*United International Journal of Engineering and Sciences*
*(UIJES – A Peer-Reviewed Journal); ISSN:2582-5887 | Impact Factor:8.075(SJIF)*
*Volume 5 | Special Issue 1 | 2025 Edition*
*National Level Conference on "Advanced Trends in Engineering Science & Technology" – Organized by RKCE*

# Decentralised and Secure E-Voting System Using Blockchain, Face Recognition, and Homomorphic Encryption

**Mr. Shabaaz Shaik[1], Mrs. D. Sudha Rani[2]**

[1,2]Assistant Professor Department of Computer Science and Engineering

RK College Of Engineering

Vijayawada, India

[1]shabaaz.rkce@gmail.com ; [2]sudha.sathwika@gmail.com

***Abstract-*** **Electronic voting has emerged as a modern alternative to traditional paper-based elections, yet it faces significant challenges related to security, voter authentication, transparency, and privacy. While blockchain technology offers decentralisation and immutability, existing e-voting systems often lack robust identity verification and privacy-preserving mechanisms. A decentralized and secure e-voting system that integrates blockchain, face recognition for biometric authentication, and homomorphic encryption to ensure both transparency and voter privacy. The proposed system utilises face recognition for voter authentication, preventing identity fraud and unauthorised access. Once authenticated, the voter casts their encrypted ballot, which is immutably recorded on the blockchain through smart contracts, ensuring tamper-proof and auditable elections. Homomorphic encryption is employed to allow vote tallying without decrypting individual votes, preserving voter anonymity while maintaining election integrity. To validate our approach, we deployed the system on Ethereum and Hyperledger Fabric, comparing their performance in terms of speed, security, and scalability. Our results demonstrate that both public and private blockchains can support secure and transparent e-voting with minimal computational overhead. By combining biometric authentication, cryptographic security, and decentralised ledger technology, our system provides a trustworthy, fraud-resistant, and privacy-preserving voting mechanism, ensuring fairness and accessibility in digital elections.**

***Keywords:*** **Blockchain, e-voting, homomorphic encryption, biometric authentication, face recognition, decentralised elections.**

## I. INTRODUCTION

### 1.1 Background & Motivation

Voting is the foundation of democratic governance, enabling citizens to express their choices in political, organisational, and institutional decisions. Historically, elections have relied on paper-based voting systems, which, despite their simplicity, present significant challenges related to security, transparency, and accessibility. Over the past two decades, electronic voting (e-voting) has gained traction as a means to streamline the voting process, reduce human error, and improve efficiency. However, conventional e-voting systems are often centralised, vulnerable to cyber threats, and prone to electoral fraud, raising concerns about trust and integrity in elections.

Blockchain technology has emerged as a promising solution to address these issues due to its decentralised, immutable, and transparent nature. A blockchain-based voting system ensures that once a vote is recorded, it cannot be altered or deleted, mitigating risks of vote tampering or election rigging. Additionally, smart contracts can automate election rules, ensuring fairness and eliminating third-party

manipulation. However, while blockchain provides a secure framework, challenges remain regarding voter authentication, privacy protection, and scalability.

### 1.2 Problem Statement

Existing voting systems, both paper-based and electronic, suffer from the following critical issues:

1. **Lack of Transparency** – Traditional voting methods require trusted intermediaries, which can lead to potential fraud or manipulation.
2. **Voter Identity Fraud** – Weak authentication methods in e-voting can lead to impersonation, duplicate voting, or unauthorised access.
3. **Tampering and Data Breaches** Centralized e-voting databases are vulnerable to cyberattacks, vote manipulation, and hacking.
4. **Lack of Voter Privacy** – Many blockchain-based e-voting solutions store votes transparently but fail to protect the secrecy of individual votes.
5. **Limited Accessibility** – Paper-based voting requires physical presence, while some e-voting systems demand complex registration processes, limiting participation.

To address these issues, we propose a secure, privacy-preserving, and tamper-resistant e-voting system that ensures:

- **Decentralization:** Eliminating the need for a central authority through blockchain.
- **Strong Voter Authentication:** Using face recognition for biometric verification.
- **Immutability and Security:** Storing encrypted votes on the blockchain.
- **Privacy Preservation:** Implementing homomorphic encryption to ensure voter anonymity.
- **Automated Vote Counting:** Using smart contracts for a secure and transparent tallying process.

### 1. 3 Objectives of the Proposed System

The primary objectives of this system are:

1. To ensure secure and verifiable elections by leveraging blockchain's immutability and decentralization.
2. To implement biometric-based voter authentication using facial recognition, preventing impersonation and fraud.
3. To protect voter privacy by employing homomorphic encryption, ensuring that votes remain confidential even on a public ledger.
4. To enable real-time transparency while preventing manipulation through cryptographic mechanisms and smart contracts.
5. To create a scalable and efficient voting system deployable on both public and private blockchains (e.g., Ethereum and Hyperledger Fabric).
6. To enhance accessibility and inclusivity, allowing users to vote remotely while maintaining high security standards.

# II. LITERATURE SURVEY

Electronic voting has evolved significantly from traditional paper ballots to electronic and online voting systems. However, concerns regarding security, transparency, privacy, and scalability have hindered widespread adoption. Blockchain technology has been proposed as a solution to these challenges due to its immutability, decentralization, and cryptographic security. This section reviews previous research on blockchain-based e-voting, highlighting their strengths and limitations.

### 2.1 Blockchain for Secure Electronic Voting

Zyskind et al. (2015) proposed a decentralised voting system using blockchain to ensure transparency and auditability. Their approach utilised a public blockchain for vote recording and verification. While their system improved security, it lacked a proper voter authentication mechanism, making it vulnerable to Sybil attacks, where multiple fake identities could be created to manipulate the election outcome.

### 2.2 Follow My Vote: Blockchain-Based Online Voting

Khan et al. (2018) developed an Ethereum-based online voting system that leveraged smart contracts to automate vote counting and verification. The system ensured vote integrity and transparency, allowing voters to verify their votes on the blockchain. However, the use of Ethereum led to high transaction costs (gas fees) and scalability issues, making it impractical for large-scale elections.

### 2.3 Homomorphic Encryption for Secure Voting

Gennaro et al. (2016) explored the use of homomorphic encryption in e-voting, allowing votes to be computed without decryption, thereby maintaining voter privacy. Their approach prevented vote tampering and ensured secrecy. However, the computational cost was high, making real-time vote counting impractical. The lack of blockchain integration also meant that the system relied on central authorities, reducing decentralisation.

# III. RELATED WORK

### 3.1 Traditional Voting Systems

Traditional voting methods, such as paper ballots, postal voting, and electronic voting machines (EVMs), have been widely used across the globe. However, these systems face multiple challenges:

- **Paper ballots** are prone to human errors, ballot stuffing, and fraud.
- **Postal voting** introduces security risks like lost or manipulated ballots.
- **EVMs**, while faster, suffer from vulnerabilities such as hacking, tampering, and lack of transparency in vote counting.

Due to these concerns, researchers and governments have explored electronic and blockchain-based voting systems to improve security and efficiency.

### 3.2 Existing E-Voting Models

Several electronic voting models have been proposed and implemented. Below are key e-voting models and their limitations.

#### 3.2.1 Centralized E-Voting Systems

Centralized e-voting platforms store votes in a single database, making them vulnerable to attacks. Examples include:

- **Direct Recording Electronic (DRE) Voting Machines** – Store votes electronically but are susceptible to software tampering.
- **Internet-Based Voting (i-Voting)** – Used in countries like Estonia, but faces concerns regarding authentication and cyber threats.

### 3.3 Innovations in Our Approach

Our Decentralized and Secure E-Voting System introduces three key enhancements:

**Face Recognition for Authentication** – Ensures only registered voters can cast votes, eliminating identity fraud.
**Homomorphic Encryption for Privacy** – Votes are encrypted, preventing unauthorized access while allowing computations.
**Full Blockchain Integration** – No central authority controls the system, making it tamper-proof.

Unlike previous models, our system ensures security, transparency, privacy, and decentralization in a single framework.

## IV. SYSTEM ARCHITECTURE

**4.1 Overview of the E-Voting System** Our system integrates blockchain, homomorphic encryption, and facial recognition to ensure a secure and transparent e-voting process. The decentralised approach records all transactions on a blockchain ledger while preserving voter privacy.

**Key Components:**

1. **Voter Registration & Authentication** – Biometric verification via face recognition.
2. **Vote Encryption & Casting** – Homomorphic encryption secures votes.
3. **Blockchain Network** – Stores encrypted votes using smart contracts.
4. **Vote Counting & Results** – Secure tallying via homomorphic decryption.

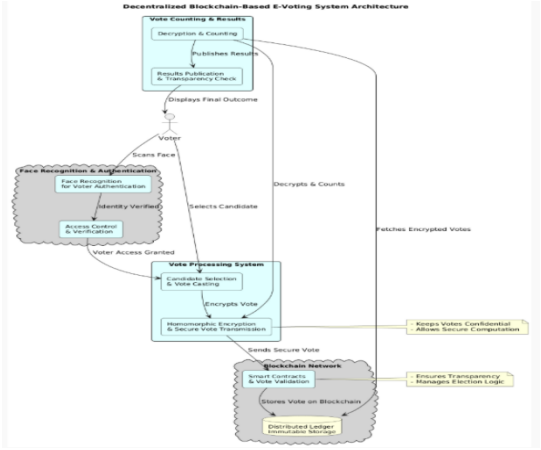


Fig.1. System Architecture

### 4.2 System Components & Workflow

Voter's register using biometric data (face scan) via a secure portal. A deep-learning model verifies identity and assigns a cryptographic keypair. Identity data is securely stored on a private blockchain.

Authenticated voters cast votes via a web/mobile dApp.Votes are encrypted using homomorphic encryption before submission. Encrypted votes are stored as blockchain transactions.

Uses a permissioned/public blockchain with smart contracts. Ensures immutable, tamper-proof vote storage. Homomorphic decryption allows tallying without exposing individual votes. Secure multi-party computation prevents centralised control. Results are publicly verifiable on the blockchain.

**Table I: Security & Privacy Mechanisms**

| Feature | Technology | Purpose |
|---|---|---|
| Face Recognition | OpenCV, TensorFlow | Prevents identity fraud |
| Homomorphic Encryption | Paillier | Ensures vote privacy |
| Blockchain Ledger | Ethereum, Hyperledger | Stores immutable votes |

## V. IMPLEMENTATION & EVALUATION

Our **blockchain-based e-voting system** uses **Ethereum & Hyperledger Fabric** for secure, transparent voting.

- **Authentication:** Face recognition + homomorphic encryption.
- **Smart Contracts:** Manage voting rules & validation.
- **Blockchain Storage:** Ensures tamper-proof vote recording.
- **Vote Counting:** Decryption after polling ensures confidentiality.

**Ethereum:** Uses Solidity smart contracts, encrypted vote submission, and blockchain validation. **Hyperledger Fabric:** Uses secure chaincode, permissioned voting, and vote visualization.

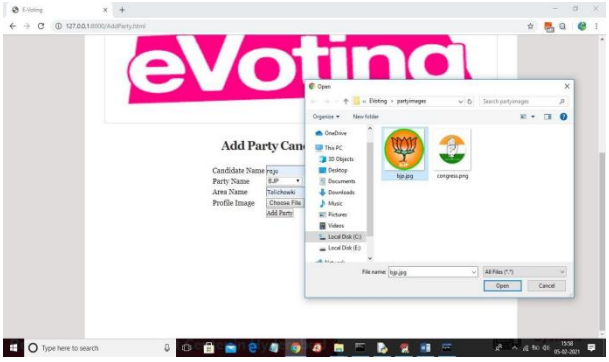


**Fig.2. User Login**


**Fig.3. Vote Polling**

## VI. CONCLUSION

secure and decentralized e-voting system utilizing blockchain, homomorphic encryption, and face recognition to enhance election transparency, security, and voter privacy. Tamper-proof voting using blockchain immutability.Privacy-preserving encryption ensuring ballot confidentiality.Scalable and cost-effective deployment using Ethereum and Hyperledger.Facial recognition authentication reducing voter fraud risks.

## REFERENCES

[1] N. Kshetri and J. Voas, "Blockchain-Enabled E-Voting," IEEE Software, vol. 35, pp. 95-99, jul 2018.

[2] M. Pawlak, J. Guziur, and A. Poniszewska-Maranda, "Voting Processwith Blockchain Technology: Auditable Blockchain Voting System," inLecture Notes on Data Engineering and Communications Technologies, pp. 233-244, Springer, Cham, 2019.

[3] B. Singhal, G. Dhameja, and P. S. Panda, "How Blockchain Works," in Beginning Blockchain, pp. 31-148, Berkeley, CA: Apress, 2018.

[4] Agora, "Agora Whitepaper," 2018.

[5] R. Perper, "Sierra Leone is the first country to use blockchain duringan election - Business Insider," 2018.

[6] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," tech.rep., 2008.

[7] G. Wood et al., "Ethereum: A secure decentralized generalized transaction ledger," Ethereum project yellow paper, vol. 151, pp. 1-32, 2014.

[8] S. Landers, "Netvote: A Decentralized Voting Platform – Netvote Project Medium," 2018.

[9] P. McCorry, S. F. Shahandashti, and F. Hao, "A Smart Contract for Boardroom Voting with Maximum Voter Privacy," in Lecture Notes in Computer Science, ch. FCDS, pp. 357-375, Springer, Cham, 2017.

[10] Z. Brakerski and V. Vaikuntanathan, "Efficient Fully Homomorphic Encryption from (Standard) LWE,"SIAM Journal on Computing, vol. 43,pp. 831-871, jan 2014.

[11] O. Goldreich and Y. Oren, "Definitions and properties of zero knowledge proof systems," Journal of Cryptology, vol. 7, no. 1, pp. 1-32, 1994.