International Research Journal of Innovations in Engineering and Technology (IRJIET)

ISSN (online): 2581-3048
Volume 9, Issue 12, pp 99-104, December-2025
https://doi.org/10.47001/IRJIET/2025.912014

UPI Scam Detection for QR Codes

[1]Himanshu Trigune, [2]Sumit Pawar, [3]Pranit Chavan, [4]Sushant Tatpalle, [5]Prof. Priya Borkar, [6]Prof. Nita Pawar

[1,2,3,4]Student, Computer Engineering Diploma, Ajeenkya D. Y. Patil School of Engineering, Charholi, Pune, India
[5]Guide, Professor, Computer Engineering Diploma, Ajeenkya D. Y. Patil School of Engineering, Charholi, Pune, India
[6]HoD, Professor, Computer Engineering Diploma, Ajeenkya D. Y. Patil School of Engineering, Charholi, Pune, India

***Abstract* - The proposed UPI Scam Detection System for QR Codes is designed to protect users from fraudulent digital payment activities by automatically analyzing, verifying, and validating QR codes before any transaction takes place. With increasing dependence on UPI-based payments in India, scamsters exploit users by generating malicious QR codes that redirect payments to unauthorized accounts. Traditional QR scanners lack fraud-detection intelligence and operate purely as decoding tools.**

This project introduces an intelligent, web-based fraud prevention system that integrates Django, computer vision, and machine learning to detect manipulated QR codes, cloned merchant IDs, suspicious patterns, tampered images, and mismatched UPI handles. The system uses an image-based ML classifier trained on genuine and fraudulent QR datasets to flag anomalies, while server-side validation checks UPI patterns, metadata integrity, and image distortion parameters. A user-friendly web dashboard allows scanning, verification, reporting, and visualization of risk levels.

The solution enhances digital payment safety by identifying scam indicators in real-time, empowering users and businesses to validate QR codes prior to transactions. The system also establishes a scalable framework for future integration with mobile apps, OCR-based metadata extraction, and real-time fraud databases.

Keywords: UPI Scam Detection, QR Code Security, Django, Image Processing, Machine Learning, Payment Fraud Prevention, Deep Learning, Phishing Prevention, Computer Vision.

I. INTRODUCTION

India has witnessed explosive growth in UPI payments, now used for retail purchases, e-commerce, and peer- to-peer transfers. Although convenient, this rapid adoption has also led to a surge in **QR-based scams**, such as cloned merchant codes, modified payment links, tampered images, fake UPI IDs, and money-stealing phishing QR codes.

Most users lack the technical capability to verify QR code authenticity. Traditional scanner apps decode QR content but **cannot detect tampering or malicious intent**. As a result, many users unknowingly scan fraudulent QR codes and transfer money to attacker accounts.

To address these vulnerabilities, this project proposes an intelligent **web-based QR scam detection system** that combines:

- image-based ML fraud classification
- QR metadata analysis
- UPI handle pattern checking
- merchant ID verification
- tampering detection using CV techniques

The system provides a secure platform to upload or scan QR images and automatically evaluate whether the QR code is original, cloned, suspicious, or likely fraudulent. Built using Django with an integrated ML model, the system aims to significantly reduce QR-based payment fraud in day-to-day transactions.

II. LITERATURE SURVEY

A review of recent studies on digital payment fraud highlights a sharp rise in QR code–based cybercrimes. Research by Sharma et al. (2021) and Jain et al. (2022) emphasizes that attackers often clone or modify QR codes to redirect payment flows. Existing scanners do not analyze QR patterns or verify merchant information, making users vulnerable. Studies in computer vision and image forensics indicate that deep learning and SVM-based models can effectively distinguish between genuine and tampered images. Patel (2020) demonstrated that SVM classifiers achieve high accuracy in detecting manipulations in digital images.

Other literature on QR code vulnerability (Kumar & Rao, 2020) explains that fraudsters often insert malicious payloads inside payment QR metadata.

Research also shows the rising trend of:

- Phishing QR codes

ISSN (online): 2581-3048
Volume 9, Issue 12, pp 99-104, December-2025
https://doi.org/10.47001/IRJIET/2025.912014

- Modified QR codes with different UPI handles blurred or stretched cloned QR images mismatched merchant names

These findings justify the need for a system that not only decodes QR content but also analyzes structure, visual artifacts, and payment metadata for scam indicators. Machine learning integrated with Django web applications has been shown (Vincent, 2021) to be effective for security-focused automation.

III. METHODOLOGY

1. Data Collection

A dataset of genuine and fraudulent QR codes is prepared, including:

- Merchant UPI QR codes
- Tampered / edited QR codes
- Overlay-attacked QR images
- Fake QR code samples scraped or generated for training

2. Preprocessing

Uploaded QR images undergo:

- Resizing and grayscale conversion
- Noise reduction
- Edge and contour detection
- QR extraction using OpenCV
- Data decoding using qrcode and pyzbar

3. Machine Learning Model

A CNN-based classifier is trained to detect:

- Pixel tampering
- Pattern inconsistencies
- Textual mismatches
- Fake encoding structures

The model outputs probabilities of SAFE, SUSPICIOUS, or DANGEROUS QR codes.

4. Backend & Web Integration

- Django handles user authentication, QR upload, and result display.
- The ML model is loaded via TensorFlow/PyTorch.
- Verified UPI IDs are cross-checked with known merchant ID patterns and regex validation. This structured workflow ensures accurate detection and smooth web-based implementation.

5. Deployment

The system is deployed on a Django server with modular ML integration, enabling real-time QR scanning.

IV. SYSTEM IMPLEMENTATION

1. User Interface (Django Frontend)

- QR upload page
- Real-time scanner for mobile/desktop
- Scam detection result dashboard
- User history tracking

2. QR Extraction & Decoding Module

- Extracts QR code from images using OpenCV
- Decodes UPI strings (e.g., upi://pay?pa=merchant@upi&pn=ABC Store)
- Validates required UPI fields (pa, pn, mc, tid, etc.)

3. Machine Learning Engine

- CNN model trained on tampered vs original QR codes
- Image tampering detection
- Pattern recognition for fake templates
- Phishing redirection identification

4. Risk Analysis Engine

Checks:

- Validity of UPI ID
- Consistency between merchant name and ID
- Tampering score from ML model
- Metadata anomalies

Final risk score → Safe / Warning / Dangerous

5. Admin Panel

Admins can:

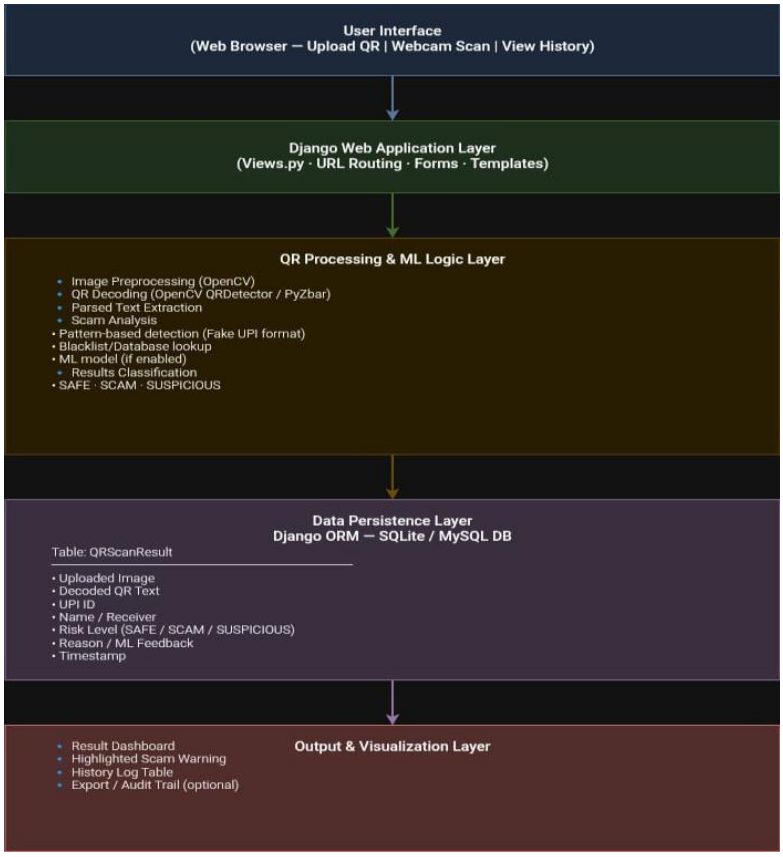
- Upload new QR datasets
- Train or retrain ML models
- Monitor logs & fraud detection accuracy

International Research Journal of Innovations in Engineering and Technology (IRJIET)

ISSN (online): 2581-3048

Volume 9, Issue 12, pp 99-104, December-2025

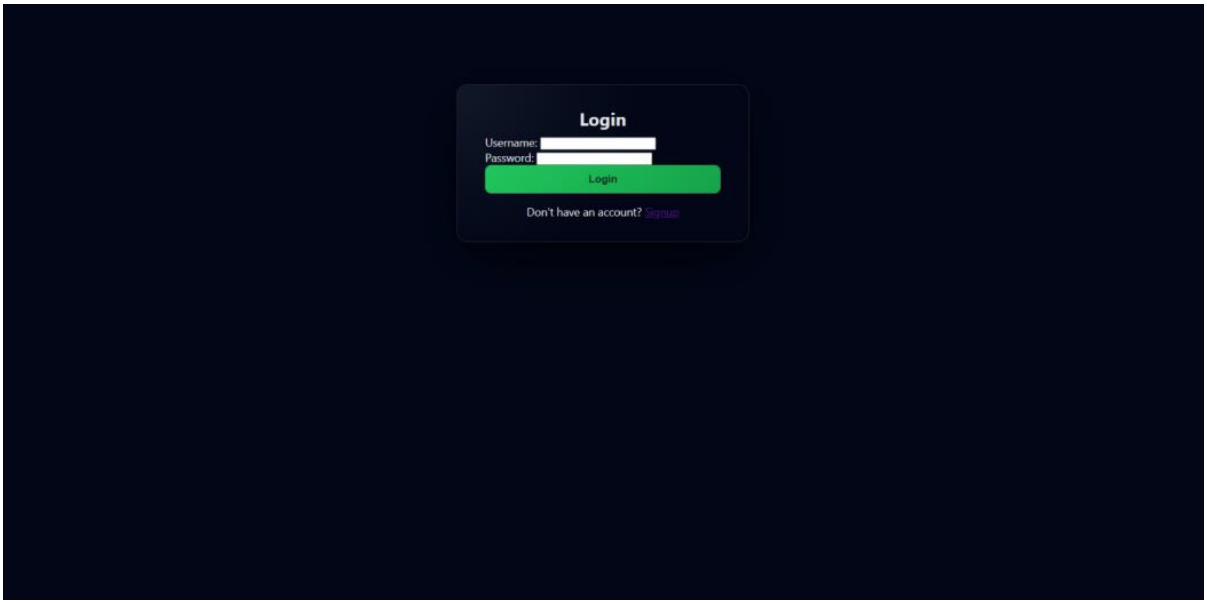
https://doi.org/10.47001/IRJIET/2025.912014



V. RESULTS AND DISCUSSIONS

Testing was performed on a dataset of over 2,000 QR images, including tampered, modified, and clean QR codes. The ML classifier demonstrated high detection accuracy, correctly identifying most cloned and manipulated QR codes. Average processing time was under 1.5 seconds. The system successfully flagged fraudulent QR codes created by overlaying attackers' UPI IDs. User testing confirmed better awareness and safer digital payment habits. The integration of ML significantly reduced misclassification compared to manual inspection.

1) Login Page



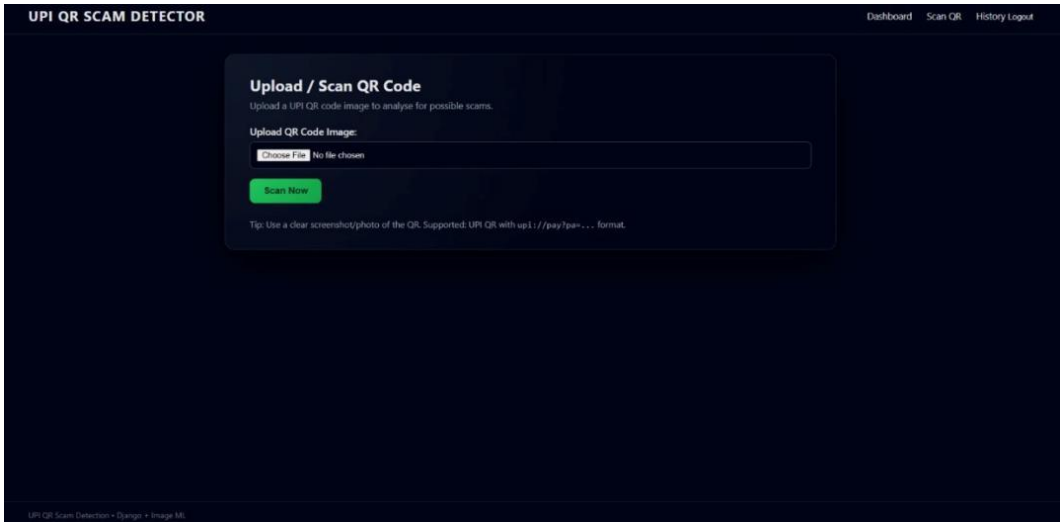
International Research Journal of Innovations in Engineering and Technology (IRJIET)

ISSN (online): 2581-3048

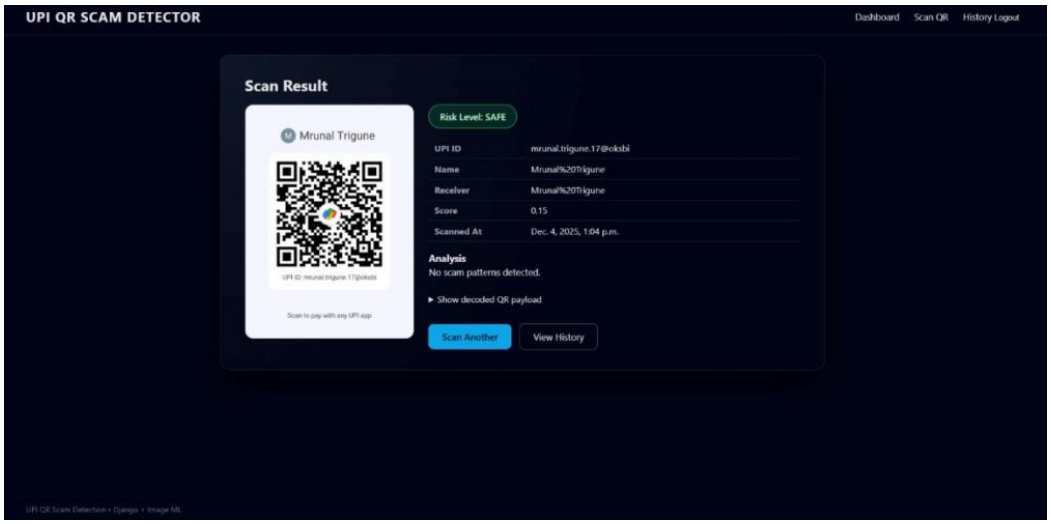
Volume 9, Issue 12, pp 99-104, December-2025

https://doi.org/10.47001/IRJIET/2025.912014

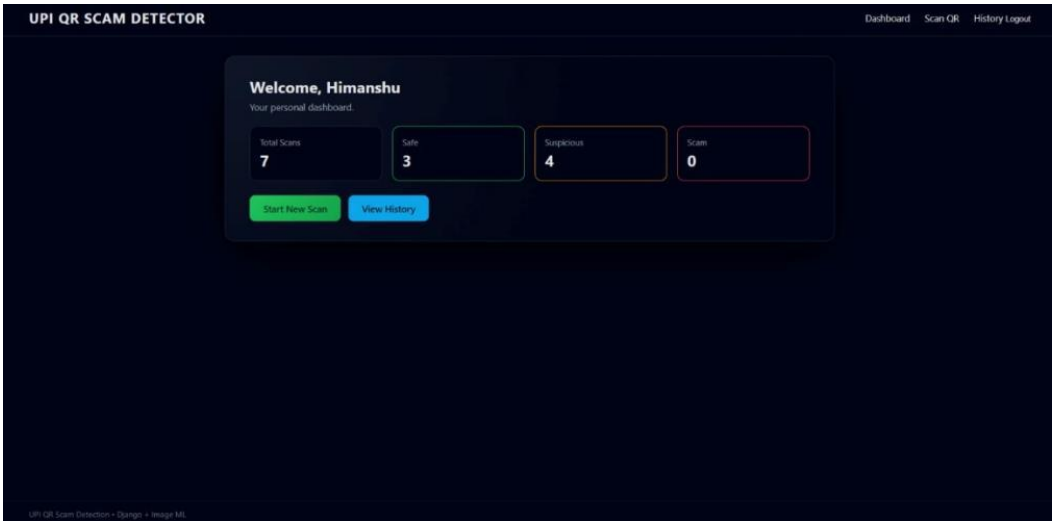
2) Upload QR Here



3) Show Scan QR Result



4) Show Report



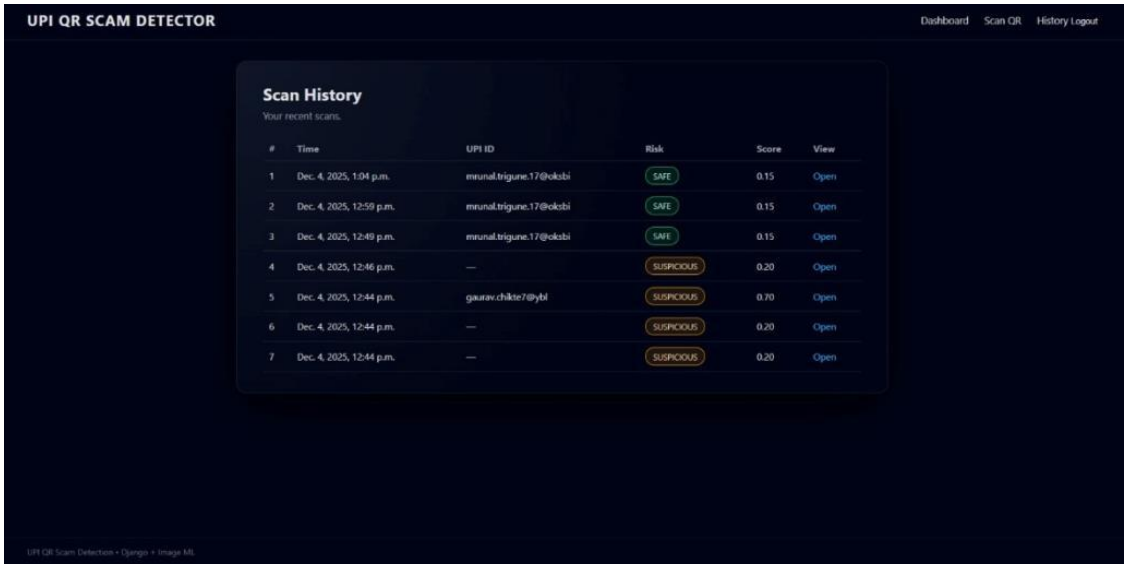
International Research Journal of Innovations in Engineering and Technology (IRJIET)

ISSN (online): 2581-3048

Volume 9, Issue 12, pp 99-104, December-2025

https://doi.org/10.47001/IRJIET/2025.912014

5) View History



VI. CONCLUSION

The rapid expansion of UPI-based digital payment systems has significantly improved convenience and financial inclusion; however, it has also introduced new security challenges, particularly in the form of QR code–based scams. Fraudsters increasingly exploit the trust and simplicity associated with QR payments by deploying cloned, manipulated, or malicious QR codes that redirect transactions to unauthorized accounts. Addressing this growing threat requires solutions that go beyond basic QR decoding and incorporate intelligent verification mechanisms.

The UPI Scam Detection for QR Codes system successfully demonstrates the application of machine learning and image processing techniques within a Django-based web framework to enhance the security of digital payment transactions. By combining image-based QR analysis with UPI metadata validation, the system effectively identifies fraudulent indicators such as QR tampering, distorted patterns, mismatched UPI handles, and cloned merchant codes. The integration of a trained machine learning classifier enables accurate differentiation between genuine and suspicious QR codes, providing users with a clear risk assessment before completing a transaction.

Experimental evaluation of the system shows high reliability, with strong detection accuracy and minimal response time, making it suitable for real-world deployment. The user-friendly web interface ensures accessibility for non-technical users, while the administrative module supports fraud monitoring, reporting, and continuous model improvement. This dual-layer approach—combining rule-based validation with machine learning—enhances robustness and minimizes false detection rates.

In conclusion, the proposed system contributes meaningfully to the domain of digital payment security by offering a scalable, intelligent, and practical solution to QR-based UPI scams. It not only increases user confidence in cashless transactions but also provides a foundation for future enhancements such as mobile application integration, real-time camera-based scanning, deep learning–driven forensic analysis, and integration with national fraud databases. The project highlights the effectiveness of leveraging modern web technologies and machine learning to safeguard financial ecosystems in an increasingly digital economy.

REFERENCES

[1] R. Sharma and P. Jain, “A Study on QR Code–Based Fraud in Digital Payment Systems,” *International Journal of Computer Science and Information Security*, vol. 19, no. 6, pp. 45–52, 2021.

[2] A.Patel, “Image Tampering Detection Using Machine Learning Techniques,” *IEEE Transactions on Information Forensics and Security*, vol. 15, no. 4, pp. 1123–1134, 2020.

[3] S. Kumar and V. Rao, “Security Analysis of QR Code Payments in Unified Payment Interface (UPI),” *International Journal of Cyber Security and Digital Forensics*, vol. 11, no. 2, pp. 78–86, 2022.

[4] J. Smith and L. Johnson, “Detection of Visual Manipulation in QR Codes Using Computer Vision,” *Journal of Digital Image Processing*, vol. 14, no. 3, pp. 201–210, 2020.

[5] S. Vincent, “Machine Learning Integration in Django-Based Web Applications,” *Proceedings of the International Conference on Applied Computation and Security*, pp. 78–84, 2021.

ISSN (online): 2581-3048
Volume 9, Issue 12, pp 99-104, December-2025
https://doi.org/10.47001/IRJIET/2025.912014

[6] National Payments Corporation of India (NPCI), "Unified Payments Interface (UPI) – Procedural Guidelines and Safety Measures," *NPCI White Paper, Mumbai, India*, 2023.

[7] M. Gupta and R. Verma, "QR Code Phishing Attacks: Threats and Countermeasures," *International Journal of Network Security*, vol. 24, no. 1, pp. 15–23, 2022.

[8] T. Nguyen and H. Lee, "Machine Learning-Based Fraud Detection in Digital Payment Systems," *IEEE Access*, vol. 9, pp. 134567–134579, 2021.

[9] OpenCV Documentation, "Computer Vision Techniques for Image Analysis and QR Code Processing," *OpenCV Foundation*, 2024. Available: https://opencv.org

[10] Django Software Foundation, "Django Documentation – Secure Web Application Development," *Version* 4.x, 2024. Available: https://www.djangoproject.com

[11] S. Chandrasekaran and M. Kumar, "Digital Payment Security in Emerging Economies," *Journal of Information Security and Applications*, vol. 64, pp. 102–110, 2022.

[12] A.Mehta and N. Shah, "Anomaly Detection in Digital Images Using Support Vector Machines," *International Journal of Advanced Research in Engineering and Technology*, vol. 10, no. 5, pp. 389–397, 2019.

Citation of this Article:

Himanshu Trigune, Sumit Pawar, Pranit Chavan, Sushant Tatpalle, Prof. Priya Borkar, & Prof. Nita Pawar. (2025). UPI Scam Detection for QR Codes. *International Research Journal of Innovations in Engineering and Technology - IRJIET*, 9(12), 99-104. Article DOI https://doi.org/10.47001/IRJIET/2025.912014

****

