

Review on QR Code-Based Secure Authentication Mechanisms in Online Voting Systems

Shivani Nishad¹, Payal Chandrakar²

¹Shri Rawatpura Sarkar University, Raipur (C.G.), India

¹Email: shivaniinishad7393@gmail.com ²Email: payalchandrakar96@gmail.com

ABSTRACT

Digital technology has revolutionized elections by introducing electronic voting systems. Although voting online is quick and easy, there are security risks related to voter verification and data integrity. Online voting can be improved using QR code technology, especially when combined with cryptography and multi-factor authentication. Recent studies suggest that using QR codes and blockchain technologies might improve election transparency. This review looks into QR code-based authentication techniques, such as cryptography and biometric systems, while addressing spoofing and the need for standardization. The findings indicate that further research is required before QR code authentication can be extensively employed, despite the fact that it is scalable and reasonably expensive.

KEYWORDS

QR codes, digital identity, blockchain, cryptography, online voting, authentication methods, and e-voting security.

I. INTRODUCTION

Election procedures must promote trust in order to ensure faith in democracy. The drawbacks of traditional paper ballot systems—such as their high cost, complexity, and vulnerability to fraud—highlight the need for more effective solutions. Electronic voting systems, which are intended to increase efficiency

and accessibility, enable online voting. They do, however, raise concerns about privacy, security, and trust, particularly when it comes to voter authentication while preserving anonymity. Many authentication methods, including cryptographic algorithms and biometrics, have been presented; nevertheless, each has its own privacy and usability problems.

QR code technology is one potential method for secure authentication in online voting systems. These 2D barcodes may reduce identity theft by facilitating quick, noncontact verification and saving encrypted voter credentials (Kumar et al., 2021; Hossain et al., 2019). Recent research combines blockchain technology with QR codes to increase security and transparency and give an immutable record of voting results (Zhang et al., 2019; Sharma et al., 2021). However, problems like QR code fraud and the need for unifying frameworks persist. In order to develop secure, scalable, and user-friendly systems in the future, this study examines previous research on QR code-based authentication in online voting and identifies gaps.

II. OBJECTIVE OF THE STUDY

This study critically reviews recent research on safe authentication in online voting, with a focus on QR code approaches. It examines how various authentication methods enhance the security, reliability, and usefulness of electronic voting systems by comparing QR codes with more conventional methods

like cryptography and biometric systems. In order to increase system resilience and transparency, the study also looks at merging QR codes with blockchain and multi-factor authentication. Additionally, it identifies gaps in the literature and offers suggestions for future directions in the study of secure, scalable online voting systems.

III. METHODOLOGY

Using a systematic literature review (SLR) technique, this study examines QR code-based authentication processes in online voting systems to provide findings that are structured, visible, and reproducible (Kitchenham, 2004). A literature search with a focus on cybersecurity and electronic voting was conducted using major academic databases, including IEEE Xplore and Scopus. Search phrases such as "QR code-based voting system" and "secure online voting authentication" guided a systematic search that was restricted to the years 2005–2025. The inclusion requirements needed peer-reviewed, relevant works regarding security and authentication; non-technical or repetitive research were disqualified. This strategy narrowed the number of high-quality papers to 50–100 for additional analysis after identifying 150–200 original studies.

Data extraction was carefully done to gather relevant information from selected research, such as publication details, methodology, authentication processes, and security measures. The data was categorized into subject areas: cryptographic systems, biometric authentication, QR code systems, blockchain voting, and hybrid systems to enable a comparative analysis of technologies addressing online voting security. The review's trustworthiness was assessed using journal impact factors, citation counts, methodological rigor, and practical application; high-impact publications from Elsevier, Springer, and

IEEE were given precedence. Potential exclusion of pertinent studies due to database limitations and the quick advancement of technology were among the limitations (Kitchenham, 2004).

IV. LITERATURE REVIEW

Voter privacy, vote integrity, and system verifiability have been the main focus of research on secure online voting systems during the last 20 years. End-to-end verifiable systems, which allowed voters to independently confirm their ballots without compromising their anonymity, were among the later developments (Benaloh et al., 2014). In order to achieve anonymous voter-ballot unlinkability, Chaum (2005) first employed mix-nets. Systems like Helios have shown web-based voting with safe homomorphic encryption (Adida, 2008). Later research brought more sophisticated cryptographic methods, such zero-knowledge proofs, although these can be difficult and inappropriate for large-scale elections. This challenge prompted academics to look at alternative authentication methods, such biometric technology, to enhance voter identity verification. According to studies, biometric methods—like fingerprint and face recognition—are more effective than passwords in preventing impersonation and duplicate voting. However, privacy issues, data security issues, and the need for specialist equipment limit their use, especially in low-resource settings. QR codes are becoming more and more used for authentication since they are inexpensive and simple to use. By providing quick, non-contact verification and encrypting voter credentials, they can lower mistakes and unauthorized access. Proposed methods generate QR codes during voter registration for identity verification during voting, and dynamic QR codes enhance security against replay attacks.

Researchers have looked on integrating QR code-based authentication with multi-

factor systems to address impersonation and unauthorized access issues in order to enhance security by combining QR codes with one-time passwords, passwords, or biometrics (Joaquim et al., 2013; Park et al., 2020). Nevertheless, there are disadvantages to QR codes, such the potential for faking and phishing. Blockchain technology is a decentralized, tamper-proof solution for online voting as it guarantees vote integrity and offers end-to-end verifiability (Yavuz et al., 2018; Zhang et al., 2019). Recent study suggests that blockchain and QR codes can be used for reliable voting systems and secure voter authentication (Sharma et al., 2021). Furthermore, hybrid authentication models—which combine many approaches to address various vulnerabilities—are gaining popularity.

By employing blockchain, encryption, biometrics, and QR codes for multi-layered security, these systems increase scalability, resilience, and usability. However, problems including complexity, interoperability, and a lack of standards make adoption difficult. While cryptographic systems are theoretically safe but sometimes impractical, biometrics provide high authentication with privacy issues and technological limitations; QR codes are appealing because they balance cost, usability, and security. Blockchain has scalability problems but increases transparency. Research gaps exist in the application of QR code authentication to online voting, and problems like spoofing and phishing remain critical. Further study is needed to develop safe, scalable, and lightweight hybrid models for electoral use.

Table 1: Comparative analysis of authentication mechanisms in online voting systems.

Author(s) & Year	Method / Approach	Key Features
------------------	-------------------	--------------

Author(s) & Year	Method / Approach	Key Features
Adida (2008)	Helios Voting System	End-to-end verifiability, web-based voting
Benaloh et al. (2014)	Verifiable Voting	End-to-end verification, voter privacy
Cortier & Smyth (2011)	Helios Security Analysis	Ballot secrecy analysis
Ryan et al. (2009)	Prêt à Voter	Secure ballot generation, anonymity
Neumann & Volkamer (2016)	Biometric Voting	Identity-based authentication
Hossain et al. (2019)	QR + Biometric System	Multi-factor authentication
Kumar et al. (2021)	QR Authentication	Fast and effective authentication
Singh & Sharma (2020)	QR-Based System	Encoded credential verification
Park et al. (2020)	Multi-Factor QR System	Layered authentication
Joaquim et al. (2013)	Code Voting	Secure remote voting
Yavuz et al. (2018)	Blockchain Voting	Immutable vote storage
Zhang et al. (2019)	Blockchain E-Voting	Tamper-proof records
Sharma et al. (2021)	Blockchain + Voting	Secure distributed system
Kulyk et al. (2018)	Usability Study	Security vs usability trade-off

Table 1 shows how online voting authentication methods have evolved. While cryptographic alternatives are secure but complex, biometric methods enhance verification but raise privacy concerns. QR code solutions balance cost and scalability, whereas blockchain offers transparency but has scalability problems. Combining QR codes with other technologies is safer and more beneficial.

V. SECURITY MECHANISMS IN QR CODE-BASED ONLINE VOTING SYSTEMS

Online voting systems must provide security through voter authentication, vote secrecy, data integrity, and cyberattack protection. Several security precautions are used by QR code-based systems to prevent unauthorized access and data alteration. Cryptographic encryption, which employs methods like AES and RSA to maintain secrecy even in the event that QR codes are intercepted, protects sensitive data both during transmission and storage. In addition to ensuring the integrity of QR code data and making it possible to detect attempts at fabrication or manipulation, digital signatures provide authenticity and non-repudiation.

Multi-factor authentication (MFA) increases the security of QR code voting by reducing the risk of unauthorized access through the use of several verification methods, such as fingerprints and one-time passwords. By restricting their validity to a single session, one-time or dynamic QR codes reduce fraud. To eliminate eavesdropping, data flow is encrypted using secure communication protocols like SSL and TLS. By providing integrity and transparency, blockchain technology also guarantees that votes are immutable and verifiable. These actions taken together offer a robust security foundation for online voting.

Table 2: Security and Performance Comparison of Authentication Mechanisms in Online Voting Systems.

Approach	Authentication Strength	Data Security	Privacy Protection	Scalability	Cost	Usability	Real-World Applicability
Cryptographic Systems	Very High	Very High	Very High	Low	High	Low	Limited
Biometric Systems	High	High	Medium	Medium	High	Medium	Moderate
QR Code-Based Systems	High	High	Medium	High	Low	High	High
Blockchain-Based Systems	Very High	Very High	High	Medium	Medium	Medium	Emerging
Hybrid Systems (QR +)	Very High	Very High	High	High	Medium	Very High	Very High

Approach	Authentication Strength	Data Security	Privacy Protection	Scalability	Cost	Usability	Real-World Applicability
Blockchain + Biometrics)							

- Table 2 compares several online voting authentication techniques based on security, privacy, scalability, and cost. Cryptographic systems are the safest, however they are not particularly useful. Biometric technologies offer strong authentication, but they are costly and pose privacy concerns. Because QR code systems balance security and usability, they can be advantageous for large-scale voting. Blockchain has scalability problems but increases transparency. Security and scalability may be enhanced via hybrid systems that use blockchain, biometrics, and QR codes. Nevertheless, QR code systems are still vulnerable to phishing and spoofing. A comprehensive security plan that incorporates encryption and multi-factor authentication, along with ongoing research to counter emerging threats, is necessary for reliability.

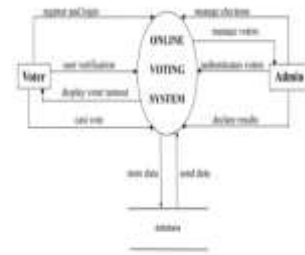


Fig: 01



Fig: 02



Fig: 03

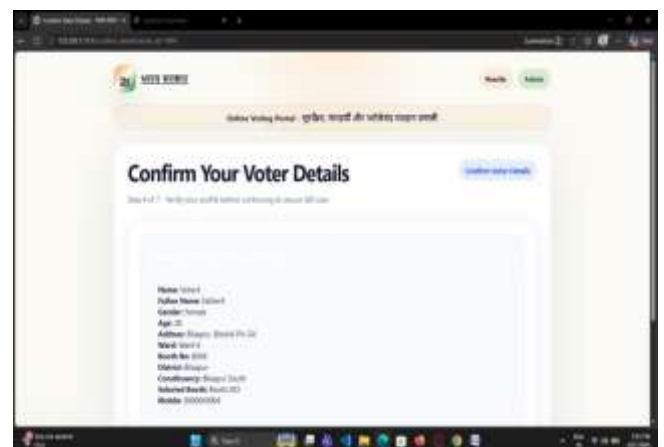


Fig: 04



Fig: 05

VI. ADVANTAGES OF QR CODE-BASED ONLINE VOTING SYSTEMS

For online voting, QR code-based authentication has several benefits, such as rapid, effective, contact-free authentication that lowers human mistake. These systems are affordable, scalable for big populations, and can improve security by integrating multi-factor authentication and cryptographic techniques. Furthermore, QR codes may be integrated with cutting-edge technologies like blockchain to enhance data security and transparency.

VII. LIMITATIONS OF QR CODE-BASED ONLINE VOTING SYSTEMS

Online voting systems that rely on QR codes have advantages, but they also have serious drawbacks, such as the possibility of phishing and spoofing, which might jeopardize the integrity of authentication. Because virus might reveal private data, device security is essential. Access in remote locations may be impeded by reliance on internet connectivity, and uneven deployment standards result in differences in security. Additionally crucial are user knowledge and appropriate

credential use. For safe deployment, robust security protocols and user education are crucial.

VIII. FUTURE SCOPE

Combining cutting-edge technology can result in safe, scalable frameworks that improve QR code-based authentication in online voting. Real-time anomaly analysis and fraud detection are made possible by combining AI and machine learning. By offering a decentralized vote verification method, blockchain integration may foster openness and trust, and multi-layer authentication using biometrics can improve security even further. In order to increase user interface accessibility, define protocols for consistency and interoperability, and discover implementation issues through comprehensive real-world testing, future research should concentrate on these areas.

IX. CONCLUSION

Online voting systems are made more secure, effective, and user-friendly by QR code-based authentication methods. This analysis looks at a number of approaches, emphasizing that QR code solutions provide scalability, cost-effectiveness, and modest security appropriate for contemporary digital voting. While combining QR codes with blockchain and multi-factor authentication increases security, it also highlights problems like device vulnerabilities and QR code spoofing. To solve these issues, more study is required. All things considered, QR code-based systems have the potential to revolutionize online voting; but, their successful deployment will require sophisticated security mechanisms, user education, and validation. Future advancements are essential for safe and reliable electoral systems.

REFERENCES

- Adida, B. (2008). Helios: Voting in the web using open-audit. In 17 th USENIX Security Symposium Proceedings (pp. 335–348).
- Benaloh, J., Byrne, M., Kortum, P., McBurnett, N., Pereira, O., Rivest, R. L., Sherman, A. T., & Teague, V. (2014). End-to-end verifiability. *IEEE Security & Privacy*, 12(4), 40–46.
- Chaum, D. (2005). Secret-ballot receipts: Proper voter-verifiable elections. *IEEE Security & Privacy*, 2(1), 38–47.
- Cortier, V., & Smyth, B. (2011). An analysis of ballot secrecy: Attacking and fixing Helios. *Journal of Computer Security*, 19(1), 89–148.
- Hossain, M. S., Muhammad, G., and Alamri, A. (2019). QR code and biometrics Smart authentication system. *IEEE Access*, 7, 123–135.
- Joaquim, R., Ribeiro, C., & Ferreira, P. (2013). Enhancing remote voting and security with code voting. *Computers & Security*, 37, 1–10.
- Krimmer, R. (2020). Electronic voting: Advantages and obstacles. *International Journal of Electronic Governance*, 12 (2), 101-120.
- Kulyk, O., Teague, V. and Volkamer, M. (2018). Electronic voting systems security and usability. *ACM Computing Surveys*, 50(4), 1–40.
- Kumar, S., Gupta, R., & Singh, A. (2021). Secure authentication system of online applications based on QR codes. *International Journal of Computer Applications*, 174(5), 20-26.
- Neumann, S., and Volkamer, M. (2016). Civitas and Helios: A comparison. *Lecture Notes in Computer Science* (Vol. 10076, pp. Electronic Voting (E-Vote-ID 2016). 15–30). Springer.
- Park, J., Lee, S., & Kim, H. (2020). Multi-factor verification of secure QR code authentication system. *IEEE Access*, 8, 56789–56800.
- Ryan, P. Y. A., Bismark, D., Heather, J., Schneider, S., & Xia, Z. (2009). Prêt a voter: A voter verifiable voting system. *IEEE Transactions on Information Forensics and Security*, 4(4), 662673.
- Sharma, V., Singh, P., & Kumar, R. (2021). Secure e-voting system based on blockchain. *Journal of Information Security and Applications*, 58, 102-110.
- Singh, P., & Sharma, K. (2020). Secure transactions done via QR codes. *International Journal of Engineering Research and Technology*, 9(6), 112118.
- Yavuz, A. A., Koc, A. K., & Ozmen, M. (2018). A move towards safe e-voting with blockchain technology. In *IEEE Conference on Communications and Network Security* (pp. 1–5).
- Zhang, Y., Xue, R., & Liu, L. (2019). Electronic voting system based on blockchain with enhanced security. *Future Generation Computer Systems*, 93, 1-12.