International Journal of Scientific Research and Engineering Development-– Volume 9 Issue 1, Jan-Feb 2026
Available at www.ijsred.com

RESEARCH ARTICLE OPEN ACCESS

A Study on Security Challenges and Adoption Trends of QR Code in India

Mr. Mohanraj S[1], Mr. Pradheep G[2]
[1]Assistant Professor, Department of Computer Science, Sri Ramakrishna College of Arts & Science, Coimbatore.
[2]Ill B.Com CA, Sri Ramakrishna College of Arts & Science, Coimbatore.

Abstract

In India, QR codes are used for delivering digital services such as payments, identity, retail, healthcare and public services. The rapid adoption of QR codes can be attributed to the common availability of smartphones, low costs of QR code implementation, and demand for contactless transactions and services during COVID-19 pandemic. However, in their rapid deployment, these systems have introduced security and privacy questions that remain largely unaddressed in the academic literature. The present study investigates the QR code adoption trends, and explores the security issues and concerns involved in the use of QR codes in everyday digital transactions. The study used a combination of quantitative survey, semi-structured interviews from key industry stakeholders, and a case study of popular QR code-based applications in India. The research surveys user awareness, existing user protection mechanisms, and the level of exposure of various QR systems to phishing, malicious redirection, data leakage and exposure, and unauthorized access or control. Conclusions reached are that while QR technology has had positive impacts on service accessibility and efficiency, static architecture and weak user verification practices have prevented common trust in the technology. The study provides insights on integrating QR codes in a more secure and sustainable way into India's emerging digital payment ecosystem.

Keywords QR Codes; Digital Payments; UPI; Contactless Transactions; Cybersecurity; Phishing Attacks; Data Privacy; Financial Inclusion; Mobile Payments; Digital Identity;

Introduction

The ubiquity of smartphones and mobile internet has a disruptive effect on the way information is retrieved and transactions are made. Off all the digital technologies used to create a distinctive shopping experience, Quick Response (QR) codes are one of the most widely adopted interfaces between physical and virtual environments. QR codes were developed within Japan in the early 1990s, and have since been widely adopted in the retail, healthcare, banking, transportation, and public administration industries. In India, the QR code ecosystem expands when digital services like Unified Payments Interface (UPI) and Aadhaar authentication services introduce contactless payments and other digital services which include citizens financially, make operations efficient, and allow citizens and service providers to adopt rapidly. People easily generate and scan QR codes However, as the use of QR codes for accessing private services increases, concerns are rising regarding QR code security and privacy, since they hide the targeted information and the links cannot be validated before scanning. They can fall prey to phishing. They can fall prey to malicious redirection. They can fall prey to malware. They can fall prey to unauthorized data access. With QR-based transactions beginning to replace payment and authentication methods more common in the modern world, the potential for loss of user trust grows. Although QR codes are widely used in the digital landscape of India, their security implications have not been systematically studied. Furthermore, users have limited awareness of the threats associated with QR codes, leaving them vulnerable to cyber threats.

Review of Literature

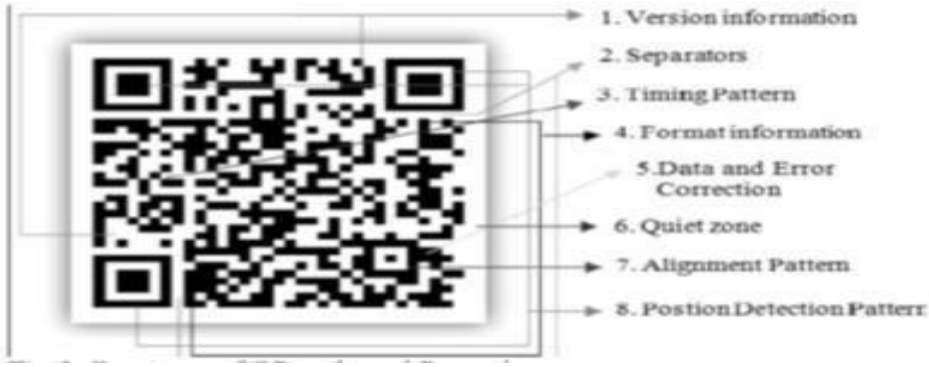
Dey, Panda, Sen, and Bhatt (2025) found evidence for the effective use of QR codes in Indian college libraries, helping easy access to electronic resources and user engagement. They noted that while technology implementation is important, user awareness is the key success factor for QR code adoption.

According to Mishra, Jha, and Gupta (2024), small merchants adopted QR-based digital payments in post-demonetization India because of the low cost of operations and conveniences in transacting through a QR code within. People saw cybersecurity concerns, infrastructure inadequacies, and low digital literacy blocked common adoption.

In 2023, Hoxhunt's phishing metric reported that QR codes comprised approximately 22% of all phishing attacks**,** indicating how attackers leveraged QR scanning behavior to bypass traditional security filters and exploit user trust.
Amoah and Hayfron-Acquah (2022) examined security threats in QR code technology, with a specific focus on *quishing*—QR code phishing where malicious codes direct users to fraudulent websites.
Kishor Kumar *et al.(2021)* focused on security requirements and enhancements for QR code systems in their study "Cryptography by Using QR Code Encryption and Decryption Method."

QR code

The Quick Response (QR) code is a distinguished form of two-dimensional matrix barcode. This symbology exhibits a high degree of functional versatility and possesses an extensive data capacity. It is capable of encoding a wide variety of information structures, including numerical sequences, alphanumeric strings, binary data, and complex ideographic character sets, such as Kanji. Physically, the QR code is presented as a compact, square modulus composed of a densely populated matrix of contrasting geometric patterns, typically black modules set against a light field. The specific spatial arrangement and configuration of these constituent modules function as the mechanism for data storage, effectively establishing a unique visual signature for the encoded information. Data retrieval is executed through the efficient process of image acquisition utilizing a camera-equipped device, most frequently a contemporary smartphone or tablet. Owing to their predominant application in mobile computing environments for rapid informational retrieval, these codes have consequently acquired the common designation of "mobile codes." Quick Response (QR) codes function as highly versatile instruments, primarily owing to their capacity to encode a broad spectrum of digital information. Their extensive utility allows them to facilitate access across diverse applications, routinely linking to discrete text, geographical addresses, contact telephone numbers, email designations, Uniform Resource Locators (URLs), application downloads, payment processing portals, and the complex configuration parameters requisite for instant Wi-Fi network access.



Adoption of QR code

QR codes are being deployed in numerous sectors due to their low deployment cost, usability and ability to support contactless digital transactions. Smartphones widely proliferate and government initiatives digitalize. Therefore, QR codes matter within the digital ecosystem in India. Retail and E-commerce are the largest adopters of QR codes with use in digital payment, product information, advertising, and inventory management. Its integration with the Unified Payments Interface (UPI) has brought real-time payment infrastructure to large retail chains as well as micro, small and medium enterprises. Banking and Financial Services use QR codes for account verification, payments and purchases with merchants. Their use requires little infrastructure, and they are widely used by micro-merchants to support financial inclusion. In Healthcare, QR codes are used in processes like patient registration, scheduling appointments, e-prescriptions, vaccination status, and accessing medical records. The use of QR codes improves administrative efficiency and data accuracy and accessibility. In Educational institutions have used QR codes for taking attendance, accessing electronic resources, registering for exams, and library services for hybrid learning. QR codes are used in

Hospitality and Tourism for digital menus, ticketing, restaurant reservations, and visitor information, allowing for minimal contact with customers. In Public Administration, QR codes are used in e-governance systems, for identity verification, document verification, service delivery, and public information dissemination. In general, the uptake by sectors shows the versatility and scalability of QR code.

Challenges of QR code

Using QR codes effectively isn't just a matter of pointing and scanning; it demands sticking to some established best practices. If we don't, we're asking for trouble, because there are a few serious operational hurdles we need to clear right out of the gate.

1. Addressing Security and Transparency Issues

The primary security risk is the potential to be used as a vector for other malicious activities including more advanced types of phishing attempts, malware, and data breaches. When using a QR code, users are encouraged to only use reputable QR code scanner apps and to verify the source and origin. When QR code scanning applications have URL preview functionality, users should use it to confirm the actual destination before visiting the link.

This can greatly reduce the chance of scanning malicious URLs. Also, a QR code's 'black box' nature, where the user does not know which digital content is encoded until the code is used, could be addressed by a text alternative, as well as an integrated preview for code content, if it is hosted on a URL shortening service; this information should be sufficient for users to assess such codes' suitability

2. Analysis of Technical Constraints and Limitations

Technical implementation presents several limitations. Interoperability failures sometimes arise, leading to inconsistent functionality across diverse mobile devices and scanning applications. Creators of QR codes are obligated to conduct extensive testing across multiple platforms and adhere strictly to universally accepted data formats to guarantee optimal accessibility. Furthermore, QR codes possess stringent *data capacity limitations, restricting storage to approximately three kilobytes of information. A crucial constraint is the persistent **reliance on internet connectivity*. In the majority of instances, a QR code becomes non- functional in environments characterized by network unavailability or unreliable wireless fidelity (Wi-Fi) signals. Should connectivity impediments be anticipated, the code design should prioritize offline functionality.

3. The Critical Role of User Cognizance and Education

Finally, the dimension of user awareness and education must be comprehensively addressed. A substantial segment of the user population remains insufficiently cognizant of the intrinsic security liabilities and optimal scanning protocols. Through the implementation of robust user education programs concerning QR code safety, the promotion of judicious behavioral practices, and the delivery of highly articulated instructions, the potential for security compromises can be substantially mitigated, thereby enhancing the overall safety profile of QR code deployment.

Existing System(The Prevailing System: Where We Stand Today)

QR codes are ubiquitous and are now the standard interface for providing contactless services in virtually every sector of business transactions. Their simplicity and minimal infrastructure requirements have led to their adoption for financial transactions using UPI-based mobile payments. They have considerably reduced the dependency on cash for goods and services. The retail and hospitality industries use QR codes for digital menus and bills, while travel and transport industries use them for tickets and boarding. Logistics and supply chains use QR codes to track inventories and authenticate products, while public health systems use QR codes to provide health services. Despite their advantages, the conventional QR code ecosystem has shortcomings. High usage of static QR codes that do not provide authentication and encryption can expose users to risks such as QR phishing (quishing), code replacement, redirection to noxious websites, fraud during payment, and unintentional information leakage. Since the information encoded in the code is not visible until scanned, many users unknowingly scan harmful QR codes. Many users believe QR codes are intrinsically secure. The lack of

awareness of this problem and the use of static architecture has contributed to an increase in vulnerabilities.

Proposed System (To overcome these challenges, a Secure Dynamic QR Code Framework is proposed)

The authors proposed a new framework called the Secure Dynamic QR Code Framework to combat the above attack scenarios against QR codes and to increase the QR codes' trust and security in transactions. Static QR codes remain the same, whereas dynamic QR codes will be regenerated upon scanning or every specified period. The embedded payload is encrypted to protect the confidentiality of messages if intercepted or stored. Domain verification is applied at scan time in order for the destination to be validated as a trusted provider before anything is fetched. Generally, QR codes expire after a period of time lapses, and will no longer work if people reuse or replace the code. The code contains a digital signature that is verified to ensure that the issuer is legitimate. The app verifies the domain, digital signatures, and expiration through a short, multi-step process when it scans. If verification fails, the security warning displays immediately, and the user cannot access the content. This layered security solution reduces the risks from fraudulent activity, unauthorized access, or data compromise considerably, and it provides users with a more secure alternative compared to the conventional static QR code solution.

Methodology

The methodology employed relied exclusively upon secondary research, which commenced with a systematic review of numerous peer-reviewed journals, all sourced in Portable Document Format (PDF).Fundamentally, the process began by executing a structured and meticulous reading of all identified scholarly papers, systematically extracting and documenting all observed architectural patterns, conceptual models, and associated methodologies. Subsequent to this foundational extraction phase, a comprehensive comparative analysis of Quick Response (QR code) .Ultimately, these extensive findings were synthesized and categorized into four major thematic areas: architecture, critical challenges, adoption strategies, and future directions.

To reduce security, technical, and user awareness issues associated with customary QR code usage, we propose the Secure Dynamic QR Code Framework as a replacement for static QR codes with a multilayered and dynamic security framework. Unlike static QR codes - which do not change over time and can be copied or altered - the proposed QR codes rely on a dynamic generation approach triggered automatically after every scan or after a specific time period, reducing code replacement and replay attacks. Data embedded in each QR code is encrypted so the content can be kept secret even if the QR code is captured in transit, and domain verification helps ensure that the destination URLs have not been changed before the content is opened. Each QR code has a expiration date, and copied, reused codes will not work after this expiry date. To ensure the issuing organization cannot be impersonated, the codes include a digital signature, and the application validates the domain name, the signature and the expiry parameters in multiple steps, as the browsing session is underway. If verification fails, the application blocks the content and shows a security warning. This prevents the user from opening malicious content and acts as a more secure version of existing QR code applications.

Result and Discussion

The findings from this study indicated that QR codes have emerged as an important component of digital services in India across different sectors such as retail, financial services and banking, healthcare, education, and hospitality and public administration. The primary reasons for common adoption have been their ease of use, low infrastructure requirement, and alignment with UPI systems. However, these results also exposed meaningful security and privacy problems in the current static design of QR codes, e.g., the lack of encryption, digital signatures, or expiry limits on the techniques we reviewed make them vulnerable to phishing, code replacement, redirection attacks, and payment fraud. The rise of "quishing "attacks and associated scams involving fraudulent UPI redirections shows the increased use of QR codes in cybercrime. The Secure Dynamic QR Code Framework addresses these issues by implementing encrypted payloads, limiting the validity time, using digital signatures and performing domain validation of the scanned content. Additionally, real-time notifications when a scan occurs, can prevent an user from accessing harmful content or files such as those

found on phishing pages. While QR codes have improved the speed of transactions and service delivery in India, the pace of adoption has outstripped the extent of security-related governance. The study provides a case for the necessity of standards and security protocols for dynamic QR codes and national-level digital literacy to ensure QR codes are a sustainable, secure, and trusted method for enabling digital services in the long term.

Conclusion

The evolution of QR codes with respect to its popularity and security in rapidly growing digitization in India has been analyzed in this research. The study concludes that QR codes have gained wide acceptance and have become a key enabling technology in sectors like retail, banking, healthcare, education, hospitality, and public administration. Low implementation costs, greater ease and compatibility with digital payment systems such as unified payments interface (UPI) have considerably improved service access and transaction speed among small merchants and the unbanked. The research concurrently highlights critical security weaknesses of the widely used static QR code model. The failure to embrace encryption, authentication, and expiration opens users and service providers to threats such as phishing attacks, malicious link redirection, malware installations, and fraudulent payments. Thus, in addressing these problems, this research proposes a Secure Dynamic QR Code Framework with multiple security levels that can use encrypted payloads, digital signature, domain verification, validation period, and real-time scan notifications to prevent duplication, interception, and unauthorized access, thereby improving the security of QR code-based payment transactions. The framework is particularly suited for high-risk industries such as financial services, and healthcare and public administration. Ultimately, the sustained success of QR codes in India's digital economy will depend on standardized security systems and digital literacy programs at the national level. Policymakers, service providers, and technology developers must work together to establish secure governance frameworks for QR codes to ensure their safe adoption, maintain user trust, and support the growth of India's digital economy.

Future Enhancements

The Secure Dynamic QR Code Framework can be further extended in future research by integrating a block chain-based verification mechanism for tamper-proof assurance of QR issuance and an audit trail of high-value transactions. A threat detection mechanism based on artificial intelligence can also be integrated into the scanner application to detect suspicious redirection patterns and phishing campaigns in real-time. Additionally, offline-verifiable cryptographic tokens may be introduced to improve usability in low-connectivity environments. Standardization of dynamic QR security protocols at the national level, combined with multilingual user-awareness interfaces, can further enhance accessibility, interoperability, and long-term trust in QR-based digital service ecosystems across India.

Reference

Roberson Bolzan., Paula Ventura., Silvia Fernandes., Fatima L. Carvalho-Qr Codes: A Case of its Level of Adoption in Portugal Journal of Tourism in 2022.

Katharina Krombholz, Peter Frühwirt, Peter Kieseberg, Ioannis Kapsalis, Markus Huber & Edgar WeipplKatharina Krombholz, Peter Frühwirt, Peter Kieseberg, Ioannis Kapsalis, Markus Huber & Edgar Weippl-QR Code Security: A Survey of Attacks and Challenges for Usable Security Journal in 2014.

Kuligowska, K., & Huć, A. (2024)-Innovative QR code-based product authenticity safeguards: Case study of design considerations and technological challenges.

Akram, M. W., Sood, K., & Hassan, M. U. (2025). QRïS: A Preemptive Novel Method for Quishing Detection Through Structural Features of QR.

Sharevski, F., Devine, A., Pieroni, E., & Jachim, P. (2022). Gone Quishing: A Field Study of Phishing with Malicious QR Codes.

