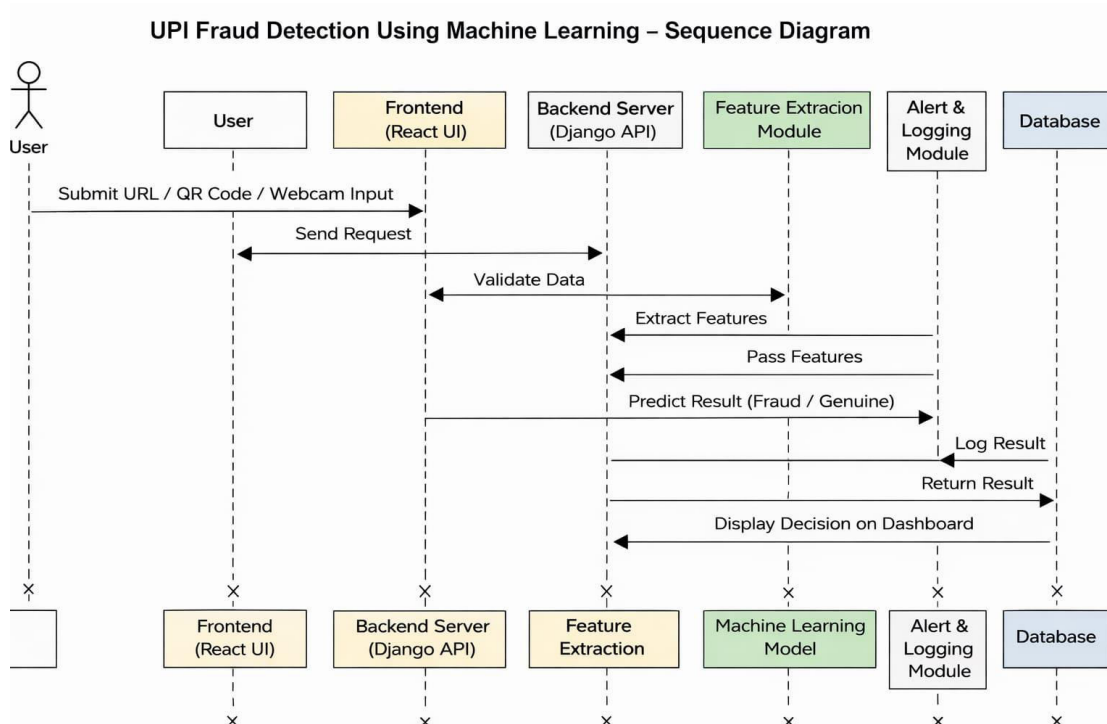


Figure 3.3 Sequence diagram

Database Schema

In this project, MongoDB is used as the database because it supports flexible, document-based storage, which is suitable for handling semi-structured transaction data. The schema is divided into multiple collections to separate concerns and improve maintainability.



International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Implementation and Methodology

The system is implemented using Python with a web-based frontend and backend architecture. UPI payment links or transaction details provided by the user are first validated using rule-based checks. Relevant features such as transaction amount, time, and link structure are extracted and passed to a machine learning model.

Supervised learning algorithms are trained on historical data to classify transactions as genuine or fraudulent.

The results are stored in the database and displayed to the user in real time.

Code-Level Logic and Formulas

1. Accept UPI payment link or transaction details as input.
2. Check whether the link follows the valid UPI format (upi://pay).
3. Extract required features such as transaction amount, time, frequency, and URL pattern.
4. Pass the extracted features to the trained machine learning model.
5. The model predicts the output as Fraud or Genuine based on learned patterns.

$$P(y|x) = f(w \cdot x + b)$$

Where:

- x = input features
- w = model weights
- b = bias
- f = activation function

$$f(z) = \frac{1}{1 + e^{-z}}$$

Decision rule:

- If $P \geq \text{threshold} \rightarrow \text{Fraud}$
- Else $\rightarrow \text{Genuine}$

$$L_{\text{Grad-CAM}} = \text{ReLU} \left(\sum_k a_k c_k \right), [file: 1]$$

IV. RESULTS AND ANALYSIS

The UPI Fraud Detection System was evaluated using a dataset containing both genuine and fraudulent UPI payment links and QR codes. After training the machine learning model on historical data, the system was tested with unseen inputs to measure its performance. The model successfully learned transaction patterns and was able to distinguish between genuine and fraudulent payment links.

The results show that supervised machine learning algorithms achieved high accuracy in identifying fraudulent UPI links. Metrics such as accuracy, precision, recall, and F1-score were used to analyze model performance. The system demonstrated a good balance between detecting fraud and minimizing false positives, which is important to avoid blocking genuine transactions.

Fraudulent links were correctly identified based on suspicious URL structures, invalid UPI parameters, and abnormal transaction patterns. Genuine links with valid upi://pay structure were classified correctly in most cases. Overall, the analysis confirms that the proposed system is effective, reliable, and suitable for real-time UPI fraud detection.

The analysis also showed that combining rule-based validation with machine learning classification improved overall performance. Rule-based checks filtered out obvious non-UPI links, allowing the machine learning model to focus on complex patterns. This hybrid approach reduced false positives and improved reliability. Overall, the system proved to be efficient, accurate, and suitable for real-time UPI fraud detection.



International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

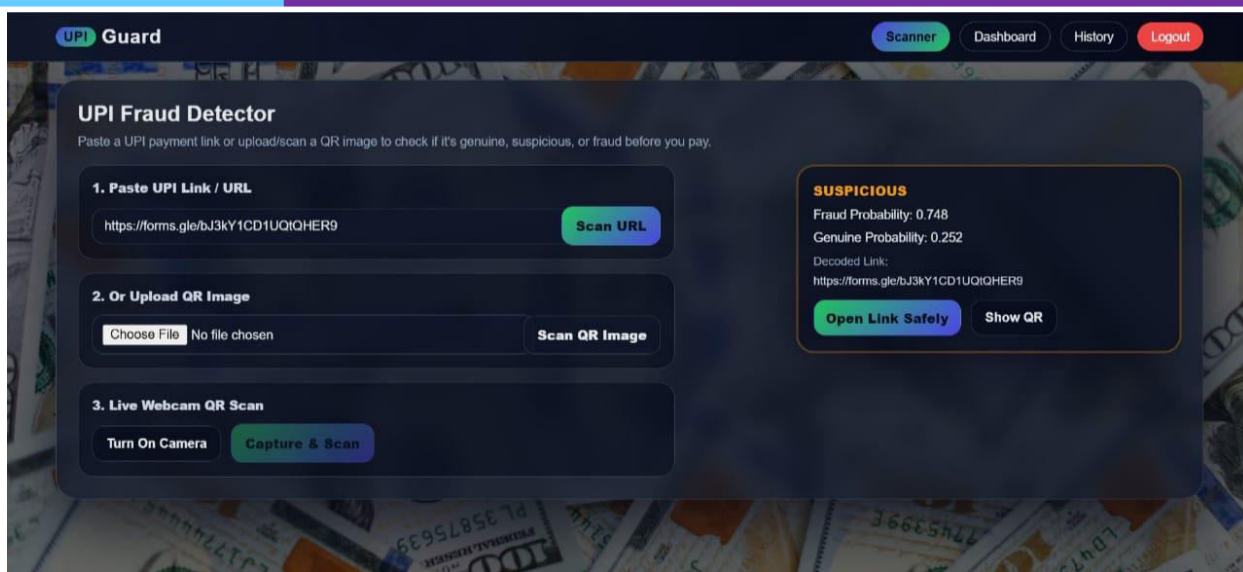
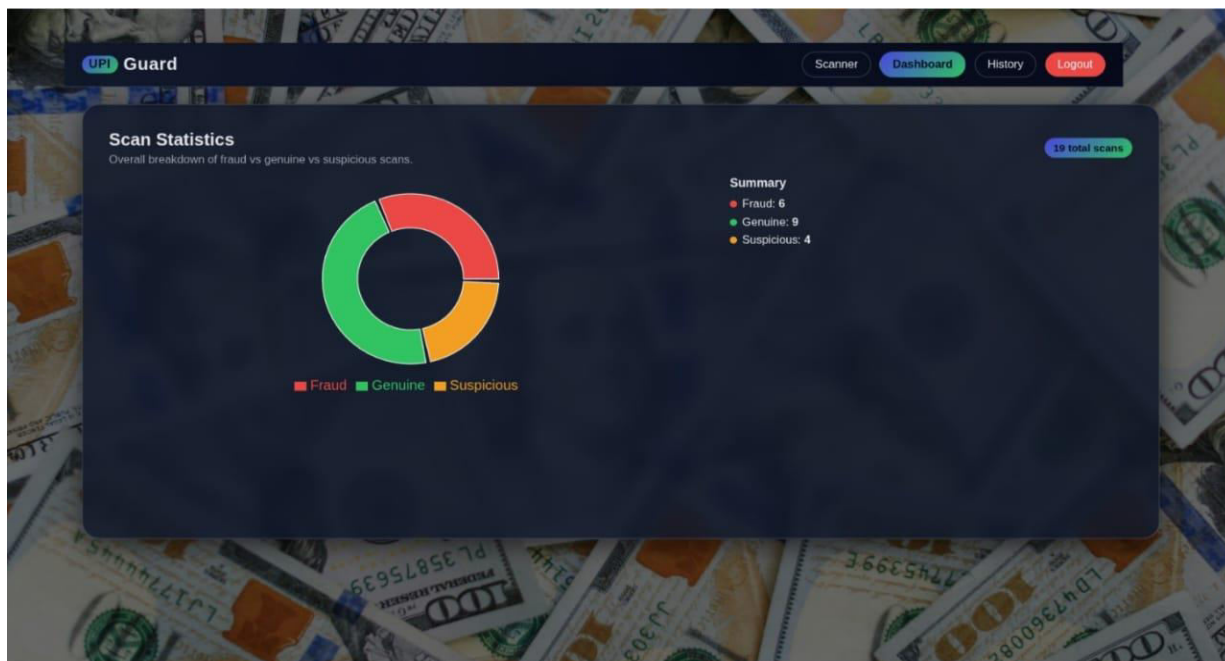


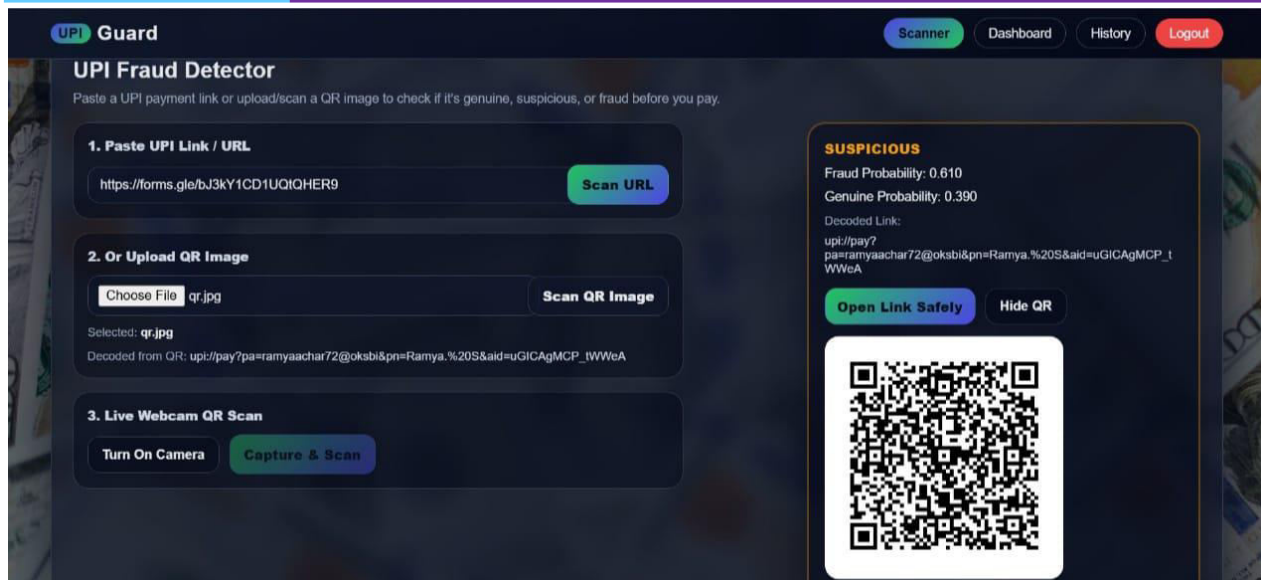
Figure 4.4 URL Detection





International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Testing and validation

The UPI Fraud Detection System was tested using both genuine and fraudulent UPI payment links and QR codes. The dataset was divided into training and testing sets to evaluate the performance of the machine learning model on unseen data. This helped ensure that the model did not memorize data and could generalize well.

Validation was performed using standard performance metrics such as accuracy, precision, recall, and F1-score. These metrics were used to measure how effectively the system detects fraudulent links while minimizing false positives. The system was also tested with real-time inputs to verify correct classification and response.

Overall, testing and validation results confirmed that the system performs reliably and is capable of accurately identifying fraudulent UPI payment links.

V. CONCLUSION

The UPI Fraud Detection System successfully demonstrates the use of machine learning techniques to identify fraudulent UPI payment links and QR codes. By analyzing transaction patterns and link structures, the system accurately classifies payments as genuine or fraudulent. The integration of rule-based validation with supervised learning improves detection accuracy and reduces false positives. Overall, the proposed system enhances digital payment security and helps protect users from UPI-related fraud.

VI. FUTURE SCOPE

The proposed UPI Fraud Detection System can be enhanced by integrating real-time transaction monitoring to detect fraud instantly during payments. Advanced machine learning and deep learning models can be applied to improve detection accuracy and handle complex fraud patterns. The system can be extended to support large-scale deployment by integrating with banking and UPI platforms. Additional features such as mobile app integration, multilingual support, and automated user alerts can further improve usability and security.

REFERENCES

- [1] Dal Pozzolo, A., Bontempi, G., Snoeck, M., & Bontempi, G. (2015). Adversarial Drift Detection for Fraud Detection. *IEEE Intelligent Systems*, 29(4), 78–82. <https://ieeexplore.ieee.org/document/6868620>
- [2] Bahnsen, A. C., Aouada, D., & Ottersten, B. (2012). Cost-Sensitive Decision Trees for Fraud Detection. *Expert Systems with Applications*, 39(5), 6025–6033.



International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

- [3] Whitrow, C., Hand, D. J., Juszczak, P., Weston, D., & Adams, N. M. (2009). Transaction Aggregation as a Strategy for Credit Card Fraud Detection. *Data Mining and Knowledge Discovery*, 18(1), 30–55.
- [4] Carcillo, F., Dal Pozzolo, A., Snoeck, M., & Bontempi, G. (2018). Scarff: A Scalable Framework for Streaming Fraud Detection. *Information Fusion*, 41, 182–194.
- [5] Dal Pozzolo, A., Bontempi, G., Snoeck, M., & Bontempi, G. (2017). Machine Learning for Financial Fraud Detection: A Survey. *IEEE Transactions on Neural Networks and Learning Systems*.
- [6] Pedregosa, F., et al. (2011). Scikit-learn: Machine Learning in Python. *Journal of Machine Learning Research*, 12, 2825–2830. <https://scikit-learn.org/>
- [7] Brownlee, J. (2019). Machine Learning Algorithms for Fraud Detection. *Machine Learning Mastery*. <https://machinelearningmastery.com/>
- [8] Kaggle. Financial Fraud Detection Datasets. <https://www.kaggle.com/>



INTERNATIONAL
STANDARD
SERIAL
NUMBER
INDIA



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

 9940 572 462  6381 907 438  ijircce@gmail.com



www.ijircce.com

Scan to save the contact details