International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 05 May 2026
Page No: 3407-3414
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0440

VoteChain: An Integrated Web-Based Framework for Decentralized Institutional Elections with Department-Specific Granular Access Control

Ms. Suvarna S. Wakchaure[1], Mr. Sarthak S. Lolge[2], Mr. Roshan V. Nagmal[3], Mr. Sarthak A. Ugale[4], Mr. Suyash R. Patil[5]

[1]Assistant Professor, Department of Computer Engineering, Sir Visvesvaraya Institute of Technology, Nashik, Maharashtra, India.

[2,3,4,5]Department of Computer Engineering, Sir Visvesvaraya Institute of Technology, Nashik, Maharashtra, India.

Email ID: *suvarna.jondhale@pravara.in[1], lolgesarthak@gmail.com[2], roshannagmal64@gmail.com[3], sarthakugle123@gmail.com[4], suyashpatil2316@gmail.com[5]*

Abstract

Student elections in academic institutions are essential for promoting leadership, participation, and democratic values among students. However, traditional voting methods, whether manual or basic digital systems, often face issues such as identity fraud, duplicate voting, lack of transparency, and data manipulation. These challenges reduce trust and affect the reliability of election outcomes. To address these limitations, this paper presents VoteChain, a secure and intelligent digital voting platform designed for student council elections. The system integrates Artificial Intelligence (AI), Machine Learning (ML), and a block chain-inspired ledger to ensure a reliable and tamper-resistant voting process. AI-based facial verification is used to authenticate voters and enforce the "one student, one vote" principle. Additionally, machine learning techniques monitor voting activities in real time to detect suspicious behavior. Votes are encrypted and stored in an immutable ledger, ensuring data integrity and security. The system also includes a user-friendly dashboard for monitoring participation and generating results instantly. Experimental results demonstrate improved security, efficiency, and transparency, making VoteChain a robust solution for modern digital elections.

Keywords: *Secure Online Voting, Artificial Intelligence, Machine Learning, Facial Recognition, Block chain-inspired Ledger, Fraud Detection, Data Integrity, Student Election System.*

1. Introduction

In the modern digital era, technology plays a crucial role in improving the efficiency, transparency, and security of institutional processes, including student council elections. Traditional voting methods, such as paper-based systems or basic online platforms, suffer from issues like manual errors, weak identity verification, impersonation, and data manipulation. Centralized systems further increase the risk of unauthorized access and reduce trust in election outcomes. To address these challenges, this paper proposes VoteChain, a secure web-based voting platform designed for student elections. The system integrates Artificial Intelligence (AI), Machine Learning (ML), and a block chain-inspired ledger to ensure a fair and tamper-proof voting process. AI-based facial recognition enables strong voter authentication, enforcing the "one student, one vote" principle, while ML techniques detect suspicious activities in real time. [1]- [3] Additionally, votes are encrypted and stored in an immutable ledger, ensuring data integrity and transparency. The platform also provides a user-friendly interface for voters and administrators, enabling secure voting, real-time monitoring, and instant result generation.

Overall, the proposed system aims to transform the traditional election process into a secure, transparent, and efficient digital solution. By combining AI-driven authentication, real-time fraud detection, and

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 05 May 2026
Page No: 3407-3414
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0440

secure vote storage, VoteChain ensures reliability and fairness in student elections while encouraging greater participation and trust in the system.

2. Literature Survey

The development of secure and reliable online voting systems has attracted significant attention in recent years. Various researchers have proposed different approaches to improve election security, transparency, and accessibility. However, many existing systems still suffer from limitations related to authentication, data integrity, and fraud prevention. This section reviews some of the relevant research works and highlights their drawbacks along with improvements introduced in the proposed VoteChain system. As Shown in Table 1.[4]- [8]

Table 1 Comparative Analysis of Existing Voting Systems and Proposed VoteChain Improvements

Sr. No.	Author & Year	Title / Approach	Limitations	Improvement in VoteChain
1	R. Sharma et al., 2024	Online Voting with OTP Authentication	Weak identity verification; OTP can be shared leading to impersonation	Uses AI-based facial recognition for strong and real-time identity verification
2	A. Kumar & S. Jain, 2023	Blockchain-Based Voting System	High computational cost; not suitable for small-scale institutional use	Uses lightweight blockchain-inspired ledger for efficiency and scalability
3	M. Gupta et al., 2025	Web-based Campus Voting Portal	Login credentials can be misused; allows multiple voting	Ensures one-student-one-vote using facial + ID validation
4	S. Patel & D. Singh, 2024	ML-based Election Data Analysis	Fraud detection performed only after voting ends	Implements real-time anomaly detection during voting
5	L. Thomas et al., 2023	Cloud-Based Voting Application	Risk of data tampering and limited transparency	Provides encrypted and immutable vote storage for enhanced trust

2.1.Discussion

From the above analysis, it is evident that while existing systems attempt to digitize the voting process, they lack a comprehensive approach that combines secure authentication, real-time monitoring, and tamper-proof data storage. For example, OTP-based systems improve accessibility but fail to ensure that the actual voter is present. Similarly, block chain-based systems provide strong security but are often computationally expensive and impractical for small-scale academic environments. Web-based voting portals improve convenience but rely heavily on username-password authentication, which can be easily compromised. By combining these features, VoteChain provides a balanced solution that is both secure and practical for institutional use, overcoming the major shortcomings of previously proposed systems.

3. Problem Statement

In many educational institutions, student elections still rely on traditional or basic digital systems that lack strong security and verification mechanisms. These systems are vulnerable to issues such as identity fraud, duplicate voting, and data manipulation. Authentication methods like usernames, passwords, or OTPs do not ensure that the actual authorized student is voting. Additionally, centralized data storage increases the risk of unauthorized access and tampering, while limited

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 05 May 2026
Page No: 3407-3414
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0440

transparency reduces trust in the process. Accessibility is also a concern, as students may not always be present on campus to vote. Furthermore, the lack of intelligent monitoring makes it difficult to detect fraudulent activities such as repeated login attempts or suspicious voting patterns. Therefore, there is a strong need for a secure, intelligent, and transparent voting system that ensures proper identity verification, prevents fraudulent activities, maintains data integrity, and provides reliable election results.

4. Objectives of The Proposed System

The primary goal of the Vote Chain system is to develop a secure and efficient digital voting platform that overcomes the limitations of traditional and existing online voting systems. The specific objectives of the proposed system are as follows:

4.1. Secure Voter Authentication

To implement AI-based facial recognition and identity verification mechanisms that ensure only authorized students can access the voting system and cast their vote.[9]

4.2.Prevention of Fraudulent Activities

To integrate machine learning techniques for detecting suspicious behaviors such as duplicate voting attempts, multiple logins, and abnormal activity patterns in real time.

4.3. Ensuring Data Security and Integrity

To use encryption techniques such as AES and hashing mechanisms like SHA-256 to protect vote data and maintain confidentiality. Additionally, to store votes in a block chain-inspired ledger to prevent any modification or tampering.

4.4.One Student – One Vote Enforcement

To strictly enforce the rule that each registered student can cast only one vote per election, ensuring fairness in the voting process.

4.5.Real-Time Result Processing

To provide instant vote counting and result generation through an automated system, eliminating delays and human errors associated with manual counting.

4.6.Transparency and Auditability

To maintain detailed logs of all system activities, including authentication attempts and voting transactions, ensuring complete transparency and enabling audit verification.

5. Proposed System & Methodology

Vote Chain is a secure web-based voting platform designed to modernize student elections. It integrates Artificial Intelligence (AI), Machine Learning (ML), and secure data handling to ensure a transparent, reliable, and tamper-resistant voting process. The system uses a multi-layered architecture for authentication, secure vote processing, and real-time monitoring, allowing only verified users to participate while maintaining data integrity. It supports both voters and administrators, enabling secure voting, efficient election management, and instant result generation.

5.1.System Architecture

The architecture of Vote Chain is structured into multiple functional layers that work together to provide a secure voting environment. According to the diagram shown in your document, the system follows a modular approach. As Shown in Figure 1.

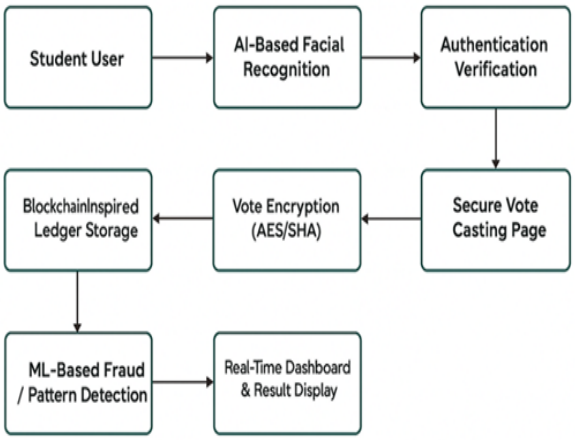

Figure 1 System Architecture

5.2.Main Layers of Architecture

1.User Interface Layer

- Provides interaction between users and the system.
- Includes voter dashboard and admin panel

2.Authentication Layer

- Performs AI-based facial recognition and identity validation.
- Ensures only authorized users can access the system.

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 05 May 2026
Page No: 3407-3414
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0440

3.Voting Layer

- Allows authenticated users to cast their vote.
- Maintains anonymity of the voter.

4.Encryption Layer

- Encrypts vote data using secure cryptographic techniques.
- Protects data from unauthorized access.

5.Ledger Storage Layer

- Stores votes in a block chain-inspired immutable format.
- Prevents tampering or modification.

6.Analytics & Result Layer

- Displays real-time voting statistics and final results.
- Accessible only to authorized users.

This layered design ensures security, transparency, and scalability throughout the election process.

5.3.System Workflow

The VoteChain system follows a structured sequence of operations to conduct elections securely and efficiently.

Step 1: Voter Registration

- Student details and identification data are stored in the system database.
- Each voter is assigned a unique identity.

Step 2: AI-Based Authentication

- The system captures the user's face through a webcam.[10]
- Facial data is matched with stored records to verify identity

Step 3: Access to Voting Portal

- Once authentication is successful, the user is granted access to the voting interface

Step 4: Vote Casting

- The voter selects a candidate and submits the vote
- The system ensures that no personal identity is linked with the vote

Step 5: Vote Encryption

- The vote is encrypted using AES encryption
- Additional hashing (SHA-256) is applied for security

Step 6: Secure Storage

- Encrypted votes are stored in a block chai-inspired ledger
- Each vote is recorded as a unique and immutable transaction

Step 7: Fraud Detection

- Machine learning algorithms monitor system activity.
- **Detects anomalies such as:**
  a. Multiple login attempts.
  b. Duplicate voting attempts.
  c. Suspicious behavior patterns

Step 8: Result Generation

- After voting ends, results are automatically calculated.
- **Dashboard displays:**
  d. Total votes.
  e. Participation rate.
  f. Final results.

This workflow ensures accuracy, security, and real-time monitoring of the election process.

5.4.Key Features of the System

- **AI - Based Authentication** → Prevents impersonation
- **Encrypted Voting Mechanism** → Ensures data confidentiality
- **Immutable Ledger Storage** → Prevents data tampering
- **Real-Time Fraud Detection** → Enhances security
- **Automated Result Generation** → Reduces manual effort
- **User - Friendly Interface** → Improves usability

5.5.Functional Objectives

The system is designed to achieve the following functional goals:

- Ensure one-student-one-vote policy.
- Maintain vote privacy and anonymity.
- Detect and prevent fraudulent activities.
- Provide real-time monitoring and analytics.
- Deliver accurate and transparent results.

6. Materials & Implementation

The implementation of the VoteChain system requires a combination of hardware and software components to ensure smooth execution of authentication, voting, and data processing

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 05 May 2026
Page No: 3407-3414
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0440

operations. The selected components are designed to support real-time interaction, secure data handling, and efficient system performance.

6.1.Hardware Requirements

The hardware setup is minimal and practical, making the system easy to deploy within educational institutions without requiring specialized equipment. As Shown in Table 2.

Table : Hardware Components Used in VoteChain System

Component	Description
Laptop / Desktop System	Used by administrators and developers to configure and manage the election system
Webcam / Camera Device	Captures user facial data for AI-based authentication
Server (Local / Cloud)	Stores voter data, encrypted votes, and system logs securely

6.2.Software Requirements

These software tools work together to provide a complete full-stack solution for secure online voting. As Shown in Table 3.

Table 3 Software Tools and Technologies Used in VoteChain System

Software / Tool	Purpose
Frontend Technologies (React.js, HTML, CSS, JavaScript)	Design of user interface and dashboards
Backend (Node.js / Express.js or Flask/Django)	Handles server-side logic and API communication
Database (MySQL / MongoDB)	Stores user data, votes, and logs
AI/ML Libraries (OpenCV, Scikit-learn, TensorFlow)	Facial recognition and fraud detection
Development Tools (VS Code)	Coding and debugging

6.3.System Modules

The VoteChain system is divided into multiple modules, each responsible for a specific function within the election process.[11]

1. **Voter Registration Module**
   - Stores student information in the database.
   - Prepares voter list before election.
2. **Authentication Module**
   - Performs AI-based facial recognition.
   - Verifies user identity before voting.
3. **Voting Module**
   - Allows authenticated users to cast votes.
   - Ensures anonymity of voting process.
4. **Encryption Module**
   - Encrypts vote data before storage.
   - Protects sensitive information.
5. **Storage Module (Ledger System)**
   - Stores votes in immutable format.
   - Prevents tampering or modification.
6. **Fraud Detection Module**
   - Monitors voting activity in real-time.
   - Detects suspicious behavior patterns.
7. **Result & Dashboard Module**
   - Displays voting statistics and final results.
   - Accessible to authorized users only.

These modules work together to ensure a secure, efficient, and reliable voting system.

6.4.Implementation Details

The VoteChain system is implemented as a web-based application using a client-server architecture where the frontend provides an interactive interface for users and the backend handles authentication, vote processing, and data storage. The main user dashboard provides access to active elections, user profile details, and recent activities.[12]

- **Welcome Dashboard Interface:** Serves as the primary entry point for users to navigate their profile and access active elections.
- **Voting Interface with AI-Based Face Verification and Candidate Selection:** Authenticates users through AI-driven facial recognition before they select a candidate, ensuring only legitimate participation.

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 05 May 2026
Page No: 3407-3414
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0440

- **KYC Verification Interface with Biometric Authentication:** Provides a secure layer for identity confirmation through integrated biometric protocols.
- **Blockchain Vote Confirmation Interface:** Records each cast vote with specific transaction details to guarantee the transparency and immutability of the process.

The system performance comparison highlights the improved efficiency, security, and accuracy of the proposed VoteChain system over traditional voting methods. Furthermore, the distribution of valid votes and detected fraudulent attempts demonstrates the effectiveness of real-time fraud detection mechanisms. Together, these interfaces validate the reliability, security, and practical.[13]

6.5.Implementation Flow

1. User accesses the system through a web browser.
2. Authentication is performed using facial recognition.
3. Verified users are allowed to cast their vote.
4. Votes are encrypted and securely stored.
5. System continuously monitors for anomalies.
6. Results are generated automatically after voting ends.

The implementation ensures that the system operates in a secure and controlled environment while maintaining usability for students and administrators.

6.6.Testing Scenarios

To validate the functionality of the system, several test cases are considered:

- Valid voter successfully casting a vote.
- Unauthorized user attempting access.
- Detection of duplicate voting attempts.
- Accurate vote counting and result generation

These scenarios help ensure the reliability and robustness of the system under different conditions.

7. Results and Discussion

The VoteChain system was evaluated based on multiple performance parameters including authentication accuracy, system security, voting integrity, and overall usability. The results demonstrate that the proposed system provides a reliable and efficient solution for conducting secure student elections.

7.1.Authentication Performance

The AI-based facial recognition module was tested under normal operating conditions using webcam input. The system successfully authenticated registered users with high accuracy, ensuring that only authorized students could access the voting platform.

- Accurate identification of valid users.
- Prevention of impersonation attempts.
- Reliable performance under standard lighting conditions.

This confirms that integrating AI-based verification significantly improves identity validation compared to traditional login methods. As Shown in Figure 2.

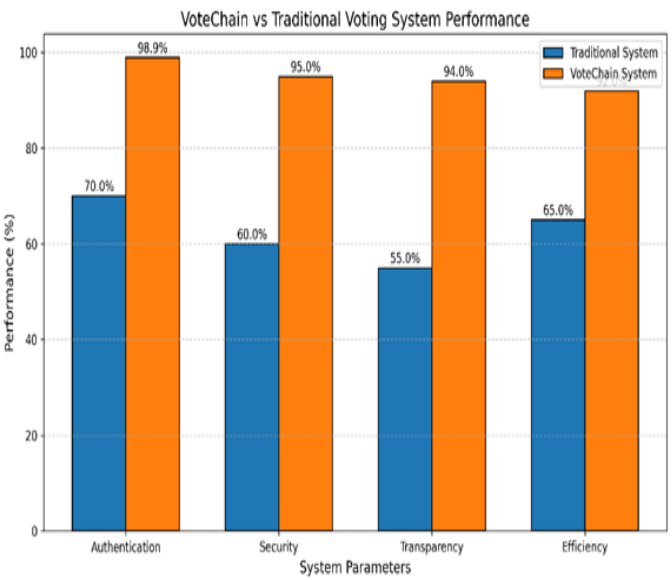

Figure 2 Performance Comparison between Traditional Voting System and Proposed VoteChain System

7.2.Voting Integrity and Security

The system ensures that each vote is securely processed and stored without any possibility of alteration. The use of encryption techniques and immutable storage guarantees data integrity throughout the election process.[14]

- Votes are encrypted before storage.
- No modification possible after submission.
- Maintains complete confidentiality of voters.

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 05 May 2026
Page No: 3407-3414
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0440

The blockchain-inspired ledger structure plays a key role in maintaining trust and transparency in the system.[15]

7.3. Discussion

The experimental results indicate that VoteChain successfully addresses the major limitations of traditional and existing online voting systems. By integrating AI, ML, and secure data handling techniques, the system provides a comprehensive solution that ensures both security and usability.

Overall, the results validate that the proposed system is effective, scalable, and suitable for deployment in educational institutions. It provides a modern approach to digital voting while maintaining security, transparency, and efficiency.

8. Conclusion & Future Scope

8.1.Conclusion

This paper presents VoteChain, a secure digital voting system designed to address identity fraud, duplication, and transparency issues in educational institutions. By integrating Artificial Intelligence, Machine Learning, and blockchain-inspired mechanisms, the system ensures authorized participation through facial recognition and proactive fraud detection. Votes are stored in a tamper-resistant ledger using encryption to guarantee data integrity and transparency. Furthermore, automated results reduce manual errors and processing time, providing an efficient, reliable, and user-friendly experience that transforms traditional academic voting into a modern, transparent solution.

8.2.Future Scope

- **Integration with Full Blockchain Technology:** The system can be enhanced by implementing complete blockchain frameworks (e.g., Ethereum) to achieve full decentralization and higher security.
- **Advanced Biometric Authentication:** Future versions can include more advanced biometric methods such as deep learning-based facial recognition or multi-modal biometrics (face + fingerprint).
- **Mobile Application Development:** A dedicated mobile app can be developed to increase accessibility and allow users to participate in elections from anywhere.
- **Multi-Factor Authentication (MFA):** Additional security layers like OTP, device verification, or biometric combinations can be integrated for stronger authentication.

References

[1]. U. Jafar, M. M. Jhanjhi, M. N. Brohi and M. Humayun, “Blockchain for Electronic Voting System—Review and Open Research Challenges,” IEEE Access, 2021.
[2]. M. Sharp, “Blockchain-Based E-Voting Mechanisms: A Survey and a Novel Approach,” Electronics (MDPI), vol. 4, no. 4, 2024.
[3]. M. Pawlak, “Towards Intelligent Agents for Blockchain E-Voting System,” Procedia Computer Science, Elsevier, 2018.
[4]. B. Sujatha et al., “Blockchain-Powered E-Voting: A Novel Approach to Secure Voter Authentication, Online Voting and Election Automation,” Indian Journal of Science and Technology, vol. 17, no. 47, 2024.
[5]. S. Chouhan et al., “Secure Online Voting System Using Blockchain Technology,” ACM International Conference Proceedings, 2022.
[6]. A. Sah and A. Kumar, “Leveraging Blockchain Technology for Secure Online Voting Systems,” Journal of Mobile Multimedia, 2025.
[7]. U. Jafar et al., “A Systematic Literature Review on Blockchain-Based Electronic Voting Systems,” IEEE Access, 2022.
[8]. H. Kim, K. E. Kim, S. Park and J. Sohn, “E-Voting System Using Homomorphic Encryption and Blockchain Technology,” arXiv preprint
[9]. A. Russo, A. F. Anta, M. I. G. Vasco and S. P. Romano, “Chirotonia: A Scalable and Secure E-Voting Framework Based on Blockchains,” arXiv preprint arXiv:2111.02257, 2021.
[10]. Q. Zhang, B. Xu, H. Jing and Z. Zheng, “Ques-Chain: An Ethereum-Based E-Voting System,” arXiv preprint arXiv:1905.05041, 2019.
[11]. U. C. Cabuk, E. Adiguzel and E. Karaarslan,

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 05 May 2026
Page No: 3407-3414
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0440

"A Survey on Feasibility and Suitability of Blockchain Techniques for E-Voting Systems," arXiv preprint arXiv:2002.07175, 2020.

[12]. T. Chafiq et al., "Blockchain-Based Electronic Voting Systems: A Case Study for Transparency and Integrity," Elsevier Journal, 2024.

[13]. R. Sharma, N. Verma and S. Kulkarni, "Secure Online Voting System Using OTP-Based Authentication," International Journal of Computer Applications, 2024.

[14]. A. Kumar and S. Jain, "Blockchain-Based Secure Voting Framework for Academic Institutions," IEEE Conference Paper, 2023.

[15]. M. Gupta, P. Yadav and R. Borse, "Web-Based E-Voting Portal for Campus Elections," International Journal of Advanced Research in Computer Science, 2025.