

# Secure Vote using Block chain and Face Recognition, Designed to ensure a secure voting process.

Naveen Kumar Pattipati<sup>1</sup>, Abhishek Singh<sup>2</sup>, Dandetikar Deepthi<sup>3</sup>, Dhareddy Keerthi<sup>4</sup>, Chinmaya Kumar Patra<sup>5</sup>

<sup>1</sup>Associate Professor, Dept. of Computer Science Engineering, Joginpally BR Engineering College, Ranga Reddy, Telangana, India.

<sup>2</sup>Dept of Computer Engineering, Joginpally BR Engineering College, Ranga Reddy, Telangana, India.

<sup>3</sup>Dept of Computer Engineering, Joginpally BR Engineering College, Ranga Reddy, Telangana, India.

<sup>4</sup>Dept of Computer Engineering, Joginpally BR Engineering College, Ranga Reddy, Telangana, India.

<sup>5</sup>Dept of Computer Engineering, Joginpally BR Engineering College, Ranga Reddy, Telangana, India.

\*\*\*

**Abstract** - Secure Vote is a decentralized digital voting platform that combines blockchain technology with biometric face recognition to provide secure, transparent, and trustworthy elections. The system is designed for student elections, organizational polls, and local governance, where traditional online voting methods often face challenges such as centralized control, identity fraud, and a lack of transparency. Instead of relying on manual verification methods such as ID uploads or OTPs, Secure Vote uses AI-powered face recognition to accurately and conveniently authenticate voters. Each vote is recorded on the Ethereum blockchain using Solidity-based smart contracts, ensuring immutability and tamper-proof validation. Votes are encrypted and stored on-chain, preserving voter privacy while maintaining transparency and verifiability. The system architecture includes biometric enrollment, deep learning-based face recognition, a secure voting interface, blockchain-enabled vote storage, and an admin dashboard for real-time monitoring and result management. Web3.js is used to interact with the blockchain and provide instant, consistent results across the decentralized network. The platform is developed using Python, Solidity, TensorFlow, OpenCV, and Flask/React, and tested on Ethereum using Ganache. By integrating biometric authentication with decentralized blockchain infrastructure, Secure Vote provides a reliable, scalable, and tamper-proof voting solution that enhances trust, security, and fairness in modern digital election environments.

**Key Words:** Blockchain , Digital Voting, Face Recognition, Biometric Authentication, Ethereum, Smart Contracts, Web3 .js, Secure Voting, Decentralized System, E-Voting.

## 1. INTRODUCTION

Digital voting systems are becoming increasingly important for conducting elections in a fast, efficient, and accessible manner. However, traditional online voting methods often rely on centralized databases and basic authentication techniques such as passwords, ID cards, or OTP verification. These approaches are vulnerable to

identity fraud, vote tampering, and lack of transparency, which reduces trust in the voting process.

Blockchain technology provides a decentralized and immutable platform for securely recording votes, ensuring that once a vote is cast, it cannot be modified or deleted. At the same time, biometric authentication using face recognition improves voter verification by allowing only authorized individuals to participate in the election. Combining these technologies enhances both security and transparency in digital voting systems.

This project proposes **Secure Vote Using Blockchain and Face Recognition**, a secure electronic voting system that integrates facial biometric authentication with blockchain-based vote storage. The system verifies voters using face recognition and records votes using smart contracts on the blockchain. This approach prevents impersonation, ensures data integrity, and provides transparent result generation. The proposed system aims to deliver a reliable, secure, and tamper-proof voting solution suitable for modern digital election environments.

### 1.1 OBJECTIVE

The primary objective of the project "Secure Vote Using Blockchain and Face Recognition" is to develop a secure, transparent, and reliable electronic voting system by integrating blockchain technology with facial biometric authentication. The system aims to enhance the integrity of elections while ensuring voter privacy and eliminating common vulnerabilities present in traditional voting methods.

The specific objectives of the project are:

- To design a secure e-voting system that ensures the authenticity and integrity of votes.
- To implement face recognition-based biometric authentication for accurate voter identification.

- To prevent voter impersonation and multiple voting using unique biometric verification.
- To utilize blockchain technology for tamper-proof, transparent, and immutable vote storage.
- To eliminate centralized control by adopting a decentralized voting mechanism.
- To ensure privacy and confidentiality of voters during the voting process.
- To enhance trust, reliability, and efficiency in the electoral system.

This project demonstrates how emerging technologies such as blockchain and artificial intelligence can be effectively combined to improve the security and credibility of modern electronic voting systems.

## 1.2 SCOPE AND CHALLENGES

### [1] Scope

The proposed system focuses on implementing a decentralized voting platform that integrates facial biometric authentication with blockchain-based vote storage. It covers voter enrollment with facial data capture, face recognition-based login, secure vote casting, and recording votes through smart contracts on the blockchain. An administrative module is included for election creation, voter management, and result monitoring. The system is intended for controlled environments such as academic institutions, organizations, and pilot-level elections. The design also provides a framework that can be extended with higher-capacity blockchain networks and improved infrastructure for larger deployments.

### [2] Challenges

Face recognition performance may vary due to lighting conditions, camera resolution, and changes in facial appearance, which can affect authentication reliability. Blockchain transaction time and network congestion may introduce delays during peak voting periods. Secure handling of biometric templates is critical to prevent unauthorized access or misuse. Integration between the face recognition module and blockchain layer also requires careful synchronization to avoid duplicate voting or transaction failures. Additionally, maintaining usability while enforcing strong security mechanisms remains a key implementation challenge.

## 1.2 PROBLEM ANALYSIS

Many digital voting systems rely on centralized servers for authentication, vote storage, and result generation. This creates risks such as unauthorized database modification, insider manipulation, and single points of failure. If administrative access is compromised, vote records can be altered without clear traceability, affecting election integrity.

Authentication methods such as passwords, ID numbers, or OTPs do not ensure the physical presence of voters. These credentials can be shared or misused, leading to impersonation and multiple voting. Additionally, conventional databases allow update or deletion of stored votes, making them vulnerable to post-election manipulation.

Another challenge is maintaining transparency while preserving voter privacy. Existing systems either expose sensitive voter information or lack mechanisms for independent verification. These limitations highlight the need for a voting system that provides strong biometric authentication, immutable vote storage, decentralized control, and verifiable yet privacy-preserving election results.

## 2. LITERATURE REVIEW

[1] M. V. Vladucu et al., 2023 – “E-Voting Meets Blockchain: A Survey”. This survey reviews blockchain-based electronic voting systems, identifying their strengths (immutability, decentralization) and challenges (scalability, voter privacy). It provides a broad overview of existing architectures and highlights future directions.

[2] S. Minaee et al., 2020 – “Biometrics Recognition Using Deep Learning: A Survey”. The authors summarize deep learning techniques applied to biometric recognition, including face, iris, fingerprint, and voice. It demonstrates how AI enhances accuracy but raises concerns about privacy and ethics in real-world deployment.

[3] M. Khasawneh et al., 2020 – “A Biometric-Secure e-Voting System.” This project implements an e-voting prototype combining blockchain and biometric authentication. Their focus was on securing elections by binding each vote to a unique biometric identity, reducing fraud.

[4] I. Grishchenko et al., 2018 – “Security Analysis of Ethereum Smart Contracts. This work presents a semantic framework to analyze Ethereum smart contracts for vulnerabilities like reentrancy and overflow. Since e-voting often uses Ethereum, these findings are critical for preventing attacks on election smart contracts.

[5] M. Specter et al., 2020 – “The Ballot is Busted Before the Blockchain.” The authors audit the Voatz mobile voting system (used in U.S. elections) and uncover serious vulnerabilities in its blockchain-based backend and mobile app. Their work shows the importance of rigorous testing in e-voting.

[6] R. Ananthkrishnan and M. Venkatesan, 2022 – “Survey of Blockchain E-Voting Mechanisms.” This paper compares different blockchain models (permissioned vs. public blockchains) used in voting systems and evaluates their trade-offs in scalability, security, and transparency.

### 3. METHODOLOGY

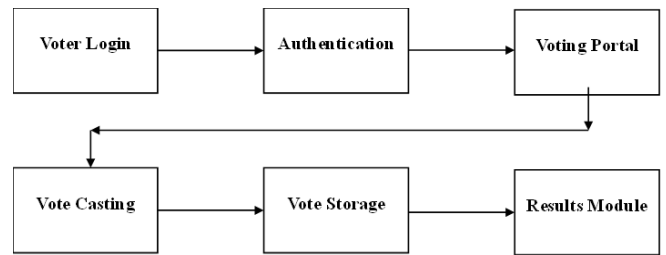
The proposed Secure Vote system follows a structured implementation approach that integrates biometric authentication with blockchain-based vote recording. The workflow consists of the following stages:

#### 1. System Architecture Design

The system is structured into functional modules, including voter enrollment, facial authentication, vote casting, blockchain transaction handling, and result visualization. The architecture defines the interaction between the biometric layer, application layer, and blockchain network.

2. **Voter Enrollment:** Users register by submitting basic details along with facial data captured through a camera. Multiple facial samples are collected and stored as reference templates for identity verification during voting.
3. **Image reprocessing:** Captured facial images are processed using face detection, cropping, resizing, and grayscale conversion. This step standardizes the dataset and improves feature extraction accuracy.
4. **Face Recognition Authentication:** A deep learning-based model extracts facial features and generates embeddings for each registered voter. During login, a live image is captured and matched with stored templates to confirm voter identity before allowing access to the ballot.
5. **Blockchain-Based Vote Recording:** After authentication, the selected vote is converted into a blockchain transaction. The transaction is submitted to the Ethereum network, ensuring decentralized and immutable storage.
6. **Smart Contract Logic:** Voting rules are implemented using Solidity smart contracts. These contracts validate voter eligibility, restrict duplicate voting, and permanently store vote data on-chain.
7. **Application Interface:** A web interface enables voter registration, authentication, and vote submission. The frontend communicates with the blockchain using Web3 integration for transaction execution.
8. **Result Processing:** Votes stored on the blockchain are retrieved and aggregated. The admin dashboard displays real-time counts without exposing voter identities.
9. **System Testing:** The complete system is evaluated for authentication accuracy, transaction reliability, and module integration before deployment.

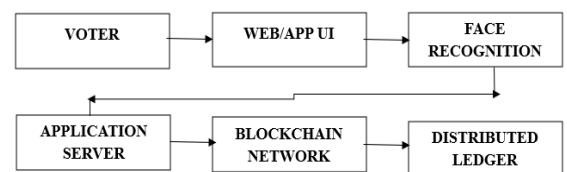
### 4. MODULES



#### System Workflow (Methodology Steps)

1. **Voter Login:** Registered user accesses the system and initiates the voting session.
2. **Authentication:** A live facial image is captured and matched with a stored biometric template for identity verification.
3. **Voting Portal:** Verified voter is redirected to the ballot interface displaying candidates or voting options.
4. **Vote Casting:** The selected option is submitted after checking duplicate voting constraints.
5. **Vote Storage:** The vote is encrypted and recorded as a blockchain transaction through smart contract execution.
6. **Results Module:** On-chain votes are retrieved, aggregated, and displayed through the result dashboard.

### 5. ARCHITECTURE



#### System Architecture Flow

1. **Voter:** Initiates interaction with the voting system to participate in the election.
2. **Web/App UI:** Interface collects voter input, manages navigation, and forwards authentication requests.
3. **Face Recognition:** Captures live facial image and performs biometric matching with registered templates.
4. **Application Server:** Processes authentication response, controls voting logic, and prepares transaction data.
5. **Blockchain Network:** Receives a vote transaction from the server and executes smart contract validation.

6. **Distributed Ledger:** Validated vote is appended as an immutable record and used for result computation.

## 6. ALGORITHM

1. Capture a live image from the camera.
2. Detect faces using Haar Cascade/CNN.
3. Convert the image to grayscale.
4. Extract facial features.
5. Compare with stored face templates.
6. If match score  $\geq$  threshold: Authentication successful.
7. Else: Reject user.

## 7. BENEFICIARIES

- **Voters:** Secure authentication, single vote enforcement, and privacy-preserving participation.
- **Election Administrators:** Automated vote handling, reduced manual intervention, and transparent result computation.
- **Organizations and Institutions:** Digital election management with reduced operational overhead and improved reliability.
- **Research and Academic Use:** Reference implementation for blockchain-based voting and biometric authentication studies.
- **General Public / Decision-Making Bodies:** Improved transparency, tamper-resistant voting, and increased trust in digital election processes.
- **Educational Institutions:** Department-level elections, student council polling, and committee selections with automated verification.
- **Corporate Organizations:** Board voting, policy approvals, and internal decision polling with audit-ready records.
- **Non-Government Organizations (NGOs):** Member voting, leadership selection, and resolution approval with verifiable outcomes.
- **Remote Participants:** Location-independent participation without physical presence requirements.
- **Event Management Committees:** Contest judging, award selection, and audience voting with controlled access.
- **Professional Associations:** Member-based elections, certification body decisions, and governance voting.

- **Research Groups:** Survey-based voting experiments and controlled participant validation.
- **Startup Communities:** Founder voting, funding decisions, and proposal prioritization with transparent tracking.
- **Online Communities:** Moderated polls, governance voting, and community-driven decision making.
- **Audit and Compliance Teams:** Verifiable vote logs, traceable transactions, and integrity validation.

## 8. RESULTS AND OUTPUTS

The implemented system successfully authenticated voters using facial recognition before granting ballot access. Each verified voter was allowed a single submission, enforced through smart contract validation. Cast ballots were converted into blockchain transactions and appended to the distributed ledger, preventing modification after submission. The authentication pipeline matched live facial input with stored templates and rejected unmatched identities.

Vote data retrieved from on-chain records produced consistent counts without exposing voter information. The administrative dashboard displayed aggregated results generated directly from blockchain entries. End-to-end execution from biometric verification to ledger storage operated without manual handling. Testing confirmed stable recognition performance, single-vote enforcement, and reliable transaction recording across multiple voting sessions.

### OUTPUTS:

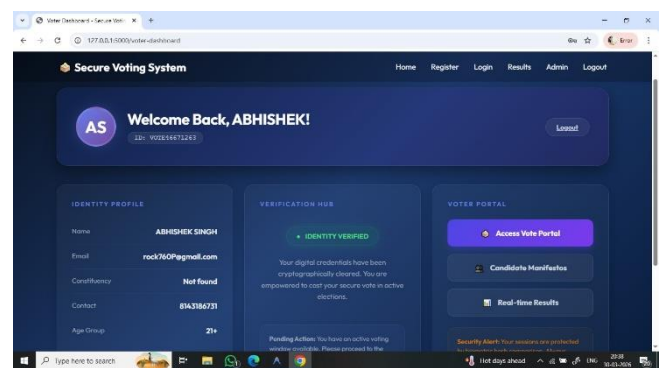


Fig 8.1 Voter Dashboard

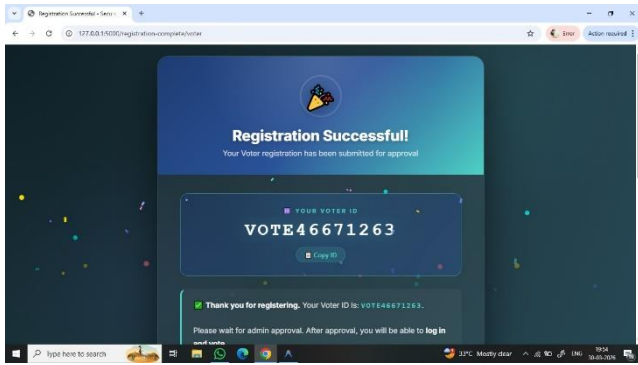


Fig 8.2 Voter Successful Registration

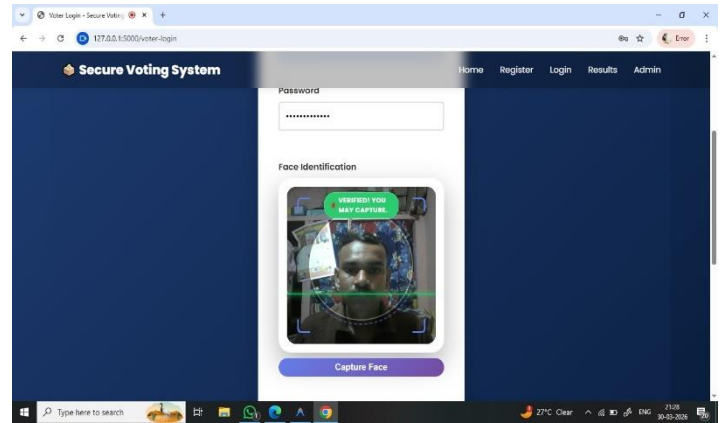


Fig 8.6 FACE AUTHENTICATION

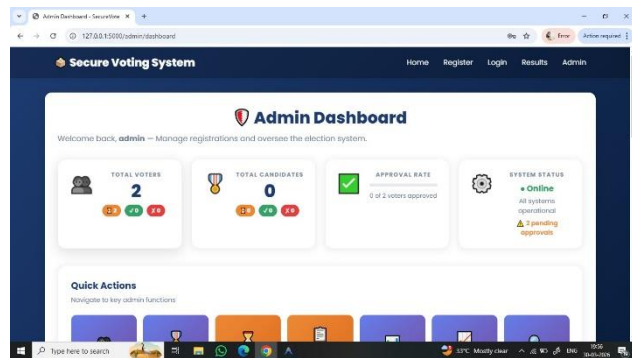


Fig 8.3 Admin Dashboard

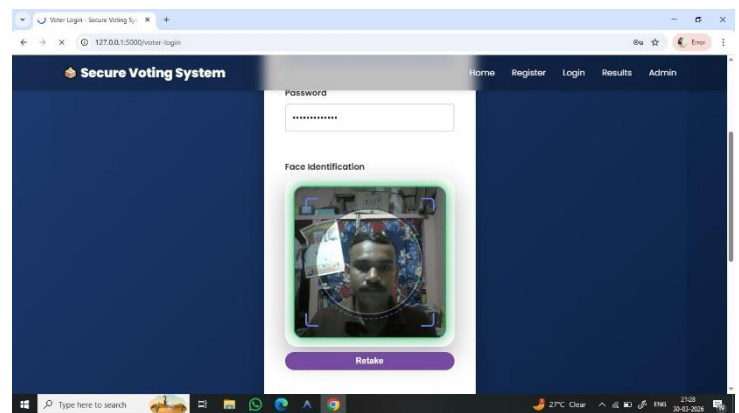


Fig 8.7 FACE RECOGNITION

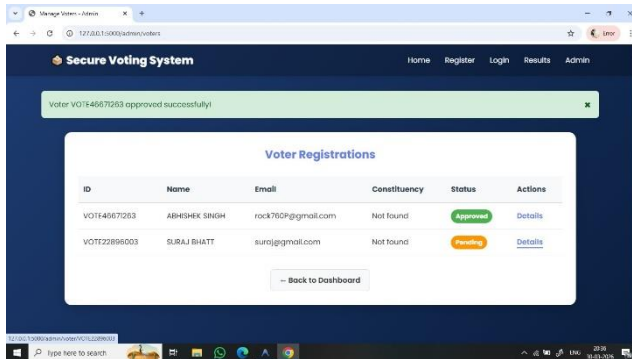


Fig 8.4 Voter Approval by Admin

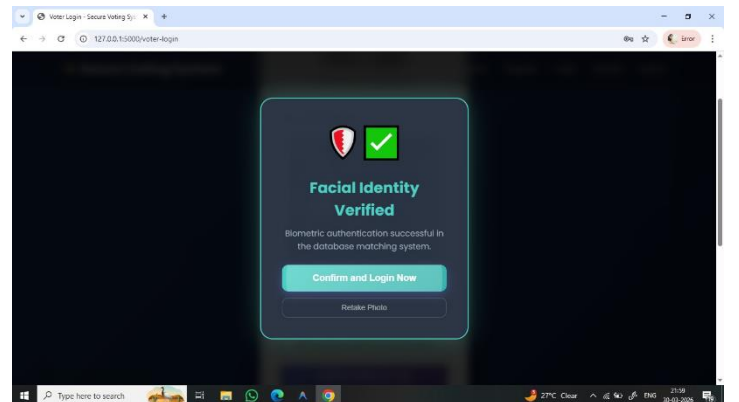


Fig 8.8 Face identity verified

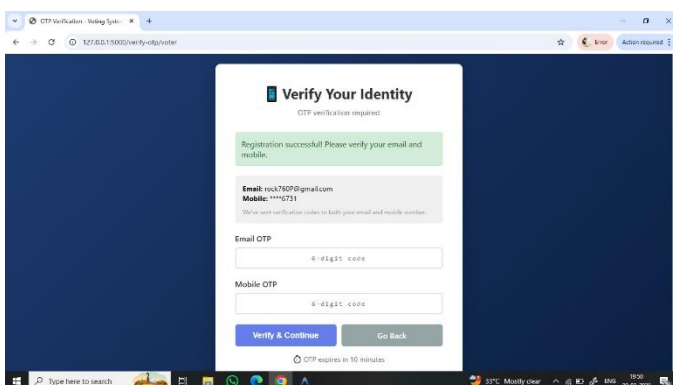


Fig 8.5 Credentials Verification

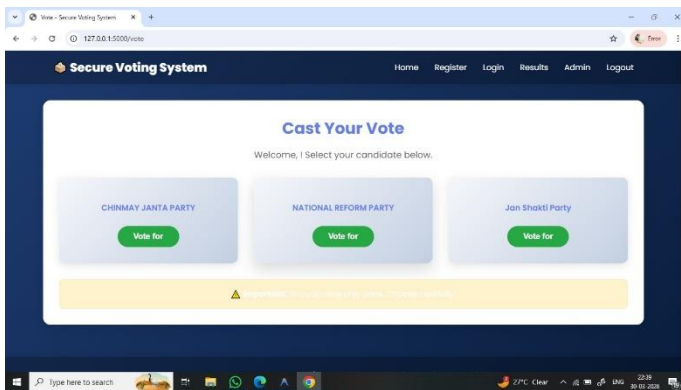


Fig 8.9 Voting Dashboard

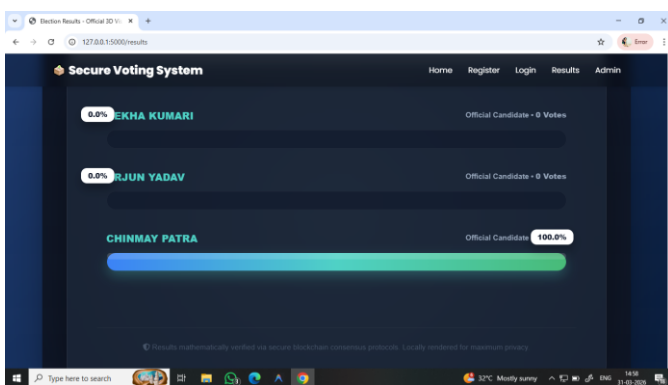


Fig 8.10 result Dashboard

## 9. FUTURE ENHANCEMENTS

1. The proposed Secure Vote framework can be extended through multiple advanced technological integrations to improve robustness, scalability, and resilience against emerging threats in digital election ecosystems.
2. **Multi-Modal Biometric Fusion:** Incorporating additional biometric modalities such as iris recognition and fingerprint verification can enable sensor-level or decision-level fusion, thereby increasing authentication confidence and minimizing false acceptance and rejection rates.
3. **Decentralized Identity (DID) Integration:** Adopting decentralized identity frameworks can eliminate reliance on centralized identity providers. Self-sovereign identity mechanisms can allow voters to control their credentials while enabling cryptographic verification.
4. **Layer-2 Blockchain Optimization:** Transitioning from base-layer blockchain networks to Layer-2 scaling solutions such as rollups or sidechains can significantly reduce gas costs, improve throughput, and mitigate latency during high-concurrency voting scenarios.

5. **Zero-Knowledge Cryptographic Protocols:** The implementation of zero-knowledge proofs (ZKP) can enable verifiable vote validation without disclosing voter identity or vote content, thereby strengthening privacy guarantees while maintaining auditability.
6. **Liveness Detection and Anti-Spoofing Models:** Advanced deep learning-based liveness detection mechanisms, including temporal feature analysis and 3D depth estimation, can be integrated to counter presentation attacks using images, videos, or synthetic media.
7. **Homomorphic Encryption for Vote Computation:** Incorporating homomorphic encryption techniques can allow vote aggregation to be performed on encrypted data without requiring decryption, thereby preserving end-to-end confidentiality.
8. **Distributed Storage Integration (IPFS):** Sensitive off-chain data such as biometric templates or encrypted vote metadata can be stored using distributed storage systems like IPFS, ensuring data availability and resistance to centralized failure points.
9. **Adaptive Consensus Mechanisms:** Exploring alternative consensus protocols such as Proof-of-Authority (PoA) or Delegated Proof-of-Stake (DPoS) can optimize transaction validation efficiency in permissioned or semi-permissioned election environments.
10. **Anomaly Detection using AI Models:** Behavioral analytics and anomaly detection models can be deployed to identify irregular voting patterns, bot-driven participation, or coordinated manipulation attempts in real time.
11. **Edge Computing for Biometric Processing:** Shifting facial recognition computations to edge devices can reduce server load, decrease latency, and enhance privacy by minimizing transmission of raw biometric data

## 10. CONCLUSION

The Secure Vote system introduces a technologically rigorous paradigm for electronic voting by synergizing decentralized blockchain infrastructure with AI-driven biometric authentication. This integration effectively mitigates critical vulnerabilities inherent in conventional voting architectures, including centralized data control, identity spoofing, and post-election data manipulation. The utilization of blockchain ensures cryptographic immutability, distributed consensus, and verifiable audit trails, thereby reinforcing the integrity and non-repudiation of cast votes. Concurrently, the deployment of deep learning-based facial recognition establishes a high-assurance authentication mechanism that binds each vote

to a unique biometric identity, significantly reducing the probability of impersonation and duplicate participation. Furthermore, the system maintains a balanced trade-off between transparency and privacy by leveraging encryption and controlled data exposure, ensuring that electoral outcomes remain verifiable without compromising voter confidentiality. The modular architecture also supports extensibility, enabling integration with advanced cryptographic protocols and scalable blockchain solutions.

Although certain operational constraints such as network latency, biometric variability, and computational overhead persist, the proposed framework demonstrates substantial potential for refinement and large-scale adaptation. With continued advancements in distributed systems, artificial intelligence, and cryptographic engineering, such hybrid voting models can redefine the standards of trust, security, and efficiency in digital electoral processes.

In essence, Secure Vote represents a forward-looking, resilient, and tamper-resistant voting infrastructure capable of addressing the evolving demands of modern democratic and organizational decision-making systems.