

FRAUDEYE: Secure QR Scam Detection System

Sarthak Salunke, Sakshi Fuke, Sarika Rathi, Dr. Madhuri Kawarkhe

Graduate Student, School of Engineering and Technology(SOET)

Project Guide, School of Engineering and Technology(SOET)

MGM University, Chh. Sambhajinagar, Maharashtra, India

Abstract: QR codes are used extensively in the digital payment, web login, authentication, ticketing, and information sharing sectors. The convenience, however, has also made it an easier target for cybercriminals to run QR based phishing attacks, also referred to as quishing attacks. QR codes can lead to malicious websites, gather personal data, spread malware, or alter transactions. Proposed QR scam detection system FraudEye, analyzes the data in QR code before it lets the user go to the destination. The suggested framework involves QR decoding, URL analysis, checking the domain reputation, suspicious-pattern detection, and risk scoring. FraudEye is not just looking for a QR code, but also checking the destination as well as its security features. The system will categorize QR codes into Safe, Suspicious, Dangerous and give understandable warnings to the user. The proposed framework can provide an additional security layer for users of digital services, particularly in digital-payment environments.

Keywords: QR code, quishing, phishing, cybersecurity, fraud detection, QR security, rule-based and threat-intelligence analysis, digital payment.

I. INTRODUCTION

QR codes are a vital element in today's digital world. Users can use QR code for payments, opening websites, digital menus, downloading apps or getting digital information. QR-based payments also play a crucial role in contemporary digital-payment solutions, such as the UPI payment system in India, under the auspices of the National Payments Corporation of India [NPCI] (n.d.).[4][5]

Attackers can take advantage of this convenience too. A criminal can change a legitimate QR code to a malicious code, or send out a QR code via email, SMS, social media, posters and/or real-world locations. The website created may look like a trusted website and ask for a password, banking information, card details, or any other confidential information. Malicious QR codes may lead to fake websites or to content that is harmful (Federal Trade Commission (FTC), 2023).[3]

FraudEye aims to solve this issue by adding an extra security barrier between the QR scanning and user interaction. As opposed to the immediate opening of the decoded destination, the system assesses the destination and offers a risk-based warning.

II. RELATED WORK

Several studies have investigated QR-code security and phishing detection using URL analysis, machine learning, and threat-intelligence techniques. Traditional QR security approaches mainly rely on blacklists to identify previously reported malicious URLs. However, blacklist-based methods may not detect newly created phishing domains. Researchers have also proposed URL-based phishing detection using lexical, structural, and domain-related features. Some approaches analyze QR content and URL characteristics to identify suspicious destinations. Other systems use machine-learning and deep-learning techniques for automated phishing classification. Secure QR-scanning solutions have combined blacklists, URL analysis, host-based features, and content analysis to improve detection accuracy. Threat-intelligence services such as Google Safe Browsing and



VirusTotal can further support malicious URL identification. However, many existing solutions focus on only one or a few security indicators. FraudEye addresses this gap by combining QR decoding, URL/content extraction, SSL verification, domain analysis, redirect analysis, threat intelligence, suspicious-keyword detection, and weighted risk scoring to provide a unified trust assessment and user warning.

The conceptual model of FraudEye, as shown in Figure 1, involves seven major phases:

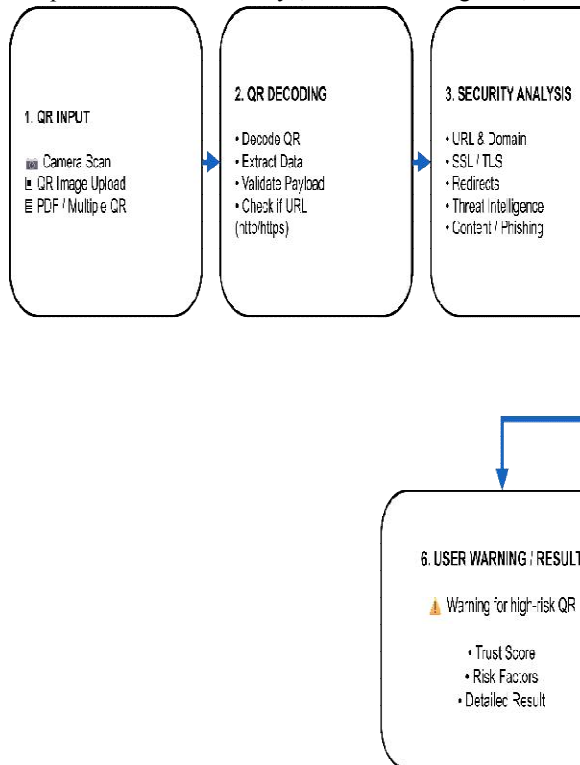


Figure 1: Model of FraudEye

III. REVIEW OF LITERATURE

Research on QR-code security and phishing detection has explored QR decoding, QR-based phishing attacks, malicious URL detection, and machine-learning approaches [1], [24]. Recent studies have investigated QR-based phishing, commonly known as quishing, and proposed machine-learning and deep-learning techniques for identifying malicious QR codes and phishing URLs [1], [10], [12], [15], [20]. Blockchain-based verification has also been investigated to improve the security, integrity, and trustworthiness of QR codes [2].

Several researchers have developed malicious URL detection methods using lexical features, machine-learning algorithms, convolutional neural networks, and other intelligent techniques [7], [8], [14], [17], [21], [22]. Systematic reviews have examined phishing URL and website detection techniques and identified challenges related to reliable and effective detection [9], [11], [13], [18], [19]. Research has also investigated QR-code and UPI-related phishing attacks and their detection using machine-learning techniques [6], [12].

Rafsanjani et al. proposed QsecR, a secure QR-code scanner based on a malicious URL detection framework that analyzes multiple URL-related security features [24]. The study demonstrates the importance of analyzing the URL embedded within a QR code rather than relying only on the visual characteristics of the QR code.

Recent research has further explored multimodal learning, deep-learning techniques, and incremental approaches for adapting phishing detection systems to evolving threats [1], [15], [23]. The Federal Trade Commission (FTC) has also



warned users about malicious QR codes and advised them to verify the destination before providing sensitive information [3].

Based on these studies, FraudEye integrates QR decoding, URL analysis, domain reputation, security checks, redirect detection, and risk scoring into a multi-layered QR scam detection system. The system combines multiple security parameters to generate a Trust Score and corresponding risk classification, helping users assess the security of QR-linked websites before accessing them.

3.1 Research Gap

Current QR security solutions typically concentrate on one element of the problem, such as URL blacklists, user awareness, image analysis or cryptographic verification. These techniques may be ineffective if attackers use new domains or new tactics.

The practical system should be a combination of several markers and give a simple answer to the common users. There's thus a requirement for a lightweight system that can decode QR codes, analyze their destination, check reputation, score risk, and notify users simultaneously in one workflow.

FraudEye addresses this gap through an integrated multi-layer architecture using rule-based security checks and threat-intelligence analysis.

3.2 Research Problem

The main issue that this research aims to tackle is the potential for user interaction with an imposter QR code, without the user being aware of the security status of the destination.

Most QR scanners process the QR code and activate the content, without checking whether the destination is reliable. This leaves a window of opportunity to create a security vulnerability between scanning the QR code and the destination you can interact with.

3.3 Research Objectives

The main objective of FraudEye is to develop a safe QR-code scanning and verification system that decodes QR content without automatically opening the destination. The system aims to detect suspicious URLs and domains using multiple security indicators and classify QR codes according to their risk level. It also provides clear warnings before users proceed to potentially unsafe destinations. Additionally, FraudEye focuses on protecting user privacy by minimizing unnecessary storage of user data.

IV. METHODS AND MATERIALS

4.1 Hypothesis

H1: A multi-layer QR analysis system using URL, domain, security, reputation, and threat-intelligence indicators can identify potentially malicious QR destinations more effectively than basic QR scanning.

H0: There is no significant difference between the identification performance of a multi-layer QR analysis system and basic QR scanning.

4.2 Research Methodology

The research is based on design and development approach. FraudEye is a web-based security solution suggested to analyze QR codes prior to opening their destination.

4.3 Data Collection

The proposed dataset may include both legitimate and malicious QR codes found in publicly available databases of known QR codes, legitimate sites, controlled testing environments, and phishing reports. There should be no personal information included.



4.4 QR Decoding

This is the first piece that is able to detect and decode the QR image. The untrusted information is not automatically opened and is treated as untrusted input.

4.5 Feature Extraction

Feature extraction identifies important security characteristics from the QR-linked URL and website. extracts features such as HTTPS status, SSL/TLS validity, domain age, and blacklist status. It also checks for malware, phishing indicators, suspicious redirects, and webpage content. These features provide the necessary information for security analysis. The extracted features are passed to the Risk Scoring Engine for evaluation. Finally, they are used to generate the Trust Score and risk classification.

4.6 Detection

A rule based system can detect obvious threats. Threat-intelligence analysis is used to evaluate multiple security indicators and contribute to the overall risk score.

V. EVALUATION, RESULTS AND DISCUSSION

5.1 Evaluation Criteria

Accuracy, precision, recall, F1-score, false-positive rate (FPR), and false-negative rate (FNR) can be used to measure the performance of the system. Where machine-learning models are used, separate training and testing datasets should be used to reduce the risk of overfitting.

TABLE 5.1 DETAILED ANALYSIS

Feature	Summary
Core Concept	"Scan first, trust later" (prevents websites from opening automatically).
Valid QR	Contains known payment IDs or trusted websites.
Suspicious QR	Uses new domains, long links, multiple redirects, or fake brand names.
Risk Engine	Weighs security indicators to assign safety scores.
Safe	No major suspicious signals (note: zero-day threats may still exist).
Suspicious	Some risk indicators detected.
Dangerous	High levels of phishing or fraud detected.
User Education	Shows context-aware warnings based on NPCI guidelines before sensitive actions.
Privacy	Minimizes personal data transmission and avoids saving full scan histories.

5.2 Secure QR/Website Scan Report

Figure 1.3 presents the security scan report generated by the proposed FraudEye system for a QR-code-derived URL. The report evaluates multiple security parameters, including transport security, SSL/TLS certificate validity, domain age, blacklist status, malware detection, phishing indicators, suspicious redirects, and webpage content. In the presented test case, the URL received a Trust Score of 39/100 and was classified as Dangerous with a HighRisk Level, advising users not to visit the website. Although the domain is 21 years old, uses HTTPS, and has a valid SSL/TLS certificate, the URL failed several security checks because it was identified as blacklisted, associated with malware, and containing malware test content. No suspicious redirects or phishing indicators were detected in this case. These findings demonstrate that FraudEye combines multiple security parameters rather than relying on a single indicator to determine the final risk classification. This multi-layered URL analysis approach supports the detection of potentially malicious QR-linked destinations.



Scan Report

Detailed security report for your scan



Figure 1.2: Secure QR/Website Scan Report

5.3 Malicious QR/Website Scan Report

Figure 1.3 presents the security scan report generated by the proposed FraudEye system for a QR-code-derived URL. The report evaluates multiple security parameters, including transport security, SSL/TLS certificate validity, domain age, blacklist status, malware detection, phishing indicators, suspicious redirects, and webpage content. In the presented test case, the URL received a Trust Score of 39/100 and was classified as Dangerous with a High Risk Level, advising users not to visit the website. Although the domain is 21 years old, uses HTTPS, and has a valid SSL/TLS certificate, the URL failed several security checks because it was identified as blacklisted, associated with malware, and containing malware test content. No suspicious redirects or phishing indicators were detected in this case. These findings demonstrate that FraudEye combines multiple security parameters rather than relying on a single indicator to determine the final risk classification. This multi-layer URL analysis approach is consistent with recent research on QR-based phishing and malicious URL detection.



Scan Report

Detailed security report for your scan



Figure 1.3: Illustrative Malicious QR/Website Scan Report (Prototype Test)

VI. FUTURE SCOPE

The future development of FraudEye can focus on real-time QR verification using updated domain reputation and security databases, along with a multi-layered detection approach that combines URL, domain, redirect, and content analysis. The system can also provide clear risk warnings and require user confirmation before opening high-risk QR destinations. Furthermore, secure payment guidance can help users identify suspicious QR-based payment requests. Future improvements should also emphasize enhanced privacy and security by minimizing the storage of user information while maintaining effective QR-code protection.

VII. CONCLUSION

QR technology offers a great convenience in digital payments, communication, authentication and information sharing. QR codes, however, are also a possible tool for phishing and financial fraud because of their capacity to conceal destinations.

FraudEye proposes a multi-layer security system, which checks QR destinations before users engage with them. The proposed framework involves QR decoding, URL analysis, DNS reputation, rule-based detection, risk scoring, and user warnings.

The system is designed to be used as an extra security layer and not as a substitute for the current cybersecurity system. Moving forward, the focus could be on real-time threat intelligence, enhancing secure payment verification, and privacy-preserving analysis. Through an appropriate testing and regular updates, FraudEye could offer a practical guideline for minimizing the threats of a malicious QR code.



REFERENCES

- [1]. Association for Computing Machinery. (2026). Incremental phishing defense method based on QR code decoding and multimodal deep learning. Proceedings of the 2026 5th International Conference on Cryptography, Network Security and Communication Technology, 209–214. <https://doi.org/10.1145/3802927.3802959>
- [2]. B-PhishQR—A blockchain-based framework for secure QR code verification against phishing attacks. (2026). Telematics and Informatics Reports, 21, 100289. <https://doi.org/10.1016/j.teler.2025.100289>
- [3]. Federal Trade Commission. (2023). Scammers hide harmful links in QR codes to steal your information. Consumer Advice.
- [4]. National Payments Corporation of India. (n.d.). BHIM UPI. NPCI.
- [5]. National Payments Corporation of India. (n.d.). Fraud awareness. NPCI.
- [6]. Yuniati, S. E., Widjajarto, A., & Hediyanto, U. Y. K. S. (2026). Implementation and analysis of QR code phishing attacks on Indonesian internet banking using attack tree and time-based metrics. Jurnal Teknik Informatika, 7(1). <https://doi.org/10.52436/1.jutif.2026.7.1.4819>
- [7]. Abad, S., Gholamy, H., & Aslani, M. (2023). Classification of malicious URLs using machine learning. Sensors, 23(18), 7760. <https://doi.org/10.3390/s23187760>
- [8]. Ahammad, S. K. H., Kale, S. D., Upadhye, G. D., Pande, S. D., Babu, E. V., Dhumane, A. V., & Jang Bahadur, D. K. (2022). Phishing URL detection using machine learning methods. Advances in Engineering Software, 173, 103288. <https://doi.org/10.1016/j.advengsoft.2022.103288>
- [9]. Aljabri, M., Altamimi, H. S., Albelali, S. A., Al-Harbi, M., Alhuraib, H. T., Alotaibi, N. K., Alahmadi, A. A., AlHaidari, F., Mohammad, R. M. A., & Salah, K. (2022). Detecting malicious URLs using machine learning techniques: Review and research directions. IEEE Access, 10, 121395–121417. <https://doi.org/10.1109/ACCESS.2022.3222307>
- [10]. Alsulami, A. A., Abu Al-Haija, Q., Alturki, B., Yafoz, A., Alqahtani, A., Alsini, R., & Binyamin, S. S. (2025). Efficient malicious QR code detection system using an advanced deep learning approach. Computer Modeling in Engineering & Sciences, 145(1), 1117–1140. <https://doi.org/10.32604/cmescs.2025.070745>
- [11]. Asiri, S., Xiao, Y., Alzahrani, S., Li, S., & Li, T. (2023). A survey of intelligent detection designs of HTML URL phishing attacks. IEEE Access, 11, 6421–6443. <https://doi.org/10.1109/ACCESS.2023.3237798>
- [12]. Charan, G. R., & Thilak, K. D. (2023). Detection of phishing link and QR code of UPI transaction using machine learning. In 2023 3rd International Conference on Innovative Mechanisms for Industry Applications (ICIMIA). IEEE. <https://doi.org/10.1109/ICIMIA60377.2023.10426613>
- [13]. El Aassal, A., Baki, S., Das, A., & Verma, R. M. (2020). An in-depth benchmarking and evaluation of phishing detection research for security needs. IEEE Access, 8, 22170–22192. <https://doi.org/10.1109/ACCESS.2020.2969780>
- [14]. Gupta, B. B., Yadav, K., Razzak, I., Psannis, K., Castiglione, A., & Chang, X. (2021). A novel approach for phishing URLs detection using lexical based machine learning in a real-time environment. Computer Communications, 175, 47–57. <https://doi.org/10.1016/j.comcom.2021.04.023>
- [15]. Kritikaa. (2026). A systematic literature review on deep learning approaches for QR code-based phishing (quishing) detection: Emerging attack vectors, multimodal feature fusion and open research challenges. Journal of Cyber Security Technology, 10(1). <https://doi.org/10.1080/23742917.2026.2696261>
- [16]. Mahajan, S. (2023). Phishing uniform resource locator detection using machine learning: A step towards secure system. Security and Privacy, e311. <https://doi.org/10.1002/spy2.311>
- [17]. Raja, S. A., Vinodini, R., & Kavitha, A. (2021). Lexical features based malicious URL detection using machine learning techniques. Materials Today: Proceedings, 47(1), 163–166. <https://doi.org/10.1016/j.matpr.2021.04.041>
- [18]. Safi, A., & Singh, S. (2023). A systematic literature review on phishing website detection techniques. Journal of King Saud University - Computer and Information Sciences, 35(2), 590–611. <https://doi.org/10.1016/j.jksuci.2023.01.004>



- [19]. Sánchez-Paniagua, M., Fidalgo, E., Alegre, E., Al-Nabki, W., & González-Castro, V. (2022). Phishing URLdetection: A real-case scenario through login URLs. IEEE Access, 10, 42949–42960. <https://doi.org/10.1109/ACCESS.2022.3168681>
- [20]. Trad, F., & Chehab, A. (2025). Detecting quishing attacks with machine learning techniques through QR code analysis. arXiv. <https://arxiv.org/abs/2505.03451>
- [21]. Wei, W., Ke, Q., Nowak, J., Korytkowski, M., Scherer, R., & Woźniak, M. (2020). Accurate and fast URL phishing detector: A convolutional neural network approach. Computer Networks, 178, 107275. <https://doi.org/10.1016/j.comnet.2020.107275>
- [22]. Xiao, X., Zhang, D., Hu, G., Jiang, Y., & Xia, S. (2020). CNN–MHSA: A convolutional neural network and multi-head self-attention combined approach for detecting phishing websites. Neural Networks, 125, 303–312. <https://doi.org/10.1016/j.neunet.2020.02.013>
- [23] E. Daoud, J. Garcia-Blas, S. Alawadi, and J. Carretero, “Phishing in the age of distributed intelligence: taxonomies, detection strategies, and the emerging role of federated learning,” Progress in Artificial Intelligence, 2026, doi: 10.1007/s13748-026-00448-6.
- [24] A. S. Rafsanjani, N. B. Kamaruddin, H. M. Rusli, and M. Dabbagh, “QsecR: Secure QR Code Scanner According to a Novel Malicious URL Detection Framework,” IEEE Access, vol. 11, 2023, pp. 92523–92540, doi: 10.1109/ACCESS.2023.3291811.

