International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 09 Issue: 11 | Nov - 2025 SJIF Rating: 8.586 ISSN: 2582-3930

Voting System Using Blockchain Technology

Mrs. K Padmaja[1], Ankita[2], Brunda S P[3] , Chaitra M K[4] , Kanchan S[5]

[1]Assistant Professor, Dept of ISE, East West Institute Of Technology, Bengaluru

[2,3,4,5] Student, Dept of ISE, East West Institute Of Technology, Bengaluru

---

Abstract - A secure electronic voting system integrating blockchain technology and face-based authentication is proposed to ensure transparency and data integrity in elections. Blockchain provides a secure and distributed ledger for storing votes, preventing unauthorized access, fraud, or result manipulation. To verify voter identity, a KNN classifier is utilized in the system to carry out facial recognition tasks, which accurately matches voters with their pre-registered biometric data and prevents impersonation or multiple voting attempts. This two-factor authentication system enhances the reliability of the voting process. This system is scalable, user-friendly, and suitable for large-scale elections, ultimately improving trust, security, and voter participation in modern democratic environments.

Key Words: Blockchain Technology, Cybersecurity, Web Development, Cryptography, Distribution Systems.

1. INTRODUCTION:

Electronic voting improves efficiency and lowers election costs compared to traditional paper-based systems. However, many existing e-voting platforms are still vulnerable to cyberattacks and often lack strong security protections. To tackle these issues, we introduce ACB-Vote, a blockchain-based score voting system designed to enhance security, flexibility, and voter privacy.

With blockchain technology, ballots are stored in a decentralized and tamper-proof way, preventing attacks that typically target centralized servers. ACB-Vote uses BBS+ signatures and a Signature of Knowledge to create anonymously convertible ballots. These ballots hide both the voter's identity and their voting scores, while a secure chain structure helps prevent any manipulation of scores.

The system also includes a conversion mechanism that detects and removes duplicate votes without exposing personal data or score details. After conversion, the voting scores can be tallied efficiently—without relying on heavy zero-knowledge proof computations. Additionally, an aggregate verification algorithm supports batch verification, reducing the blockchain's computational load and improving scalability for large-scale, real-world elections.

1.1 PROBLEM STATEMENT:

Existing voting systems encounter several challenges, such as security risks involving vote tampering, unauthorized access, and inaccurate counting. They also suffer from a lack of transparency, as the processes are often opaque and make it difficult to verify or track votes. Additionally, limited accessibility due to the need for in-person voting contributes to low voter turnout. Finally, traditional systems are often inefficient, requiring significant time and labor to conduct and process elections.

1.2 KEY OBJECTIVE:

This research aims to achieve the following:

Blockchain technology to create a secure, decentralized, and transparent system for storing votes, ensuring that ballots cannot be altered or tampered.

Use facial recognition technology to verify voter identities, guaranteeing that only registered and authenticated individuals are able to cast their votes.

Enable secure remote voting through a web or mobile application, allowing voters to participate in elections conveniently from anywhere while promoting accessibility and inclusivity.

Protect voter privacy by anonymizing identities on the blockchain and encrypting all biometric data, ensuring confidentiality and compliance with data protection standards.

2. RELATED WORK AND LITERATURE SURVEY:

2.1 E-Voting Using One-Time Password and Face Detection and Recognition

A secure electronic voting system is proposed that uses both facial recognition and OTP-based authentication to improve elector verification. During registration, a elector's facial image is stored, and at the time of voting, it is compared with a live image using the Viola-Jones algorithm. After successful face verification, the system sends a unique code to the registered phone to confirm your identity before you vote. This dual-layer authentication increases security, prevents fraudulent voting, and ensures that only legitimate electors participate. However, system performance may be affected by

poor lighting or low-quality image capture, which can reduce facial recognition accuracy.

2.2 Smart Online Voting Web-Based Application Using Face Recognition

This study presents a secure and user-friendly online voting platform that modernizes elections through multi-layered verification including facial recognition, Aadhar authentication, and OTP confirmation. The voter's face is matched with stored data, Aadhar details are validated, and an OTP is sent to the registered number to ensure only genuine voters can cast their vote. This system enhances security, transparency, accessibility, and convenience by enabling remote participation through digital devices. However, its dependency on internet access and adequate digital literacy may limit its capability in remote or underdeveloped areas, highlighting the need to bridge the digital divide for wider adoption.

2.3 Online Voting System Using Face Recognition and OTP

This study introduces a safe online voting platform that combines facial recognition with one-time password verification to make elections more secure and reduce the risk of fraud. Using a webcam, the voter's face is detected and verified through the Haar Cascade algorithm, and upon successful recognition, an OTP is sent to the registered mobile number for final authentication. Developed with Python, OpenCV, and SQLite, the system offers a user-friendly interface and supports remote voting with improved accessibility and accuracy. While it ensures strong security and reliable voter identification, its performance can be affected by poor lighting and low-quality images, which may reduce recognition accuracy in different environments.

2.4 Smart Voting System Using Face Recognition and OTP

This study proposes a reliable and streamlined voting method that combines facial recognition and OTP verification for voter authentication. The system enables both remote and offline voting, aiming to improve transparency, accessibility, and security. Its key benefits include enhanced security, real-time transparency, and convenience for voters. However, it faces challenges such as privacy concerns, data protection issues, technological dependency, and potential system vulnerabilities.

3. METHODOLOGY:

The proposed blockchain-based voting system is designed to make elections more secure, transparent, and tamper-proof. It runs on a decentralized blockchain network where every encrypted vote is stored as an unchangeable block.

To begin, voters register by submitting their personal details and facial images. Each voter then receives a unique ID and a secret key to ensure that everyone can vote only once. When it's time to vote, the system uses facial recognition powered by the K-Nearest Neighbors (KNN) algorithm to confirm the voter's identity. This is followed by a one-time password (OTP) for two-factor authentication, adding an extra layer of security.

After successful verification, voters cast their encrypted votes through a secure web interface. Each vote is recorded as a blockchain transaction, guaranteeing data integrity and preventing any kind of tampering or manipulation.

Smart contracts—written in Solidity—handle key election processes such as validating votes, preventing duplicates, automating result tallying, and maintaining overall transparency. Once voting ends, these smart contracts decrypt and tally the votes securely, ensuring that the final results are both verifiable and trustworthy.

The system is thoroughly tested and deployed on a private Ethereum network to simulate real-world conditions and evaluate its performance and reliability.

3. SYSTEM ARCHITECTURE:

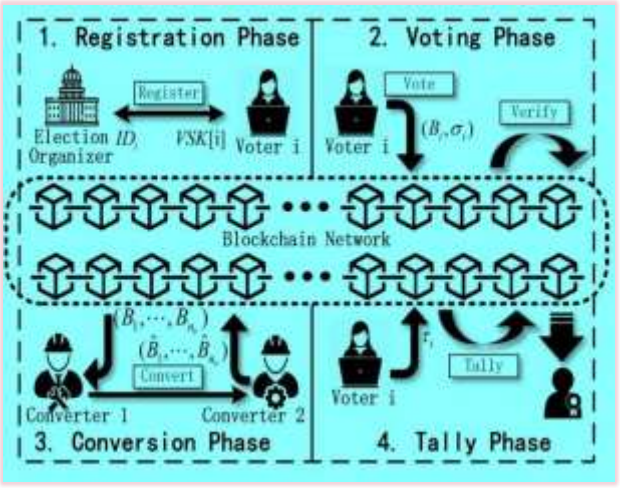

Fig: Architecture design

3.1 Registration Phase:

Election ID | Organizer: A unique Election ID is created for each election. An Organizer oversees and manages the election process.

Register: A potential voter initiates registration by interacting with the system. The system verifies the voter's identity and eligibility *to vote.*

VSK[i] (Voter Secret Key): Each registered voter is issued a unique, secret key VSK[i]. This key ensures vote anonymity, security, and integrity.

Voter i: Represents the individual voter in the system after successful registration. Identified in the system only through their VSK[i], preserving privacy.

3.2 Voting Phase:

Vote Submission: Elector submits their vote as a ballot-signature pair**.**

Digital Signature: is created using the voter's secret key to prove High precision minimizes authenticity.

Verification: System checks: Voter is registered and Signature is valid using the voter's public key.

3.3 Conversion Phase:

ballots undergo a transformation or conversion process. This might be done for various reasons, such as: Mixing or Shuffling: To further enhance vote privacy, the ballots might be mixed or shuffled to obscure the link between (B'_1, ..., B'_n) and (B''_1, ..., B''_n): This notation suggests that the n a voter and their vote. Format Standardization: The ballots might be converted into a standard format suitable for tallying. Converter 1 & Converter 2: These represent entities responsible for the conversion process. The presence of two converters might imply a multi-party computation or a distributed approach to enhance security and prevent single points of failure.

3.4 Tally Phase:

τ_i: This symbol likely represents a partial tally or a component of the final tally computed based on the converted ballots. Tally: The system aggregates the partial tallies (τ_i) to produce the final election results. This icon represents the final, verified tally, indicating the completion of the voting process and the determination of the election outcome.

4. RESULTS:

Voting system using Blockchain Technology proposes a secure, transparent, and scalable e-voting platform that leverages blockchain technology and biometric authentication to ensure election integrity. It uses face recognition with a KNN classifier for accurate voter verification and OTP-based two-factor authentication to prevent impersonation or multiple voting. Votes are stored on a decentralized blockchain, ensuring tamper-proof, transparent, and privacy-preserving records. The system supports remote voting for greater accessibility, provides real-time vote tallying through smart contracts, and prevents duplicate or fraudulent voting via biometric and blockchain validation, making it suitable for large-scale, reliable elections.

5. CONCLUSION:

The project successfully integrates blockchain technology and face recognition to create a secure, transparent, and tamper-proof e-voting system. By combining blockchain's immutability with facial authentication using the KNN classifier, the system effectively prevents voter fraud, duplication, and unlawful entry. It makes the voting system more secure and transparent, ensuring accuracy and protecting voter confidentiality. The throughput in terms of secure vote storage, real-time verification, and scalability demonstrates this technology has the ability to reshape election systems and make democratic participation more inclusive and secure.

ACKNOWLEDGEMENT:

We wish to express our profound gratitude to our project guide, *Mrs. K Padmaja*, Assistant Professor, Department of Information Science and Engineering, East West Institute of Technology (EWIT), for her invaluable expertise, persistent encouragement, and meticulous guidance throughout this project. We also extend our sincere thanks to the Head of the Department, ** Dr Raja Meyyan **, for providing the necessary facilities and support.

REFERENCES:

1. Samuel, O., Bi, L., and Muazu, T. (2022). It is a decentralized trust management system that leverages federated learning with blockchain technology. 15(1) Sustainability, 374.
2. Prakash, P., S., Parra-Fuente, J., Crespo, R. G., & Trivedi, M. C. (2023). Enhancing the security of medical records in blockchain-powered digital healthcare ecosystems facilitated by the Internet of Things Information Sciences, 629, 703-718.
3. D. Di, W., and Ahmed, W. (2022). A threshold ring signature system combined with blockchain technology to provide incentive trust management and validate traffic events in VANETs. 6715 in Sensors, 22(17).
4. Saba, T., Lloret, J., Rehman, A., Haseeb, K., & S. A. (2023). Decentralized blockchain system based on trust, utilizing Internet of Agriculture.