Grenze International Journal of Engineering and Technology, January Issue

A Comparative Review of QR Code Scanner According to a Malicious URL Detection Framework

Prof. Lokesh S. Khedekar[1] and Prof. Dr. Mohit Kumar[2]
[1]Vishwakarma Institute of Technology, Pune, India
lokeshkhedekar@gmail.com
[2]MIT Art, Design, & Technology University, Pune, India
mohit.kumar@mituniversity.edu.in

***Abstract*—The rapid use of Quick Response (QR) codes in various sectors, including marketing, banking, and object identifications, underscores the pressing need for some techniques required for the to detect the external malicious attacks on QR code. This paper focus on the examine the different attack methods on QR code which affects the integrity and security of QR code. It reviews and compares existing detection techniques, such as QR shield, QsecR, BarAI and BarSec, among others, to safeguard against these vulnerabilities for different use cases. In this comprehensive analysis, the paper categorizes detection methodologies based on their operational paradigms, including cryptographic solutions, anomaly detection-based approaches. The comparative study is anchored on several evaluation metrics such as detection accuracy, computational efficiency, and ease of implementation, aiming to delineate the optimal methods suitable for varying scenarios and threat models. The review process adopts a systematic approach, critically analyzing each method's effectiveness against common QR code attacks like overlay, phishing, and malware injections. The paper also explores the integration of artificial intelligence and machine learning techniques to enhance detection capabilities and adaptability against evolving threats. The impacts of this work are multifaceted, offering significant contributions to both academic research and practical applications. By providing a detailed comparison of attack detection techniques, the paper aids in identifying gaps in current security measures and proposes directions for future research. Furthermore, the findings serve as a valuable resource for developers and security analysts in implementing more robust and efficient QR code security solutions, ultimately fostering a safer digital environment for users.**

***Index Terms*— Security, Malicious QR Code, QR Code attacks, Scanner, AI Classifier, QR Shield, QRSec, Bar AI, BarSec.**

I. INTRODUCTION

Quick Response (QR) codes, essentially two-dimensional barcodes, were designed to store a significant amount of information, ranging from URLs to personal data, in a compact, machine-readable format [1,4]. Developed initially for tracking automotive parts, QR codes have transcended their original purpose, finding widespread adoption in diverse sectors such as retail, marketing, healthcare, and banking due to their ease of use and efficiency in data transmission. However, the ubiquity of QR codes has rendered them an attractive target for malicious actors [2,3]. Malicious QR codes are manipulated versions of standard QR codes, designed to execute unauthorized actions when scanned [5]. These actions can include directing users to phishing websites, initiating

Grenze ID: 01.GIJET.11.1.527_1

unauthorized payments, or injecting malware into the user's device. The deceptive nature of QR codes, which do not allow the contents to be visually inspected before scanning, exacerbates their potential as a tool for cybercrime. The attacks on QR codes can be broadly categorized into several types, including but not limited to, phishing attacks, where users are directed to malicious sites; overlay attacks, where legitimate codes are covered with stickers bearing malicious codes; and malware injections, which compromise the user's device security. The sophistication and variety of these attacks necessitate continuous evolution and enhancement of detection techniques to safeguard users from potential threats [6,7]. The scope of this paper encompasses a thorough review and comparative study of existing attack detection techniques for QR codes. It aims to identify, categorize, and evaluate different methods based on varied parameters such as accuracy, efficiency, and ease of implementation. This review not only highlights the current state of QR code security but also sheds light on the limitations and challenges faced by existing solutions.

The impact of this review is significant, extending beyond academic circles to influence practical security strategies and policies. By providing a comprehensive analysis of QR code attack vectors and their countermeasures, this paper aids in the development of more secure QR code generation and scanning practices. Furthermore, it sets the groundwork for future research and development in the field, promoting a proactive approach to QR code security that keeps pace with the evolving landscape of cyber threats. This, in turn, contributes to a safer digital environment, enhancing user trust and confidence in QR code-based applications and services.

The rest of this paper is organized as follows: Section II outlines the general framework of QR code attacks. Section III discusses various types of QR code attacks. The motivation and objectives of this study are presented in Section IV. Section V provides a comprehensive review of existing systems. Section VI evaluates the performance of current QR code scanners and includes a discussion of their capabilities. A general discussion of this study, including its limitations, is provided in Section VI. Finally, Section VII presents the conclusion and suggests directions for future research.

II. Typical Structure of or Code Attack

The surging popularity of Quick Response codes as a smartphone- oriented media element has rendered the attractive targets for malicious software authors.

Figure 1: Typical Structure of QR code attacks

An illustrative representation of a typical Quick Response code attack can be observed in Figure 1. The following steps outline the general progression of events when a victim engages with a malicious QR code.

Step 1: Typically, victims place their trust in QR codes, often scanning them blindly using their smartphones.

Step 2: Consider a QR code that initiates a web request; this request is then transmitted to the corresponding web server.

Step 3: Subsequently, a remote attacker injects malicious code into the web server.

Step 4: The server then redirects the victim to a malicious website.

Step 5: Once on the malicious website, the victim's smartphone is susceptible to the loading of harmful content or malware.

Step 6: At this point, the hacker gains complete control over the victim's smartphone.

III. Types of QR code attacks

Malicious URL Injection: Attackers can create QR codes containing URLs that lead to malicious websites. These websites might host malware or phishing scams, attempting to steal personal information or infect the user's device [8].

Data Manipulation: QR codes possess the capability to encode diverse forms of information, ranging from textual content and URLs to contact details. There exists a risk wherein malevolent actors could temper with the encoded data within a QR code, potentially directing users towards uninitiated destination or causing them to execute unintentional actions.[9]
Social Engineering Attacks: QR codes are susceptible to exploitation in social engineering schemes, wherein perpetrators deceive user into scanning QR codes that execute actions unintended by the user. An instance could involve a QR code purportedly providing a discount only to covertly enrol the user into a premium rate service without their consent [10].
Steganographic Attacks: Steganography involves hiding information within other media. Attackers might embed malicious data within QR codes, which appears innocuous but contain hidden instructions or payloads [11].
Denial of Service (DoS): QR codes can be used to trigger DoS attacks by leading users to websites or resources that overwhelm their device or networks, causing them to become unresponsive [12].
Exploiting QR Code Reader Vulnerabilities: QR code reader apps may have vulnerabilities that attackers can exploit to execute arbitrary code on the user's device or gain unauthorized access to sensitive information [13].
Physical Tampering: Attackers might physically tamper with QR codes in public places, such as on advertisements or products packing, to redirect users to malicious websites or to alter encoded data [14].
Cross-Site Scripting (XSS): QR codes containing JavaScript or other executable code could potentially be used to execute XSS attacks when scanned by vulnerable web applications [15].
Data Leakage: QR codes can be used to encode sensitive information such as payment details or authentication tokens. If these QR codes are intercepted by attackers, they could potentially gain unauthorized access to the encoded data [16].
Replay Attacks: Attackers can capture legitimate QR codes and replay them at a later time to gain unauthorized access to systems or services [17].

IV. MOTIVATIONS AND OBJECTIVES

The advent of Quick Response (QR) codes has revolutionized the landscape of data sharing and accessibility, offering a bridge between physical and digital realms through their capacity to store vast amounts of information in a compact, machine-readable format. However, the ubiquity of QR codes also presents a double-edged sword, as their widespread adoption has opened new avenues for cybercriminals, leading to the emergence of malicious QR codes designed to exploit user trust and security vulnerabilities. These malicious variants can redirect users to phishing sites, initiate unauthorized downloads, or even compromise sensitive personal and financial information. The motivation behind this research stems from the escalating incidents of QR code-related security breaches and the pressing need for robust detection mechanisms. Traditional security measures are often inadequate against sophisticated QR code attacks, underscoring the necessity for innovative and effective solutions to protect users from potential threats. The dynamic nature of cyber threats, coupled with the unique challenges posed by QR code technology, demands a comprehensive study to understand and counteract these risks effectively. This paper contributes to the field by providing a thorough review and comparative analysis of existing attack detection techniques tailored to QR codes. It categorizes these methods based on their underlying principles and operational frameworks, offering a holistic view of the current landscape. By evaluating these techniques against a set of critical metrics, the study identifies their strengths, weaknesses, and applicability in different scenarios, guiding practitioners and researchers in selecting appropriate security measures. Furthermore, this work sheds light on the gaps and limitations present in current methodologies, sparking a discourse on future directions and innovations needed in QR code security. By mapping out the contours of existing approaches and highlighting emerging threats, the paper aims to galvanize further research and development in this pivotal area. The ultimate goal is to enhance the resilience of QR codes against malicious attacks, ensuring their safe and secure utilization across various domains. This endeavour not only contributes to advancing the academic understanding of QR code security but also has profound implications for the practical implementation of safer digital communication channels.

V. LITERATURE REVIEW

The increasing prevalence of Quick Response (QR) codes in various applications has brought attention to the security challenges they pose, particularly concerning the distribution of sensitive information and susceptibility to cyber threats. Several studies have explored different aspects of QR code security, ranging from detecting

malicious URLs to enhancing data storage capacity and ensuring secure transactions. This Literature review synthesizes the finding and contributions of relevant research in this domain.

A. Cryptographic-Based Approaches

Cryptographic methods are used in QR code scanners to encrypt, sign, and regulate access to QR content, ensuring confidentiality and privacy, and protecting against unauthorized access or manipulation. Bani-Hani et al. [19] developed a secure QR code system that uses the Digital Signature Algorithm (DSA) and hashing algorithms for data integrity. This system also generates a public and private key pair, and performs a verification process to alert users of potentially malicious QR codes if verification fails. Similarly, Mavroeidis and Nicho [20] introduced the Secure QR Code Solution (QRCS), a cryptographic system that uses hash functions and digital signatures to verify the integrity and authenticity of QR codes. The QRCS blocks malicious QR codes if verification fails during the scanning phase. Niranjan Hegde et al. [21] presented the Anti-Malware Phishing Scanner (AMPS), which includes features for detecting malicious content and encrypting QR codes using the Advanced Encryption Standard (AES). Wahsheh and Luccio [11] introduced BarSec, an extensive barcode scanner utilizing both symmetric and asymmetric cryptographic techniques to ensure secure barcode creation and scanning. BarSec offers authentication, data integrity, confidentiality, and access control functionalities.

However, adding security features to QR code scanners presents challenges such as inadequate key lengths, weak encryption algorithms, and the requirement for users to generate and read cryptographic QR codes using the same application. These challenges may explain the limited adoption of cryptographic-based methods in QR code security [22].

B. URL-Based Approaches

A common threat involves embedding malicious URLs in QR codes. Various technologies, including artificial intelligence (AI) and blacklist-based approaches, have been proposed to detect these malicious URLs. The blacklist approach compares URLs against a database of known phishing URLs. Yao and Shin [24] developed SafeQR, which uses Google Safe Browsing [25] and PhishTank [26] datasets to detect phishing and malware attacks, providing preemptive notifications to users. The AMPS scanner by Niranjan Hegde et al. [21] also uses blacklist datasets from the VirusTotal Service [28] to detect malicious URLs. Ohigashi et al. [29] proposed methods to identify fake QR codes by analyzing information from the error-correcting process, demonstrating robust results through a combination of detection methods.

AI techniques have proven effective in detecting malicious URLs in QR codes. Al-Zahrani et al. [31] developed an AI-based barcode scanner called BarAI, which achieved a 90.24% accuracy rate with a Decision Tree (DT) classifier. Maheshwari et al. [32] compared seven machine learning classifiers, finding the Random Forest (RF) classifier to be the most effective with a 92.65% accuracy rate. Another study utilized a bidirectional Long Short-Term Memory (LSTM) classifier, achieving an 83.79% accuracy rate in detecting malicious URLs [33].

Rafsanjani et al. [34] proposed QsecR, an Android application focused on secure QR code scanning through malicious URL detection, achieving a 93.50% accuracy rate. QR Shield, which uses a benchmark dataset of URLs, demonstrated an accuracy rate of 96.8% in identifying and detecting malicious links in QR codes [35].

VI. Analysis and Discussion

A. Analysis based on Detection Method

Blacklist: A blacklist is a list or database containing entities, such as people, email address, websites, or IP addresses, that are considered undesirable, untrustworthy, or potentially harmful. The purpose of a blacklist is to prevent or restrict access to these entities, typically to product users or systems from security threats, spam, or other malicious activities.[31]

Machine Learning: Machine learning methods have indeed gained significant popularity for enhancing the detection of malicious URLs. Traditional rule-based or signature-based approaches to detecting malicious URLs often struggle to keep up with the rapidly evolving landscape of cyber threats.[34]

Blacklist: A blacklist is a list or database containing entities, such as people, email address, websites, or IP addresses, that are considered undesirable, untrustworthy, or potentially harmful. The purpose of a blacklist is to prevent or restrict access to these entities, typically to product users or systems from security threats, spam, or other malicious activities.[31]

B. Analysis Based on Feature Extraction and AI Classifier

Feature extraction techniques are used to transform URLs into a structured format, making them suitable for analysis by machine learning models and enhancing overall performance. In various studies, key attribute groups for detecting malicious URLs have been identified as follows:
Lexical Features: These involve metrics such as the average path length, the average token count within the domain, the maximum token length, URL length, and main domain attributes. Lexical features provide valuable insights into the structural characteristics of URLs.
Network-Based Characteristics: Derived from information about the URL's host, these attributes offer insights into server behavior and identity, aiding in the classification of malicious URLs.
Content-Based Characteristics: Extracted from the content of web pages after downloading, these features involve a higher data load and raise security concerns due to the extensive data extraction required. This section provides an overview of the artificial intelligence (AI) classifiers implemented in this study:
Naive Bayes (NB):
The Naive Bayes algorithm is a probabilistic method grounded in Bayes' theorem. It operates under the assumption that the features within a dataset are independent of each other, facilitating efficient classification by computing the probability of a particular outcome based on existing evidence.[38]
Support Vector Matchin SVM):
The Support Vector Machine (SVM) is a versatile supervised learning algorithm employed for both classification and regression task. It functions by determining the best hyperplane that divides data points into distinct classes, thereby precise categorizations.[31]
Logistic Regression (LR) :
Logistics Regression is widely utilized technique for binary classifications. It uses a logistic function to predict the likelihood of an outcome based on input features, making favoured option for predictive modelling in numerous disciplines.[34]
K-Nearest Neighbours (K-NN):
K- Nearest Neighbours is a straightforward machine learning algorithm that uses instance-based learning. It classifies data points by considering the majority votes of their K closest neighbours, making it suitable for both classification and regression tasks.[35]
A Decision tree is a popular supervised learning model utilized for classification tasks. It operates as a decision support tool with a tree-like structure, where nodes signify decisions based on input features and branches represent different outcomes. This structure offers clear and interpretable classification rules. [35].
Table I. Lillustrate the summary of the related scanner which can express a which methodology used by the scanner for to detect Malicious QR code.

TABLE I. SUMMARY OF RELATED SCANNER

Scanner	Detection Method	Feature Extraction	Classifier
[36]	Blacklist & Machine Learning	Host Based & Content Based	J48, Random Trees, Navie Bayes
[37]	Blacklist	Google safe Browsing, Phish tank	-
[38]	Blacklist & Machine Learning	Blacklist, lexical & host based	NB
[31]	Blacklist	Lexical Features	NB,SVM,LR,N-NN and DT
[39]	Blacklist	Blacklist features	-
[40]	Blacklist	Blacklist features	
[34]	Machine Learning	Redirection, Blacklist, Lexical, Host-Based, Content-Based	DT,LR,NB,RF,KNN
[35]	Machine Learning	Lexical feature, Host based, Content Based	DT,LR,NB,RF,KNN

Analysis based on Evolution Matrix
To evaluate model performance, four specific metrics were used, incorporating the following variables:
True Positives (TP): True Positives (TP) refer to the count of malicious URLs that a detection system correctly identifies as threats. This metric is crucial in evaluating the system's effectiveness in distinguishing harmful URLs from benign ones. A high number of true positives indicates a strong capability of the system to accurately detect and flag dangerous web addresses, thereby enhancing overall cybersecurity measures.

True Negatives (TN): rue Negatives (TN) represent the count of benign URLs correctly classified as non-threatening by a detection system. This metric is crucial in evaluating the system's ability to accurately identify safe web addresses, thereby avoiding unnecessary alerts or false alarms. A high number of true negatives indicates the system's proficiency in distinguishing between harmless URLs and potentially harmful ones, contributing to effective cybersecurity measures.
False Positives (FP): The number of benign URLs incorrectly labelled as malicious.
False Negatives (FN): The number of malicious URLs incorrectly categorized as benign.
Accuracy, calculated as shown in provides a comprehensive measure of the model's prediction success.

$$\text{Accuracy} = \frac{TP+TN}{TP+FP+TN+FN}$$

Precision measures the percentage of true positive predictions among all positive predictions. A low precision value indicates that the method tends to incorrectly classify benign URLs as malicious, reflecting a higher rate of false positives.

$$\text{Precision} = \frac{TP}{TP+FP}$$

Recall, quantifies the ratio of actual positive cases that are correctly identified.

$$\text{Recall} = \frac{TP}{TP+FN}$$

The F1 Score is utilized for a holistic assessment of model performance. It combines precision and recall into a single metric, effectively balancing the trade-off between them.

$$\text{F1 Score} = \frac{2*(\text{Precision}* \text{Recall})}{\text{Precision} + \text{Recall}}$$

Precision and recall play a crucial role in handling imbalanced datasets, particularly when benign URLs outnumber malicious ones.
In this section, we conduct a comprehensive systematic analysis of Android QR code scanner applications, evaluating various scanner applications concerning security and privacy concerns.
Table 2. Illustrate the performance evaluation of the QR existing Scanner.

TABLE II. PERFORMANCE EVALUATION OF EXISTING QR SCANNER

Scanner	Accuracy%	Pre%	FPR	Rec	F1
BarSec	78.63	77.30	0.211	79.40	78.34
BarAI	90.24	90.4	0.095	90.00	90.2
QsecR	93.50	93.80	0.065	93.52	93.66
QRShield	96.60	97.00	NA	97.00	97.00

These applications were chosen based on a combination of factors including previous research findings, user popularity, and the presence of security features. Table 2 outlines the specifics of the reviewed applications.
Figure 2. Illustrate the performance of the existing scanner.

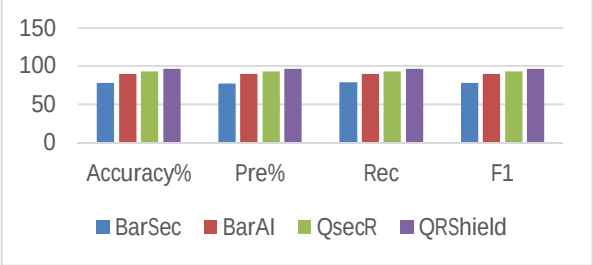

Figure 2. Illustrate the performance of the existing scanner

VII. Conclusion

The extensive review of methods for securing QR codes presented in the literature highlights the diverse approaches and techniques employed to enhance the security, privacy, and functionality of QR code systems. From cryptographic algorithms to watermarking techniques, from blockchain integration to steganographic methods, researchers have explored a wide array of strategies to mitigate various security threats and address specific application requirements. Furthermore, the effectiveness of each method is influenced by various factors, including the nature of the application, the type of data being encoded, the computational resources available, and the potential threat landscape. For example, techniques such as dynamic QR code generation with cryptographic algorithms excel in ensuring the security of real-time transactions but may incur performance trade-offs due to computational overhead. On the other hand, approaches like visual cryptography schemes offer secure data sharing and authentication but may face scalability challenges when handling large volumes of data or complex distributions. In light of these observations, it is essential to adopt a holistic approach to QR code security, combining multiple techniques and layers of protection to achieve robust defense against a wide range of threats. For instance, integrating cryptographic algorithms for data encryption, watermarking techniques for authentication, and blockchain technology for tamper-proof record-keeping can create a comprehensive security framework for QR code-based systems. Moreover, continuous research and innovation are crucial to stay ahead of emerging threats and evolving security requirements. Future efforts should focus on developing lightweight and efficient encryption schemes, improving resistance to adversarial attacks, enhancing compatibility with existing infrastructures, and addressing usability challenges to promote widespread adoption. In conclusion, while QR codes offer convenience and versatility in data encoding and retrieval, ensuring their security and integrity is paramount, especially in applications involving sensitive information or critical transactions. By leveraging a combination of encryption, authentication, and robust error correction mechanisms, QR code systems can be fortified against malicious attacks and unauthorized access, paving the way for their secure deployment across diverse domains.

References

[1] Huang, Chang, Li, and Liu (2020) proposed a secret embedding approach for QR codes utilizing Hamming code for improved efficiency, as reported in their IEEE Access article (vol. 8, pp. 86706-86714, doi: 10.1109/ACCESS.2020.2992694.

[2] Zhou, Hu, Zhang, and Cai (2021) explored the application of cryptographic algorithms in dynamic QR code payment systems, as detailed in their paper published in IEEE Access (vol. 9, pp. 122362-122372, doi: 10.1109/ACCESS.2021.3108189.

[3] Akta, C. (2017). The Evolution and Emergence of QR Codes. Cambridge Scholars Publishing, United Kingdom

[4] Wahsheh, H. A. M. (2019). In their PhD thesis titled 'Secure and Usable QR Codes,' Wahsheh examines security and usability concerns related to QR codes. This work was conducted at Università Ca' Foscari Venezia in Italy in 2019

[5] Krombholz, Frühwirt, Kieseberg, Kapsalis, Huber, and Weippl conducted a comprehensive survey on QR code security, discussing the various attacks and challenges associated with achieving usable security in this context. The work was published by SBA Research in Vienna.

[6] Li, Tie; Kou, Gang; and Peng, Yi. The authors discuss methods for enhancing the detection of malicious URLs using feature engineering, incorporating both linear and nonlinear space transformation techniques. Their research is conducted at the School of Management and Economics at the University of Electronic Science and Technology of China, Chengdu, China.

[7] Hu, Jianwei, Wei Zhao, and Yanpeng Cui. "An overview of SQL injection attacks: Detection and preventive measures." In Proceedings of the 12th International Conference on Machine Learning and Computing, 2020

[8] Arock, M. (2021). Presented research on detecting SQL injection attacks efficiently through a pattern-based neural network model at the International Conference on Computing, Communication, and Intelligent Systems (ICCCIS). IEEE.
[9] Subairu, S., and colleagues (2020) presented a review of methods for detecting phishing attacks involving Quick Response codes in their work at the 2nd International Conference on Computer and Information Sciences. The paper is published by IEEE.
[10] Salahdine and Kaabouch (n.d.) conducted a comprehensive survey of social engineering attacks in the School of Electrical Engineering and Computer Science at the University of North Dakota. For further correspondence, contact Naima Kaabouch at naima.kaabouch@und.edu.
[11] Ke, Y., Liu, J., Zhang, M.Q., Su, T.T., & Yang, X.Y. (2018). Steganography Security: Concepts and Implementation. IEEE Access. Available at IEEE Xplore
[12] Kumar, G. (2016). An updated perspective on denial of service attacks. Published in Systems Science & Control Engineering by Taylor & Francis.
[13] Kharraz, A., Kirda, E., & Robertson, W. (2014). The researchers presented a study on the prevalence and risks of malicious QR codes in a paper at the 44th Annual IEEE/IFIP International Conference on Dependable Systems and Networks.
[14] Sung, S., Lee, J., Kim, J., Mun, J., & Won, D. (Year). Conducted a security analysis of mobile authentication using QR codes in a study. This work was published at Samsung Electronics and the College of Information and Communication Engineering at Sungkyunkwan University in Suwon, Korea."
[15] An article titled "XSStudent: A Proposal for Avoiding Cross-Site Scripting (XSS) Attacks in Universities" was presented at the 3rd Cyber Security in Networking Conference (CSNet) in 2019
[16] Li, Fan, and Wang discuss a lightweight approach to secure QR codes in their work titled "LWSQR: Lightweight Secure QR Code." This study is part of the Communications in Computer and Information Science series, volume 879.
[17] An article published in Journal for Research, Volume 2, Issue 2 (April 2016), explores the use of QR codes for card-less ATM transactions. The work offers insights into the potential advantages and challenges of implementing such technology in banking systems (ISSN: 2395-7549).
[18] Wahsheh and Luccio (2020) conducted a comprehensive study on the security and privacy of QR code applications, offering guidelines and solutions in their article published in Information (vol. 11, no. 4, p. 217).
[19] Bani-Hani, Wahsheh, and Al-Sarhan (2014) presented a secure QR code system in their paper published at the 10th International Conference on Innovations in Information Technology (IIT). The paper can be found on pages 1-6
[20] Mavroeidis and Nicho (2017) introduced a cryptographically secure tool designed to prevent phishing attacks involving quick response (QR) codes. Their work was presented at the 7th International Conference on Mathematical Methods, Models, and Architectures for Computer Network Security (MMM-ACNS 2017), held in Warsaw, Poland from August 28-30, 2017. The paper can be found in the conference proceedings published by Springer (pp. 313–324).
[21] Hemavathi, Hegde, Bharti, Sur, and Priyanka (2018) developed an antimalware and phishing QR scanner, as described in their publication in the International Journal of Innovative Science and Research Technology (vol. 3, no. 5).
[22] Focardi, Luccio, and Wahsheh (2018) conducted a comparative study on the security risks and mitigation strategies for two-dimensional barcodes. The research is documented in their work published in Computer and Network Security Essentials (pp. 207–219)
[23] Latif, Sugiantoro, and Prayudi (2019) presented a method for real-time protection against QR code phishing attacks. Their approach leverages both address bar-based and domain-based techniques on smartphones to enhance security. The study was published in the International Journal of Cyber-Security and Digital Forensics, volume 8, issue 2, on pages 134–144.
[24] H. Yao and D. Shin, “Towards preventing qr code based attacks on android phone using security warnings,” in Proceedings of the 8th ACM SIGSAC symposium on Information, computer andcommunications security, 2013, pp. 341–346.
[25] Focardi, Luccio, and Wahsheh (2018) conducted a comparative study on security threats and solutions related to two-dimensional barcodes, as detailed in Computer and Network Security Essentials, pages 207–219
[26] Latif, Sugiantoro, and Prayudi (2019) explore a real-time technique for mitigating QR code phishing attacks by using address bar-based and domain-based methods on smartphones. Their research is published in the International Journal of Cyber-Security and Digital Forensics (Vol. 8, No. 2, pp. 134-144.
[27] “Safe Browsing – Google Safe Browsing.” [Online]. Available: https://safebrowsing.google.com/
[28] “PhishTank | Join the fight against phishing.” [Online]. Available: https://www.phishtank.com/
[29] 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.
[30] “VirusTotal - Home.” [Online]. Available: https://www.virustotal.com
[31] M. S. Al-Zahrani, H. A. Wahsheh, and F. W. Alsaade, “Secure realtime artificial intelligence system against malicious qr code links,” Security and Communication Networks, vol. 2021, pp. 1–11, 2021.
[32] B. Janet, R. J. A. Kumar et al., “Malicious url detection: a comparative study,” in 2021 International Conference on Artificial Intelligence and Smart Systems (ICAIS). IEEE, 2021, pp. 1147–1151.

[33] A. Pawar, C. Fatnani, R. Sonavane, R. Waghmare, and S. Saoji, “Secure qr code scanner to detect malicious url using machine learning, in 2022 2nd Asian Conference on Innovation in Technology (ASIANCON). IEEE, 2022, pp. 1–8.
[34] 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, 2023.
[35] QR Shield: A Dual Machine Learning Approach Towards Securing QR Codes Hissah Almousa1, Arwa Almarzoqi*1, Alaa Alassaf1, Ghady Alrasheed1 and Suliman A. Alsuhibany1 1Department of Computer Science, College of Computer, Qassim University, Buraydah 51452, Saudi Arabia
[36] J. Song, K. Gao, X. Shen, X. Qi, R. Liu, and K.-K.-R. Choo, ‘‘QRFence: A flexible and scalable QR link security detection framework for Android devices,’’ Future Gener. Computer. Syst., vol. 88, pp. 663–674, Nov. 2018,doi: 10.1016/j.future.2018.05.082.
[37] H. Wahsheh. (2018). BarSec Droid. Accessed: Jul. 28, 2022. [Online]. Available: https://m.apkpure.com/barsec-droid/barcode_security.heider.bsr
[38] A. Y. Alnajjar, M. Anbar, S. Manickam, O. Elejla, and H. El-Taj,‘‘QRphish: An automated QR code phishing detection approach,’’ J. Eng. Appl. Sci., vol. 11, no. 3, pp. 553–560, 2016.
[39] G Data CyberDefense AG. (2021). G DATA QR Code Scanner. [Online].Available: https://www.gdatasoftware.com/
[40] Lionic. (2022). Lionic Secure QR Code Scanner. [Online]. Available:https://play.google.com/store/apps/details?id=com.lionic.scanner.qrcode