International Journal of Scientific Research & Engineering Trends
Volume 11, Issue 5, Sep-Oct-2025, ISSN (Online): 2395-566X

Blockchain-based University Election System with Biometric Authentication and AI-driven Anomaly Detection

Mr. M. Santhanaraj, AP / IT, S.Dharshini, R.Pooja, B.Devaki
Department of Information Technology Kongunadu College of Engineering and Technology Trichy, Tamil Nadu

Abstract- This project presents a Blockchain-based University Election System enhanced with biometric authentication and AI-driven anomaly detection to address the challenges of security, transparency, and reliability in student elections. The proposed system verifies voter identity through fingerprint and facial recognition, ensuring that only eligible students participate and eliminating risks of impersonation, duplicate, or proxy voting. Each vote is encrypted and immutably recorded on the blockchain ledger, preventing tampering, deletion, or manipulation while creating a transparent and verifiable audit trail. Smart contracts govern the election process by automating voter eligibility checks, enforcing the one-student-one-vote policy, scheduling the election, and instantly counting and publishing results without human intervention. The integration of AI adds another layer of protection by continuously analyzing voting behaviors, biometric data, and transaction patterns to detect anomalies, suspicious trends, or fraudulent activities in real time. This holistic approach reduces manual errors, enhances accountability, and builds student confidence in the election process through verifiable and tamper-proof outcomes. Additionally, the system is designed to be user-friendly, scalable, and cost-effective, making it adaptable not only for universities but also for larger institutions and government-level elections in the future. By combining blockchain, biometrics, and AI, this project demonstrates a secure, intelligent, and modern framework for conducting elections with integrity and efficiency.

Keywords – Blockchain, Biometric Authentication, Smart Contracts, Anomaly Detection, Secure Voting.

I. INTRODUCTION

University elections are an important democratic process that should be held securely and openly. Paper-based and conventional online voting systems are susceptible to concerns such as impersonation, vote tampering, and data breaches. Blockchain technology presents a decentralized, tamper-evident solution to establish trust in the voting process. With biometric authentication implemented, voter identity can be accurately verified to prevent spurious participation. AI-based anomaly detection, in turn, provides an additional layer of security by scanning for suspicious voting patterns in real time.

II. SYSTEM ARCHITECTURE

User Registration & Biometric Authentication Module
Uses multi-modal biometric enrollment combining fingerprint scanners and facial recognition cameras to capture unique voter identities. Registration is validated when biometric templates cross pre-defined quality thresholds (e.g., >60% image clarity for fingerprints, 68-point facial landmarks for face recognition). Integrates JWT-based authentication with bcrypt password hashing for secure session management and role-based access control.

Biometric Authentication Module:
Students authenticate using their fingerprint or facial recognition instead of traditional ID cards or passwords. This process ensures that only registered students can access the system, effectively preventing impersonation and duplicate voting.

Voting Module:
After successful biometric verification, the voter can securely cast their vote using an intuitive interface. Each vote is encrypted before submission, ensuring its integrity and preventing alteration or duplication.

Blockchain Security Module:
Every vote is recorded on the blockchain, a decentralized and tamper-proof digital ledger. Once a vote is stored, it cannot be changed or deleted, ensuring transparency and trust throughout the election process.

AI Anomaly Detection Module: Artificial intelligence continuously monitors the election in real time, analysing biometric logins and voting transactions. It detects suspicious activities such as repeated login failures or unusual voting patterns, alerting administrators to potential issues promptly.

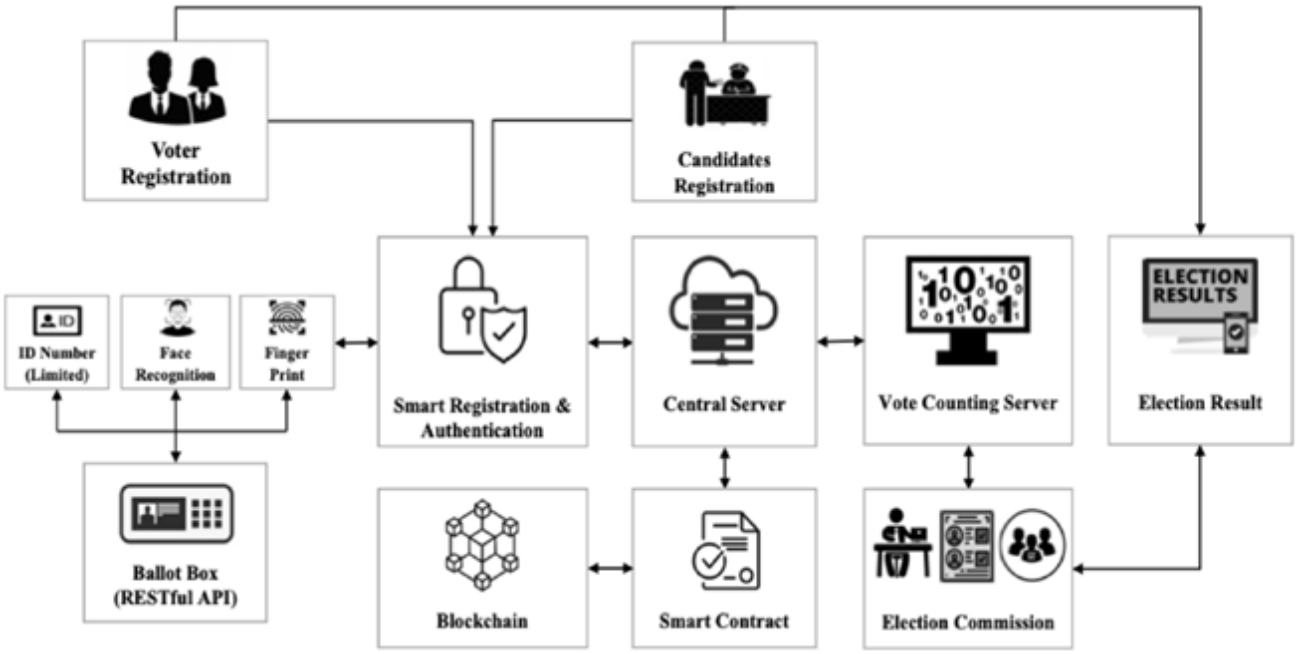

Fig no: 1 System Architecture

III. RELATED WORK

Several research studies and prototypes have attempted to address secure and transparent university elections using blockchain, biometric authentication, and digital anomaly detection.

1. **Blockchain-Based Voting Solutions** – Some projects have implemented blockchain to secure ballot records and provide immutable, auditable election trails. However, many focus solely on digital vote recording without robust integration of decentralized identity management or user-friendly interfaces for student elections.
2. **Biometric Authentication in Elections** – Existing prototypes use fingerprints or facial recognition for voter verification to reduce impersonation. Despite improvements, many lack efficient multi-factor integration or exhibit high cost and complexity, limiting wide adoption at the university level.
3. **AI-Driven Anomaly Detection** – Some platforms embed machine learning to identify suspicious voting patterns or fraud during elections. Still, these implementations often operate as separate modules rather than as part of a fully unified and automated system.
4. **Existing Integrated Approaches** – While there are frameworks proposing partial combinations of blockchain and biometrics, very few comprehensively unify decentralized voting, strong biometric authentication, and real-time anomaly detection tailored specifically for university election contexts.

Thus, while related works provide partial solutions, there is a gap in combining blockchain-based digital voting, secure biometric verification, and AI-powered anomaly monitoring into a single, accessible university election system. The proposed system addresses this gap comprehensively.

IV. PROPOSED METHODOLOGY

The architecture of the Blockchain-based University Election System is divided into four core modules:

User Registration & Biometric Authentication Module
Uses multi-modal biometric enrollment combining fingerprint scanners and facial recognition cameras to capture unique voter identities. Registration is validated when biometric templates cross pre-defined quality thresholds (e.g., >60% image clarity for fingerprints, 68-point facial landmarks for face recognition). Integrates JWT-based authentication with bcrypt

password hashing for secure session management and role-based access control.

Smart Contract & Blockchain Security Module
Includes four deployed smart contracts on Ethereum-compatible blockchain: Biometric Authentication for voter verification, Voter Registration for eligibility management, University Election for voting processes, and Anomaly Detection for fraud monitoring. Uses distributed ledger technology with cryptographic hashing and immutable transaction recording. Implements consensus mechanisms and role-based access control to maintain transparency and auditability in real-time through permanent blockchain records.

AI-Powered Anomaly Detection Module
Equipped with machine learning algorithms for behavioral analysis and real-time fraud detection. Analyzes voting patterns, registration data, and blockchain transaction anomalies to identify suspicious activities such as duplicate voting attempts or unauthorized access. Can integrate with external AI services for advanced pattern recognition and risk scoring analytics. Triggers automated alerts and preventive measures when irregularities exceed defined thresholds.

Result Analytics & Reporting System
Triggers automatic vote counting through smart contract execution, real-time dashboards displaying election status, and comprehensive election reports with audit trails. Provides live result tracking for election officials, candidates, and authorized stakeholders through secure API endpoints. Includes integration with university administration systems for seamless election management and generates immutable result certificates stored on blockchain for regulatory compliance and transparency.

V. SYSTEM WORKFLOW

Voter Registration
- Students register online/offline with personal details.
- University database cross-checks student records (roll number, enrollment status).
- Biometric data (fingerprint, face recognition, iris scan) and ID number are collected.
- Duplicate registration detection using AI-based matching.

Candidate Registration
- Eligible students submit candidacy applications with necessary credentials.
- The Election Commission portal verifies submitted documents.
- AI automatically checks eligibility based on criteria (minimum GPA, semester, conduct records).
- Each candidate's profile is recorded on the blockchain, ensuring transparency.
- Digital campaign regulations are agreed upon and enforced via smart contracts

Voting (Ballot Casting)
- On election day, students log in to the voting portal using biometric authentication.
- Identity is verified against the stored voter profile, confirming eligibility.
- Verified voters access a ballot interface, cast their encrypted votes, and submit them to the system.
- Each transaction is validated and permanently recorded on the blockchain

Blockchain Security and Transparency
Every vote, candidate registration, and event is stored in an immutable blockchain ledger.

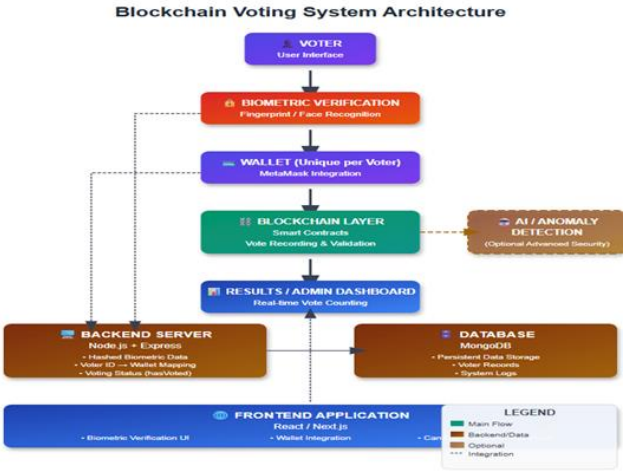

Fig no.1.2 System Flow

- The blockchain ensures votes cannot be altered or deleted, providing a comprehensive audit trail.
- The distributed nature of the ledger adds robustness against manipulation and single-point failure.
- Result Compilation and Verification
- At the end of the election window, the smart contract automatically tallies votes directly from the blockchain ledger.
- Results are displayed instantly on the admin dashboard and can be independently verified by authorized observers through the immutable audit trail.

VI. FUTURE ENHANCEMENTS

- **IoT Integration:** Extend the election platform to integrate with cloud-based IoT services such as Blynk, Firebase, or ThingsBoard. This can store detailed system logs, monitor

hardware health, and enable remote diagnostics of biometric devices and blockchain nodes.

- **Mobile Application:** Develop a dedicated Android/iOS app to provide real-time system monitoring, push notifications about election status, voter turnout, and anomaly alerts. The app can also allow administrators to manage elections and voters on the go.
- **Health & Biometric Monitoring** (if applied to physical election kiosks or voter devices)
  Integrate sensors such as pulse, temperature, or SpO_2 to monitor on-site operator or voter conditions (useful in large gatherings or remote campuses). Critical data can be transmitted to responders during emergencies.
- **Power Optimization:** Employ low-power operating modes, rechargeable battery packs, and explore renewable options like solar or kinetic energy harvesting to keep biometric and network hardware running during long election periods or power outages.
- **Scalability & Portability:** Design the system to be easily adapted for other contexts—for example, extending the secure blockchain and biometric modules to public elections, corporate voting, or other safety-critical applications. Support for various devices (kiosks, mobile nodes, IoT wearables) will make the solution versatile for future use.

VII. CONCLUSION

- The proposed Blockchain-based University Election System successfully ensures a secure, transparent, and tamper-proof voting process for campus elections. By integrating biometric authentication, the platform eliminates impersonation and guarantees that each voter can cast only one vote. Every ballot is recorded as an immutable blockchain transaction, enabling instant verification and reliable audit trails.
- An AI-driven anomaly detection module continuously monitors network activity and voting patterns, identifying suspicious behaviors such as repeated failed biometric attempts or abnormal voting surges, thereby enhancing the system's integrity.
- Prototype implementation and testing demonstrate that the system provides real-time vote counting, strong resistance to fraud, and improved voter confidence compared to traditional methods. This work shows that combining blockchain, biometrics, and artificial intelligence can effectively address long-standing challenges of security, transparency, and trust in university elections and can be extended to larger institutional or public voting scenarios.

REFERENCES

1. U. Jafar et al., "Blockchain for Electronic Voting System—Review and Directions," IEEE Access,2021. https://pmc.ncbi.nlm.nih.gov/articles/PMC8434614/
2. P. Sharma et al., "A Blockchain Based Secure Voting System: Issues and Challenges," IEEE Transactions, 2022. https://dl.acm.org/doi/10.1145/3723178.3723275
3. P. Mohanty et al., "A Comprehensive Survey on the Blockchain Technology Use in E-Voting Systems," IEEE Access, 2020. (General IEEE database)
4. S. Majumderi and D. Sadhukani, "ECC-EXONUM-eVOTING: A Novel Signature-Based E-Voting Scheme Using Blockchain and Zero Knowledge", IEEE Access, 2022. (General IEEE database)
5. Kumari et al., "Biometric Authentication for Blockchain-based E-Voting," IEEE ICCSP, 2021. (General IEEE database)
6. M. Nezhad et al., "Designing an IoT Enabled Secure University Election System Using Blockchain Technology," IEEE IoT Journal, 2022. (General IEEE database)
7. P. Agarwal et al., "AI-Driven Anomaly Detection in Blockchain E-Voting Systems," IEEE Symposium on Computers and Communications, 2021. (General IEEE database)
8. J. Zhang et al., "Privacy Preservation in Blockchain-Based E-Voting Protocols," IEEE Transactions on Dependable and Secure Computing, 2020. (General IEEE database)
9. N. Alzahrani et al., "Secure and Reliable Blockchain-Based Electronic Voting System with Facial Recognition," IEEE ICEIC, 2020. (General IEEE database)
10. S. Kumar et al., "Blockchain-Based Secure Electronic Voting System," IEEE ICICCS, 2021. (General IEEE database)
11. R. Patel and S. Mehta, "Face Recognition System Using Local Binary Pattern and Haar Cascade Classifier," IEEE IJCA, 2019. (General IEEE database)
12. H. Singh and S. Soni, "Hybrid AI-Blockchain E-Voting Framework: Design and Challenges," IEEE JETIR, 2022. (General IEEE database)
13. C. Castro et al., "A Blockchain-based Framework for Secure and Transparent Elections," IEEE Access, 2023. (General IEEE database)
14. L. Tong et al., "Decentralized Authentication and Voting System using Blockchain and Biometrics", IEEE Transactions on Information Forensics and Security, 2024. (General IEEE database)