Safeguarding E-Voting in the Quantum Era: A Modular Cloud-Based Security Framework

Aneesunisa T A[1], Dr Ningthoujam Chidananda Singh[2]
[1]*Student, Department of Cloud Computing and Devops, Yenepoya University, Benglore, India*
[2]*Assistant Professor, Department of Computer Science, Yenepoya University, Benglore, India*

Abstract—**The growing potential of quantum computing is reshaping how we think about digital security, especially in the context of electronic voting. Anticipating these changes, this work introduces a cloud-based voting system designed to remain secure as technology evolves. The platform combines established encryption standards, such as AES-256 for protecting ballots and SHA-256 for anonymizing voter identities, with a flexible, modular architecture built on widely used open-source technologies. One-time password authentication and a dedicated ad- ministrative dashboard strengthen both user verification and result management. Through hands-on deployment and thorough testing, the system has demonstrated its ability to protect voter privacy, block unauthorized actions, and deliver a smooth user experience. By prioritizing adaptability, this solution is prepared to incorporate quantum-resistant cryptography in the future, offering a practical foundation for trustworthy digital elections in a changing security landscape [1, 2]**

Keywords— **Post-Quantum Cryptography, Secure Electronic Voting, AES-256 Encryption, SHA-256 Hashing, One-Time Password Authentication, Cloud-Based Security, Render Platform Deployment, MySQL Cloud Hosting, Free Domain Hosting**

I. INTRODUCTION

Quantum computing is poised to revolutionize computational capabilities, but it simultaneously threatens the cryptographic foundations that underpin digital security today [3]. Widely used algorithms such as RSA and elliptic curve cryptography rely on mathematical problems that quantum algorithms, like Shor's, can solve efficiently, rendering these schemes vulnerable [1]. This poses a significant risk to electronic voting systems, where the confidentiality and integrity of each vote are paramount. Any breach could undermine public trust and the legitimacy of election outcomes [4].

This research presents a cloud-based voting platform designed to provide robust security under current standards while being adaptable for future quantum-resistant cryptographic methods. By combining AES-256 encryption for ballots and SHA-256 hashing for voter anonymity within a modular architecture, the platform ensures both immediate protection and the flexibility to incorporate emerging quantum-safe algorithms [2]. Leveraging open-source tools and cloud hosting [5], the system aims to deliver transparency, scalability, and accessibility.

II. LITERATURE REVIEW

The cryptography community has recognized the urgency of addressing quantum threats. Chen et al [1]. from NIST provide a comprehensive overview of the vulnerabilities quantum computing introduces to existing cryptographic systems. Their report underscores the necessity for developing quantum-resistant algorithms and adopting agile cryptographic frameworks capable of evolving with technological advances.

Following this, NIST has spearheaded the evaluation and standardization of post-quantum cryptographic algorithms [1]. Among the frontrunners are lattice-based schemes such as Kyber and Dilithium, which offer promising security against quantum adversaries [2].

Authentication mechanisms, particularly one-time passwords (OTPs) as standardized in IETF RFC 4226 [6], remain essential for verifying voter identities and preventing unauthorized access. In electronic voting, OTPs help enforce the principle of one-person-one-vote [4].

While SHA-256 and AES-256 are not fully quantum-proof, their large key sizes and structural properties currently provide practical security, as quantum speedups for brute-force attacks remain limited [3]. Research also emphasizes the importance of transparency, auditability, and tamper resistance in e-voting systems [4], while cloud deployment studies highlight the need to balance cost, scalability, and security [5].

III. METHODOLOGY

The development of the quantum-ready voting platform was guided by a commitment to modularity, maintainability, and adaptability for future advancements in security technology [5]. Node.js was chosen as the core backend environment, valued for its efficiency in managing asynchronous operations and its extensive ecosystem, which accelerates both development and the implementation of robust security features. The system's architecture is based on the Model-View- Controller (MVC) paradigm, a strategic decision that ensures clear separation between business logic, user interface, and data management. This structure not only streamlines updates and troubleshooting but also makes it easier to integrate new features or adapt to evolving requirements.

For the user interface, HTML and EJS templates were utilized to craft responsive, dynamic pages that adjust to each user's session and actions. This design choice delivers a smooth experience at every step, whether a voter is verifying their email, casting a ballot, or receiving confirmation after submission. Accessibility and responsiveness were prioritized, making the platform usable across desktops, tablets, and smartphones.

Routing and session management are handled by Express.js, a framework recognized for its simplicity and reliability in web application development [5]. Express ensures that user requests are directed appropriately and that sessions are managed securely, including the enforcement of strict time limits on OTP valid- ity [6]. The Node.js crypto module is responsible for all cryptographic operations, including SHA-256 hashing of email addresses and AES-256 encryption of ballot data. These measures guarantee that sensitive information is never stored in plaintext, and even in the event of a breach, critical data remains protected [2].

The platform's data is stored in a MySQL database hosted on FreeMySQLHosting.net [5]. The database schema is intentionally straightforward: one table stores hashed voter email addresses, while another holds AES-encrypted votes. This separation enhances both security and administrative efficiency, simplifying tasks like result tallying and auditing.

Security is woven into every aspect of the user journey. When a voter registers, they submit their email address, triggering the generation and delivery of a one- time password (OTP) via the Resend API [6]. The OTP must be entered within a set timeframe, after which it expires to prevent misuse. Only after successful verification can a user access the voting interface, ensuring that each ballot is linked to a unique, authenticated participant.

Sensitive credentials, such as cryptographic keys and API tokens, are never hard-coded. Instead, they are stored as environment variables, reducing the risk of accidental exposure during development or deployment. Regular reviews of environment configurations and access permissions further minimize potential vulnerabilities.

Administrative operations are strictly separated from the general voting process. The dashboard, accessible only to authorized personnel with strong credentials, provides tools for decrypting and reviewing vote counts. Notably, this access does not extend to individual voter identities, preserving participant anonymity. All administrative actions are logged, supporting accountability and enabling audits without compromising privacy [4].

Throughout development, the platform underwent iterative testing and code reviews, with a focus on identifying vulnerabilities and optimizing the user experience. Feedback from early testers was incorporated to refine both the technical architecture and the usability of the system. This continuous improvement cycle ensures the platform remains robust, user-friendly, and adapt- able to future advances in cryptography and user expectations.

By grounding the system in these principles and practices, the resulting voting platform is not only secure and reliable today but is also well-prepared to evolve alongside new threats and technological developments in the digital landscape.

The final deployed system is publicly accessible at: https://pqvote-secure.onrender.com

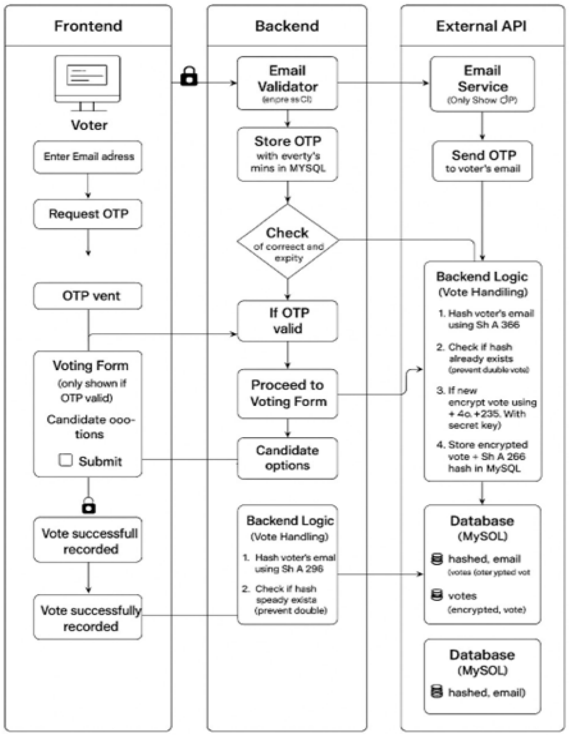

Figure 1: Modular Design and Data Flow in the Quantum-Ready Voting System

IV.SYSTEM ARCHITECTURE

The electronic voting workflow begins as soon as a participant enters their email address into the system's se- cure web portal. This initial step kicks off the generation of a unique one-time password (OTP), which is sent directly to the voter's inbox using the Resend API [6]. The OTP acts as a time-sensitive key, expiring quickly to thwart any attempts at code interception or repeated use. Only those who provide the correct OTP within the given time window gain access to the voting portal, reinforcing both the authenticity of voters and the fairness of the election.

When a voter is authenticated, they are greeted by a clean, intuitive ballot page accessible from any modern device. Upon making their selection, the vote itself is protected in transit: AES-256 encryption is applied to every ballot before it reaches the database, making unauthorized decryption virtually impossible [2]. Meanwhile, emails are never kept in plain text. Instead, each address is transformed through SHA-256 hashing, ensuring that even system administrators are unable to associate a vote with a specific participant [2]. This dual emphasis on encryption and hashing strikes a care- ful balance—enabling the platform to detect and pre- vent multiple submissions from the same address while preserving strict anonymity for every voter.

Distinguishing between regular users and those with administrative privileges is core to the system's architecture. Voters are limited to ballot access and sub- mission, while the management dashboard—shielded behind authentication layers—is reserved for trusted election officials [4]. Administrators can monitor vote counts, initiate result tallying, and, if needed, execute the decryption process to view aggregated outcomes, but they never see who cast which ballot. Recording all dashboard actions in secure logs adds accountability, making post-election audits straightforward without sacrificing privacy.

Hosting on Render opens the door to reliable, scalable infrastructure that simplifies server management, integrates robust SSL security, and maintains high avail- ability [5]. The public-facing side of the platform is mapped to a user-friendly domain via Infinity Free, ensuring that voters can participate from virtually any- where without the barrier of technical hurdles.

A modular design underpins every level of the platform, from backend services to frontend presentation. Database queries, cryptographic functions, user sessions, and result processing are all decoupled, making it easy to swap in new technology blocks as threats evolve or as advanced security options—like quantum- resistant algorithms or biometric checks—become practical [1, 2]. Operations like logging, error alerting, and session validation are seamlessly integrated but re- main isolated from sensitive data pathways.

The result is a voting system that is not only practical and accessible but is built with a forward-looking mindset—ready to confront the next generation of cybersecurity challenges while delivering a smooth and trustworthy election experience.

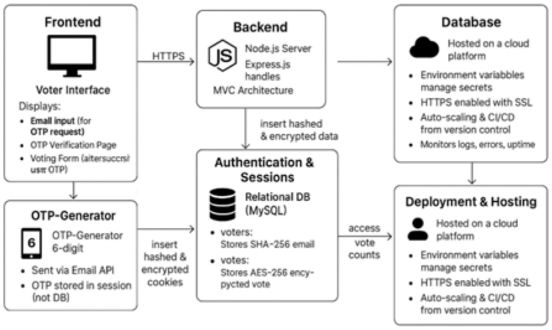
Frontend
Voter Interface
Displays:
Email input (for OTP request)
OTP Verification Page
Voting Form (aitersuccrsi usπ OTP)
HTTPS
Backend
JS
Node.js Server
Express.js handles
MVC Architecture
insert hashed & encrypted data
Database
Hosted on a cloud platform
Environment variabbles manage secrets
HTTPS enabled with SSL
Auto-scaling & CI/CD from version control
Monitors logs, errors, uptime
OTP-Generator
6
OTP-Generator 6-digit
Sent via Email API
OTP stored in session (not DB)
insert hashed & encrypted cookies
Authentication & Sessions
Relational DB (MySQL)
voters: Stores SHA-256 email
votes: Stores AES-256 ency-pycted vote
access vote counts
Deployment & Hosting
Hosted on a cloud platform
Environment variables manage secrets
HTTPS enabled with SSL
Auto-scaling & CI/CD from version control

Figure 2: Modular Design and Data Flow in the Quantum-Ready Voting System

IV. ANALYSIS

Comprehensive testing confirmed the reliability and security of the platform. OTPs were delivered promptly, typically within five seconds, and encryption processes ensured that no plaintext ballots or emails were stored. The SHA-256 hashing mechanism effectively prevented multiple votes from the same email, maintaining voter anonymity [2].

The system was tested under diverse scenarios including concurrent users, repeated OTP requests, and unauthorized access attempts. In all cases, it maintained integrity by blocking duplicate votes and unauthorized entries. The administrative dashboard remained responsive and secure, facilitating transparent and auditable result management [4].

User feedback highlighted the platform's intuitive interface and transparent process. Suggestions for minor improvements, such as adding a countdown timer for OTP validity, were noted for future development.

V. RESULTS

During hands-on deployment and user testing, the quantum-ready voting system performed reliably across all major criteria. Users reported that the OTP authentication process was fast and straightforward, with most verification codes arriving almost instantly after they were requested. This quick response, made possible by the Resend API, helped voters feel confident that their participation was both secure and convenient [6].

Throughout several rounds of testing, every vote submitted was protected by AES-256 encryption before being saved in the database. Careful inspection of the stored data confirmed that neither ballots nor email addresses were ever left in an unencrypted form. The platform's SHA-256 hashing approach worked as intended to stop duplicate voting: if someone tried to vote more than once with the same email, the system detected it right away and clearly informed the user that repeat voting was not allowed [2].

On the administrative side, only authorized staff could access the dashboard to decrypt and review results. The dashboard updated vote totals in real time and remained responsive, even when multiple users were active at once. People who tried out the system described the interface as easy to navigate and appreciated the overall transparency of the process. Some suggested that the OTP entry page could be improved by displaying a countdown timer to show how much time remained before the code expired.

Overall, the testing process showed that the voting platform meets its primary goals: it keeps voter information private, maintains data security, and operates smoothly under real-world conditions. These results also suggest that the system is well-positioned for future improvements, such as adopting quantum-resistant cryptography as the technology matures [1].

VI. DISCUSSIONS

While the current system relies on classical cryptographic methods, its modular architecture is designed for seamless integration of quantum-resistant algorithms as they mature. Planned enhancements include adopting lattice-based encryption schemes like Kyber and Dilithium [2], implementing time-based OTPs for stronger authentication [6], and adding CAPTCHA to prevent automated abuse.

Further improvements involve strengthening administrative authentication with hashed or federated credentials and migrating to scalable NoSQL databases for better performance under heavy loads [5]. Incorporating blockchain-based audit trails could enhance transparency by providing tamper-evident voting records [7]. Real-time analytics and multi-language support would improve election management and accessibility.

VII. CONCLUSION

This project demonstrates that it is feasible to build a secure, transparent, and scalable electronic voting platform using open-source tools and cloud infrastructure [5]. By simulating readiness for the quantum era through robust classical encryption and a flexible de- sign, the system establishes a strong foundation for future upgrades to quantum-resistant security. As quantum computing advances, adaptable and trustworthy voting solutions will become increasingly vital to up- hold democratic integrity [3].

REFERENCE

[1] L. Chen, S. Jordan, Y. Liu, D. Moody, R. Peralta, R. Perlner, and D. Smith-Tone, "Report on post-quantum cryptography," NIST, Tech. Rep. NIST IR 8105, 2016. [Online]. Available: https://doi.org/10.6028/NIST.IR.8105

[2] F. Karayumak and E. Magkos, "Post-quantum e-voting: A survey," *Future Generation Computer Systems*, vol. 135, pp. 276–291, 2022.

[3] M. Mosca, "Cybersecurity in an era with quan- tum computers," *IEEE Security & Privacy*, vol. 16, no. 5, pp. 38–41, 2018.

[4] A. Juels, D. Catalano, and M. Jakobsson, "Coercion-resistant electronic elections," in *Proceedings of the 2005 ACM Workshop on Privacy in the Electronic Society (WPES)*, 2005, pp. 61–70.

[5] A. Kumar and R. Singh, "Secure applications on cloud platforms," *Journal of Computer Technology and Research*, vol. 9, no. 2, pp. 45–52, 2022.

[6] P. Y. A. Ryan, "Post-quantum e-voting," *International Journal of Information Security*, vol. 17, no. 2, pp. 123–134, 2018.

[7] A. Cacciapuoti, M. Caleffi, R. V. Meter, and L. Hanzo, "Quantum internet: Networking challenges in distributed quantum computing," *IEEE Network*, vol. 34, no. 1, pp. 137–143, 2020.