© APR 2026 | IRE Journals | Volume 9 Issue 10 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV9I10-1716359

Safe Scan – A Proactive Cloud Sandboxed Firewall for QR Code Mitigation

VINODHINI S[1], SMIRTHI R[2]
[1] Assistant Professor, Department of Information Technology, Velammal Engineering College
[2] Department of Information Technology, Velammal Engineering College

Abstract- ***QR codes are widely used in digital applications such as online payments, ticketing, and advertisements due to their convenience and ease of use. However, the increasing usage of QR codes has also led to rising security threats, including phishing attacks, malicious links, and fraudulent redirections. Most existing QR code scanners directly decode and open embedded content without performing proper security checks, which exposes users to potential cyber risks. To address this issue, this paper proposes Safe Scan, an Android-based application that enhances QR code security using a proactive approach. The system scans QR codes, extracts embedded data, and analyzes it in a cloud-based sandbox environment before allowing user access. By isolating and evaluating the content, the system identifies suspicious or harmful links and classifies them as safe or unsafe. This approach significantly reduces user exposure to threats and improves overall digital security.***

Index Terms- ***Android Application, Cloud Security, QR Code Security, Sandbox Analysis, Threat Detection***

I. INTRODUCTION

QR codes have become an important part of modern digital communication due to their ability to store and share information quickly. They are widely used in online transactions, ticket booking, advertisements, and public services. With the growth of smartphones, users can easily scan QR codes to access digital content instantly. However, this convenience has also introduced serious security concerns. Unlike traditional links, QR codes hide their actual content until they are scanned. This makes it difficult for users to verify the authenticity of the information before accessing it. Attackers exploit this limitation by embedding malicious links inside QR codes, leading users to phishing websites, fake payment portals, or harmful downloads. Such attacks are commonly known as QR phishing or "quishing." Most existing QR code scanners focus only on decoding the content and providing quick access. They do not perform security checks or verify the safety of the embedded data. As a result, users are directly exposed to potential threats. Therefore, there is a need for a system that can analyze QR code content before allowing user interaction. To overcome these challenges, Safe Scan is proposed as a secure solution that integrates QR scanning with cloud-based sandbox analysis to provide proactive protection against QR code threats.

II. IDENTIFY, RESEARCH AND COLLECT IDEA

A. Literature Review

Recent studies have highlighted the growing security risks associated with QR code usage, especially in the form of phishing attacks known as "quishing." Research works such as real-world QR phishing studies demonstrate that users often scan QR codes without verifying their destination, making them vulnerable to malicious links. Existing QR code detection techniques primarily focus on decoding and URL extraction, with limited emphasis on security analysis. Several approaches have been proposed to detect malicious QR codes using machine learning and deep learning techniques. These methods analyze QR code structures or URL features to classify them as safe or unsafe. While these techniques improve detection accuracy, they are often dependent on training datasets and may fail to detect unknown or zero-day attacks. Other studies focus on malicious URL detection using heuristic and rule-based methods. These approaches analyze domain patterns, redirection behavior, and phishing indicators. However, they do not provide a secure environment to test link behavior before user interaction. Cloud-based sandboxing techniques have been widely used in malware detection systems. These systems analyze suspicious content in an isolated environment to prevent direct exposure. However, their application in QR code security is still limited. From the literature, it is evident that most existing solutions focus on either QR code analysis or URL-based detection, but do not provide a complete, integrated approach for proactive security.

B. Research Gap

Based on the analysis of existing systems and research works, several gaps have been identified in the current approaches to QR code security. Most QR code scanners focus only on decoding functionality and lack proper security mechanisms. They directly open

embedded content without verifying its safety, which exposes users to potential threats. Existing detection systems rely heavily on machine learning models or predefined databases, which may not effectively detect new or unknown attacks. Another major limitation is the absence of a secure environment for analyzing QR code content. Current systems do not provide sandbox-based analysis, which means users are directly exposed to malicious links during scanning. Additionally, many solutions are platform-dependent and lack scalability. There is a clear need for a system that combines QR code scanning with proactive threat detection and secure analysis. Such a system should be capable of identifying both known and unknown threats while ensuring that users are protected before accessing the content.

C. Problem Formulation

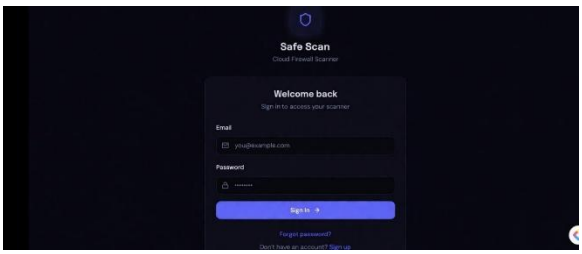
The main problem addressed in this research is the lack of a secure mechanism for analyzing QR code content before user interaction. With the increasing use of QR codes in various applications, the risk of cyber attacks has also increased significantly. Users are unable to verify the safety of QR codes before scanning, and existing systems do not provide sufficient protection against malicious content. This creates a need for a system that can act as a protective layer between the user and the QR code content. The problem can be formulated as designing a system that can securely scan QR codes, extract embedded data, and analyze it in a controlled environment to detect potential threats. The system should be capable of classifying QR codes as safe or unsafe and providing appropriate feedback to the user. The objective is to develop a solution that ensures safe interaction with QR codes by preventing direct exposure to harmful content and improving overall digital security.

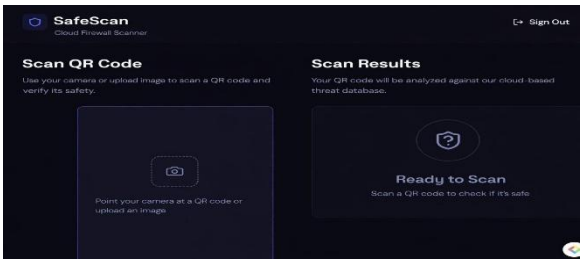
III. STUDIES AND FINDINGS

The Safe Scan system was tested using multiple QR codes containing both safe and malicious content. The Android application successfully scanned QR codes, extracted the embedded data, and transmitted it to the cloud-based sandbox environment for analysis. The system processed the data in real time and generated classification results based on the security analysis. For QR codes containing safe and legitimate links, the system displayed a confirmation message and allowed users to proceed. In contrast, when QR codes contained malicious or suspicious content, such as phishing URLs or unknown domains, the system generated warning alerts and blocked access. The response time of the system was observed to be efficient, providing results within a short duration. The implementation demonstrates that the system can effectively differentiate between safe and unsafe QR codes. The integration of cloud-based sandbox analysis ensures that the user's device is not directly exposed to potential threats during the scanning process.

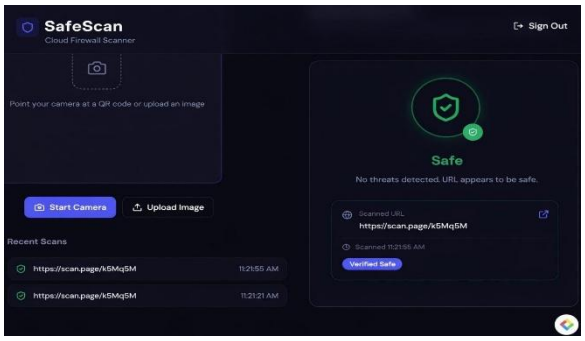
IV. RESULTS AND FINDINGS

The results obtained from the system highlight the effectiveness of combining QR code scanning with sandbox-based analysis. It was observed that the system successfully detects malicious links that are not easily identifiable through basic scanning methods. The use of a sandbox environment adds an additional layer of security by isolating the analysis process. The system shows improved performance compared to traditional QR scanners, as it prevents direct redirection to harmful content. It also enhances user awareness by providing clear feedback regarding the safety of scanned QR codes. However, the performance of the system depends on the efficiency of the cloud server and network connectivity. In scenarios with limited internet access, the response time may be slightly affected. Despite this limitation, the overall results indicate that the proposed system provides a reliable and proactive solution for QR code security.





© APR 2026 | IRE Journals | Volume 9 Issue 10 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV9I10-1716359



V. PEER REVIEWS

After completing the development of the Safe Scan system, the research work was reviewed by peers and subject experts. Feedback was collected regarding the system design, implementation, and effectiveness. Suggestions were provided to improve clarity, enhance security features, and refine the overall presentation of the paper. Peer review helped in identifying minor issues and improving the quality of the research work. It also ensured that the system meets academic standards and provides a reliable solution to the problem.

V. IMPROVEMENT AS PER REVIEWER COMMENTS

Based on the feedback received during the peer review process, necessary improvements were made to the system and documentation. The clarity of explanations was enhanced, and additional details were included to better describe the system architecture and working. Security aspects were further strengthened by refining the analysis process and improving result presentation. These improvements helped in making the system more effective and user-friendly.

VI. CONCLUSION

The Safe Scan system provides an effective solution to address the security challenges associated with QR code usage. By integrating Android-based QR scanning with cloud-based sandbox analysis, the system ensures that QR code content is verified before user access. The system reduces the risk of phishing attacks and malicious links by analyzing content in a secure environment. It is simple, efficient, and suitable for real-world applications. Safe Scan enhances user safety and promotes secure digital interactions. Future enhancements can include integration of machine learning models and real-time threat intelligence to further improve detection accuracy.

ACKNOWLEDGMENT

The authors would like to express their sincere gratitude to the project guide and faculty members for their valuable guidance and support throughout the development of this project. Special thanks to the institution for providing the necessary resources and encouragement.

REFERENCES

[1] K. Krombholz et al., “Exploring Phishing Threats through QR Codes in Practice,” NDSS Workshop on Usable Security (USEC), 2024.

[2] S. Gupta et al., “Hooked: A Real-World Study on QR Code Phishing,” arXiv preprint arXiv:2407.16230, 2024.

[3] A. Sharma et al., “Detecting Quishing Attacks with Machine Learning Techniques Through QR Code Analysis,” arXiv preprint arXiv:2505.03451, 2025.

[4] M. Rahman et al., “QRiS: A Preemptive Novel Method for Quishing Detection,” arXiv preprint arXiv:2510.17175, 2025.

[5] S. Jain and B. B. Gupta, “QRphish: An Automated QR Code Phishing Detection Approach,” International Conference on Information Systems Security, 2016.

[6] R. Singh et al., “Exemplifying Emerging Phishing: QR-based Browser-in-TheBrowser Attack,” arXiv preprint arXiv:2505.18944, 2025.

[7] N. Kumar et al., “A Survey on QR Code Phishing Attacks and Detection Techniques,” International Journal of Computer Applications, 2025.

[8] J. Ma et al., “Learning to Detect Malicious URLs,” ACM Transactions on Intelligent Systems and Technology, vol. 2, no. 3, 2011.

[9] Y. Zhang et al., “Phishing Website Detection Based on URL Features Using Deep Learning,” Applied Sciences (MDPI), 2024.

[10] S. Garera et al., “A Framework for Detection of Phishing Attacks Using URL Features,” Proceedings of IEEE, 2007.