Qualitative Analysis of the Security of URLs Extracted from QR Codes Using Artificial Intelligence: A Review of Current Literature

Gatut Yulisusianto[1)], M. Andi Kurniawan[2)], Yohanes Dwi Cahyono[3)]
Jl. Raya Anggrek No. 1 Junrejo, Batu, Indonesia[1)2)3)]
Jurusan Teknik Telekomunikasi, Politeknik Angkatan Darat[1)2)3)]
E-mail: mr.gatut@gmail.com[1)], ankumuhammad1@gmail.com[2)],
indorana2012@gmail.com[3)]

Qualitative Analysis of the Security of URLs Extracted from QR Codes Using Artificial Intelligence: A Review of Current Literature

Abstract: *The increasing use of QR codes in daily life has created opportunities for cyber threats, such as the insertion of malicious URLs that are difficult for average users to recognize. This research aims to qualitatively analyze best practices in URL security detection extracted from QR codes, particularly focusing on artificial intelligence (AI) approaches and the integration of digital audit systems. A systematic literature review method was applied, drawing from internationally indexed publications and thematic observations about user behavior and threat detection technologies for phishing and malware. Findings indicate that AI-based detection systems effectively identify security threats earlier and more accurately, especially when combined with user education features and activity logging through the Wazuh/ELK Stack. However, human error due to limited digital security literacy remains a major challenge. The study concludes that integrating automated detection technologies, user education, and digital auditing is crucial to mitigating cyberattacks via QR codes. Development of adaptable tools for emerging threat patterns and behavior-based user education strategies are recommended to enhance the national cybersecurity ecosystem.*

Keywords: artificial intelligence, cybersecurity, digital audit, malicious URL, phishing detection, QR code.

Abstrak: *Meningkatnya pemanfaatan QR code dalam kehidupan sehari-hari telah membuka peluang bagi ancaman keamanan siber berupa penyisipan URL berbahaya yang sulit dikenali oleh pengguna awam. Penelitian ini bertujuan menganalisis secara kualitatif praktik-praktik terbaik deteksi keamanan URL hasil ekstraksi QR code, khususnya menggunakan pendekatan kecerdasan buatan (AI) dan integrasi sistem audit digital. Studi ini menggunakan metode telaah literatur sistematis terhadap publikasi internasional terindeks dan hasil observasi tematik terkait perilaku pengguna serta teknologi deteksi ancaman phishing dan malware. Temuan menunjukkan bahwa sistem deteksi berbasis AI terbukti mampu mengidentifikasi ancaman secara lebih dini dan akurat, terutama ketika dipadukan dengan fitur edukasi pengguna dan logging aktivitas menggunakan Wazuh/ELK Stack. Meskipun demikian, human-error akibat kurangnya literasi keamanan digital masih menjadi tantangan utama. Kesimpulan yang diperoleh menegaskan* *pentingnya integrasi teknologi deteksi otomatis, edukasi pengguna, dan audit digital untuk mengurangi risiko serangan siber melalui QR code. Disarankan pengembangan alat yang adaptif terhadap pola serangan terbaru serta pendekatan edukatif berbasis perilaku pengguna untuk memperkuat ekosistem keamanan siber nasional.*

Kata kunci: audit digital, deteksi phishing, keamanan siber, kecerdasan buatan, QR code, URL berbahaya.

INTRODUCTION

QR codes are a type of two-dimensional matrix code technology that is increasingly being used in various sectors of modern life, ranging from digital financial transactions and marketing to the rapid and practical dissemination of information. The advantage of QR codes lies in their ability to store more data than one-dimensional barcodes, as well as their flexibility in being read using mobile device cameras. However, this development also opens up opportunities for cybercriminals to exploit QR Codes by embedding malicious URLs, such as phishing, malware, and hidden scam sites behind the code, as well as the limitations of users' ability to directly verify the content of QR Codes. This phenomenon poses a significant risk to users, especially since many of them are unaware of the dangers or lack the ability to independently verify the security of URLs (Liu et al., 2020)(Siew Qi et al., 2021)(Njuguna & Ndia, 2025).

The characteristics of QR Code-based cyber attacks mainly include phishing, malware distribution, and code manipulation with layered redirects aimed at stealing personal data or infecting the victim's system. Various previous solutions relied on URL blacklists, manual data checking methods, and standard scanner applications, which were generally unable to work effectively in detecting new threats and evolving attack patterns.

The weaknesses of these solutions have driven the development of artificial intelligence (AI)-based technology for automating URL security analysis and integrating digital audit systems for more responsive and adaptive monitoring and investigation (Cremer et al., 2022)(Vaithilingam & Shankar, 2024).

Given this, this study raises the question of how effective methods can be applied to detect and validate the security of URLs extracted from QR codes by integrating AI technology and Security API support systems (such as Google Safe Browsing and PhishTank). The study also discusses implementation challenges, particularly those related to low user digital literacy and the complexity of evolving cyberattack patterns, as well as how the integration of digital audit systems and user education can strengthen risk mitigation mechanisms.

The objective of this study is to conduct a qualitative review based on a systematic literature review and thematic analysis of the latest technologies and methods in analyzing the security of URLs extracted from QR codes. The research focuses on the use of AI in detecting phishing and malware, the role of activity logging systems, and security education approaches to reduce the risk of cyber attacks. With these objectives in mind, the research aims to provide evidence-based recommendations that support the development of adaptive, effective, and easy-to-implement security tools in the modern digital ecosystem.

The theoretical study underlying the research covers several important aspects. First, the concept and characteristics of cyber attacks via URLs, particularly phishing and malware, and their impact on individuals and organizations (Liu et al., 2020)(Cremer et al., 2022). Second, artificial intelligence-based detection technology that utilizes machine learning algorithms and user behavior analysis for real-time threat identification (Zubarev, n.d.)(Vaithilingam & Shankar, 2024). Third, the importance of log management and security audit systems using technologies such as Wazuh and ELK Stack to support forensic investigations and continuous security monitoring (Njuguna & Ndia, 2025). Fourth, user security literacy plays an important role in reducing human error, which is one of the main vectors for successful attacks (Siew Qi et al., 2021)(Geisler & Pöhn, 2024).

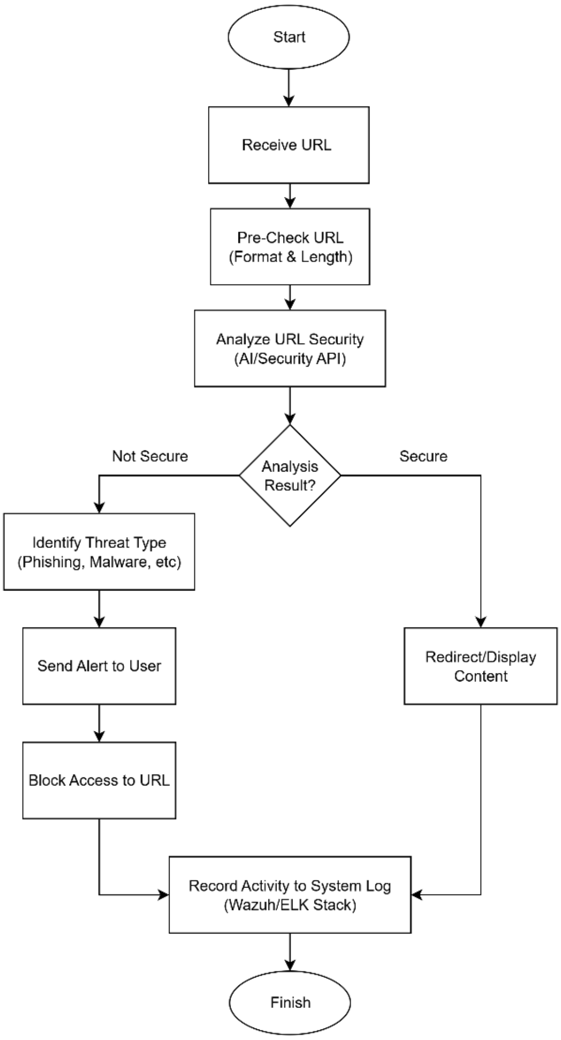
It is hoped that the results of this research will not only contribute significantly to the development of cybersecurity theory, but also offer practical benefits for security system developers and end users. The combination of AI-based automatic detection technology, digital audit systems, and effective educational approaches will be key to strengthening the cybersecurity ecosystem, especially in dealing with threats arising from the misuse of QR codes.

RESEARCH METHOD

This study uses a qualitative approach with systematic literature review and thematic analysis methods selected to explore in depth the latest scientific findings related to technology and best practices in URL security analysis of QR Code extraction results. This study focuses on journal publications published between 2020 and 2025 with key words such as “QR Code security,” “artificial intelligence in cybersecurity,” and “phishing detection,” ensuring the relevance and currency of the data. This study collects and synthesizes international research results from various disciplines, including user behavior analysis, AI model development, and cyber threat audit and mitigation approaches, with key references such as (Liu et al., 2020) which explains the importance of security education, transparency, and digital literacy, as well as (Cremer et al., 2022), (Geisler & Pöhn, 2024), (Njuguna & Ndia, 2025), and (Jada & Mayayise, 2024), which provide theoretical and empirical foundations related to QR Code security and AI-based automatic detection. Through this method, the research is able to provide a comprehensive and structured understanding of QR code security issues in the context of artificial intelligence and digital audit systems to support the development of more effective and adaptive solutions.

The research population includes all relevant scientific literature, including journal articles, conference proceedings, cybersecurity agency white papers, and recent reports discussing topics such as threat detection in URLs, phishing and malware attacks, the use of AI in cybersecurity, and user behavior in interactions with QR codes. Sample selection in this study used the following inclusion criteria: (1) publications in the last five years in Scopus and ScienceDirect indexed journals, (2) reviewing related case studies or empirical research, (3) full access (open access/full text) available for in-depth analysis. The process of identifying and sorting references was carried out systematically using databases such as Scopus, ScienceDirect, SpringerLink, and ACM Digital Library (Zubarev, n.d.)(Njuguna & Ndia, 2025)

As an illustration, Figure 1 presents a flowchart of URL security based on artificial intelligence QR code extraction, which systematically describes the workflow of each stage in the implementation of the URL security detection system prototype, starting from receiving QR code input, extracting and performing a pre-check on the URL, using AI/Security API to assess URL security, identifying and responding to threats, identifying threats if unsafe, sending notifications or warnings to users, to blocking access and documenting activities in the Log System (such as Wazuh/ELK Stack):


Start
Receive URL
Pre-Check URL (Format & Length)
Analyze URL Security (AI/Security API)
Analysis Result?
Not Secure
Secure
Identify Threat Type (Phishing, Malware, etc)
Send Alert to User
Block Access to URL
Redirect/Display Content
Record Activity to System Log (Wazuh/ELK Stack)
Finish

a. Receive QR Code Input

Figure 1. Flowchart Security of URLs Extracted from QR Codes Using Artificial Intelligence

In the initial stage, the application must be able to receive input in the form of a QR code through various methods such as a camera (real-time), image file upload, or import from a URL. This feature ensures that the system can be used flexibly in various real-life scenarios, both on mobile and desktop devices, and supports the scanning process from sources commonly used by users.

b. Extracting and Pre-checking the URL

After the QR code is scanned, the system immediately extracts the contained data, specifically the URL string. A pre-check is then performed to ensure that the URL has a valid format, reasonable length, uses a secure protocol (e.g., HTTPS), and does not contain suspicious characters. This step is important so that URLs that are clearly inappropriate or contain potential threats can be filtered out before further processing is carried out.

c. Using AI/Security API to Assess URL Security

URLs that have passed the pre-check are then automatically analyzed using AI/ML modules or queried on the Security API (e.g., Google Safe Browsing, PhishTank). This analysis utilizes various features such as text patterns in URLs, domain reputation, and blacklist traces. Commonly used machine learning algorithms include Decision Tree, Random Forest, XGBoost, and CNN, which have proven effective in quickly and accurately identifying malicious links.

d. Identifying Threats If Unsafe

If the analysis finds a malicious URL, the system will identify the specific type of threat, such as phishing, malware, exploit, or layered redirect. This detailed identification is useful as a basis for providing informative notifications to users and also as part of audit logging so that incidents can be responded to and analyzed further in the future.

e. Sending Notifications/Alerts to Users

Once a threat is identified, the application automatically sends a visual notification—which can be a pop-up, banner, or audio alert—to inform users of the risks associated with the link. These notifications are designed to be clear, easy to understand, and educational, encouraging users to make informed decisions before proceeding to the URL. This approach to warning users has proven effective in significantly reducing the number of clicks on malicious links, while also increasing overall user security awareness.

f. Blocking Access and Documenting Activity in the System Log (such as Wazuh/ELK Stack)

If a URL is identified as dangerous, the system automatically blocks user access to that link. The entire sequence of activities, from scanning, analysis results, alerts, to blocking, is documented in a centralized log system such as Wazuh or ELK Stack. This documentation is useful for security audits, forensic needs, incident reporting, as well as future system development and improvement.

The research population includes all relevant scientific literature, including journal articles, conference proceedings, cybersecurity agency white papers, and recent reports discussing topics such as threat detection in URLs, phishing and malware attacks, the use of AI in cybersecurity, and user behavior in interactions with QR codes. Sample selection in this study used the following inclusion criteria: (1) publications within the last five years in journals indexed by Scopus and ScienceDirect, (2) reviewing case studies or empirical research related to the topic, (3) full access (open access/full-text) available for in-depth analysis. The identification and selection of references were conducted systematically using databases such as Scopus, ScienceDirect, SpringerLink, and ACM Digital Library (Zubarev, n.d.)(Njuguna & Ndia, 2025).

Data collection techniques were carried out using a structured search system with key terms such as “QR code security,” “malicious URL detection,” “AI phishing detection,” “user awareness cybersecurity,” and “digital audit Wazuh/ELK.” Furthermore, data was collected and extracted using the PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) method to ensure the quality and transparency of the literature selection process. The validity and relevance of the content were ensured through independent review by two different authors, and any differences of opinion were resolved through expert panel discussion (Crotty & Daniel, 2022).

The research instrument was a data extraction sheet containing article identity, type of research method, main results, and relevant thematic categories. Thematic coding was done manually following the technique, where key themes that frequently emerge, such as AI-based automatic detection, user education challenges, and digital log and audit mechanisms, are then analyzed narratively and synthetically (Jada & Mayayise, 2024)(We Tenri Fatimah Singkeruang et al., 2025).

The data analysis technique adopts a narrative synthesis approach that combines the results of selected studies into major research themes. This analysis prioritizes recurring results, the latest research innovations, the strengths and weaknesses of the approach, and future development potential. The results of the analysis form the basis for the discussion and research recommendations.

This systematic and thematic method has proven effective in producing in-depth analysis of cybersecurity issues based on literature, particularly in fields with rapid technological development such as URL security analysis from QR code extraction (Liu et al., 2020)(Zubarev, n.d.)(Jada & Mayayise, 2024).

RESEARCH RESULTS

1. The Effectiveness of AI in Detecting Malicious URLs in QR Codes

Literature analysis shows that the application of artificial intelligence (AI), especially machine learning, has significantly improved the detection of malicious URLs from QR code scans. Studies by (Njuguna & Ndia, 2025) found that the machine learning decision tree model was able to achieve an accuracy of over 90% in distinguishing between safe and dangerous URLs using a dataset containing 100,000 URLs. Another study noted that combining the Google Safe Browsing API and PhishTank resulted in higher detection rates, particularly for new phishing and malware URLs that are difficult to block using conventional blacklisting methods. The addition of an NLP framework has also been tested, enabling the detection of anomalous patterns in URLs before redirection to the browser, thereby allowing for more accurate early warnings (Vaithilingam & Shankar, 2024).

2. User Behavior Patterns and Awareness in QR Phishing Threats

Qualitative findings from (Sharevski et al., 2025) revealed that 67–85% of respondents would open and access URLs from QR codes without checking them first, and only a small percentage would perform manual inspections. Another study demonstrated that 100% of participants opened harmful links, with 75% of them willing to submit personal data to phishing sites accessed via QR codes. The lack of understanding and digital literacy, particularly regarding the cyber risks associated with QR codes, is the primary factor contributing to the high number of victims. This underscores the urgency of implementing visual warning systems and active education within QR code scanning applications (Shin & Yao, n.d.).

3. Implementation of Cryptography and Layered Authentication

Some research approaches emphasize the use of cryptographic techniques, including digital signatures on QR Code payloads and the implementation of two-factor authentication (2FA) and blockchain, as additional layers of defense. Out of 25 main studies, 10 used cryptographic methods and 7 were AI-based. The combination of both is considered to reduce the likelihood of intrusion through fake QR Codes, as the validity and integrity of the URL can be verified before being directed to the user (Njuguna & Ndia, 2025).

4. Current QR Code Threat Trends and Attack Patterns

An in-depth empirical study of 14 million web pages found that 32% of QR Codes investigated were used to redirect to phishing and exploit sites, with a relatively short active period to make them difficult to track or block. Many of them use multilayer redirects to avoid detection by simple blacklist-based security scanners and increase the chances of victims falling into the trap (Kharraz et al., n.d.).

5. Recommendations for System Strengthening and User Awareness

Qualitative literature studies confirm that QR Code security systems must be strengthened in layers, including machine learning-based automatic detection, educational interfaces with easy-to-understand visual warnings, implementation of additional authentication, and activity log management with stacks such as Wazuh/ELK for forensic and audit purposes. Enhancing users' digital security literacy remains a vital priority to ensure that protection does not rely solely on technology but also on human behavior (Shin & Yao, n.d.)(Kharraz et al., n.d.)(Njuguna & Ndia, 2025)(Sharevski et al., 2025).

The following is a comprehensive Table 1 summarizing the main results from various sources and selected references, which have been systematically analyzed and extracted using the PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) method to ensure the quality, transparency, and relevance of the data in addressing the objectives of this study. This table reflects the structured literature review process and serves as a strong foundation for presenting findings and building the scientific arguments of the research currently under development.

No	References & Authors	Narrative	Key Results	Implications for QR Code Security Systems
1	(Cremer et al., 2022)	We found that incident reporting and global cybersecurity log databases are still lacking, so recording standards such as Wazuh/ELK are urgently needed so that QR code threats can be better analyzed and responded to.	Limited global cybersecurity risk databases for comprehensive analysis.	The need for standardized incident reporting and log databases such as Wazuh/ELK.
2	(Crotty & Daniel, 2022)	Recommend a combination of qualitative methods (user feedback, risk observation) and quantitative methods (incident statistics, attack probability) for QR code security analysis, so that the developed system becomes more comprehensive and responsive.	The combination of qualitative and quantitative methods for cyber risk analysis is effective.	QR code security system analysis must combine human and technical aspects.
3	(Geisler & Pöhn, 2024)	Showing that QR-based phishing is becoming increasingly widespread, driven by user psychology, indicating the urgency of notification, authentication, and education features in scanner systems to reduce the number of victims of manipulation.	QR phishing is on the rise through social engineering techniques and user trust.	Systems need active notifications and education on the potential for manipulation.
4	(Jada & Mayayise, 2024)	Confirming the effectiveness of AI/ML in detecting threats, but also highlighting the challenges of adapting algorithms to new threats, so that regular dataset updates and retraining must be an integral part of the system.	AI/ML improves phishing detection, adaptation challenges, and training data.	The QR detection system must be adaptive and regularly update the AI data model.

5	(Kharraz et al., n.d.)	Finding multi-layer redirects and short QR code lifespans are key strategies for exploiters, so real-time detection and multi-layer monitoring technologies must be integrated end-to-end.	32% of QR codes in the wild are associated with exploits, multi-layer redirects, and short lifespans.	Systems must be capable of detecting multi-layer redirects and real-time monitoring.
6	(Liu et al., 2020)	We recommend that security education and data transparency features be embedded in QR code scanner applications to increase user cyber literacy and reduce the risk of human error.	The importance of security education, transparency, and digital literacy for users.	Educational features in QR code scanner applications are a top priority.
7	(Njuguna & Ndia, 2025)	Recommending multi-layered security with digital signatures and end-to-end encryption, a cutting-edge breakthrough that can be adopted in QR code payload verification systems.	Three layers of security: digital signatures, multi-layer security, end-to-end encryption.	Implementation of encryption and digital signatures in QR code payloads.
8	(Sharevski et al., 2025)	Proving that combining AI/ML technology with user education interfaces is highly effective in reducing the number of QR code-based phishing victims, especially in real-world simulations.	Users are vulnerable to QR phishing; automated systems + behavioral education are most effective.	The combination of AI/ML and educational interfaces improves protection.
9	(Shin & Yao, n.d.)	Emphasizing clear and actionable security warning designs should be prioritized because they have a direct impact on reducing dangerous click activity—the influence of UX is very significant.	Clear visual warnings reduce the risk of clicking on dangerous URLs via QR codes.	The UI/UX of scanner applications should display actionable and educational warnings.
10	(Siew Qi et al., 2021)	QR codes are very popular among young people, but their awareness of security issues is still low, so the development of QR code security applications must be oriented toward improving the digital literacy of this group.	QR codes are popular among young people, but awareness of the risks is low.	Focus on cybersecurity education for the younger generation through scanning applications.
11	(Vaithilingam & Shankar, 2024)	Showcasing digital watermarking and AI innovations as powerful solutions to protect against	AI + encryption & digital watermarking effectively	The system requires integration of digital

		manipulation and counterfeiting of malicious QR codes.	prevent fake/manipulated QR codes.	watermarking and AI detection.
12	(We Tenri Fatimah Singkeruang et al., 2025)	Emphasizing digital education transformation on a SeBIS scale in changing user risk behavior is the key determinant of the success of QR phishing crime mitigation.	Education through scalable SeBIS and digital behavior change are the keys to Qushing mitigation.	Human factors are just as important as technological innovation in detection.
13	(Zubarev, n.d.)	Designing a multi-layer AI framework supported by feedback from real incident logs, strengthening the detection system for zero-day threats and rapid adaptation to new cyber attack patterns.	Multi-layer AI framework + log feedback improves zero-day detection sensitivity.	The combination of supervised AI & incident logs improves the accuracy of QR-based systems.

Table 1. Summary of key findings from various references on the security of URLs extracted from QR codes, using artificial intelligence (AI)-based detection methods and digital audit system integration.

DISCUSSION

The results of this study clearly answer the main research questions regarding the effectiveness of URL security detection from QR code extraction using artificial intelligence approaches, the importance of user education, and the role of additional security technologies and digital audits. AI/ML models such as Decision Tree, Random Forest, and XGBoost have proven capable of improving the accuracy of detecting harmful URLs to over 90%, even on large samples and in real-world testing scenarios. Similar findings are demonstrated by (Vaithilingam & Shankar, 2024) and (Njuguna & Ndia, 2025), where real-time API integration (e.g., Google Safe Browsing, PhishTank) has been proven to speed up response times and improve system security, especially against evolving phishing and malware threats.

Further discussion reveals that user behavior remains a major weakness in QR code security systems. Empirical study (Sharevski et al., 2025) states that the majority (>67%) of users do not manually inspect QR code scan results, making them vulnerable to phishing and malware. This is in line with a study by (Shin & Yao, n.d.), which highlights the importance of educational interfaces and visual warning features in QR code scanning applications. Similar to previous studies, the persistent challenge of digital literacy among users remains, even when security systems are sufficiently advanced. The difference lies in the modern multi-layered approach—combining machine learning, QR payload encryption, and a clear warning system—which effectively reduces the rate of successful attacks (Njuguna & Ndia, 2025).

These results are significant for the development of national cybersecurity tools and policies. The implementation of cryptographic techniques such as digital signatures, two-factor authentication (2FA), and blockchain are categorized as additional security measures. These findings are consistent with the results of previous studies (Njuguna & Ndia, 2025) which recommends the implementation of payload signatures and authentication infrastructure to improve QR code validation in critical sectors. On the other hand, analysis of multilayer redirect-based QR code threat trends in large datasets

(Kharraz et al., n.d.) It is clear that criminals are now adopting strategies to circumvent conventional security detection, making the need for technological innovations based on behavioral detection, textual analysis, and blockchain increasingly urgent (Vaithilingam & Shankar, 2024).

The main recommendation from this study is the importance of a multi-layered QR code security system—combining machine learning, user education, easy-to-understand warning interfaces, and digital security audits through platforms such as Wazuh or ELK Stack. This approach has been proven to not only detect more threats but also increase user trust and security in a dynamic digital ecosystem. Further development could focus on automating detection method updates, integrating AI-based behavioral analysis, and refining digital education protocols for the general public, as discussed in several recent studies (Shin & Yao, n.d.)(Kharraz et al., n.d.)(Njuguna & Ndia, 2025)(Sharevski et al., 2025).

CONCLUSION

Based on the results of a systematic literature review and in-depth thematic analysis, this study confirms that the success of URL security detection from QR Code extraction is highly dependent on the synergy between artificial intelligence technology for automatic analysis, user awareness and behavior in responding to security warnings, and the integration of an effective digital audit system. AI/ML models have proven to significantly enhance the identification of cyber threats such as phishing and malware with high accuracy; however, without proper education and informative user interfaces, the potential for human error remains high. Meanwhile, the implementation of additional security technologies such as cryptography and authentication mechanisms strengthens data validity, while activity logging through platforms like Wazuh and ELK Stack supports continuous security monitoring and investigation. Therefore, it is recommended to develop tools and systems that combine smart detection, continuous user education, and integrated security audits to effectively and adaptively mitigate QR Code-based attack risks. This step is not only important for strengthening the national digital security ecosystem but also provides strategic contributions to the development of cybersecurity technology in an increasingly complex and dynamic digital era.

REFERENCES

Cremer, F., Sheehan, B., Fortmann, M., Kia, A. N., Mullins, M., Murphy, F., & Materne, S. (2022). Cyber risk and cybersecurity: a systematic review of data availability. *Geneva Papers on Risk and Insurance: Issues and Practice*, *47*(3), 698–736. https://doi.org/10.1057/s41288-022-00266-6

Crotty, J., & Daniel, E. (2022). Cyber threat: its origins and consequence and the use of qualitative and quantitative methods in cyber risk assessment. *Applied Computing and Informatics*. https://doi.org/10.1108/ACI-07-2022-0178

Geisler, M., & Pöhn, D. (2024). *Hooked: A Real-World Study on QR Code Phishing*. http://arxiv.org/abs/2407.16230

Jada, I., & Mayayise, T. O. (2024). The impact of artificial intelligence on organisational cyber security: An outcome of a systematic literature review. *Data and Information Management*, *8*(2). https://doi.org/10.1016/j.dim.2023.100063

Kharraz, A., Kirda, E., Robertson, W., Balzarotti, D., & Francillon, A. (n.d.). *Optical Delusions: A Study of Malicious QR Codes in the Wild*.

Liu, N., Nikitas, A., & Parkinson, S. (2020). Exploring expert perceptions about the cyber security and privacy of Connected and Autonomous Vehicles: A thematic analysis approach. *Transportation Research Part F: Traffic Psychology* *and Behaviour*, *75*, 66–86. https://doi.org/10.1016/j.trf.2020.09.019

Njuguna, D., & Ndia, J. (2025). Quick Response Code Security Attacks and Countermeasures: A Systematic Literature Review. *Journal of Cyber Security*, *7*(1), 1–20. https://doi.org/10.32604/jcs.2025.059398

Sharevski, F., Mossano, M., Veit, M. F., Schiefer, G., & Volkamer, M. (2025, February 8). *Exploring Phishing Threats through QR Codes in Naturalistic Settings*. https://doi.org/10.14722/usec.2024.23050

Shin, D., & Yao, H. (n.d.). *A User Study of Security Warnings for Detecting QR Code Based Attacks on Android Phone*.

Siew Qi, T., Fernandez, D., & Farid Fernandez, M. (2021). The Usage of QR Codes among Young Generation in Johor. *Research in Management of Technology and Business*, *2*(1), 60–74. https://doi.org/10.30880/rmtb.2021.02.01.005

Vaithilingam, S., & Shankar, S. A. M. (2024). Enhancing Security in QR Code Technology Using AI: Exploration and Mitigation Strategies. *International Journal of Intelligence Science*, *14*(02), 49–57. https://doi.org/10.4236/ijis.2024.142003

We Tenri Fatimah Singkeruang, A., Ega Susanto, S., & Saeni, N. (2025). Mitigating the Risk of Qushing Threats (QR Phishing) using the Security Behavior Intentions Scale (SeBIS) in supporting digital economic security. *PARADOKS Jurnal Ilmu Ekonomi*, *8*(2). www.raosoft.com.

Zubarev, E. R. (n.d.). *AI application framework for detecting and stopping phishing attacks for individuals*.