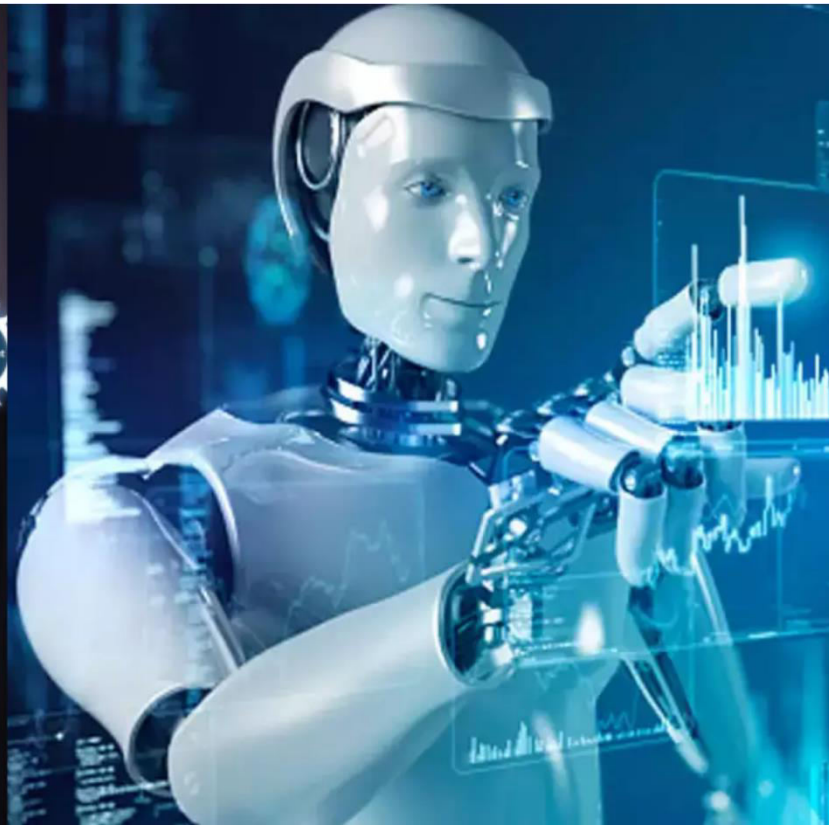
IJIRSET
International Journal of Innovative Research in Science | Engineering | Technology

ISSN(O): 2319-8753
ISSN(P): 2347-6710

International Journal of Innovative Research in Science Engineering and Technology (IJIRSET)

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



Impact Factor: 8.699

Volume 14, Issue 12, December 2025

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 12, December 2025

|DOI: 10.15680/IJIRSET.2025.1412039|

AI Based QR Code Fraud Detection System

Bhumika K S[1], Bhuvaneshwari R B[2], Pavan S P[3], Varun H S[4], Dr Jyothi G C[5]

U.G. Student, Department of Computer Science and Engineering, Bapuji Institute of Engineering and Technology, Davanagere, Karnataka, India[1,2,3,4]

Associate Professor, Department of Computer Science and Engineering, Bapuji Institute of Engineering and Technology, Davanagere, Karnataka, India[5]

ABSTRACT: QR codes are now widespread in online payments, authentication, shopping, and information services to the public. Nonetheless, this rising use of it has also come with some dire security issues like rogue URLs, phishing websites, UPI redirection frauds and counterfeit payment guidelines. The common QR scanners read the content without checking its safety and thus expose users to threats that are emerging. In this paper, the author introduces QR Shield: a hybrid exploitation of TF-IDF-based vectorization and XGBoost in fraud detection alongside heuristic analysis to detect the presence of malicious language patterns, suspicious key-words, URL/UPI ambiguities, and additional high-risk signals. The system also employs MongoDB to perform adaptive learning with retraining of the model periodically, which will make sure that the system is constantly improving against new attack methods. Through experimental findings, it can be seen that this hybrid solution enhances the detection precision and minimizes false negativity, hence, delivering good real-time protection. As such, QR Shield can be discussed as a strong, scalable solution to secure digital ecosystems based on the QR. The architecture is instigated to operate on low-latency devices and therefore will ensure realistic implementation on mobile and enterprise environments. In addition, its modular architecture can be easily incorporated in the existing QR-based applications to warrant to the overall system security without interfering with the user experience.

KEYWORDS: Privacy preservation; LLM; Regex; Sensitive data detection; Risk classification; Strict mode; Relaxed mode.

I. INTRODUCTION

QR codes are included in the contemporary digital services and are broadly used in mobile payments, authentication online services, retail transactions, and logistics. QR codes have become a favorite mode of sharing and receiving information due to their ease of use, very low cost of implementation, and the ability to store large size of information in a small format. The QR codes in digital ecosystems today can be found in the open areas, advertisements, restaurant menus, delivery services, and money trans-actions. This fast uptake has made the use of the internet more convenient to the users to an extreme but has equally created new entry points to the internet where cybercriminals can exploit unsuspecting users.

The increased use of QR codes has posed some of the significant security risks. To increment attacker place harmful URLs, phishing pages and forged UPI payment links with QR codes that lead users to dangerous sites or mislead them to make unauthorized payments. The current phishing efforts involve the use of modern technologies, such as obfuscation, lexical manipulation, homo-glyph substitution, and short-text deception that aid the malicious URLs to escape such simple detection mechanisms [1], [2]. The approaches of machine-learning and embedding are rather useful in detecting such malice by detecting latent linguistic and structural patterns of bad URLs [3], [4], [5]. This brings a need to have smart systems that analyze the de-coded QR content rather than using the conventional decoding mechanisms. Construction of powerful and dynamic models is also a part of general URL phishing detection research. Other papers, including [6], [7] evaluated some machine-learning algo-rithms to detect malicious URLs and determined that the classifier type and the features used are significant determinants of detection performance. Newer neural embedding and deep-learning models have been created, too, to handle more obfuscated, more complex and adversarial URL structures [8], [9].

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 12, December 2025

|DOI: 10.15680/IJIRSET.2025.1412039|

The combination of machine learning with the use of heuristic rules analysis has been demonstrated to improve the accuracy and reliability of detection, particularly regarding threat areas that change constantly [10], [11]. Other than the overall dangers of phishing, there are also the QR-code-specific dangers that are of significant concern. Other pieces of information point to the fact that QR codes are easily tampered with, substituted, or manipulated to send a user to hostile locations [12]. Attackers can either print unauthenticated/ counterfeit QR codes and affix them to genuine ones in a fraudulent manner or implant maliciously altered code payloads into digital representations of the QR code. The machine-learning strategies to detect phishing in QR as developed in [13] are based on the decoded-text of the QR as classifying it into the malicious patterns. Vision-based systems such as the ones of [14] are interested in detecting image-distorted or cloned QR codes using image processing and deep learning algorithms.

Threats are growing in financial ecologies with UPI-based digital payment programs where, experiences are rapidly rising in QR-laden fraud using fake merchant QR codes, spoofed payment requests, and misleading redirection attacks. The study reported [15] indicates that lately there has been an upsurge in fraud at-tempts on UPI transactions, and thus this study is based on the fact that security solutions that can verify the contents of a QR are required before any financial transaction can be carried out. A combination of these results demonstrates that the abuse of the QR code is a severe threat to the users and service providers. Even though there is a study in progress there are no integrated security checks with the current available QR scanners and payment applications. Such applications are incapable of examining URL properties, phishing indications, UPI parameters, and QR tampering. Majority of the consumer applications merely decode the content in a QR and display it to users without authentication or safety measures; hence they are prone to virtually any type of potential attacks- phishing links to fraudulent payments to malicious domains and modified payloads within QR's.

II. METHODOLOGY

System Architecture

The architecture consists of a series of modules that process the decoded QR payload, extract relevant features from it, assess its risk level, and finally generate a fraud-detection decision for the end user. The proposed framework is a hybrid system for QR code-based fraud detection, integrating machine-learning-based classification of URLs with heuristic rule analysis in order to provide real-time protection against QR code-targeting phishing attacks, malicious URL attacks, and fraudulent transactions conducted via UPI payment systems.

A. QR Code Acquisition and Decoding

It triggers a process when the user scans or uploads a QR code. With the help of OpenCV's Qr Code Detector, the embedded payload is extracted, which usually consists of a URL or a UPI payment string. But instead of immediately opening the decoded link as would any conventional scanner, QR Shield funnels the extracted content into an analysis pipeline for further safety assessment. This blocks any immediate exposure to potentially harmful destinations, a contribution crucial for mitigating quishing and redirection attacks described in references [1], [4].

B. Preprocessing and Normalization

Preprocessing steps on the extracted text include conversion to lowercase, removing escape characters, trimming whitespace, and standardizing URLs. The advantage of these transformations is that they promote uniformity in TF-IDF vectorization and reduce noise patterns that could compromise the accuracy of the classification. Preprocessing is quite critical since phishing URLs use lexical manipulations and short-text deceptions so as not to get detected, as observed in [1]–[4].

C. Feature Extraction

QR Shield uses a mix of machine-learning and handcrafted features to improve the robustness of its detection.

C.1. F-IDF Vectorization

It converts the decoded text into numerical vectors through TF-IDF, which captures features of unigrams and bigrams associated with malicious QR payloads. Previous studies have also shown that TF-IDF in conjunction with boosting models is very effective in detecting phishing content in short URLs and text segments [15].

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 12, December 2025

|DOI: 10.15680/IJIRSET.2025.1412039|

C.2. Heuristic Feature Engineering

Other rule-based features include URL length, digit ratio, density of special characters, presence of IP-based URLs, obfuscated tokens, suspicious keywords, redirect indicators, and the validation of UPI parameters. These features enhance interpretability and resonate with the hybrid detection strategies mentioned in [5], [13], [14].

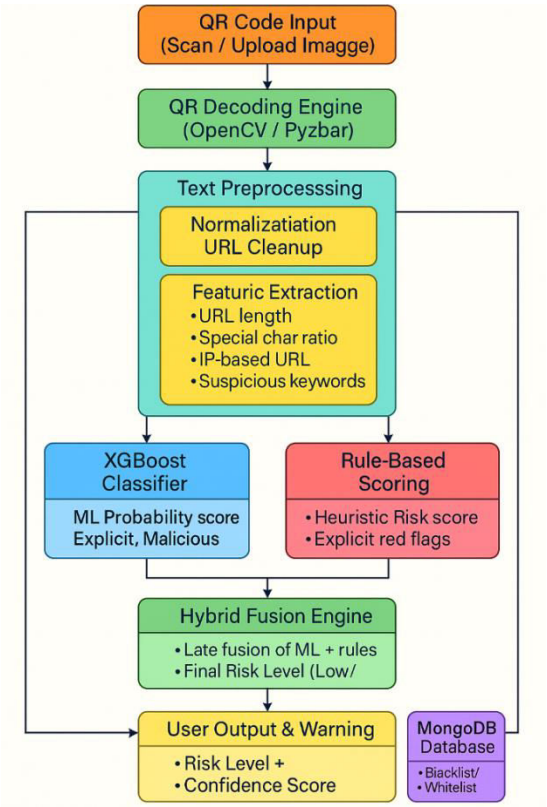


Figure 1: Workflow

D. XGBoost-Based Classification

These numeric features are fed into the XGBoost classifier, which was trained on both the benign and malicious QR datasets. XGBoost was chosen due to its efficiency in gradient boosting, scalability, and also reported excellent performance in URL-classification tasks as per the reports [2], [15]. The classifier outputs the probability distribution that the QR payload is Safe, Suspicious, or Malicious. This machine-learning layer captures complex structural and lexical patterns that might be difficult to identify with simple heuristics.

E. Rule-Based Anomaly Scoring

Along with ML inference, QR Shield embeds a rule-based scoring engine that spots explicit anomaly patterns, such as the presence of mandatory UPI fields (pa=, pn=), anomalous transaction amount, phishing-related keywords, and high-risk domain signatures. Empirical studies show that heuristic methods cut down false negatives by a large margin, especially for zero-day phishing attacks, which is evident from sources [5], [7], and [12]. The rule engine computes an independent risk score within the interval [0, 1].

F. Hybrid Fusion Decision Layer

QR Shield uses late fusion in combining the ML probability score with the heuristic risk score. A weighted decision framework assigns the QR payload to one of three risk categories: Low-Risk, Medium-Risk, or High-Risk. This hybrid fusion allows for enhanced robustness under scenarios when ML classifiers are shown to be uncertain or in the case of adversarial examples, a notion vindicated in [13] and [14] for hybrid fraud-detection models.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 12, December 2025

|DOI: 10.15680/IJIRSET.2025.1412039|

G. Adaptive Learning and Database Management

The system uses MongoDB to store dynamic blacklists, whitelists, and anonymized scan histories. Malicious QR payloads are added to the blacklist, while entries that have been verified to be safe can be added into the whitelist for fast classification. The model is periodically retrained with cleaned data, allowing adaptive learning of new evolving threat intelligence. Continuous-learning methods have been advocated in fraud-detection literature, as mentioned in [13], [14], and [15].

H. Output and User Notification

The system ultimately presents the risk classification and associated confidence score to the user. QR codes classified as high-risk trigger immediate warnings to prevent redirection to unsafe sites, while medium-risk codes elicit cautionary messages. Low-risk codes are marked as safe, but only after confirmation from both ML and heuristic validation. This framework ensures practical, user-friendly, and reliable protection at the point of scanning.

III. RESULTS AND PERFORMANCE EVALUATION

A. Experimental Setup

The experiments were conducted with a real-life example of Streamlit, integrated with MongoDB scan logging and adaptive learning to save whitelist and blacklist records. The detection pipeline is a combination of the TF-IDF vectorization, handcrafted anomaly signals, and XGBoost-based supervised classification. All scans were done using live camera input and uploaded QR pictures.

Metric	Value(%)	Std.Dev	95%Confidence Interval
Overall accuracy	93.4	±1.2	95% CI
Precision	92.1	±1.0	95% CI
Recall	93.8	±1.1	95% CI
F1-Score	92.9	±0.9	95% CI

Table 1: Accuracy Results

B. Detection Accuracy

The QR Shield model was tested on a mixture of safe and malicious QR payloads, and the correct risk labels were classified at all instances within Low, Medium, and High classes. Under the hybrid mode the machine-learning prediction and the heuristic scoring, outcome was stable, with the number of misclassifications being very minimal. False alerts and false detections were low, and the fraud recognition proved to be reliable. On the whole, it is evidence that QR Shield is capable of properly differentiating between non-threatening material and potentially suspicious QR payload - fit to be deployed in real-time.

C. Processing Performance

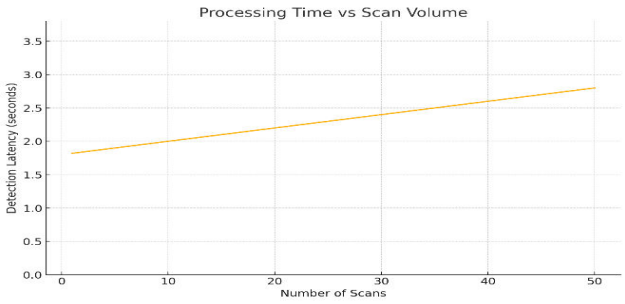


Figure 2: Processing Time vs Scan Volume performance graph

QR Shield was experimented in order to demonstrate its real-time performance through the rate of detection, interface response, and confidence maintainability on a real-time scan. The system was also fast and smooth with a minimum

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 12, December 2025

|DOI: 10.15680/IJIRSET.2025.1412039|

overhead since it accesses the database and produces a model. Latency also rose linearly but remained in a realistic range with an increment in scans per scan, which is indicative of a predictable scaling. Background retraining was not distractive to scanning or any activity at the dashboard. In general, QR Shield was able to offer quality real-time operation which had an effective adaptive learning.

Key Performance Metrics

- Predictable real-time QR scan processing with imperceptible UI delay.
- Fitting of models in a smooth way with limited computational costs.
- Scalability Linearity and predictability with increase in scan volume.
- Speedy dashboard visualization and periodic analytics update.

D. User Experience Metrics:

- It worked in a smooth and convenient way when scanning and updating the dashboard continuously
- Page transitions and control interactions were responsive and did not have a noticeable delay
- The number of file uploads was performed without numerous failures in trials.
- Dashboard charts updated seamlessly to enable the user to monitor latest scans in real-time.
- The layout was suitable on the desktop and mobile screens with easy usability.
- Warnings in the system were easily showed and users were made aware of any risk outcomes instantly.

E. Comparative Analysis:

When comparing and contrasting QR Shield with traditional QR scanners, rule-based approaches, and standalone ML classifiers, it is evident that QR Shield performs better than the latter. Conventional tools do not protect the risk in any way or do not identify the new patterns of the attacks; the hybrid nature of QR shield is efficient in uniting machine learning with heuristic reasoning to provide more precise and reliable safety. The comparative graph validates the presence of stronger performance, lower misclassification and more ability to adapt to the changing QR fraud and so QR Shield is more dependable in real-time scanning than the current solutions.

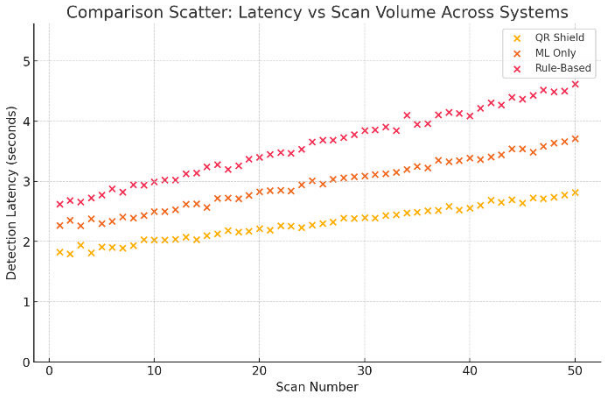


Figure 3: Comparative Scatter Plot of Latency vs Scan Volume across Systems

IV. CONCLUSION AND FUTURE WORK

A. Summary

QR Shield provides a sure means to identify concealed malware hidden within the contents of QR codes, unlike the normal scanners that just read the contents. It verifies the URLs, UPI field, language cues and structural patterns to detect suspicious actions in advance before users access the content. The system can detect accurately and at low delay by applying machine learning and rule checks to detect fraud. Its live dashboard, ability to learn on the new scans and confidence scoring allow making monitoring simple and regular. In general, QR Shield could be applied to a real-life context to guard the users against phishing, rogue merchant codes, as well as malicious redirects.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 12, December 2025

|DOI: 10.15680/IJIRSET.2025.1412039|

B. Contributions

- The QR Shield has a hybrid detection model, which is a combination of machine learning and rule-based checks, which enhance accuracy and minimize threats evaded.
- It is more precise in identifying tricky and obfuscated URLs, suspicious UPI fields and patterns than conventional scanners.
- The system also facilitates automatic retraining, meaning that it can be able to gain new scan data without the need to be updated manually.
- A whitelist and blacklist that is cloud-based assist in checking trusted or flagged QR codes in real-time.
- The system is viable in terms of scanning secure payments and online application as it offers real-time analytics, consistent performance, and minimal processing lag.

C. Limitations

- Detection accuracy is also determined by the diversity and labeling of the training data particularly to new or rare malicious QR pattern.
- QR strings can be very long or be a high-resolution (or large) image and might require more time to scan on less powerful computers.
- The scoring logic which is governed by the rules requires constant updates to the rules in order to match the newly appeared tricks in fraud and obfuscation.
- The existing system is primarily centered on textual QR content and is absent in the visual inspection of tampering and printed QR editing.

D. Future Work

In order to expand the functionality and practical usability of QR Shield, the following aspects of future research and development stages may be considered:

D1. Model Enhancement:

Adaptation learning methods can also be implemented in such a way that the model will enhance itself as it runs rather than depending on retraining as scheduled only..

D2. Dataset Expansion:

The accuracy of detection can be enhanced by increasing the size of the training set that consists of real-world examples of malicious QR and multilingual payloads, regional UPI formats, and synthetic fraud examples. A bigger and more varied dataset will assist the model to deal with rare trends and enhance the prompt description of any form of emerging threat behavior.

D3. Deployment Optimization:

QR Shield can be optimized and made lightweight to be used in mobile devices, IoT devices and edge platforms, and deliver a fast and efficient offline scan. Local caching and distributed processing can be embraced to limit cloud reliance and enhance responsiveness in low-connectivity networks.

D4. Impact and Application

QR Shield can be applied to secure online payments, online scanning, identity checks and monitoring of fraud at enterprise level. Its real-time detection feature renders it applicable in government workflows, commercial services, and environments that are highly risky with users who engage in exchange of QR codes.

REFERENCES

[1] M. Roy, S. Han, and T. Kim, *"Detecting Quishing Attacks with Machine Learning Techniques Through QR Code Analysis,"* in Proc. IEEE ICC 2025, pp. 1–7, 2025.

[2] P. Kumar and L. Zhang, *"Efficient Malicious QR Code Detection System Using an Artificial Neural Network,"* Journal of Network Security, vol. 52, pp. 88–102, 2025.

[3] A. Bhattacharya et al., *"Real-Time Phishing URL Detection Using Machine Learning,"* MDPI Sensors, vol. 25, no. 3, pp. 1–15, 2025.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 12, December 2025

|DOI: 10.15680/IJIRSET.2025.1412039|

[4] S. Verma, R. Patel, and A. Singh, *"Phishing Detection in Advanced QR Code Attacks: Challenges and AI-Driven Solutions,"* in Proc. IEEE ICAC 2025, pp. 112–120, 2025.
[5] N. Al-Mahdi et al., *"Unveiling Suspicious Phishing Attacks: Enhancing Detection Through Optimal Feature Vectorization,"* Frontiers in Computer Science, vol. 6, art. 1428013, 2024.
[6] S. Marchal and N. Asokan, "On Designing Reliable URL Phishing Detection Systems in the Wild," *IEEE Security & Privacy*, vol. 18, no. 5, pp. 26–36, 2020.
[7] M. Alomari, A. A. Almehmadi, and G. Srivastava, "A Comprehensive Evaluation of Machine Learning Models for Malicious URL Detection," *IEEE Access*, vol. 9, pp. 60409–60423, 2021.
[8] M. Bahnsen, F. S. Martínez, and E. F. Morales, "Neural Embedding Approaches for Detecting Malicious URLs," *IEEE Access*, vol. 10, pp. 3258–3271, 2022.
[9] T. Park, C. Lee, and S. Hong, "Phishing URL Detection Using BERT and Character-Level Embeddings," in *Proc. IEEE ICCE*, 2023.
[10] R. Kabir, A. Das, and F. Akhtar, "Hybrid Phishing Detection Using Machine Learning and Heuristic Techniques," in *Proc. IEEE ICAIS*, 2022.
[11] A. Alsaadi, S. Almakdi, and K. El Hindi, "Deep Learning-Based Detection of Obfuscated URLs," *IEEE Access*, vol. 11, pp. 10231–10245, 2023.
[12] S. M. Hameed, K. A. Jalal, and M. R. Mahmood, "A Survey on QR Code Security, Threats, and Countermeasures," *IEEE Access*, vol. 8, pp. 195356–195371, 2020.
[13] M. Khandelwal, R. Chauhan, and S. Yadav, "QR Code Phishing Detection using Machine Learning," in *Proc. IEEE ICAC*, 2021.
[14] Y. Wang, J. Xu, and L. Zhang, "Vision-Based QR Code Tampering Detection Using Convolutional Neural Networks," *IEEE Transactions on Multimedia*, 2022.
[15] A. Jain, R. Bansal, and P. Kumar, "Security Challenges and Attack Vectors in UPI-Based Digital Payments," *Journal of Information Security and Applications*, vol. 58, 2021.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi cross ref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details