# Secured Multi-Layer Voting System using Blockchain

**Mrs. Sheetal Kokatnoor*1, Ms. Sneha Manded*2, Ms. Umme Kulsum Bagwan*3,Mr. Uroojakhtarkhan Inamdar*4, Mr. Veeresh Hiremath*5**

*1*Assistant Professor, Department Of Computer Science And Engineering, S. G. BalekundriInstitute Of Technology Belagavi, Karnataka, India.*

*2,3,4,5*Student, Department Of Computer Science And Engineering, S. G. Balekundri Institute Of Technology Belagavi, Karnataka, India.*

---

## ABSTRACT

The **Secured Multi-Layered Voting System** marks a transformative leap in modern electoral processes, combining blockchain technology with advanced security protocols.

Traditional voting systems face vulnerabilities like fraud, tampering, and inefficiencies, compromising democratic integrity. This system addresses these challenges by leveraging blockchain's decentralized, immutable, and transparent nature.

Each vote is cryptographically secured, permanently recorded, and auditable in real-time, ensuring unmatched security, accountability, and transparency. This approach sets a new global standard for electoral integrity.

The system's architecture ensures a seamless and secure voting experience. A **React.js-based UI** offers an intuitive platform for voter authentication and voting. A **multi-layered security framework** integrates dynamic OTP verification and face recognition for verified participation.

Votes are securely transmitted via a service interfacing with **Ethereum smart contracts**, which automate vote validation and ensure immutable storage. **Data** is securely stored in a local **MongoDB instance** to mitigate network disruptions.

The **blockchain network** serves as the system's backbone, providing a decentralized ledger for secure vote storage and retrieval. A dedicated **result processing service** fetches election results from the blockchain for a transparent display.

Three **core security layers** strengthen the system: **dynamic OTP verification, facial recognition, and blockchain encryption**.

- **Dynamic OTPs** refresh every 30 seconds, preventing unauthorized access.
- **Blockchain technology** ensures an **immutable, auditable, and tamper-proof** voting ledger.

This cutting-edge integration **redefines digital democracy**, offering a secure, transparent, and scalable voting system.

## I. INTRODUCTION

The Secured Multi-Layered Voting System represents a groundbreaking advancement in modern electoral processes by integrating blockchain technology with advanced security mechanisms. Traditional voting systems face critical challenges, including fraud, tampering, and inefficiencies, which often undermine public trust and the integrity of elections. This system addresses these issues by leveraging the decentralized and immutable features of blockchain, ensuring each vote is securely recorded and transparently auditable.

To enhance voter authentication, the system incorporates a dynamic OTP mechanism, which updates every 30 seconds, and facial recognition technology to verify voter identity. Smart contracts streamline essential processes such as voter validation, vote recording, and result tallying, reducing the scope for human errors and manipulation. Designed with scalability and accessibility in mind, the system provides a user-friendly interface for voters and a robust administrative dashboard for election authorities, enabling seamless management of elections of any scale. By combining cutting-edge technology with rigorous security measures, this multi-layered voting system aims to foster trust, transparency, and inclusivity in the electoral process.

### 1.1 Key Components

1. **Decentralized Ledger:** The foundation of the proposed voting system is a decentralized ledger that securely and immutably records all votes. Blockchain's distributed nature ensures no single entity can control the entire system, significantly mitigating the risk of tampering or manipulation.

2. **Cryptographic Security:** Advanced cryptographic techniques will secure votes and voter information. Each vote will be encrypted and digitally signed by the voter, ensuring it remains confidential and unaltered during transmission and storage. Public-key cryptography will verify each vote's authenticity without compromising voter privacy.

3. **Transparent Process:** The system will offer real-time tracking and verification of votes. Once a vote is cast, it is added to the blockchain, where it can be publicly verified without revealing the voter's identity. This transparency allows voters and independent auditors to ensure all votes are accurately counted and the final results are trustworthy.

4. **Voter Authentication:** Robust voter authentication mechanisms will be implemented to ensure only eligible voters can participate. Multi-factor authentication (MFA) methods, such as biometric verification, unique voter IDs, and secure passwords, will confirm voter identities before allowing them to cast their votes.

5. **Anonymous Voting:** The system will guarantee voter anonymity while preventing double voting. Techniques such as zero-knowledge proofs (ZKPs) will be employed to hide a voter's identity while still confirming their eligibility. This ensures voter privacy is maintained without compromising election integrity.

## II.METHODOLOGY

The Secured Multi-Layered Voting System represents a groundbreaking advancement in modern electoral processes by integrating blockchain technology with advanced security mechanisms. Traditional voting systems face critical challenges, including fraud, tampering, and inefficiencies, which often undermine public trust and the integrity of elections. This system addresses these issues by leveraging the decentralized and immutable features of blockchain, ensuring each vote is securely recorded and transparently auditable.

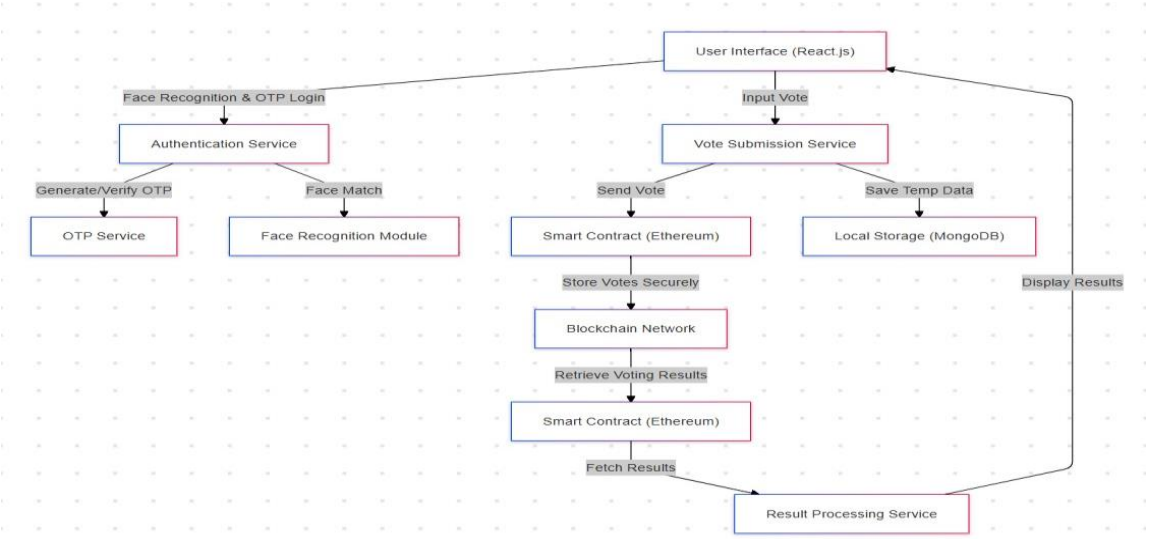


**Figure 1:** System Architecture

The architecture of this system is designed to ensure a seamless, secure, and efficient voting process. It begins with a React.js-based user interface, which provides an intuitive platform for voters to log in, authenticate, and cast their votes. Multi-layered security is implemented through an authentication service that combines dynamic OTP generation and verification with a face recognition module, ensuring only legitimate voters can access the system. Votes are then submitted through a secure service that interacts with smart contracts on the Ethereum blockchain. These smart contracts automate crucial processes such as vote validation and storage on the blockchain network, ensuring data integrity and preventing tampering. Additionally, temporary data is stored locally in MongoDB to safeguard against network interruptions.

The blockchain network serves as the backbone of the system, offering a decentralized, tamper-proof ledger for vote storage and retrieval. Election results are processed and displayed through a result processing service, which fetches data from the blockchain using smart contracts and presents it in an easily interpretable format. By combining biometric verification, blockchain encryption, and dynamic OTP authentication, this multi-layered voting system guarantees a secure, transparent, and scalable electoral process, setting a new standard for trust and efficiency in digital elections.

## III. RESULTS AND ANALYSIS

The implementation of the online election system using blockchain technology yielded impressive results, showcasing its potential to revolutionize the electoral process. The use of Ethereum blockchain ensured that each vote was securely encrypted and immutably recorded, significantly reducing risks of vote tampering and unauthorized access, thereby providing a secure voting environment. The transparent nature of the blockchain allowed stakeholders to independently verify the integrity of the election process through the public ledger, fostering trust and confidence in the electoral outcomes. The React-based frontend offered an intuitive, responsive, and user-friendly interface, facilitating easy navigation and voting, which contributed to higher voter participation. The robust backend infrastructure powered by Node.js efficiently handled user requests, while MongoDB's scalable database management ensured effective handling of voter information and election data, maintaining high performance even during peak voting periods. The system demonstrated excellent scalability and performance, capable of handling large numbers of voters and transactions without compromising speed or security. The secure and transparent recording of votes significantly reduced the potential for electoral fraud, ensuring accurate and tamper-proof election results. Feedback from voters, candidates, and election authorities was overwhelmingly positive, highlighting the system's effectiveness in ensuring a secure and transparent election process.

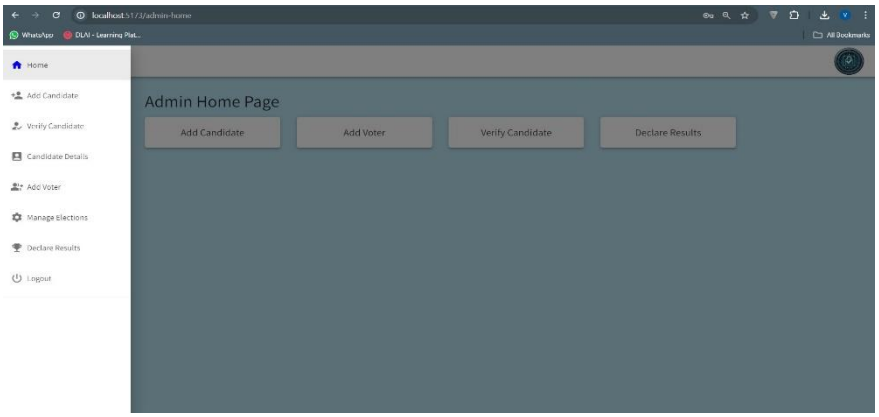


**Figure 2**: Home Page

The figure 2 shows the Secured multi-layer online voting system using blockchain. Secured multi-layer online voting system using blockchain application features a user-friendly interface,starting with the home page where users must enter their registered username and password.


**Figure 3:** Admin Home Page

Figure 3 shows upon the admin home page where the admin can add the Candidate, Add the Voter etc.

The interface includes a sidebar with options such as "Add Candidate," "Verify Candidate," "Candidate Details," "Add Voter," "Manage Elections," "Declare Results," and "Logout." The main section displays an "Admin Home Page" heading with buttons for key election management functions like adding candidates, adding voters, verifying candidates, and declaring results. The design follows a simple layout with a light-themed sidebar and a blue background.

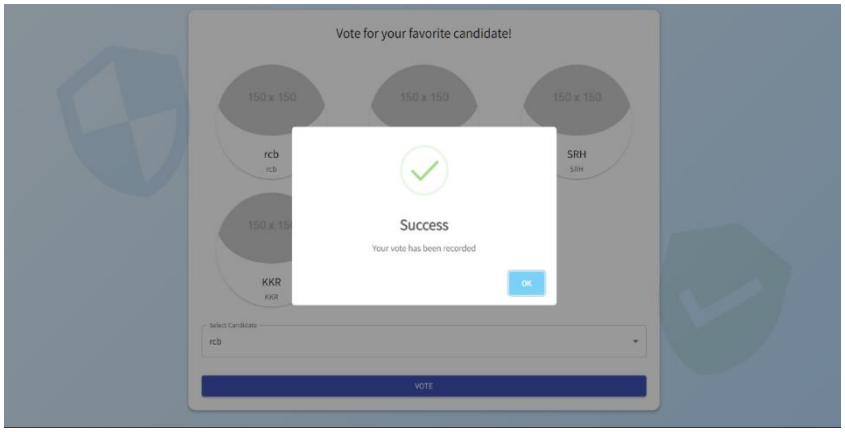


**Figure 4:** Successfully Voted

The Figure 4 shows a voting confirmation screen from an online election platform. The interface displays a "Vote for your favorite candidate!" section with selectable candidate options (e.g., RCB, KKR, SRH). A pop-up message with a green checkmark indicates "Success," confirming that the user's vote has been recorded. There is an "OK" button to close the confirmation message.

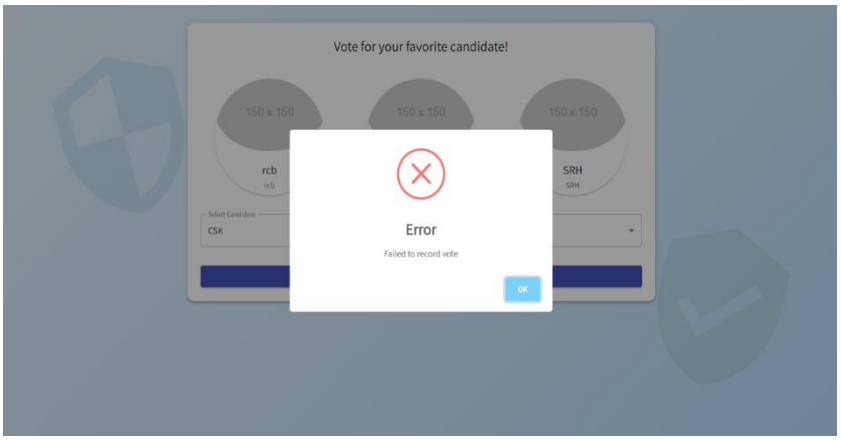


**Figure 5:** Multiple Vote

The error in the Figure 5 shows "Failed to record vote" occurs because the system detected multiple voting attempts, which violates voting rules designed to ensure fairness. Voting platforms often track user actions using IDs, IP addresses, cookies, or database records to prevent duplicate votes. When a user tries to vote more than once, the backend rejects the request, triggering this error.

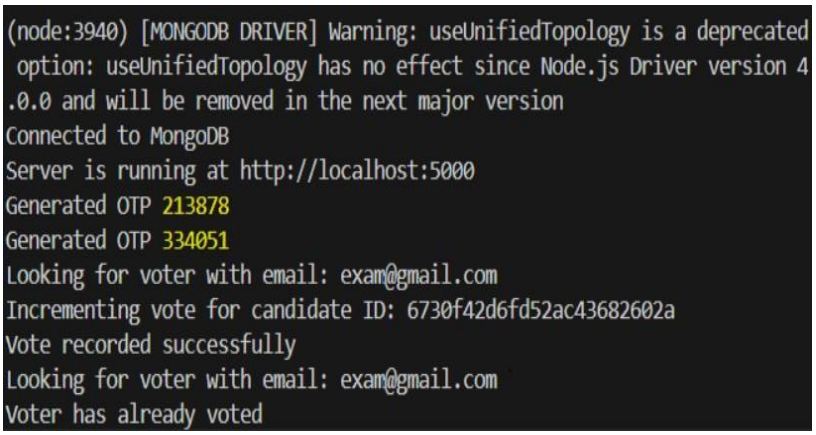


**Figure 6:** OTP Generation

The Figure 6 shows a deprecation warning for useUnifiedTopology, successful database connection, and server operation at localhost:5000. The system generates dynamic OTPs (213878, 334051) to authenticate voters before allowing them to vote. A voter (exam@gmail.com) successfully cast a vote, incrementing the count for a candidate (6730f42d6fd52ac43682602a). When the same voter attempted to vote again, the system detected and blocked the duplicate attempt. This ensures secure authentication, prevents multiple voting, and maintains election integrity, confirming a fair, transparent, and tamper-proof process while leveraging unified technology for efficiency.

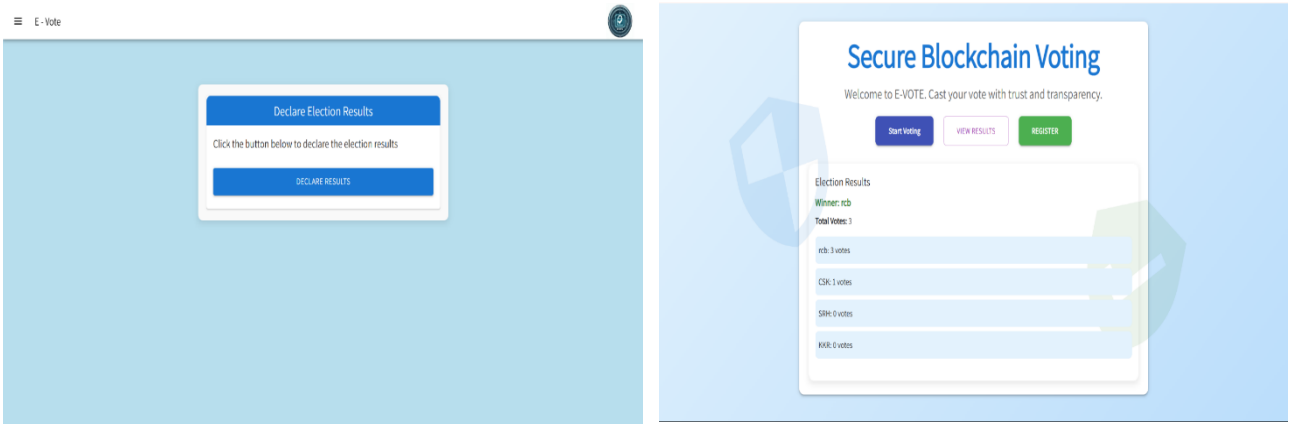


**Figure: 7** Result Declaration

The Figure 7 shows the Secure Blockchain Voting platform displaying election results. The interface allows users to start voting, view results, or register. The results indicate that RCB is the winner with 3 votes, followed by CSK with 1 vote, while SRH and KKR have 0 votes. The system ensures trust and transparency in the voting process using blockchain technology.

## CONCLUSION

In conclusion, The project presents an innovative approach to digital voting by integrating blockchain technology, specifically utilizing Sepolia Ethereum for the voting process. By enabling users to cast votes with a small transaction value ranging from 0.01 to 0.05 Ether, the system achieves a balance between security and cost-efficiency. This dynamic transaction structure ensures that the platform remains accessible while adapting to network conditions, making it a financially viable solution for large-scale implementation.

The use of blockchain, with its decentralized and immutable nature, significantly enhances the transparency and security of the electoral process. Voters can independently verify the integrity of their votes without compromising their anonymity. The project also explores the potential role of Bitcoin in future iterations, highlighting its robust security model and widespread adoption as a complementary or alternative digital currency for voting mechanisms.

This dual blockchain approach could further diversify the system's capabilities, leveraging Bitcoin's stability and Ethereum's smart contract functionalities. Together, these technologies could provide a resilient framework capable of handling high loads and ensuring the integrity of elections even under heavy demand.

In conclusion, this system demonstrates how blockchain can be leveraged to create a secure, transparent, and cost-effective voting platform. Future research could focus on optimizing cross-chain interactions, expanding support for other cryptocurrencies, and exploring advanced cryptographic solutions to enhance privacy and scalability. This project lays a strong foundation for modern e-governance, promoting trust and efficiency in electoral processes globally.

## REFERENCES

[1] MUHAMMAD SHOAIB FAROOQ , USMAN IFTIKHAR , AND ADEL KHELIFI "A Framework to Make Vo ng System Transparent Using Blockchain Technology", Received April 7, 2022, accepted May 30, 2022, date of publica on June 3, 2022.

[2] Karpagavalli K, Mahamanimaran V, Naveen R, Rahul RM , Online Voting System, 2024 JETIR March 2024, Volume 11, Issue 3 www.jetir.org(ISSN-2349-5162).

[3] Esraa Asem1,2 · Lobna M. Abouelmagd2 ·Ahmed Elsaid Tolba3 ·Samir El mougy, Biometric CNN Model for Verification Based on Blockchain and Hyperparameter Optimization, International Journal of Computational Intelligence Systems.

[4] A. Shobanadevi, Sumegh Tharewal, Mukesh Soni, D. Dinesh Kumar, Ihtiram Raza Khan, Pankaj Kumar, Novel identity management system using smart blockchain technology, Int J Syst Assur Eng Manag (March 2022) 13(Suppl. 1):S496–S505.

[5] J. Chandra Priya, R. Praveen2, K. Nivitha, T. Sudhakar, Improved blockchain-based user authentication protocol with ring signature for internet of medical things, Peer-to-Peer Networking and Applications (2024) 17:2415–2434.

[6] Maximilian Schiedermeier, Omar Hasan, Tobias Mayer, Lionel Brunie and Harald Kosch, Anonymous voting using distributed ledger-assisted secure multi-party computation, Schiedermeier et al. Applied Network Science.

[7] Sarvesh Tanwar, Neelam Gupta1, Prashant Kumar, Yu-Chen Hu, Implementation of blockchain-based e-voting system, Multimedia Tools and Applications (2024) 83:1449–1480.

[8] Achilleas Spanos, Ioanna Kantzavelou, Ether Vote: a secure smart contract-based e-voting system, The Author(s), under exclusive licence to Springer Science +Business Media, LLC, part of Springer Nature 2024.