VOTEX: AI-ENHANCED NEXT-GEN BLOCKCHAIN VOTING WITH MULTIMODAL AUTHENTICATION

Project Reference No.: *49S_BE_3338*

College : Jain Institute of Technology Davanagere
Branch : Department of Computer Science and Engineering
Guide(s) : Prof. Priyanka G V
Prof. Babu Sab
Student(s) : Ms. Apoorva Mallappa Jampannanavar
Ms. Savita P N
Ms. Sinchana G S
Ms. Sindu M M

Keywords:

Blockchain Voting, Multi-modal Biometrics, Facial Recognition, Iris Detection, Liveness Verification, Emotion Analysis, Video Proctoring, Digital Democracy, Election Security, Fraud Detection.

Introduction:

As countries work to increase the effectiveness, transparency, and accessibility of the democratic process, electronic voting has become a crucial technical substitute for conventional paper-based elections. However, security flaws, poor identity verification, a lack of real-time monitoring, and a lack of tools to identify or stop voter coercion and impersonation continue to pose serious problems for current electronic voting systems. Due to their reliance on centralized databases, the majority of modern digital voting platforms are vulnerable to cyberattacks, single points of failure, database manipulation, and unauthorized access. Furthermore, there are significant hazards associated with the widespread adoption of single-biometric authentication techniques like fingerprint or facial recognition since these modalities can be faked utilizing sophisticated deepfake technology, printed photos, or films. [1] Through decentralized consensus methods, recent developments in blockchain technology have demonstrated encouraging possibilities for protecting vote records, guaranteeing data immutability, and facilitating transparent audit trails. Blockchain improves vote integrity, but there is still a lack of interaction between it and strong, intelligent authentication methods in current systems. [2] Additionally, conventional e-voting systems sometimes lack thorough fraud detection capabilities, do not keep an eye on the voter during the voting process, and neglect to take into account behavioral or emotional indicators that point to coercion or unusual activity. These drawbacks emphasize the necessity of a multi-layered, more robust authentication and monitoring system. This study presents Votex, an AI-enhanced next-generation blockchain voting system with intelligent real-time security monitoring and a thorough multi-biometric authentication methodology, to address these issues. In order to enable extremely accurate voter identification and prevent attempts at impersonation, the suggested system combines facial recognition, iris pattern analysis, liveness detection, facial emotion recognition, behavioral biometrics, and location verification.[3] In order to identify suspicious activity, guarantee voter presence, and guard against coercion or outside influence, Votex also uses continuous video proctoring during

the voting session. Votex stores votes as immutable transactions on the backend using a unique blockchain architecture built on SHA-256 hashing and Proof-of-Work (PoW) consensus, guaranteeing transparency, integrity, and auditability while maintaining voter anonymity.

Objectives:

1. Ensure secure voter authentication using biometrics, OTP, and validation checks.
2. Develop a scalable, multilingual blockchain-based digital voting platform.
3. Enhance security using AI for fraud detection and real-time monitoring.
4. Enable transparent auditing with continuous monitoring and blockchain records.

Methodology:

Votex is a secure online voting system designed to ensure voter authenticity, vote integrity, and fraud prevention by integrating advanced technologies such as biometric authentication, blockchain, artificial intelligence, and real-time monitoring. The system uses multi-modal biometric authentication, combining facial recognition, iris pattern analysis, liveness detection, emotion analysis, and behavioral biometrics to verify voter identity. Facial recognition is implemented using 128-dimensional embeddings generated by the dlib framework. Initially, CNN and HOG-based techniques detect the face, followed by the extraction of 68 facial landmarks for accurate alignment under various conditions. The aligned face is then converted into a 128-dimensional feature vector, which is compared with stored embeddings using Euclidean distance with a threshold value of 0.3. Iris recognition is performed using the Circular Hough Transform along with Local Binary Pattern (LBP) descriptors represented as a 26-bin histogram, and correlation-based matching is applied for verification. Liveness detection enhances security by analyzing blur, texture, eye movement, and depth cues to ensure the presence of a real human and prevent spoofing attacks such as photos, videos, or masks. Emotion analysis detects expressions such as fear, stress, or coercion, while behavioral biometrics monitor user interaction patterns, device consistency, and session behavior. All these biometric outputs are combined using a weighted fusion model to generate a final security score.

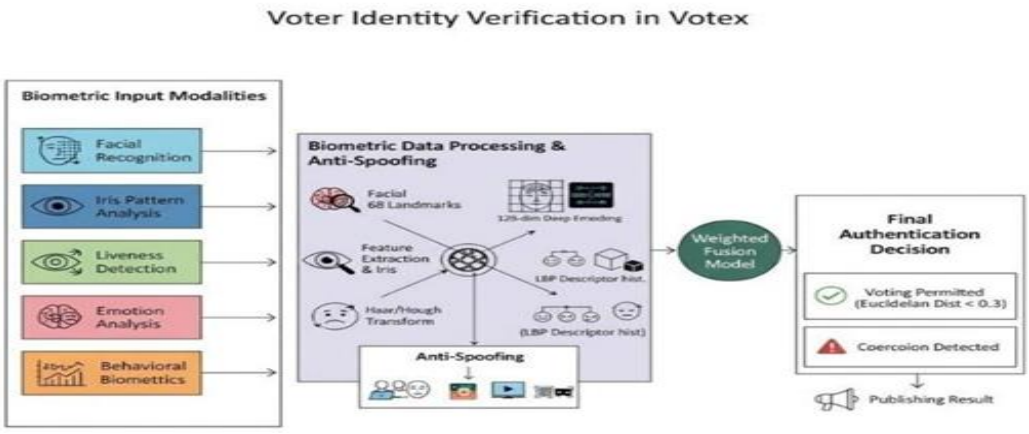

Fig.1: Multimodal Biometric Identity Verification Workflow in Votex

In addition to biometric verification, the system performs location-based verification using HTML5 Geolocation APIs to capture GPS coordinates along with timestamps. These coordinates are converted into human-readable addresses through reverse geocoding, and consistency checks ensure that the voting location matches the registered location. The system also detects VPN or proxy usage and identifies mismatches between IP and GPS data, thereby preventing geographic fraud. During the voting process, real-time video proctoring continuously monitors the voter through video stream analysis. It detects facial presence, occlusions, multiple individuals, and suspicious activities, while gaze tracking ensures voter attention. The entire session is recorded in encrypted WebM format and stored with timestamps to maintain a verifiable audit trail.

To ensure vote integrity, Votex uses a private blockchain for secure vote logging. Each block contains an anonymized voter identifier, encrypted vote, timestamp, previous block hash, nonce, and a SHA-256 hash. A lightweight Proof-of-Work mechanism is used for block validation, and blockchain chaining ensures that any tampering attempt invalidates subsequent blocks, thereby maintaining an immutable and transparent record. Furthermore, an AI-powered fraud detection system continuously analyzes biometric, behavioral, geographic, temporal, and device-related data to identify anomalies such as duplicate registrations and spoofing attacks including deepfakes. A risk score is generated based on these factors, and the system decides whether to allow the session, request additional verification, escalate for manual review, or block the voter.

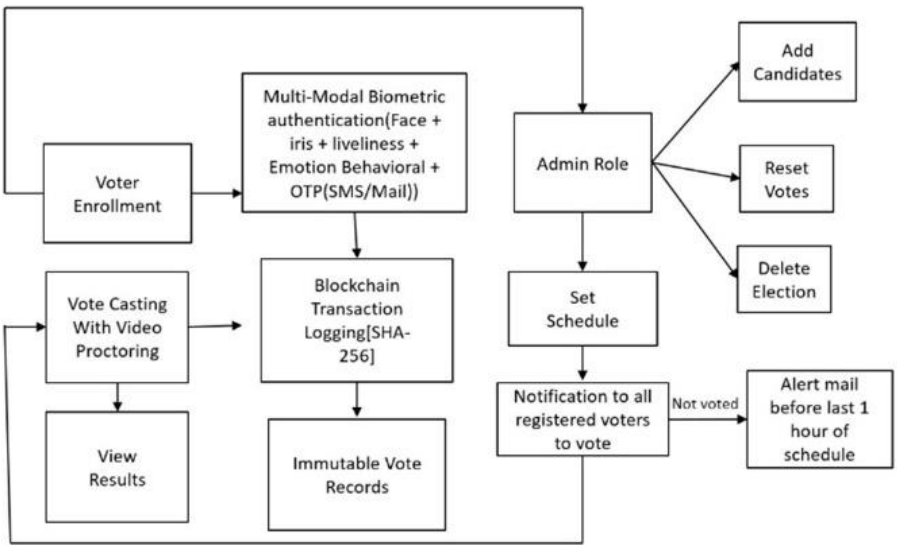

Fig. 2: Architecture of System

The system also includes an administrative control panel that enables secure management of the entire election process. Administrators can configure candidate details, schedule elections, adjust security thresholds, and monitor real-time statistics, system health, and blockchain activity. It also manages voter databases, generates audit logs, and compiles results directly from the blockchain. Additionally, Votex incorporates a voter notification and confirmation system that uses OTP-based authentication through services like Twilio to ensure secure access. The system sends election notifications, reminders, and confirmation messages to voters, improving participation and security.

The complete voting workflow begins with voter registration, where biometric, device, and location data are collected to create a secure profile. During authentication, the system performs multi-modal biometric verification, liveness detection, emotion analysis, and location validation. Once verified, the voter enters a monitored session where video proctoring ensures independent voting.

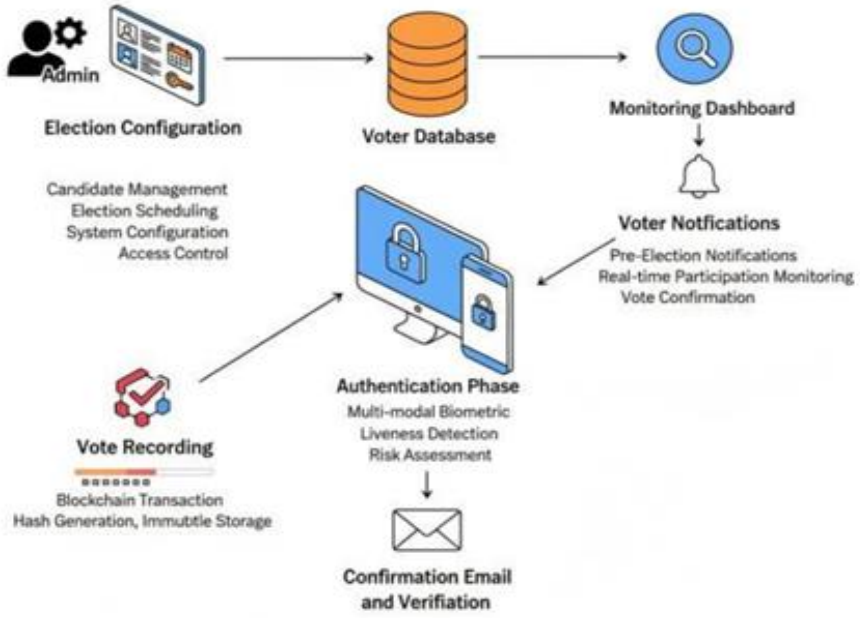

Fig.3: Administrative Workflow and End-to-End Voting Process in the Votex System

The selected vote is then encrypted, hashed, and stored on the blockchain, and a confirmation hash is provided to the voter. The session is securely recorded for auditing purposes, and final vote counting is carried out directly from the blockchain ledger to ensure accuracy, transparency, and reliability. Overall, Votex provides a comprehensive, secure, and efficient online voting solution by integrating multiple layers of security and advanced technologies.

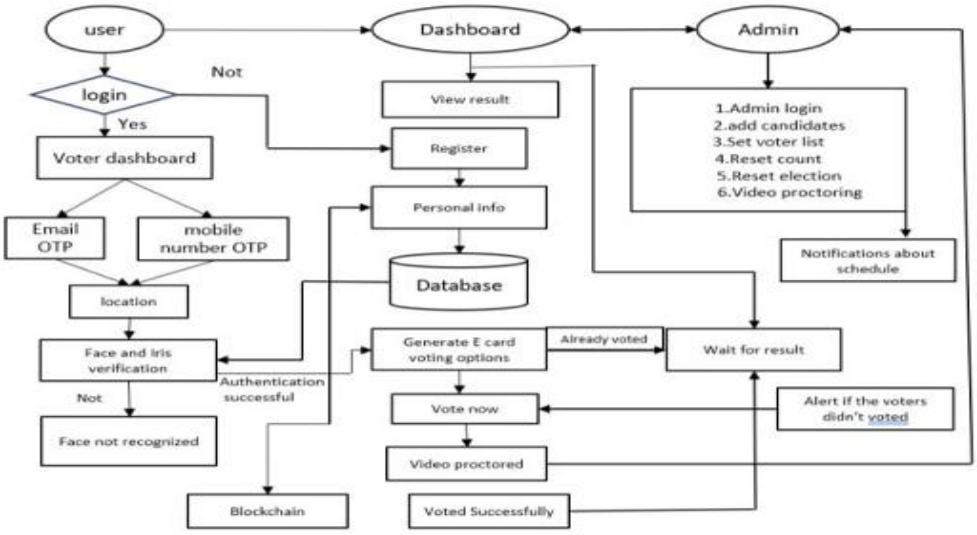

Fig.4: Workflow Diagram

Result and Conclusion:

The Votex system was tested using functional, performance, security, and UI validation methods. It successfully integrates biometric authentication, OTP verification, blockchain logging, and video proctoring. The homepage provides easy navigation for login, registration, and results viewing. The admin dashboard efficiently manages elections with a response time of 1.3 seconds. Voter registration captures face, iris, and location data securely within 3.2 minutes.

The login system uses multi-layer authentication (face, iris, OTP, password) with 99.2% overall accuracy. OTP delivery is 100% successful with an average time of 2.7 seconds. After authentication, a Digital Voter E-Card with QR code is generated instantly. Real-time video proctoring detects suspicious activities with high accuracy and low latency. Blockchain ensures 100% secure and immutable vote storage with 2.1-second block generation time. The results interface verifies data integrity and ensures transparency in the election process.

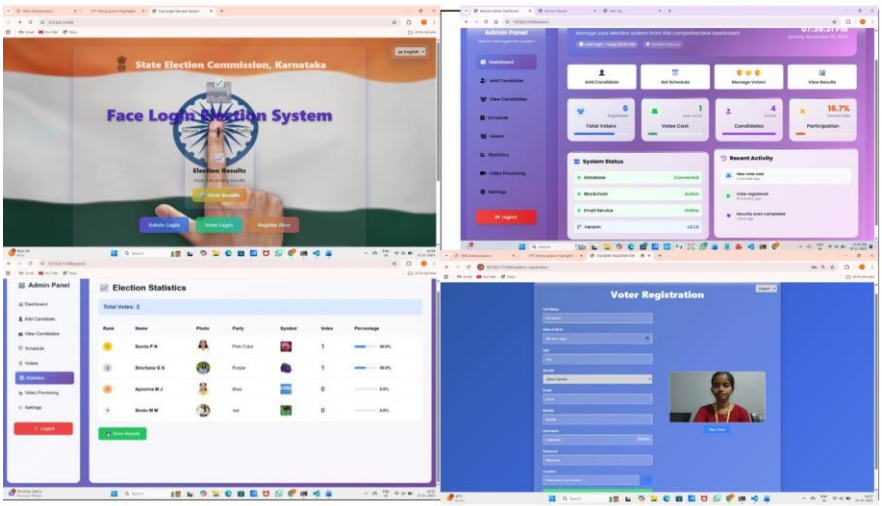

Fig. 5: Votex System Interfaces – Face Login Page, Admin Dashboard, Election Statistics Panel, and Voter Registration with Biometric Capture

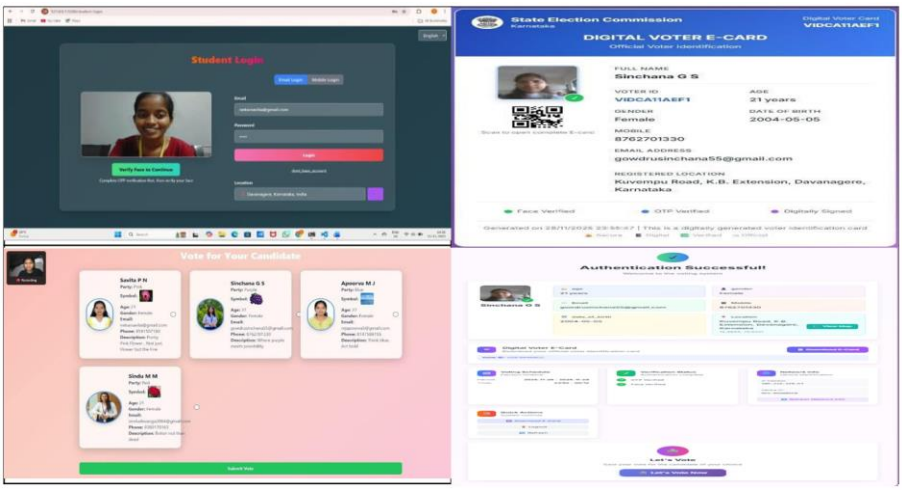

Fig. 6: Votex System Interfaces – Login with Facial Verification, Digital Voter E-Card, Candidate Voting Page, and Authentication Success Dashboard

Conclusion:

This article introduced Votex, an AI-enhanced next-generation blockchain-based electronic voting system that aims to assure secure, transparent, and tamper-proof elections. Votex avoids impersonation, duplicate voting, spoofing, and voter coercion by combining multi-modal biometric authentication, which includes facial recognition, iris detection, liveness verification, emotion analysis, behavioral biometrics, OTP verification, and real-time video proctoring. The usage of a SHA-256-based private blockchain with Proof-of-Work consensus ensures immutable vote storage, transparent auditability, and voter privacy. The experimental evaluation showed a combined authentication accuracy of 99.2%, reliable fraud detection, and strong system performance, confirming the feasibility of the suggested approach for safe digital elections.

Project outcomes:

1. Secure & Transparent: Blockchain + AI face recognition
2. Trustworthy: Tamper-proof, auditable records
3. Reliable & Convenient: Real-time biometric authentication & Convenient to Mobile & web access.
4. Efficient & Scalable: Fast, automated vote counting from local to national elections.

Industry relevance

1. Useful in e-governance and digital voting systems.
2. Applicable in cybersecurity and identity verification domains.
3. Combines trending technologies like AI, blockchain, and biometrics.

Working Model Vs. Simulation Study:

The Votex project is developed as a **functional working software prototype** rather than a purely theoretical or simulation-based study. The system has been practically implemented as a web-based application integrating biometric authentication, OTP verification, blockchain-based vote storage, and real-time video proctoring. Its performance and reliability have been validated through controlled testing and simulated real-time user interactions, demonstrating its feasibility for secure digital voting.

Learnings:

1. Understanding of blockchain and hashing techniques.
2. Knowledge of AI-based biometric authentication systems.
3. Experience in full-stack development and system integration.

References:

1. [1] Subramanian, Siva Shankar, et al. "Face recognition voting system." AIP Conference Proceedings. Vol. 3157. No. 1. AIP Publishing LLC, 2025.

2. [2] Ohize, Henry O., et al. "Blockchain for securing electronic voting systems: a survey of architectures, trends, solutions, and challenges." Cluster Computing 28.2 (2025): 132.
3. [3] REDDY, B. AMARNATH, and K. SUNEEL BABU. "MACHINE LEARNING BASED IRIS RECOGNITION MODERN VOTING SYSTEM." Journal of Nonlinear Analysis and Optimization 16.1 (2025).
4. [4] Nugraha, Tatang. "Pembuatan Evoting dengan Model Multi Vote Berdasarkan Kategori Menggunakan Hashing SHA-256: Studi Kasus SMK Plus YSB Suryalaya." Bridge: Jurnal Publikasi Sistem Informasi dan Telekomunikasi 3.3 (2025): 102-116.

Future Scope:

The future scope of this project includes:

1. Enhance scalability and efficiency by adopting energy-efficient blockchain consensus mechanisms.
2. Strengthen voter privacy using advanced cryptographic techniques and improve accessibility with multilingual and assistive interfaces.
3. Enable real-world deployment through large-scale testing and integration with national digital identity systems.