Journal Publication of International Research for Engineering and Management (JOIREM)
Volume: 04 Issue: 02 | Feb-2026
ISSN (O) 3107-6696

A Survey on Secure QR Code Document Locker

[1]K. M. Sudharsan, [2]Dr. V. Malathi

Department of Computer Science with Cybersecurity, Dr. N.G.P Arts and Science College, Coimbatore, India,
mohansudhar89@gmail.com

Department of Computer Science with Cybersecurity, Dr. N.G.P Arts and Science College, Coimbatore, India,
malathi.v@drngpasc.ac.in

Abstract - With the rapid growth of digital transformation, the storage and sharing of sensitive documents have become a major security concern. Traditional document-sharing methods are vulnerable to unauthorized access, data leakage, and misuse. To overcome these challenges, secure document locker systems integrated with QR code technology have gained significant attention. QR codes provide fast and contactless access, while encryption techniques ensure data confidentiality and integrity. This survey paper reviews various research works related to secure QR code–based document locker systems. It analyzes different security mechanisms, authentication techniques, encryption methods, and access control models used in existing systems. A comparative study is presented to highlight the advantages and limitations of each approach. Finally, the paper identifies research gaps and discusses future directions for improving the security and efficiency of QR code–based document storage systems.

Keywords: QR Code, Document Security, Encryption, Authentication, Secure Document Locker, Access Control

1. Introduction

In the digital era, the storage and sharing of important documents have become common in educational institutions, healthcare organizations, government offices, and corporate sectors. Documents such as academic certificates, medical reports, identity proofs, and confidential business files are increasingly maintained in digital format. While digital documentation improves efficiency, accessibility, and cost-effectiveness, it also introduces serious security risks. Traditional methods of document sharing such as email attachments, cloud links, and portable storage devices are vulnerable to unauthorized access, data theft, and document manipulation. Weak passwords, phishing attacks, unauthorized link forwarding, and lack of access tracking often result in security breaches. Hence, there is a strong need for secure document storage and access control systems that can protect sensitive information.

QR code technology has emerged as an efficient method for providing quick and contactless access to digital information. When combined with encryption and authentication mechanisms, QR codes can enhance document security by allowing controlled and verified access. Secure QR code–based document locker systems store documents in encrypted form and grant access only to authorized users through validated QR codes. This survey paper reviews existing research works on secure QR code document locker systems, focusing on security techniques, authentication methods, access control mechanisms, and system challenges.

2. Background of QR Code Technology

Quick Response (QR) codes are two-dimensional barcodes designed to store and retrieve information quickly using digital devices such as smartphones and scanners. Unlike traditional one-dimensional barcodes, QR codes can store a larger amount of data and can be scanned from any orientation. Due to their speed, accuracy, and ease of use, QR codes are widely adopted in applications such as digital payments, authentication systems, ticketing, and information sharing.

One of the key features of QR codes is error correction capability, which allows data recovery even if a part of the code is damaged. This makes QR codes reliable for real-world usage. In secure document locker systems, QR codes are mainly used as access identifiers rather than data storage units. The QR code typically contains a unique encrypted token or reference linked to a document stored securely on a server.

By separating the document data from the QR code, the risk of data exposure is minimized. When combined with encryption, authentication, and access control mechanisms, QR code

technology plays a vital role in enabling secure and controlled access to digital documents.

Literature Review

Several research works have been carried out to enhance document security using QR code–based access systems. Existing studies mainly focus on combining QR codes with encryption and authentication techniques to prevent unauthorized document access. Many researchers have proposed systems where documents are encrypted using symmetric or asymmetric encryption algorithms before being stored in secure databases.

Some studies emphasize the use of one-time or time-bound QR codes to limit repeated access and reduce the risk of misuse. These QR codes automatically expire after a specific time or number of uses, thereby preventing unauthorized reuse. Other research works integrate additional authentication mechanisms such as One-Time Passwords (OTP), email verification, or biometric authentication along with QR code scanning. These methods significantly improve security but may increase system complexity and access time.

Cloud-based secure document locker systems using QR code access have also been explored in the literature. These systems offer scalability, remote accessibility, and centralized management. However, they introduce challenges related to cloud security, privacy, trust in third-party service providers, and dependency on internet connectivity. Overall, the reviewed literature shows that QR code–based document locker systems provide effective security solutions, yet there is scope for improvement in usability, key management, scalability, and real-time monitoring.

4. Security Techniques in Document Locker Systems

Security is the core component of QR code–based document locker systems. To protect sensitive documents, various security techniques are implemented at different stages of storage and access. Encryption is commonly used to convert documents into unreadable formats before storage, ensuring confidentiality even if unauthorized access occurs. Symmetric encryption algorithms such as Advanced Encryption Standard (AES) are widely used due to their speed and efficiency, while asymmetric algorithms such as RSA are used for secure key exchange.

Authentication mechanisms play an important role in verifying the identity of users accessing documents. Common authentication methods include username and password authentication, One-Time Password (OTP), email-based verification, and biometric authentication. These methods ensure that only authorized users can access the documents even if the QR code is compromised.

Access control techniques such as role-based access control, time-based QR code validation, one-time access, and device-based restrictions are used to limit document usage. Hashing techniques are employed to maintain document integrity, and logging mechanisms are used to track access history. Together, these security techniques ensure confidentiality, integrity, and availability of documents.

5. Comparative Analysis

A comparative analysis of existing secure QR code–based document locker systems helps in understanding the effectiveness of different security approaches. Various research works adopt different combinations of encryption, authentication, and access control techniques to enhance document security. Some systems focus mainly on strong encryption algorithms, while others emphasize multi-factor authentication for improved access control.

Time-bound and one-time QR code mechanisms are effective in preventing repeated or unauthorized access, whereas cloud-based systems provide better scalability and remote access. However, systems with multiple security layers may increase complexity and affect user convenience. The comparison of existing approaches highlights the need for a balanced solution that ensures high security while maintaining ease of use and system efficiency.

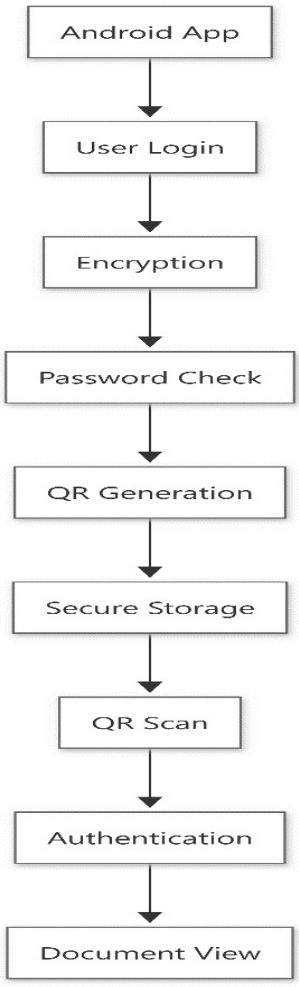
6. Research Gap and Future Scope

From the literature survey and comparative analysis, it is observed that existing secure QR code–based document locker systems still face certain limitations. Many systems do not provide real-time access monitoring and detailed logging of user activities. Secure key management and key storage remain challenging in several approaches. In addition, some systems lack advanced authentication mechanisms such as multi-factor or device-based verification.

Future research can focus on developing more efficient key management techniques, integrating real-time monitoring and alert systems, and improving system usability without compromising security. Technologies such as blockchain for tamper-proof logging, artificial intelligence for anomaly

detection, and zero-trust security models can be explored to enhance the reliability and effectiveness of secure QR code document locker systems.

7. Flow Chart



8. Advantages of Secure QR Code Document Locker Systems

Secure QR code document locker systems offer enhanced data security, controlled access, and reduced risk of document leakage. They provide fast and convenient access using mobile devices and reduce dependency on physical documents. These systems also support access tracking and audit logs, improving accountability and transparency.

Applications of Secure QR Code Document Locker Systems

Secure QR code document locker systems can be applied in various domains such as education for certificate verification, healthcare for patient record management, government services for identity and document verification, and corporate organizations for protecting confidential data. These applications demonstrate the practicality and effectiveness of QR code–based secure document storage.

10. Conclusion

This survey paper presented a comprehensive review of secure QR code–based document locker systems. Various encryption techniques, authentication mechanisms, and access control strategies were analyzed in detail. A comparative study highlighted the strengths and limitations of existing approaches. The survey concludes that QR code–based document locker systems provide an effective solution for secure document storage and access when combined with robust security mechanisms. However, further research is required to address challenges related to key management, real-time monitoring, scalability, and user experience.

References

[1] A. Kumar and R. Sharma, “Secure Document Storage System Using QR Code and Encryption,” *International Journal of Computer Applications*, vol. 175, no. 12, pp. 15–20, 2021.

[2] S. Patel, M. Shah, and N. Joshi, “QR Code Based Authentication System for Secure Data Access,” *IEEE International Conference on Computing*, pp. 234–239, 2020.

[3] R. Gupta and P. Verma, “A Survey on Document Security Techniques Using Cryptography,” *International Journal of Advanced Research in Computer Science*, vol. 11, no. 3, pp. 45–50, 2019.

[4] J. Lee and H. Kim, “Secure Digital Locker System Using Encryption and Access Control,” *IEEE Access*, vol. 8, pp. 112345–112354, 2020.

[5] M. Singh and K. Kaur, “Time-Based QR Code Authentication for Secure Document Access,” *International Journal of Information Security*, vol. 18, no. 4, pp. 301–309, 2019.

[6] A. Rahman, S. Das, and T. Roy, "Cloud-Based Secure Document Management System Using QR Codes," *Procedia Computer Science*, vol. 167, pp. 2390–2397, 2020.

[7] N. Chandra and V. Rao, "Multi-Factor Authentication Using QR Code for Secure Systems," *International Journal of Network Security*, vol. 22, no. 2, pp. 180–186, 2020.

[8] P. Mehta and S. Jain, "Encryption and Key Management Techniques for Secure Data Storage," *International Journal of Cyber Security and Digital Forensics*, vol. 9, no. 1, pp. 22–28, 2021.

[9] K. Zhao and L. Wang, "A Study on QR Code Security and Privacy Issues," *Journal of Information Security*, vol. 10, no. 3, pp. 145–152, 2019.