INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD)
© 2026 IJNRD | Volume 11, Issue 4, April 2026 | ISSN: 2456-4184 | IJNRD.ORG

SECURE SMART VOTING SYSTEM USING BLOCK CHAIN

Dr. B. Siranthini, Uppunuthula Sai Teja, Vankayalapati Sarala, Tirlangi Akhil, Vankayala Sandeep

Assistant Professor(CSE), UG Scholar, UG Scholar, UG Scholar, UG Scholar

Department of Computer Science & Engineering

Bharath Institute of Science and Technology, BIHER

173,Agaram Road , Selaiyur, Tambaram, Chennai, Tamil Nadu, India

Abstract : In this digital age, security and fairness of an election are extremely crucial matters. The Secure Smart Voting System will use facial recognition, OTP verification, and blockchain technology to ensure that the voting is done securely and fairly. Through this technology, no one except the genuine voters can cast their votes by using facial verification and receiving OTPs on their phone. Once the voter casts his/her vote, the vote is recorded safely on a blockchain and cannot be altered or manipulated. This technology will help in avoiding any kind of fraud such as fake voting or duplication, among other problems.

IndexTerms – Face Recognition, OTP Authentication, E-Voting, Security, Smart Contract, Block chain

I. INTRODUCTION

Voting is the cornerstone of any democratic system, serving as the primary mechanism through which citizens elect representatives to voice their interests in government bodies. However, traditional voting methods—whether paper-based ballots or electronic voting machines—face several critical challenges. These include voter impersonation, vote tampering, lack of transparency in result processing, delayed counting, and vulnerability to human errors or malicious manipulation. Such limitations undermine public trust and highlight the urgent need for a more secure, transparent, and technologically advanced voting system.

With the rapid advancement of information technology, modern solutions can be leveraged to address these challenges effectively. One promising approach is the integration of biometric authentication, particularly face recognition, to ensure that each vote is cast only by a legitimate and registered voter. Unlike conventional identification methods, biometric systems are difficult to forge or duplicate, thereby significantly reducing the risk of identity fraud and unauthorized access.

In addition to biometric verification, implementing One-Time Password (OTP) authentication adds an extra layer of security. OTP ensures that even if login credentials are compromised, only the authorized user with access to the registered device can proceed with the voting process. This multi-factor authentication mechanism strengthens the integrity of voter verification.

Furthermore, blockchain technology plays a crucial role in revolutionizing the voting process. A blockchain is a decentralized and distributed ledger that records transactions in a secure and immutable manner. Each vote, once recorded as a block, cannot be altered or deleted, ensuring data integrity and preventing tampering. The decentralized nature of blockchain eliminates the need for a central authority, reducing the risk of manipulation and enhancing transparency. Additionally, blockchain enables real-time verification and auditing of votes, allowing stakeholders to independently validate election results.

By combining face recognition, OTP-based authentication, and blockchain technology, the proposed Secure Smart Voting System provides a robust, transparent, and tamper-proof solution. This integrated approach not only eliminates the risks of voter impersonation and election fraud but also enhances trust, efficiency, and accessibility in the electoral process. The system aims to pave the way for a new era of digital democracy where elections are secure, reliable, and verifiable by design.

II.PROPOSED METHODOLOGY

For the security of the Smart Voting System, the proposed methodology makes use of an efficient and effective methodology. For making the voting system a secure and foolproof process, face verification, OTP authentication, and blockchain are adopted. In voter registration, which is the step where all the voters provide their details such as name, voter id and mobile number, face verification comes into play. Besides providing the above-mentioned details, the voter is also required to upload their facial images using the help of a camera. The facial images provided by the voters get processed by means of a face recognition algorithm and then get stored in the database. In the process of authentication, there is a use of two-step authentication process. The first step includes face verification whereby the facial image of the voter gets captured and compared with the database facial image. If the facial images match, then only the voter can proceed further. with the second step where OTP gets generated and is delivered on the mobile phone number of the voter.

In particular, the system incorporates a sophisticated multi-factor approach for ensuring that the identification of the voter is done correctly at the authentication phase. Facial verification in particular begins with capturing of an image of the user, which is then matched against facial characteristics recorded in the system database with the aid of pattern recognition approaches. When there is a match in terms of facial characteristics, the next phase of verification is activated, whereby a One Time Password (OTP) is generated and sent to the user's mobile phone number via a safe and secure channel. In particular After the authentication of the voter, the system allows access to the voting interface, where candidates' list is presented. The voter can choose their candidate and confirm his choice. To record the vote, the system carries out the validation to determine whether the voter has already voted; hence duplicate votes are eliminated through validation of the system. To ensure confidentiality, the vote recorded is encrypted with a reliable cryptographic technique. After the encryption process, the vote is transformed into a blockchain transaction that is included in the distributed ledger. These transactions are contained in blocks that include information such as encrypted vote data, timestamp, and cryptographic hash of the previous block. Blocks are connected to form chains, making it impossible to alter data in blocks since any change of data will render other blocks invalid. With regard to decentralization, blockchain technology makes it impossible for a single party to have control over the information stored. The last step in this regard is the use of the data stored within the blockchain to tally up the votes. With the data stored in the blockchain not being subject to deletion and manipulation in any way, the entire process will be conducted in an accurate manner. This process will be highly efficient while ensuring that those interested can validate the same process without compromising voter privacy. In brief, this model establishes a mechanism for conducting online voting through the use of biometric authentication, OTPs, and blockchains.

III. SYSTEM ARCHITECTURE

The architectural design of the **Secure Smart Voting System** is developed using a layered approach to ensure high levels of security, scalability, and reliability. This system is structured into multiple layers, each responsible for a specific function, including user interaction, authentication, data processing, and secure storage. The architecture mainly consists of the Frontend Layer, Authentication Module, Application Server (Backend Layer), Database, Blockchain Layer, and Admin Module. These layers work together seamlessly to provide a secure and efficient voting experience.

The **Frontend Layer**, also known as the user interface, serves as the entry point for both voters and administrators to interact with the system. It is designed to be user-friendly and responsive, allowing voters to perform actions such as registration, login, facial verification, OTP submission, and vote casting. This layer collects essential user inputs, including personal information, facial images, and voting choices. It ensures smooth communication with the backend while maintaining a secure and intuitive interface.

The **Authentication Module** plays a critical role in preventing unauthorized access and ensuring that only legitimate users can participate in the voting process. This module uses a multi-factor authentication approach, combining face recognition and OTP verification. The face recognition system captures the user's live image and compares it with stored data using machine learning algorithms to confirm identity. Additionally, the OTP verification system sends a one-time password to the user's registered mobile number, adding an extra layer of security. Together, these methods significantly reduce the risk of impersonation and fraud.

The **Application Server**, or backend layer, acts as the core component of the system, managing all logical operations and communication between different modules. It handles user data processing, executes face recognition algorithms, generates and verifies OTPs, and ensures that each vote is valid and not duplicated. The server also encrypts votes before storing them and acts as a bridge between the frontend interface and the blockchain network. This centralized processing unit ensures smooth coordination of all system activities.

The **Database** is responsible for storing critical user information required for the functioning of the system. It securely stores details such as user names, identification numbers, mobile numbers, and facial data used for authentication. All sensitive data is encrypted to protect against unauthorized access and data breaches. The database ensures data integrity and quick retrieval while maintaining strict privacy standards

The **Blockchain Layer** is the most crucial part of the system in terms of security and transparency. Once a vote is cast, it is encrypted and converted into a blockchain transaction. This transaction is then added to a block along with a timestamp and

cryptographic hash. Each block is linked to the previous one, forming a continuous and tamper-proof chain. This ensures immutability, meaning that votes cannot be altered once recorded. Additionally, blockchain provides transparency and decentralization, making the system more trustworthy and resistant to manipulation.

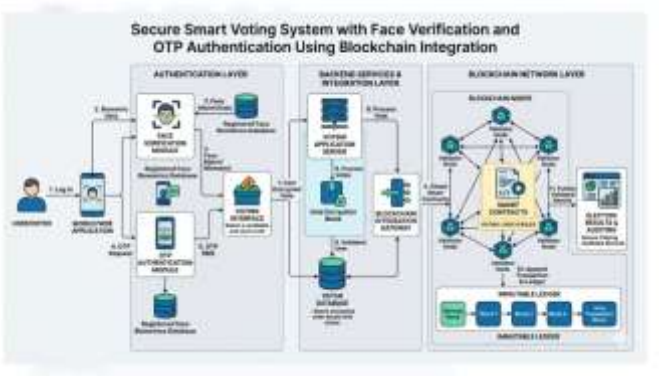

Fig. 1. System Architecture

The **Admin Module** provides necessary controls for election authorities to manage the entire voting process efficiently. Administrators can oversee voter registration, monitor the voting process, and view election results. However, due to the integration of blockchain technology, administrators do not have the ability to modify or tamper with votes, ensuring fairness and integrity in the election process.

The overall workflow of the system begins with user interaction through the frontend interface. The backend server receives and processes the input data, while the authentication module verifies the user's identity through facial recognition andOTP validation. Once authenticated, the user is allowed to cast their vote. The backend validates the vote and ensures no duplication occurs. Finally, the vote is securely stored on the blockchain, maintaining a permanent and tamper-proof record. This structured workflow ensures a secure, transparent, and efficient voting system.

IV. RESULTS AND DISCUSSION

The Secure Smart Voting System proposed was developed and tested with an aim to guarantee authentication, proper vote counting, and result production. The system is successful in demonstrating the importance of using face verification, OTP authentication, and blockchain technology for improving the entire voting process. In terms of implementation, the face verification feature has proven to verify successfully the faces of registered voters, minimizing impersonation. By integrating OTP authentication, the system has ensured security in that only users who have access to the phone number registered in the system can proceed with voting. The use of multi-level authentication has minimized any risks of security breach and has verified user identity. One of the most prominent characteristics of the system is that the use of blockchain technology for storing the votes is made in the system.

The votes have been encrypted and safely stored in the form of transactions using blockchain technology. As the technology used is decentralized, no one can make changes or manipulate the information recorded in the system. The votes have been tallied using the blockchain and the results produced were accurate and cannot be tampered with. In contrast to the traditional method of voting, apart from saving time, the accuracy of the results has been ensured in this system.However, there are certain limitations of the system as well. First, the face recognition may get disturbed by environmental factors like light. Also, the use of the internet is essential for real-time transactions in the block chain. Overall, the results indicate that the proposed system provides a secure, transparent, and efficient solution for digital voting. The integration of advanced technologies significantly enhances election integrity, making the system a promising approach for future implementation in large-scale electoral processes.

V. CONCLUSION

The suggested Secure Smart Voting System is a robust way to counter any deficiencies associated with conventional voting. Through using face authentication, OTP, and blockchain technologies, the voting process is made highly secure and transparent. Moreover, using multi-factor authentication makes the system secure from any attempts of hacking and fraud, while the blockchain technology ensures votes' immutability and safety.

One significant feature of this system is the fact that it successfully implements the "one-person one-vote" principle since there will be no chance for voters to cast multiple votes. Blockchain technology ensures increased confidence due to its transparency and non-manipulability. Another important aspect is the automation of votes counting that significantly speeds up the whole process.

REFERENCES

1. N. Sundareswaran et al., "A Secure E-Voting System With Blockchain Using Face Authentication Technology," in *Proc. ICITSM*, 2025,doi: 10.4108/eai.28-4-2025.2357779.
2. H. Mittal and N. Sengar, "A Blockchain and Face Recognition Based E-Voting System," *Int. J. Recent Adv. Sci. Eng. Technol.*, 2025, doi: 10.22214/ijraset.2025.68648.
3. H. O. Ohize et al., "Blockchain for securing electronic voting systems: a survey of architectures, trends, solutions, and challenges," *Cluster Computing*, 2024, doi: 10.1007/s10586-024-04709-8.
4. S. Paudel et al., "Enhancing Electoral Integrity and Accessibility: A Blockchain and Facial Recognition-Based Electronic Voting System," *Information Dynamics and Applications*, 2025, doi: 10.56578/ida040203.
5. S. A. Joni et al., "Hybrid-Blockchain-Based Electronic Voting Machine System Embedded with Deepface, Sharding, and Post-Quantum Techniques," *Blockchains*, 2024, doi: 10.3390/blockchains2040017.
6. H. R. Nargide et al., "E-Voting System Using Blockchain and Face Recognition," *Int. J. Recent Adv. Sci. Eng. Technol.*, 2024, doi: 10.22214/ijraset.2024.60890.
7. A. Poudel et al., "A Quantum-Secure and Blockchain-Integrated E-Voting Framework with Identity Validation," 2025, doi: 10.48550/arXiv.2511.16034
8. Wang et al., "An efficient and versatile e-voting scheme on blockchain," *Cybersecurity*, 2024, doi: 10.1186/s42400-024-00226-8.
9. S. Ahmed et al., "Hybrid-blockchain-based electronic voting machine system embedded with deepface, sharding, and post-quantum techniques," *Blockchains*, 2024, doi: 10.3390/blockchains2040017.
10. N. Janwe et al., "Online voting system using face recognition and fraud detection," *Int. J. Eng. Res. Technol.*, 2025, doi: 10.17577/IJERTV14IS120233.
11. C. V. Nalawade et al., "Understanding AI-powered blockchain voting systems incorporating biometric verification," *Int. J. Adv. Electr. Electron. Eng.*, 2025, doi: 10.65521/ijaeee.v14i1.8392.
12. .K. Giridhar et al., "Leveraging blockchain for the design and realization of a secure e-voting mechanism," in *Proc. ICITSM Part II*, 2025, doi: 10.4108/eai.28-4-2025.2358030.