SECURE E-VOTING WITH BLOCKCHAIN:ENHANCING AES AND RSA ENCRYPTION WITH FACE AUTHENTICATION TECHNOLOGY

Ms.PAUL T JABA M.E.,(Ph.d)
Assistant Professor - Computer Science and Engineering,
St. Joseph College of Engineering, Chennai-602117, Tamil Nadu,
Email Id – jabapt2@gmail.com

Mr.PRINCE JOSEPH . U
UG Student, Computer Science and Engineering,
St. Joseph College of Engineering, Chennai-602117, Tamil Nadu,
Email Id –princejoseph2209@gmail.com

Mr.KOSALRAM . P
UG Student, Computer Science and Engineering,
St. Joseph College of Engineering, Chennai-602117, Tamil Nadu,
Email Id –kosalpalani1@gmail.com

ABTRACT: Electronic voting (e-voting) systems are becoming increasingly important in modern democratic processes. However, traditional e-voting systems face critical challenges such as vote tampering, identity fraud, lack of transparency, and centralized control vulnerabilities. This project proposes a Secure E-Voting System that integrates Blockchain technology, Advanced Encryption Standard (AES), Rivest–Shamir–Adleman (RSA) encryption, and Face Authentication Technology to enhance security, transparency, and voter verification. The proposed system utilizes Blockchain to create a decentralized and tamper-proof ledger for storing votes. Advanced Encryption Standard is used for fast and secure encryption of voting data, while RSA ensures secure key exchange and digital signatures. Additionally, face authentication powered by Face Recognition verifies voter identity, preventing impersonation and duplicate voting. By combining cryptography and biometric authentication within a blockchain framework, the system ensures confidentiality, integrity, transparency, and voter anonymity. This approach enhances trust in digital elections while reducing electoral fraud and administrative overhead.

I. INTRODUCTION

Voting is a fundamental right in democratic societies. Traditional paper-based voting systems, while reliable, involve high costs, logistical complexity, and slow result processing. Electronic voting systems were introduced to overcome these challenges, but they often rely on centralized databases, making them vulnerable to hacking, manipulation, and unauthorized access.

To address these limitations, emerging technologies such as Blockchain offer decentralized data storage where records cannot be altered without network consensus. Blockchain ensures transparency, immutability, and traceability of votes while preserving voter anonymity.

Encryption techniques play a crucial role in securing digital votes. Advanced Encryption Standard provides high-speed encryption for vote data, while RSA ensures secure key management and digital authentication. Furthermore, biometric systems such as Face Recognition enhance identity verification, reducing voter fraud and multiple voting attempts.

This project integrates blockchain, cryptography, and biometric verification into a unified e-voting platform to provide a secure, transparent, and efficient electoral system.

II. BACKGROUND AND MOTIVATION

Over the years, several countries have experimented with electronic voting systems. However, concerns remain regarding:

- Vote tampering and cyber-attacks
- Insider manipulation
- Lack of transparency in centralized systems
- Identity theft and duplicate voting
- Data breaches

Traditional encryption methods alone cannot ensure complete trust if the system architecture is centralized. Blockchain technology offers a decentralized alternative where each vote is recorded in a block and linked cryptographically to previous blocks, ensuring immutability.

The integration of Advanced Encryption Standard and RSA strengthens data protection through hybrid encryption. Meanwhile, Face Recognition ensures that only authorized voters can cast their votes.

Motivation

The primary motivations behind this project are:

1. **Enhancing Security** – Protect votes using strong cryptographic algorithms and decentralized storage.
2. **Preventing Voter Fraud** – Use face authentication to eliminate impersonation.

3. **Ensuring Transparency** – Allow public verification of results without revealing voter identity.
4. **Improving Efficiency** – Reduce manual counting and accelerate result declaration.
5. **Building Public Trust** – Increase confidence in digital electoral systems.

By combining Blockchain, AES, RSA, and Face Authentication, the system addresses major weaknesses of existing e-voting platforms and provides a secure and scalable solution for future digital elections.

III. NOVEL APPLICATIONS OF SECURE E-VOTING WITH BLOCKCHAIN:ENHANCING AES AND RSA ENCRYPTION WITH FACE AUTHENTICATION TECHNOLOGY

The proposed **Secure E-Voting System using Blockchain with Enhanced AES, RSA, and Face Authentication** introduces several innovative features that differentiate it from traditional electronic voting platforms. The novelty of this application lies in the **integration of decentralized blockchain technology, hybrid cryptographic encryption, and biometric face authentication** into a unified, secure voting ecosystem.

1. Hybrid Cryptographic Security Model

Unlike conventional systems that rely on a single encryption technique, this application combines:

- Advanced Encryption Standard for fast and secure encryption of vote data
- RSA for secure key exchange and digital signatures

This hybrid approach ensures:

- Confidentiality of votes
- Secure transmission of data
- Protection against man-in-the-middle attacks
- Strong voter authentication

2. Blockchain-Based Immutable Voting Ledger

The system uses Blockchain to store votes in decentralized blocks.

Novelty Features:

- Votes cannot be altered once recorded
- Transparent audit trail

- Elimination of centralized authority manipulation
- Distributed consensus validation

Each vote is hashed and linked to the previous block, ensuring tamper-proof election records.

3. Face Authentication for Voter Verification

The integration of Face Recognition adds a strong biometric layer to the system.

Innovative Aspects:

- Prevents impersonation
- Eliminates duplicate voting
- Enables remote secure voting
- Reduces dependency on physical voter ID cards

This makes the system highly suitable for online elections and remote voting scenarios.

4. Decentralized + Biometric Fusion Model

The key novelty of this project is the **fusion of biometric authentication with blockchain-based decentralized security**.

Traditional e-voting systems typically use:

- Password-based login
- Smart cards
- Centralized databases

This proposed system eliminates these vulnerabilities by combining:

- Biometric verification
- Cryptographic encryption
- Distributed ledger storage

5. Real-Time Transparent Result Verification

- Encrypted votes are stored on blockchain
- Counting can be performed securely and transparently
- Public verification without revealing voter identity

This enhances trust in the election process.

6. Remote and Scalable Digital Election Platform

The system can be applied to:

- Government elections
- University and college elections
- Corporate board voting
- Shareholder decision-making
- Online surveys with secure authentication

IV.ROLE AND POTENTIAL OF SECURE E-VOTING WITH BLOCKCHAIN:ENHANCING AES AND RSA ENCRYPTION WITH FACE AUTHENTICATION TECHNOLOGY

Secure E-Voting with Blockchain: Enhancing AES and RSA Encryption with Face Authentication Technology

ROLE OF THE PROPOSED SYSTEM

The proposed system plays a critical role in modernizing digital electoral processes by integrating decentralized security, advanced encryption, and biometric authentication.

1. Role of Blockchain Technology

Blockchain serves as the backbone of the system.

Key Roles:

- Provides a **decentralized voting ledger**
- Ensures **immutability of votes**
- Enables **transparent audit trails**
- Prevents unauthorized vote modification
- Removes dependency on centralized servers

Blockchain ensures that once a vote is recorded, it cannot be altered, deleted, or manipulated.

2. Role of AES Encryption

Advanced Encryption Standard is used to encrypt the actual voting data.

Key Roles:

- Protects vote confidentiality
- Provides fast encryption and decryption
- Secures stored vote information
- Ensures data privacy during transmission

AES ensures that even if data is intercepted, it cannot be read without the correct key.

3. Role of RSA Encryption

RSA is used for secure key exchange and digital signatures.

Key Roles:

- Securely shares encryption keys
- Authenticates voting transactions
- Enables digital signatures for verification
- Prevents unauthorized system access

RSA ensures secure communication between voters and the blockchain network.

4. Role of Face Authentication

Face Recognition verifies voter identity before allowing access.

Key Roles:

- Prevents impersonation
- Stops duplicate voting
- Enables secure remote voting
- Reduces dependency on physical identity verification

Face authentication strengthens identity validation without compromising voter anonymity.

POTENTIAL OF THE PROPOSED SYSTEM

The system has significant potential across multiple domains.

1. National and State-Level Elections

- Secure remote voting for citizens
- Reduced election costs
- Faster result declaration
- Increased voter participation

2. Institutional and University Elections

- Transparent student elections
- Elimination of vote rigging
- Secure online campus voting

3. Corporate and Shareholder Voting

- Secure board-level decision making

- Transparent shareholder voting
- Tamper-proof voting records

4. Global and Remote Voting Systems

- Voting for citizens abroad
- Military personnel voting
- Pandemic-safe elections
- Accessible voting for differently-abled individuals

5. Future Smart Governance Integration

The system can integrate with:

- Smart city infrastructure
- Digital identity platforms
- E-governance portals
- AI-based fraud detection systems

IV. INNOVATIVE INTEGRRATION OF SECURE E-VOTING WITH BLOCKCHAIN:ENHANCING AES AND RSA ENCRYPTION WITH FACE AUTHENTICATION TECHNOLOGY

The innovative integration of this proposed system lies in the seamless combination of decentralized ledger technology, hybrid cryptographic encryption, and biometric authentication into a unified and secure voting architecture. Rather than using these technologies independently, the system integrates them in a layered and complementary manner to enhance overall security, transparency, and trust.

1. Integration of Blockchain with Hybrid Encryption

The system uses Blockchain as the core infrastructure while combining two powerful encryption standards:

- Advanced Encryption Standard for encrypting vote data
- RSA for secure key exchange and digital signatures

How the Integration Works:

1. The voter casts a vote.

2. The vote is encrypted using AES.
3. The AES key is encrypted using RSA.
4. The encrypted vote is stored as a block in the blockchain.
5. Each block is cryptographically linked to the previous block.

Innovation Aspect:

- Combines speed (AES) with secure authentication (RSA).
- Ensures end-to-end encryption before data reaches the blockchain.
- Provides double-layer security (cryptography + decentralization).

2. Integration of Biometric Face Authentication with Blockchain

The system incorporates Face Recognition for voter identity verification.

Integrated Workflow:

- Voter login → Face authentication → Identity verification
- Once verified → Vote encryption → Blockchain storage

Innovation Aspect:

- Eliminates password-based vulnerabilities.
- Prevents impersonation and duplicate voting.
- Enables secure remote voting from any location.

This biometric integration ensures that only legitimate voters can access the blockchain voting system.

3. End-to-End Secure Voting Architecture

The innovative architecture integrates three security layers:

Layer 1 – Biometric Authentication

Face recognition verifies voter identity.

Layer 2 – Cryptographic Protection

AES encrypts vote data, and RSA secures keys and authentication.

Layer 3 – Decentralized Storage

Blockchain ensures tamper-proof and transparent vote storage.

This layered approach provides:

- Confidentiality

- Integrity
- Availability
- Non-repudiation
- Transparency

4. Smart Contract Integration Potential

Blockchain smart contracts can automate:

- Voter eligibility verification
- Vote validation
- Real-time vote counting
- Automatic result declaration

This reduces human intervention and enhances reliability.

5. Secure Remote Voting Capability

The integrated system enables:

- Mobile-based voting
- Cloud-hosted blockchain nodes
- Secure remote participation

This is especially useful for:

- Citizens living abroad
- Military personnel
- Emergency situations (pandemics, disasters)

6. Privacy-Preserving Yet Transparent Model

Although votes are encrypted and anonymous, the blockchain ledger allows:

- Public verification of vote count
- Transparent auditing
- Tamper detection

This balances voter privacy with system transparency.

VI. RECENT ADVANCEMENT IN SECURE E-VOTING WITH BLOCKCHAIN:ENHANCING AES AND RSA ENCRYPTION WITH FACE AUTHENTICATION TECHNOLOGY

Advancements in Blockchain-Based E-Voting (2024–2026)

- **Systematic Research Growth (2022–2025)**

A 2026 systematic review highlights rapid expansion in blockchain voting research, focusing on transparency, anonymity, and integrity improvements between 2022–2025

Key Improvements:

- Enhanced smart contract security
- Scalable consensus mechanisms
- Formal verification of voting protocols
- Improved auditability models

- **National-Level Blockchain Adoption**

  - **Peru (2025)** began a pilot for blockchain-based presidential elections using a hybrid system anchored to Bitcoin
  - In India, proposals were made to integrate blockchain into electoral roll systems for transparency and tamper-proof record keeping

Impact:
Blockchain is moving from theoretical research to **government-scale experimentation**.

Post-Quantum & Hybrid Cryptography Advancements

- **Quantum-Secure Voting Framework (2025)**

A 2025 research framework integrates:

- Falcon lattice-based post-quantum signatures
- Biometric face authentication
- Permissioned blockchain storage

The system demonstrated strong spoof detection and low gas overhead for blockchain operations

Importance:
Traditional RSA may be vulnerable to quantum attacks, so research is shifting toward **post-quantum secure voting models**.

- **Improved Hybrid AES–RSA Encryption (2025)**

Recent research enhanced hybrid AES-RSA encryption for secure communication in low-power environments

Relevance to E-Voting:

- Faster encryption performance
- Better energy efficiency
- Strengthened data integrity

◇ **Quantum-Enhanced AES Security**

A 2025 study proposed a quantum-enabled AES framework with quantum-based key generation and automatic key refresh mechanisms

Benefit:
Future-proof encryption against quantum computing threats.

Secure & Privacy-Preserving Face Authentication

◇ **Fully Encrypted Face Recognition (CryptoFace – 2025)**

CryptoFace introduced fully homomorphic encryption (FHE) for secure face recognition, allowing encrypted biometric processing without exposing raw facial data

Significance:

- Protects biometric privacy
- Prevents database leaks
- Enables secure remote authentication

◇ **Advanced Anti-Spoofing & Liveness Detection**

Recent biometric security testing shows 100% spoof attack detection under ISO PAD standards using advanced liveness detection techniques

Additionally, cybersecurity experts warn about deepfake threats to facial authentication systems, emphasizing multi-layer defense mechanisms

Implication for E-Voting:
Modern systems must include:

- 3D face mapping
- AI-based liveness detection
- Anti-deepfake verification

◇ **Aadhaar-Based Face Authentication (India – 2025)**

India expanded face authentication under Aadhaar with consent-based offline verification mechanisms

This demonstrates:

- Government trust in facial biometrics
- Privacy-compliant biometric systems
- Real-world scalability

AI-Powered Blockchain Voting Systems

Recent 2025 research surveys show integration of:

- AI-based fraud detection
- Biometric verification
- Privacy-preserving mechanisms
- Decentralized voting ledgers

Trend:
AI + Blockchain + Biometrics = Next-Gen Digital Democracy.

Emerging Security Challenges

- **RSA Factorization Improvements**

Recent advances in integer factorization algorithms show improved success rates in breaking small RSA numbers

- **Reduced Quantum Requirement to Break RSA**

Community discussions highlight reduced qubit estimates required to break RSA-2048, indicating faster-than-expected quantum progress

Conclusion:
Future e-voting systems must:

- Transition toward post-quantum cryptography
- Use hybrid encryption strategies
- Implement stronger key management

VII.CHALLENGES

Blockchain-Related Challenges

◇ **Scalability Issues**

Blockchain networks can face scalability limitations when handling millions of votes simultaneously.

- High transaction volume may cause delays.
- Network congestion can slow vote confirmation.

◇ **High Storage Requirements**

- Every vote stored as a block increases ledger size.
- Long-term storage management becomes complex.

◇ **Consensus Mechanism Complexity**

- Choosing an appropriate consensus algorithm (PoW, PoS, PBFT) is critical.
- Some mechanisms consume high computational resources.

◇ **Regulatory & Legal Acceptance**

- Many governments do not yet legally recognize blockchain-based voting systems.
- Compliance with election laws can be challenging.

Cryptographic Challenges

◇ **Key Management Complexity**

Advanced Encryption Standard and RSA require secure key generation, distribution, and storage.

- Loss of private keys may result in system access issues.
- Key leakage could compromise vote confidentiality.

◇ **Quantum Computing Threat**

- RSA encryption may become vulnerable to quantum attacks in the future.
- Long-term elections require quantum-resistant alternatives.

◇ **Performance Overhead**

- Hybrid encryption (AES + RSA) increases computational load.
- Large-scale elections may experience latency.

Face Authentication Challenges

◇ **Spoofing & Deepfake Attacks**

Face Recognition systems can be targeted using:

- High-resolution photos
- 3D masks
- AI-generated deepfake videos

◇ **Biometric Privacy Concerns**

- Facial data storage raises privacy risks.
- Biometric data breaches are irreversible.

◇ **Environmental Limitations**

- Poor lighting conditions
- Camera quality variations
- Network bandwidth issues
  These factors may affect authentication accuracy.

Security Challenges

◇ **Insider Threats**

- System administrators could misuse access privileges.

◇ **Smart Contract Vulnerabilities**

- Bugs in smart contracts may cause vote manipulation or system failure.

◇ **Distributed Denial of Service (DDoS) Attacks**

- Attackers may attempt to disrupt the voting process.

Ethical & Social Challenges

◇ **Digital Divide**

- Not all voters have access to smartphones or high-speed internet.
- Elderly or rural populations may struggle with digital systems.

◇ **Trust & Public Acceptance**

- Citizens may hesitate to trust fully digital elections.
- Lack of awareness about blockchain technology.

◇ **Bias in Face Recognition**

- Face recognition systems may show accuracy variations across demographics.

Operational Challenges

- **Infrastructure Cost**
  - Setting up blockchain nodes and biometric systems requires high initial investment.
- **System Maintenance**
  - Continuous updates for encryption and security patches are required.
- **Integration with Existing Electoral Systems**
  - Migrating from traditional EVM systems to blockchain-based systems is complex.

VIII.CONCLUSION

The proposed Secure E-Voting System presents a comprehensive and multi-layered security framework by integrating Blockchain, Advanced Encryption Standard, RSA, and Face Recognition. This integrated approach addresses the major challenges of traditional electronic voting systems, including vote tampering, identity fraud, lack of transparency, and centralized control vulnerabilities.

Blockchain ensures immutability, decentralization, and transparency by maintaining a tamper-proof distributed ledger of votes. AES provides fast and secure encryption of voting data, while RSA strengthens secure key exchange and digital authentication. Face recognition adds a robust biometric verification layer that prevents impersonation and duplicate voting attempts. Together, these technologies create an end-to-end encrypted and authenticated voting environment.

The system enhances:

- Confidentiality – Votes remain encrypted and private.
- Integrity – Stored votes cannot be altered.
- Transparency – Results can be publicly verified without compromising anonymity.
- Authentication – Only legitimate voters can participate.
- Trust – Decentralization reduces reliance on a single authority.

Although challenges such as scalability, biometric privacy concerns, and evolving cyber threats exist, the proposed framework establishes a strong foundation for next-generation digital elections. With further advancements in post-quantum cryptography, AI-based fraud detection, and secure biometric processing, this system has the potential to transform democratic participation in a secure and scalable manner.

In conclusion, the integration of blockchain, hybrid encryption (AES + RSA), and face authentication represents a significant step toward building a reliable, transparent, and future-ready e-voting ecosystem suitable for national, institutional, and global digital governance platforms.