Journal of Information Systems Engineering and Management
2025, 10(33s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Performance Analysis of QR Phishing Detection Approaches

Nidhi Nigam[1*], Rajat Bhandari[2]
[1] *Research Scholar, Department of Computer Science and Engineering, SAGE University Indore, India*
[2] *Professor, Institute of Advance Computing, SAGE University, Indore, India*
*Corresponding Author : *nigam.nidhi07@gmail.com*

ARTICLE INFO

Received: 31 Dec 2024

Revised: 20 Feb 2025

Accepted: 28 Feb 2025

ABSTRACT

Modern digital interaction is made complete with QR codes, which facilitate quick and easy entry to a variety of services and information. Their adoption in finance, marketing, logistics, and healthcare attests to their versatility as well as the risks they pose in the current digital environment. Among these threats, one of the most significant is QR phishing, wherein malicious users avail themselves of both the natural trust and the apparent ease of usage of QR codes to lure victims into giving up sensitive information, visiting counterfeit websites, or downloading malware. This research will investigate vulnerabilities in QR code systems, explore techniques used in carrying out QR phishing, and analyze actual case scenarios to show the effect of such threats. Besides, it presents sophisticated mitigations with the performance analysis, including cryptographic analysis, blockchain-based authentication, and machine learning-based detection systems with the performance analysis to improve the security of QR code applications to maintain the user trust.

Keywords: QR phishing, Vulnerabilities, Blockchain-based authentication, Cryptographic analysis, Machine Learning-based detection systems.

INTRODUCTION

QR codes have changed the way people access digital services, providing a very simple way to encode and retrieve information instantaneously without scanning. It has been reported that global QR code usage increased by over 35% between 2021 and 2024 owing to mobile payment systems and contactless solutions [1]. Industries such as finance, marketing, logistics, and healthcare are increasingly relying on QR codes, made use of greatly at the same time for the effectiveness and survival of an industry. Because digital payment systems, marketing campaigns, and authentication mechanisms have widely adopted QR codes, it makes them an attractive target for attackers. This simplistic design, however, brings danger and keeps on posing security threats, particularly in QR phishing [2] attacks. Cyberspies create links that distribute QR codes containing malicious payloads to trick users, steal information, deploy malware, or access funds from financial accounts. Since QR code content is hidden and not revealed until the code is scanned, users may unwittingly be interacting with the links containing the malware. Most attackers resort to QR code spoofing by placing fake codes beside the real ones in public places, luring users onto fake sites. Furthermore, if QR codes are hacked, those containing log-in credentials may suffer serious breaches of data and privacy infringement. One kind of attack is a malicious URL redirection whereby the QR codes redirect users to phishing websites aimed at obtaining sensitive data.

DETECTION TECHNIQUES IN QR PHISHING

Using technical and human solutions together strengthens QR code security. Casayuran [3] stresses the importance that human behavior plays in QR phishing and encourages security solutions to promote user awareness. Arntz [4] discusses how QR code phishing has skyrocketed, with Microsoft credentials being the prime target, thus calling for urgent action and improved detection efforts. Security training and awareness help reduce QR code phishing incidents; for this purpose, unverified QR codes must be validated before being scanned. Awareness campaigns and regular security training help users develop the ability to detect phishing attempts and reduce risks.

Journal of Information Systems Engineering and Management
2025, 10(33s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

CRYPTOGRAPHIC-BASED APPROACH

Hardened QR code systems are storage systems that can apply digital signatures algorithms and hashing to its contents [5]. This system generates a read-write public key-private key useable to verify QR codes or warn users if fails to verify. Barcode security scanner for authentication, data integrity, access control, and confidentialities further integrates symmetric and asymmetric methods of cryptography [6]. Cryptographic techniques in QR code readers encrypt, sign, and control access, ensuring confidentiality, privacy, and security. Digital signatures provide authentication, integrity, and non-repudiation [7]. However, few applications support cryptographic QR code generation and scanning [8,12]. A Secure QR Code Solution (QRCS) employs hash functions and digital signatures to verify QR authenticity. If verification fails, it blocks malicious QR codes. Similarly, the Anti-Malware Phishing (AMP) QR Code scanner, proposed by Niranjan Hegde et al. [9], enhances security by detecting and preventing QR code-based threats.

MACHINE LEARNING BASED APPROACH

This research explores CNN integration for QR Code detection in email images to combat phishing attacks through advanced image recognition, enhancing security. A lightweight deep learning model classifies QR Codes into normal, phishing, and malware types, ensuring deployment on resource-constrained devices [10,11]. Niu et al. [13] discuss security risks of QR codes in IoT, emphasizing CNN-based autonomous detection in email security systems. Dedenok [14] highlights the prevalence of QR codes in phishing emails and the challenge they pose to conventional email security. This study builds on their dataset of attack patterns, training a CNN model for QR code detection in email images. Tekale [15] provides insights into QR code technologies, including security features, error correction, and misuse, refining machine learning models for detecting malicious QR codes. Atawneh and Aljehani [16] propose a phishing detection model using deep learning, contributing to email security research. Their focus on text-based phishing differs from this study's emphasis on image-based phishing, particularly QR codes, addressing a significant research gap. Wang et al. [17] extend CNN applications for QR Code threat detection, using pixel-based feature extraction to distinguish malicious from benign QR Codes. Zhang et al. [18] stress the need to enhance deep learning generalizability, aiding further CNN model tuning to adapt to diverse QR Code representations and email content. This research advances CNN-based QR Code detection, improving email security and addressing gaps in phishing detection methodologies.

URL BASED APPROACH

Malicious URLs embedded in QR codes pose significant security risks. The literature suggests AI techniques and black-and-whitelist approaches to detect such threats [6]. The blacklist method matches URLs against phishing databases, including Google Safe Browsing [20] and PhishTank [21], providing proactive warnings to users before accessing suspicious links. This enhances security awareness, allowing informed decisions when scanning QR codes. Ohigashi et al. [22] proposed detection techniques for spurious QR codes, leveraging error-correcting processes. Their integrated approach, combining multiple detection techniques, proved more effective than single-method solutions, strengthening QR code security against phishing attacks.

HYBRID APPROACH

Studies highlight AI's efficiency in detecting harmful URLs within QR codes. Machine learning methods ensure generalizability and robustness against real-world attacks. This research introduces BarAI, an AI-based secure barcode scanner. Among five AI classifiers, the Decision Tree (DT) classifier performed best, achieving 90.24% accuracy. Shantanu et al. [19] evaluated seven machine learning classifiers for detecting malicious URLs, finding Random Forest (RF) the most effective, with 92.65% accuracy. Another study deployed a secure QR code reader using four classifiers, with the bidirectional Long Short-Term Memory (LSTM) classifier achieving 83.79% accuracy [24]. Rafsanjani et al. [25] developed QsecR, an Android app for secure QR scanning, which identified malicious URLs with 93.50% accuracy by evaluating feature values. Despite advancements in QR code security, further improvements are needed to counter growing threats. To address this gap, QR Shield is proposed as a two-model machine learning system designed to detect and block malicious URLs hidden in QR codes, enhancing user protection [23]. QR code security relies on multiple techniques, each with strengths and limitations as shown in Figure 1. Cryptographic solutions ensure authenticity but are computationally expensive. Machine learning

Journal of Information Systems Engineering and Management
2025, 10(33s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

enhances phishing detection but requires large datasets. URL-based detection offers quick filtering through blacklists but struggles with false positives and emerging threats. A hybrid approach combining these techniques strengthens overall security, increasing defense against evolving QR code threats.

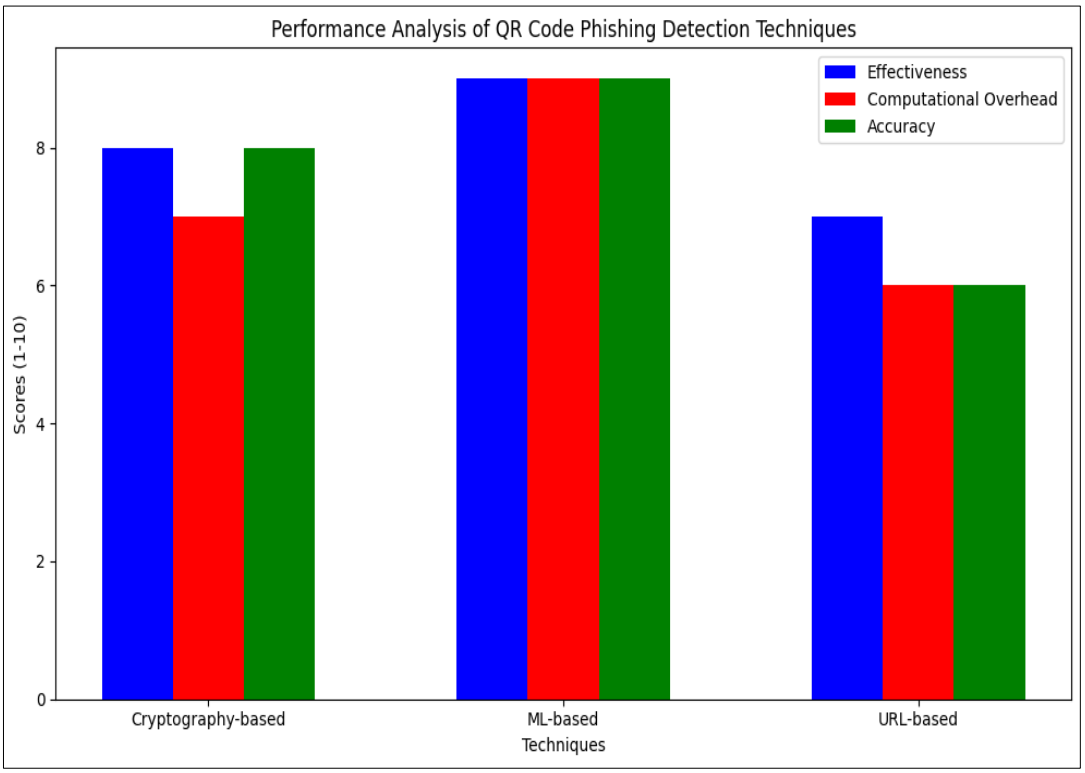

Figure 1. Performance Comparison of QR Phishing Detection

Below Table 1 shows Comparative Analysis of Detection Approaches.

Table 1: Comparative Analysis of QR Phishing Detection Techniques

Technique	Security Mechanism	Key Features	Limitations
Cryptography-Based	Encryption, Digital Signatures, Public/Private Key Infrastructure	Ensures authenticity and integrity of QR codes, Protects against tampering	- High computational overhead, - Dependent on proper implementation
Machine Learning-Based	Supervised/Unsupervised Learning, Deep Learning, Support Vector Machines	- High accuracy in phishing detection, Can adapt to new phishing patterns, Real-time detection	- Requires large, labeled datasets for training, Resource-intensive, especially for advanced models (e.g., CNNs)
URL-Based Detection	URL Blacklisting, Domain Analysis, URL Pattern Matching	- Fast and lightweight detection, Easy to implement,Scalable	- Higher false positives/ negatives, Depends on the availability and accuracy of URL blacklists, May miss new phishing domains

DATASET STUDY FOR QR CODE PHISHING ATTACK DETECTION

QR code phishing attacks are a growing threat in which attackers insert malicious URLs into QR codes to trick users into accessing fake websites. Detection and prevention of such attacks are paramount, and an extensive study of datasets is required to evaluate the performance of different detection techniques. This section discusses an

analysis of datasets employed for QR code phishing detection, features taken into account, and outcomes derived from various methods. Several datasets assist research in QR code phishing detection. Benign and Malicious QR Codes dataset (200,000 QR codes) assists detection algorithmic models, while Multi-version Benign & Malicious QR Codes dataset supports version-specific based analysis. QRphish Dataset and QR Code URL Phishing Dataset target the detection of phishing via URL based analysis. The Phishing Website Detection dataset learns ML models on malicious URL classification. Mobile QR Code Dataset and Dynamic QR Code Authentication Dataset serve mobile and dynamic QR code security, increasing cryptographic and ML-based approaches.

RESEARCH CHALLENGES AND FUTURE DIRECTIONS

QR codes are highly vulnerable to security threats, particularly phishing attacks. Mitigating these threats requires addressing key challenges. Ensuring high detection rates with minimal false positives and negatives is crucial for reliable machine learning (ML) models [27]. Real-time detection requires lightweight ML models and efficient cryptographic algorithms. Scalability is another concern, especially in healthcare and finance, that process vast amounts of QR code data without compromising performance [28]. Strong detection mechanisms are also required in the face of sophisticated phishing model attacks and adversaries [26].

Future research must therefore improve ML-based detection algorithms while simultaneously improving their accuracy by producing fewer false positives and negatives. Another consideration would be to enhance defenses against adversarial attacks and QR code manipulation in order to fight against ongoing phishing exploitation. Lastly, the integration of user education alongside advanced detection systems is crucial, as user awareness is a key factor in the efficiency of preventing phishing attacks.

CONCLUSION

QR phishing is a legitimate cybersecurity threat, which is executed by abuse of malicious QR codes in stealing sensitive data. This paper analyzes the advances in QR phishing detection in the past four years and methodically classifies the detection schemes and analyzes the datasets used for the evaluations. Major challenges include real-time detection, scalability, and user education. The review suggests a strong need for robust and adaptive solutions that integrate hybrid technologies. Future research should focus on user-centric, scalable methods for further enhancement of these security controls. Reinforcing the detection system and increasing user awareness would thus be crucial for countering the ensuing QR phishing attacks, ensuring the success of preventing emerging threats from digital environments.

REFRENCES

[1] J. Smith, "Blockchain and QR codes: Enhancing security," Blockchain Review, vol. 2, no. 1, pp. 15–22, 2023.
[2] S. Kumar and A. Agarwal, "Machine learning-based detection of malicious QR codes," International Journal of Cybersecurity Research, vol. 4, no. 2, pp. 89–104, 2022.
[3] Casayuran, M. (2023, October 5). Think Before You Scan: The Rise of QR Codes in Phishing. Spider labs Blog. https://www.trustwave.com/en-us/resources/blogs/spiderlabs blog/think-before
[4] Arntz, P. (2023, August 20). QR codes used to phish Microsoft credentials. Malwarebytes. https://www.malwarebytes.com/blog/news/2023/08/qr-codes deployed-in-targeted-phishing-campaigns
[5] R. M. Bani-Hani, Y. A. Wahsheh, and M. B. Al-Sarhan, “Secure qr code system,” in 2014 10th International Conference on Innovations in Information Technology (IIT), 2014, pp. 1–6.
[6] H. A. Wahsheh and F. L. Luccio, “Security and privacy of qr code applications: a comprehensive study, general guidelines and solutions,” Information, vol. 11, no. 4, p. 217, 2020.
[7] K. S. C. Yong, K. L. Chiew, and C. L. Tan, “A survey of the QR code phishing: The current attacks and countermeasures,” in Proc. 7th Int. Conf. Smart Comput. Commun. (ICSCC), Jun. 2019, pp. 1–5.
[8] V. Mavroeidis and M. Nicho, “Quick response code secure: a cryptographically secure anti-phishing tool for qr code attacks,” in Computer Network Security: 7th International Conference on Mathematical Methods, Models, and Architectures for Computer Network Security, MMM-ACNS 2017, Warsaw, Poland, August 28 30, 2017, Proceedings 7. Springer, 2017, pp. 313–324.

[9] P. Hemavathi, N. Hegde, R. Bharti, R. Sur, and S. Priyanka, “Anti malware phishing qr scanner,” International Journal of Innovative Science and Research Technology, vol. 3, no. 5, 2018.

[10] Alam et al., "Feasibility of Machine Learning-Enhanced Detection for QR Code Images in Email-based Threats," ResearchGate, 2023. Available: https://www.researchgate.net/publication/383909912.

[11] N. Gupta et al., "Detection of QR Code-based Cyberattacks using a Lightweight Deep Learning Model," ETASR Journal, 2022. Available: https://www.etasr.com.

[12] R. K. Sharma et al., “Secure QR Code Scanner to Detect Malicious URLs Using Machine Learning,” IEEE Transactions on Information Forensics and Security, vol. 19, no. 3, pp. 567–580, 2023. [Online]. Available: https://ieeexplore.ieee.org.

[13] Niu, X., Zhao, J., & Tian, B. (2024). View of the security threat and precautionary measures of QR code of internet of things technology. Advances in Engineering Technology Research, 11, 2790–1688. https://doi.org/10.56028/aetr.11.1.775.2024

[14] Dedenok, R. (2023, September 27). QR codes in email phishing. Secure list by Kaspersky. https://securelist.com/qr-codes-in phishing/110676/

[15] H. A. Tekale, "A Comprehensive Study on QR Codes", International Journal of Advanced Research in Science Communication and Technology (IJARSCT), vol. 4, 2024, [online] Available: https://doi.org/10.48175/IJARSCT-18935.

[16] Atawneh, S., & Aljehani, H. (2023). Phishing Email Detection Model Using Deep Learning. Electronics 2023, 12(20), 4261. https://doi.org/10.3390/electronics12204261

[17] Wang, J., Zeng, X., Duan, S., Zhou, Q., & Peng, H. (2022). Image target recognition based on improved convolutional neural network. Mathematical Problems in Engineering, 2022, 1–11. https://doi.org/10.1155/2022/2213295

[18] Zhang, C., Bengio, S., Hardt, M., Recht, B., & Vinyals, O. (2021). Understanding deep learning (still) requires rethinking generalization. Communications of the ACM, 64(3), 107–115. https://doi.org/10.1145/3446776

[19] Shantanu; Janet, B.; Joshua Arul Kumar, R. Malicious URL Detection; A Comparative Study. In Proceedings of the 2021 International Conference on Artificial Intelligence and Smart Systems (ICAIS), Coimbatore, India, 25–27 March 2021; pp. 1147–1151 .

[20] “Safe Browsing–Google Safe Browsing.” [Online]. Available: https://safebrowsing.google.com/

[21] “PhishTank | Join the fight against phishing.” [Online].Available: https://www.phishtank.com

[22] S. Egelman, L. F. Cranor, and J. Hong, “You’ve been warned: an empirical study of the effectiveness of web browser phishing warnings,” in Proceedings of the SIGCHI conference on human factors in computing systems, 2008, pp. 1065–1074.

[23] J. Yuan, Y. Liu, and L.Yu, “A novel approach for malicious url detection based on the joint model,”Security and Communication Networks,vol.2021 ,pp.1–12,2021.

[24] Almousa, H., Almarzoqi, A., Alassaf, A., Alrasheed, G., & A Alsuhibany, S. (2024). QR Shield: A Dual Machine Learning Approach Towards Securing QR Codes. International Journal of Computing and Digital Systems, 16(1), 887-898.

[25] A. Pawar, C. Fatnani, R. Sonavane, R.Waghmare, and S. Saoji, “Secure qr code scanner to detect malicious url using machine learning,” in20222ndAsianConferenceon Innovation in Technology (ASIANCON). IEEE,2022,pp. 1–8.

[26] K.A.Latif, B.Sugiantoro, and Y.Prayudi,“Anti-qrishing real-time technique on the qr code using the address bar-based and domain based approach on smartphone,” International Journal of Cyber SecurityandDigitalForensics,vol.8,no.2,pp.134–144,2019.

[27] S. Duncan, "The Role of Social Engineering in QR Code Scams," Financial Cybersecurity Reports, vol. 8, no. 5, pp. 99–112, 2021.

[28] Understanding Anti-Phishing: Your 2025 Guide to Staying Secure. [Online]. Available: https://keepnetlabs.com/blog/understanding-anti-phishing-your-2025-guide-to-staying-secure

[29] Ponemon Institute, "The Cost of a Data Breach: QR Phishing Analysis," Ponemon Institute, 2022. [Online]. Available: https://www.ponemon.org/