

Fake QR Code Detection System

Mrs. V. M. Khanapure¹, Supesh Jaware², Aryan Pande³, Rohit Shahapure⁴, Aryan Bankar⁵

Guide, Department of Information Technology¹

Students, Department of Information Technology²⁻⁵

Government Polytechnic, Pune, India

Abstract: *QR codes have become an essential part of modern digital services, particularly for online payments, website access, information sharing, authentication, and contactless transactions. However, the increasing use of QR codes has also created opportunities for cybercriminals to distribute fake or tampered QR codes that redirect users to phishing websites, fraudulent payment pages, malicious links, or unauthorized payment requests. To address this security concern, this paper presents a Fake QR Code Detection (FQRD) system designed to assess the security of scanned QR codes before users interact with the associated content. The proposed framework performs multiple security checks, including URL analysis, blacklist verification, domain-age analysis, suspicious keyword detection, brand impersonation detection, and payment-risk assessment. Instead of depending only on previously reported malicious URLs, the system combines multiple indicators to identify suspicious QR codes that may not yet be present in existing blacklists. The results obtained from these checks are combined to classify each scanned QR code into three categories: Safe, Suspicious, or Dangerous. This multi-signal approach improves the ability to detect both known and potentially emerging QR-based threats while providing users with a clear and understandable security result. The system is intended to provide an additional layer of protection against QR-based phishing, payment fraud, and website impersonation. By performing security analysis before the user proceeds to the detected URL or payment request, the proposed FQRD framework can help reduce the risk of financial loss, credential theft, and other forms of cyber fraud. The proposed approach demonstrates how automated QR analysis and multiple security indicators can be integrated into a practical security solution for safer and more informed use of QR codes in everyday digital transactions..*

Keywords: Fake QR Code, QR Security, QR Fraud Detection, Phishing Detection, URL Analysis, UPI Security

I. INTRODUCTION

QR codes are widely used for payments, website access, authentication, and ticketing, but their convenience has made them a target for cybercriminals. Attackers can swap genuine codes for fraudulent ones that redirect users to malicious sites, steal sensitive data, or trigger unauthorized payments. Traditional defenses like static blacklists and HTTPS checks fall short, since newly created phishing domains often go unlisted and HTTPS alone doesn't prove legitimacy. A stronger approach analyzes multiple signals together: domain age, URL structure, suspicious keywords, blacklist status, brand similarity, and payment-request risk. This research presents a Fake QR Code Detection system that scans and analyzes QR codes before users interact with them. It combines URL and domain analysis, blacklist verification, brand-impersonation detection, and payment-risk assessment. Results are shown as clear classifications (Safe, Suspicious, or Dangerous) with explanations of the detected risks. Scan history and reporting features further support user awareness and security monitoring. The goal is to reduce exposure to QR-based phishing and payment fraud through a simple, accessible security tool.



II. LITERATURE REVIEW

The application of artificial intelligence and heuristic analysis to online fraud detection has been an active area of research, particularly in email phishing, malicious websites, suspicious URL detection, and digital payment security. Early security systems mainly depended on blacklists containing previously identified malicious domains. Although blacklist-based methods are useful for detecting known threats, they are less effective against newly registered phishing domains. Attackers can create new domains for individual campaigns and use them before they are identified and added to security databases. This limitation is especially important in QR-code-based fraud, where malicious QR codes can be distributed rapidly through posters, advertisements, messages, and online platforms.

To address these limitations, researchers have developed heuristic and machine-learning-based techniques for analysing URLs and identifying suspicious characteristics. Commonly examined features include domain age, URL length, HTTPS usage, unusual URL structures, special characters, and lexical similarity to trusted brand names. Typosquatting detection is also widely used to identify domains designed to resemble legitimate websites. Research indicates that combining several independent indicators generally provides more reliable detection than depending on a single feature. For example, a fraudulent website may use HTTPS to appear trustworthy while having a recently registered domain or a suspiciously similar brand name. This multi-signal approach forms the basis of the fraud-detection process used in the proposed system.

QR-code fraud, commonly referred to as “quishing”, has received increasing attention because QR codes can hide their destination from users before scanning. Unlike normal hyperlinks, a QR code presents information through a visual pattern, making it difficult for users to determine whether it leads to a legitimate or malicious destination. Attackers can replace genuine QR codes with fraudulent ones or distribute malicious codes through physical and digital channels. Therefore, QR security solutions should analyse the encoded destination before allowing users to proceed. The proposed system follows this approach by automatically analysing the URL obtained from a scanned QR code.

Another important research area is QR-based digital payment fraud. The increasing use of UPI and other real-time payment systems has created opportunities for attackers to exploit users through fraudulent payment requests. One example is a fake collect request, where a victim may believe that a payment, refund, or cashback is being received but unknowingly approves a transaction that debits money from their account. Fraudsters may also use misleading payment descriptions, fake rewards, or impersonation of trusted services. Therefore, QR-code security systems should include payment-specific checks in addition to normal URL analysis.

Brand impersonation and social engineering are further challenges in detecting fraudulent QR codes. Attackers may create websites and domains that closely resemble popular banks, payment platforms, shopping services, or other trusted organizations. Small spelling changes, additional characters, or similar-looking domain names can make these websites difficult for ordinary users to distinguish from genuine services. Brand-similarity analysis and URL structure analysis can therefore provide additional evidence when determining whether a QR destination is suspicious.

Artificial intelligence and machine-learning techniques can improve fraud detection by analysing multiple security indicators together. Instead of depending only on a fixed blacklist or individual rule, an intelligent system can evaluate different characteristics and generate an overall risk assessment. However, the effectiveness of machine-learning approaches depends on the quality of training data and the ability of the system to adapt to new fraud patterns. For this reason, combining AI-based analysis with rule-based security checks can provide a more flexible approach for QR-code fraud detection.

User awareness and explainability are also important aspects of cybersecurity systems. Simply displaying a message such as “Unsafe QR” may not explain why the QR code is considered risky. Users may make better decisions when the system clearly identifies the reason, such as a newly registered domain, suspicious URL structure, blacklist match, brand similarity, or unusual payment information. A simple classification such as Safe, Suspicious, or Dangerous can make technical security analysis easier to understand for non-technical users.

The proposed Fake QR Code Detection system combines these research concepts into a single security-oriented application. The system analyses scanned QR codes using URL analysis, blacklist verification, domain-age checking,



brand-impersonation detection, and payment-related risk analysis. The results of these checks are combined to provide a clear risk classification before the user proceeds to the destination. The system also aims to maintain scan history and provide security information to improve user awareness.

Another important consideration is the changing nature of cyber threats. Attackers continuously modify domains, URLs, brand names, and payment messages to bypass existing detection techniques. Therefore, future fraud-detection systems need regularly updated threat information and improved detection models. Real-time threat-intelligence integration, larger datasets, improved machine-learning models, and advanced UPI fraud detection can further improve the reliability of QR security systems.

Overall, existing research shows that no single technique is sufficient for detecting all forms of QR-based fraud. Blacklists are useful for known threats, heuristic analysis identifies suspicious characteristics, machine learning can identify complex patterns, and clear explanations improve user decision-making. The proposed Fake QR Code Detection system combines these approaches to provide a practical, user-friendly security layer between QR scanning and user interaction, helping reduce the risks of phishing, financial fraud, credential theft, and unauthorized transactions.

The system can also support continuous improvement by recording detected patterns and using updated threat information during future analysis. Maintaining a balance between detection accuracy and false warnings is important so that legitimate QR codes are not unnecessarily blocked. Fast analysis is equally important because users generally expect immediate results while scanning QR codes, especially during digital payments. Privacy should also be considered when handling scanned URLs, payment details, and scan history. Secure storage and controlled access can help protect sensitive information processed by the application. These considerations can make the proposed system more reliable, practical, and suitable for real-world QR-code security applications.

Market Survey

Dedicated, general-purpose QR fraud-detection apps remain uncommon compared to the scale of QR-code adoption itself. Most existing QR scanner apps on mobile app stores focus purely on decoding speed and convenience features (batch scanning, QR generation) rather than safety analysis. Where safety checks exist, they are typically bundled inside a single bank's or payment provider's own app and are not available as an independent, provider-agnostic layer that a user can rely on regardless of which app they ultimately use to complete a transaction. This leaves a clear market gap for a free, standalone application that performs real-time risk analysis on any QR code, independent of the destination service.

Research Gap

While substantial research exists on web-based phishing detection individually, few publicly documented systems combine URL threat-intelligence checking, domain-age analysis, brand-impersonation detection, and UPI-specific payment-fraud heuristics into a single, real-time, mobile-first tool aimed at the general consumer. This project addresses that gap directly, and additionally integrates a conversational AI layer to make the resulting risk assessment understandable to non-technical users.

III. PROPOSED METHODOLOGY

The proposed Fake QR Code Detection System uses a multi-step approach to identify whether a QR code leads to a safe or potentially malicious destination. The methodology combines QR scanning, URL analysis, blacklist checking, domain analysis, and risk evaluation.

A. QR Code Scanning

The user scans a QR code using the mobile application camera. The QR code is decoded to obtain the information stored inside it.



B. URL Extraction

After decoding, the system checks whether the QR code contains a URL. If a URL is found, it is extracted and sent to the detection module for analysis.

C. Blacklist Verification

The extracted URL is compared with a database containing previously reported malicious or phishing URLs. If a match is found, the QR code is immediately classified as Fake/Malicious.

D. URL Feature Analysis

If the URL is not found in the blacklist, the system analyzes different URL characteristics, including:

- URL length
- HTTPS usage
- Suspicious keywords
- Special characters
- Number of subdomains
- IP address usage
- Domain structure
- Suspicious domain extensions
- Redirection patterns

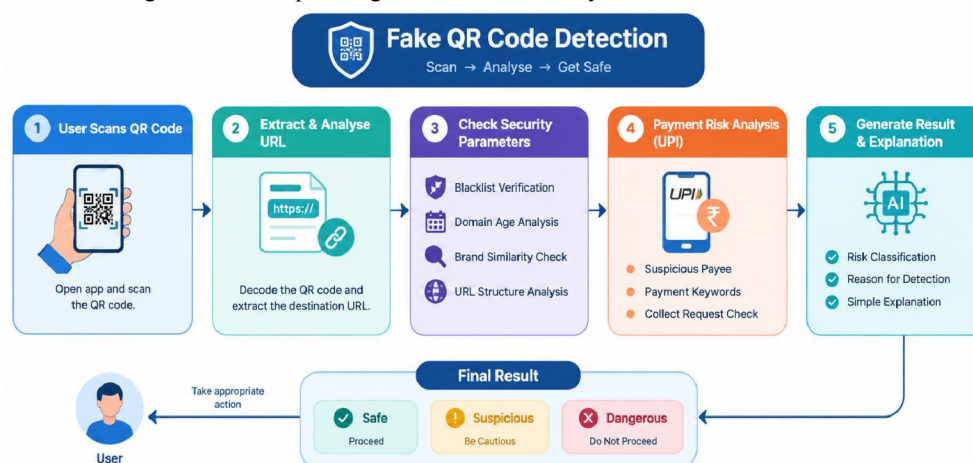
E. Domain and Brand Analysis

The system examines domain-related information such as domain age and similarity to known brand names. Small spelling changes in trusted brand names may indicate typosquatting or brand impersonation.

F. Risk Score Calculation

The results obtained from different checks are combined to calculate an overall risk level. Based on the detected characteristics, the URL is classified as:

- Safe – No significant suspicious characteristics detected.
- Suspicious – One or more potentially risky characteristics detected.
- Fake/Malicious – Strong indicators of phishing or fraudulent activity detected.



G. Result Generation

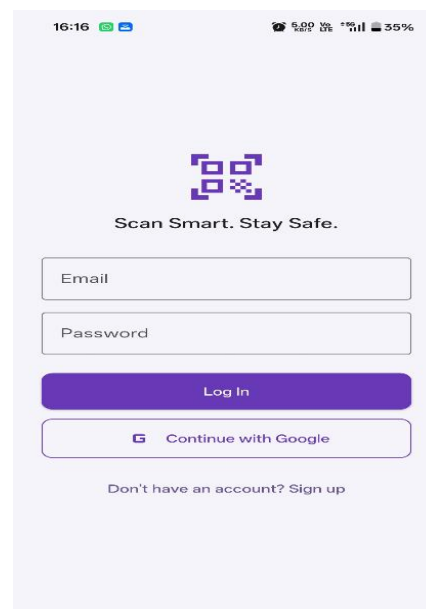
The final classification is displayed on the mobile application along with the scanned URL and relevant warning information. This allows the user to make an informed decision before opening the website.

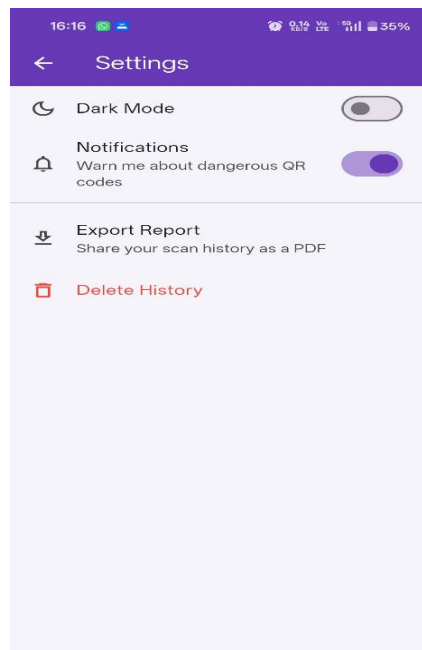
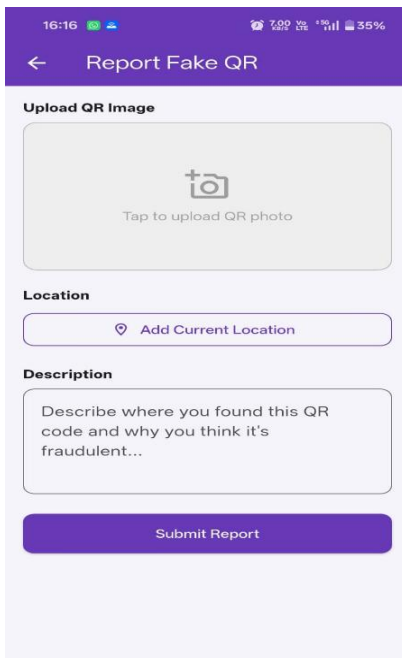
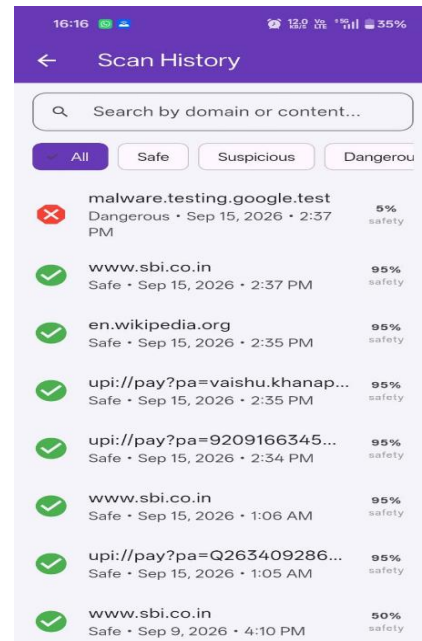
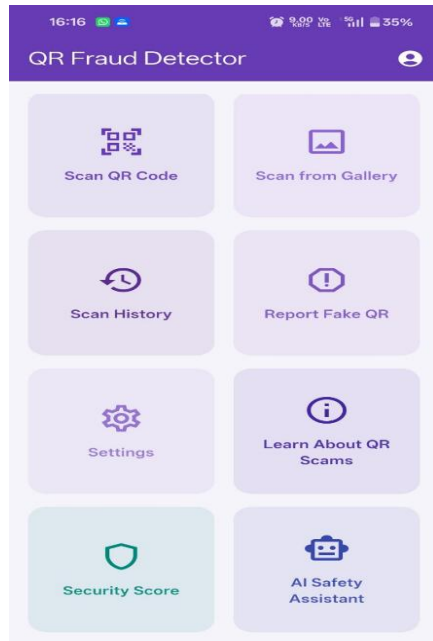
H. Scan History

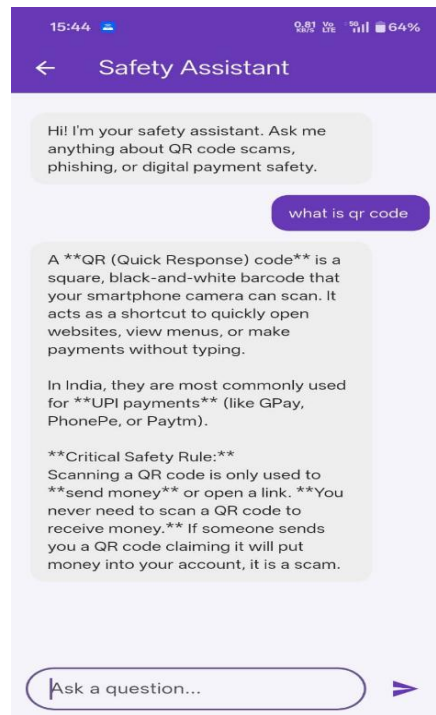
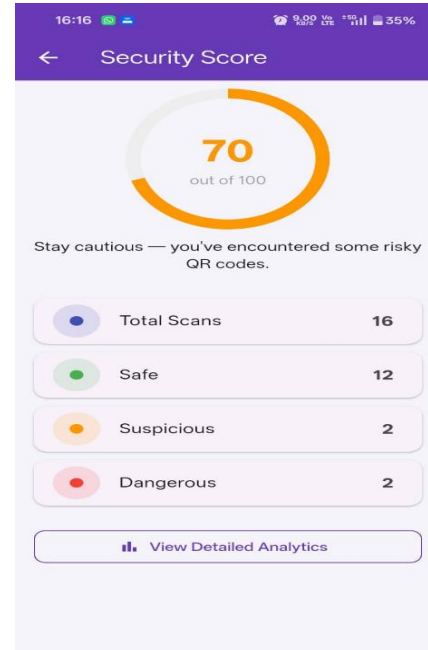
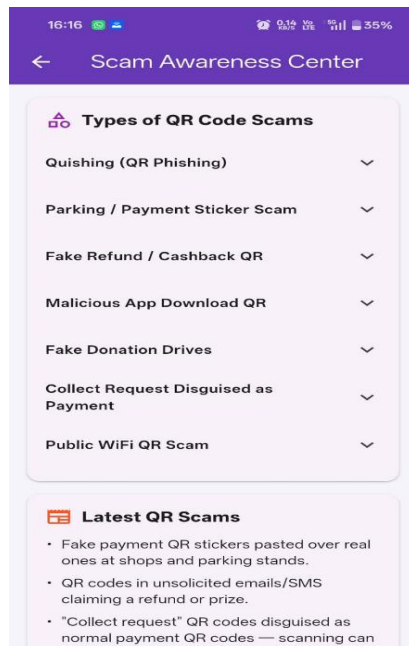
The scan result can be stored in the application database. Users can view previous scans and their corresponding security results

IV. RESULTS AND DISCUSSION

The developed system is designed to provide a quick security assessment after scanning a QR code. The result screen displays the detected URL along with its security classification. The system can identify known malicious URLs through blacklist checking and can additionally detect suspicious URLs that may not yet be present in a blacklist. URL structure, domain information, suspicious keywords, and brand similarity provide additional indicators for the final decision. The multi-signal approach is useful because a newly created phishing domain may not yet appear in a blacklist. In such cases, heuristic and domain-based analysis can provide an additional layer of protection. The system is intended as a preventive security tool rather than a complete guarantee of safety. A legitimate website can sometimes contain unusual URL characteristics, while a well-designed phishing website may appear normal. Therefore, combining multiple indicators is more useful than depending on a single feature. The system also provides users with a clear and understandable security result, allowing them to make safer decisions before opening the detected link. It can help reduce the risk of phishing attacks, fraudulent payment requests, and unauthorized access to sensitive information. The use of multiple security checks makes the detection process more reliable than relying on a single security parameter. The system can also support user awareness by explaining potential risks associated with a scanned QR code. Overall, the developed solution provides a practical and accessible approach for improving security during everyday QR code usage.







V. CONCLUSION

The proposed Fake QR Code Detection system provides a practical approach for identifying potentially unsafe QR-code destinations. Instead of depending only on known malicious URLs, the system combines blacklist checking with URL and domain-based analysis.

The system can help users identify suspicious QR codes before visiting potentially harmful websites or sharing sensitive information. The mobile-based interface also makes the detection process simple for regular users.

However, QR-code security is a continuously changing problem because attackers can create new domains and modify their techniques. Therefore, continuous updating of security databases and improvement of detection methods are required.

VI. FUTURE SCOPE

The proposed system can be further enhanced by integrating machine-learning models trained on large datasets of legitimate and malicious URLs to improve detection accuracy. Real-time threat-intelligence databases can be connected to provide continuously updated information about newly identified malicious domains. Advanced brand-impersonation and typosquatting detection can be implemented to identify fake domains that closely resemble trusted brands. The system can also perform website content analysis to detect phishing forms, suspicious pages, and other malicious indicators after scanning. Malware detection can be added to identify URLs that redirect users toward harmful files or downloads. To improve transparency, an explainable detection mechanism can clearly show the reasons behind a Safe, Suspicious, or Dangerous classification. In addition, browser protection features can warn users before accessing suspicious QR destinations, while continuous security updates and notifications can provide improved protection against newly emerging QR-based threats.

REFERENCES

- [1] Herlina, B. & Soeparno, H. (2023). "Machine Learning Model to Improve Classification Performance in the Process of Detecting Phishing URLs in QR Codes." *Journal of Theoretical and Applied Information Technology*, Vol. 101, No. 18.
- [2] Bhardwaj, A. et al. (2023). "Detection of Phishing Link and QR Code of UPI Transaction using Machine Learning." *2023 International Conference on Innovative Mechanisms for Industry Applications (ICIMIA)*.
- [3] Safi, S. & Singh, S. (2023). "A Systematic Literature Review on Phishing Website Detection Techniques." *Journal of King Saud University – Computer and Information Sciences*, Vol. 35, Issue 2, pp. 590–611.
- [4] Kalla, D. & Kuraku, S. (2023). "Phishing Website URL's Detection Using NLP and Machine Learning Techniques." *Journal on Artificial Intelligence*, Vol. 5, pp. 145–162.
- [5] "A High-Accuracy Phishing Website Detection Method Based on Machine Learning." (2023). *Journal of Information Security and Applications*, Vol. 77, 103553.
- [6] "Phishing Website Detection Using Machine Learning Methods." (2023). *2023 International Conference on Integrated Intelligence and Communication Systems (ICIICS)*.
- [7] "Enhancing Cybersecurity: A Multilayered Approach to Phishing Website Detection Using Machine Learning." (2023). *2023 International Conference on Research Methodologies in Knowledge Management, Artificial Intelligence and Telecommunication Engineering (RMKMATE)*.
- [8] "Secure QR Code Scanner to Detect Malicious URL Using Machine Learning." (2023). *International Journal of Communication Networks and Information Security (IJCNIS)*.
- [9] Sarkhi, M. & Mishra, S. (2024). "Detection of QR Code-based Cyberattacks Using a Lightweight Deep Learning Model." *Engineering, Technology & Applied Science Research*, Vol. 14, No. 4, pp. 15209–15216.
- [10] "Phishing URL Detection Using Machine Learning and Deep Learning." (2024). *2024 IEEE World AI IoT Congress (AIIoT)*.



- [11] "SafeCoder: A Machine-Learning-Based Encoding System to Embed Safety Identification Information into QR Codes." (2024). Journal of Network and Computer Applications, Vol. 227, 103874.
- [12] "QR Code Malicious URL Detection System Using Machine Learning." (2024). International Journal of Communication Networks and Information Security (IJCNIS).
- [13] Kim, D. & Hwang, K. (2024). "AutoML Machine Learning-Based for Detecting Qshing Attacks Malicious URL Classification Technology Research and Service Implementation." Smart Media Journal, Vol. 13, No. 6, pp. 9–15.
- [14] Trivedi, A., Jangal, K. & Gupta, R. (2025). "Phishing Detection in Advanced QR Code Attacks: Challenges and AI-Driven Solutions." International Journal for Research in Applied Science and Engineering Technology (IJRASET).
- [15] Trad, F. & Chehab, A. (2025). "Detecting Quishing Attacks with Machine Learning Techniques Through QR Code Analysis." arXiv:2505.03451.
- [16] Akram, M. W., Sood, K. & Hassan, M. U. (2025). "QRiS: A Preemptive Novel Method for Quishing Detection Through Structural Features of QR." arXiv:2510.17175.
- [17] Sardar, S., Saha, S., Ray, H. & Goswami, K. (2025). "Malicious QR Code Detection Using Machine Learning." International Journal of Creative Research Thoughts (IJCRT), Vol. 13, Issue 9, pp. g342–g351.
- [18] Alsulami, A. A., Al-Haija, Q. A., Alturki, B., Yafoz, A., Alqahtani, A., Alsini, R. & Binyamin, S. S. (2025). "Efficient Malicious QR Code Detection System Using an Advanced Deep Learning Approach." Computer Modeling in Engineering & Sciences, Vol. 145, No. 1, pp. 1117–1140.
- [19] Ahmed, F., Fatima, I., Hassan, M. U., Rasheed, I. & Fayyaz, U. (2025). "Malicious QR Code Detection: A Comprehensive Review of Methods and Challenges." Spectrum of Engineering Sciences.
- [20] Njuguna, D. & Ndia, J. (2025). "Quick Response Code Security Attacks and Countermeasures: A Systematic Literature Review." Journal of Cyber Security, Vol. 7, pp. 1–20.
- [21] Yeşiltepe, M., Kurulay, M., Bennour, A., Rasheed, J. & Alsubai, S. (2025). "Enhancing QR Code Security: Exploiting Hidden Message Mechanisms and Machine Learning Classification." Security and Privacy, Vol. 19, Issue 2.
- [22] Khalifa, O. Y. I. & Shah, M. Z. M. Z. (2025). "MultiPhishNet: A Multimodal Approach of QR Code Phishing Detection Using Multi-Head Attention and Multilingual Embeddings." International Journal of Innovative Computing, Vol. 15, No. 1, pp. 53–61.
- [23] Guan, Y. & Zhu, E. (2025). "A Dual-Branch Deep Learning Model for Phishing Detection in QR Code Scanning Scenarios." 2025 6th International Conference on Machine Learning and Computer Application (ICMLCA), pp. 526–531.
- [24] Mousavi, S. & Bahaghighat, M. (2025). "Phishing Website Detection: An In-Depth Investigation of Feature Selection and Deep Learning." Expert Systems, Vol. 42, Issue 3, e13824.
- [25] Barik, K., Misra, S. & Mohan, R. (2025). "Web-Based Phishing URL Detection Model Using Deep Learning Optimization Techniques." International Journal of Data Science and Analytics, Vol. 20, pp. 4449–4471.

