International Scientific Journal of Engineering and Management (ISJEM) ISSN: 2583-6129
Volume: 04 Issue: 05 | May – 2025 DOI: 10.55041/ISJEM03397
An International Scholarly || Multidisciplinary || Open Access || Indexing in all major Database & Metadata

Secure E-Voting System Using Web Technologies and Role-Based Access Control

Dr. V Manikandan, Bedalda Ravi Prakash Reddy, Roshan Singh Department of Computer Science and Engineering,
Faculty of Engineering and Technology, JAIN (Deemed-to-be) University Bangalore, India
v.manikandan@jainuniversity.ac.in ,roshansinghrajput20003@gmail.com, raviprakashbedadala3@gmail.com

Abstract- This research explores the development of a secure, reliable, and accessible electronic voting system leveraging modern web technologies and robust access control mechanisms. With democratic institutions increasingly turning to digital solutions for civic processes, there is a pressing need to ensure these systems maintain high standards of security, transparency, and user-friendliness. The proposed system is built using Angular as the frontend framework and Spring Boot for backend services. It incorporates essential security features such as JSON Web Tokens (JWT) for authentication and authorization, and BCrypt encryption for password protection. A key architectural component is Role-Based Access Control (RBAC), which separates system privileges between administrators and voters, thereby reinforcing operational integrity and data security. This paper presents a detailed system architecture, workflow, and highlights the implementation challenges and their solutions. The proposed system demonstrates the potential to improve trust and efficiency in the electoral process.

1 INTRODUCTION

The The integrity of democratic elections is foundational to societal trust in governance. Traditional voting systems, while reliable in many respects, suffer from limitations such as logistical inefficiencies, accessibility issues, and potential for manual errors or manipulation. As digital technology matures, electronic voting (e-voting) systems have emerged as promising alternatives, capable of enhancing voter participation and operational transparency. However, digitization introduces its own set of challenges—particularly around security, scalability, and usability. In this paper, we propose a web-based secure e-voting platform that mitigates these issues through the integration of modern web technologies and a robust access control strategy. By employing Angular and Spring Boot, we ensure a responsive and modular application structure. Security is enforced through JWT-based session handling and BCrypt password hashing. Additionally, RBAC ensures users only access functionality relevant to their role, reducing the risk of unauthorized actions or data breaches.

2 . LITERATURE REVIEW

1. In Traditional Voting Systems: These systems, typically involving paper ballots and manual counting, are vulnerable to logistical errors, ballot tampering, and accessibility issues. Ensuring anonymity and preventing fraud often require substantial manual oversight.
2. Development of E-Voting Systems: Early digital voting systems included Electronic Voting Machines (EVMs), which provided quicker tabulation but limited remote accessibility. The rise of web technologies enabled scalable and accessible voting platforms.
3. Security Concerns in E-Voting: The main risks include impersonation, vote tampering, denial-of-service attacks, and unauthorized data access. Effective encryption, session management, and input validation are vital countermeasures.

International Scientific Journal of Engineering and Management (ISJEM) ISSN: 2583-6129
Volume: 04 Issue: 05 | May – 2025 DOI: 10.55041/ISJEM03397
An International Scholarly || Multidisciplinary || Open Access || Indexing in all major Database & Metadata

4. Role-Based Access Control (RBAC): RBAC models have been widely adopted in high-security domains such as healthcare and banking. In an e-voting context, it ensures voters cannot perform administrative actions and vice versa.
5. Web Technologies in Voting Systems: Angular enables responsive and component-based frontend applications. Spring Boot provides REST APIs and secure backend services. Combined, they form a resilient architecture suitable for sensitive data handling.

.

3. PROPOSED WORK

The proposed system is designed to facilitate a secure and transparent voting process that ensures both administrative control and voter privacy. The application architecture incorporates a dual-role mechanism for users—admins and voters—with features tailored to their specific access levels.

3.1 Voter Module

- User Authentication: Voters log in using secure credentials, authenticated via JWT.
- Eligibility Verification: The system checks voter eligibility and ensures the user has not voted already.
- Ballot Display: Presents candidates/parties clearly with one-click vote functionality.
- Vote Submission: Votes are securely stored and cannot be altered post-submission.
- Confirmation and Logging: Acknowledges vote submission with a digital receipt and logs the activity.

3.2 Admin Module

- User Management: Admins can register new voters and manage access permissions.
- Election Configuration: Set up election details, timelines, and constituency parameters.
- Candidate & Party Management: Add, remove, or update candidate and party details.
- Live Monitoring: Track voter turnout and vote count in real-time.
- Audit Logs: Maintain tamper-proof logs of every administrative and voting action.

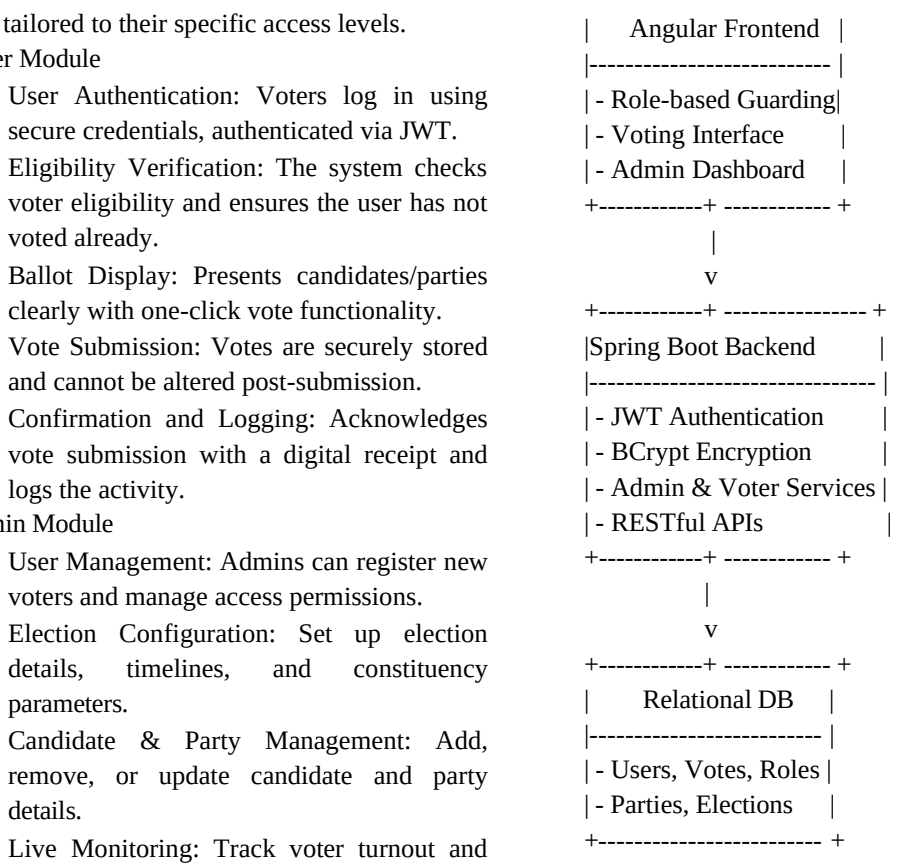
3.3 Security Framework

- JWT Tokens: Provide stateless, role-based session validation for both voters and admins.
- BCrypt Encryption: Secures stored credentials and prevents brute-force attacks.
- RBAC Enforcement: Restricts access based on user role, enforced across both frontend and backend.
- CORS Management: Ensures only permitted domains can interact with backend APIs.

Networking Events: The portal organizes networking events and workshops to facilitate interaction between startups, mentors, and investors.

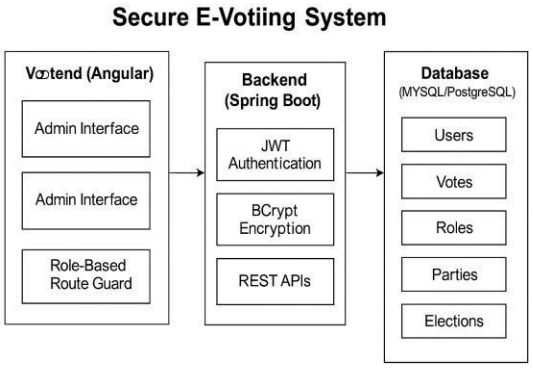
Monitoring and Evaluation: The portal continuously monitors the progress of supported startups and evaluates the impact of funding and mentorship support.

System Architecture /Model:

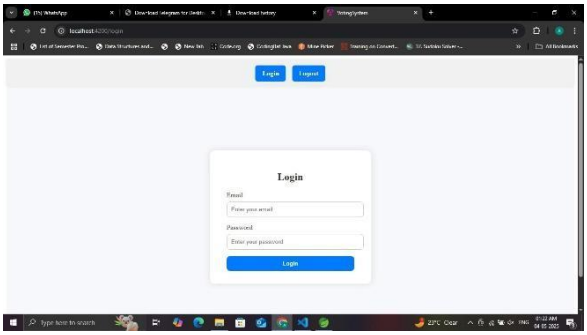


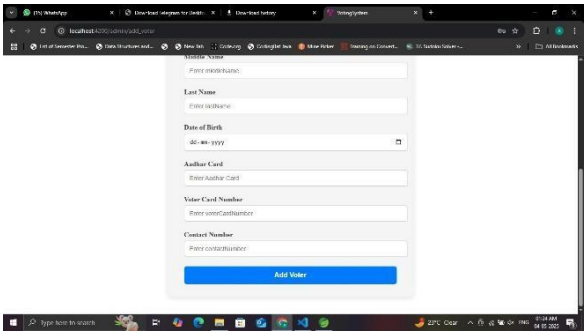
International Scientific Journal of Engineering and Management (ISJEM) ISSN: 2583-6129
Volume: 04 Issue: 05 | May – 2025 DOI: 10.55041/ISJEM03397
An International Scholarly || Multidisciplinary || Open Access || Indexing in all major Database & Metadata

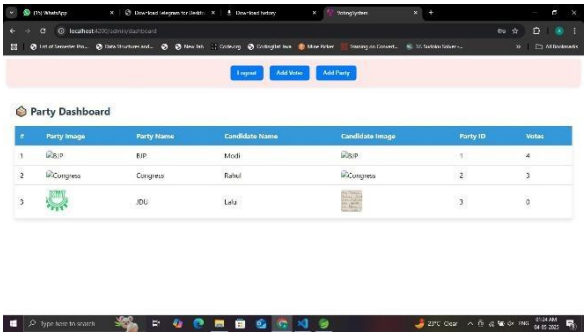
Working Model:



Snapshots of website:







4. CONCLUSION & FUTURE SCOPE

In conclusion, this research presents a comprehensive and secure e-voting system framework that effectively integrates Angular and Spring Boot technologies with advanced security mechanisms such as JWT and BCrypt. Through the implementation of role-based access control, the platform successfully separates administrative and voter functionalities, thereby maintaining the integrity of the voting process.

The system not only meets the core requirements of modern electronic voting—such as usability, security, and transparency—but also lays the groundwork for future enhancements. With the continuous evolution of web and authentication technologies, this solution has the potential to serve as a reliable digital alternative to traditional voting methods, encouraging broader civic participation while upholding democratic values.

Future Scope:

Looking forward, the proposed e-voting system can benefit significantly from the integration of advanced technologies. One of the most promising directions is the adoption of blockchain, which can ensure that vote records are immutable and transparently auditable by all stakeholders. Biometric authentication methods such as fingerprint or facial recognition could also enhance identity verification and prevent impersonation.

Moreover, developing a dedicated mobile application would improve accessibility and allow users to receive notifications about election events in real-time. Adding multilingual support would cater to a more diverse voter base, making the system more inclusive. Introducing an offline voting capability could also

help areas with poor internet connectivity, syncing data once a connection is re-established. Finally, a real-time analytics dashboard would provide administrators with actionable insights and increase transparency throughout the election process.

5. REFERENCES

1. Spring Security Reference Documentation (2024). "Authentication and Authorization"
2. Angular.io Documentation (2024). "Security Best Practices"
3. JWT.io Documentation (2024). "JSON Web Tokens"
4. BCrypt Implementation Guide (2023)
5. NIST SP 800-63: Digital Identity Guidelines (2023)
6. OWASP Top Ten Web Application Security Risks (2024)
7. Hibernate ORM and JPA Docs (2024)
8. WebAuthn Specification (2024)
9. REST API Best Practices (2023)