International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 10 Issue: 03 | March - 2026 SJIF Rating: 8.659 ISSN: 2582-3930

VOTECHAIN

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

[1,2,3,4,5] Department of Computer Engineering, Sir Visvesvaraya Institute of Technology, Nashik, Maharashtra, India

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 blockchain-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.

Keyword: Secure Online Voting, Artificial Intelligence, Machine Learning, Facial Recognition, Blockchain-inspired Ledger, Fraud Detection, Data Integrity, Student Election System

1. INTRODUCTION

In the modern digital era, technology has become an essential tool for improving the efficiency, transparency, and security of various institutional processes. One such critical process in educational institutions is the student council election, which plays a significant role in promoting leadership, responsibility, and democratic participation among students. These elections allow students to represent their peers and contribute to decision-making within the institution. Despite their importance, traditional voting methods—such as paper-based systems or simple online platforms-face multiple limitations. These include manual counting errors, lack of proper identity verification, risks of impersonation, and the possibility of vote manipulation. Additionally, centralized systems are vulnerable to unauthorized access or tampering, which can compromise the fairness and credibility of election results. These issues often reduce trust in the election process and discourage student participation. With advancements in emerging technologies, it is now possible to design intelligent and secure voting systems that address these challenges effectively. Technologies such as Artificial Intelligence (AI) and Machine Learning (ML) provide powerful capabilities for identity verification and fraud detection, while secure data storage mechanisms help ensure transparency and data integrity. To address the limitations of existing systems, this paper proposes **VoteChain**, a secure and intelligent web-based voting platform specifically designed for student council elections. The system integrates multiple layers of security and intelligence to ensure a fair and tamper-proof voting process. It utilizes AI-based facial recognition to verify voter identity, ensuring that only authorized individuals can participate in the election. This approach helps eliminate impersonation and enforces the principle of "one student, one vote."

In addition, the system incorporates machine learning techniques to monitor voting behavior and detect anomalies such as repeated login attempts or suspicious voting patterns. Unlike traditional systems where fraud detection occurs after voting is completed, VoteChain performs real-time monitoring, enabling immediate identification and prevention of fraudulent activities. Another key component of the system is the use of a blockchain-inspired ledger mechanism. Instead of relying on a fully decentralized blockchain, the system

uses a lightweight and efficient ledger structure to store votes in an encrypted and immutable format. Each vote is securely recorded, ensuring that it cannot be altered or deleted once submitted. This enhances transparency and builds trust among users. Furthermore, VoteChain provides a user-friendly interface for both voters and administrators. Students can easily access the voting portal, complete authentication, and cast their votes securely. Administrators, on the other hand, can monitor election progress, analyze participation data, and generate results instantly through an integrated dashboard.

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 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.

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

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, blockchain-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 council elections are still conducted using traditional methods or basic digital platforms that lack advanced security and verification mechanisms. These systems are often vulnerable to multiple issues such as identity fraud, duplicate voting, and manipulation of election data. Since authentication is usually based on simple credentials like usernames, passwords, or OTPs, there is no strong guarantee that the person casting the vote is the actual authorized student. Another major concern is the centralized nature of existing systems, where election data is stored and managed in a single location. This increases the risk of unauthorized access, data tampering, or misuse by administrators or external attackers. Additionally, many systems do not provide transparency in the voting process, which reduces trust among participants. Accessibility is also a challenge in traditional election setups, as students may not always be physically present on campus to participate in voting. Moreover, the absence of intelligent monitoring mechanisms makes it difficult to detect fraudulent activities such as repeated login attempts or abnormal voting patterns during the election process.

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 VoteChain 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:

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.

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.

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 blockchain-inspired ledger to prevent any modification or tampering.

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.

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.

6. User-Friendly Interface
To design an intuitive and responsive web-based interface that allows students to easily participate in elections and enables administrators to manage the process efficiently.

7. 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

The proposed system, **VoteChain**, is a secure and intelligent web-based voting platform designed to modernize student council elections. The system combines Artificial Intelligence (AI), Machine

Learning (ML), and secure data handling mechanisms to ensure a transparent, reliable, and tamper-resistant voting process. Unlike traditional voting systems, VoteChain follows a multi-layered architecture that focuses on authentication, secure vote processing, and real-time monitoring. The system ensures that only verified users can participate in elections while maintaining the confidentiality and integrity of vote data. The platform is designed to support both voters and administrators. Students can securely log in, complete identity verification, and cast their votes, while administrators can configure elections, monitor activities, and generate results efficiently.

5.1 SYSTEM ARCHITECTURE

The architecture of VoteChain is structured into multiple functional layers that work together to provide a secure voting environment. According to the *diagram shown in your document (page 5)*, the system follows a modular approach.

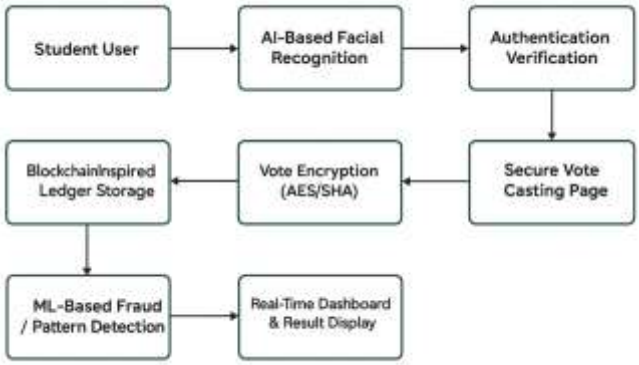

Fig. 1: System Architecture

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
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 blockchain-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.

5.2 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
- 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 blockchain-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:
  - Multiple login attempts
  - Duplicate voting attempts
  - Suspicious behavior patterns

Step 8: Result Generation

- After voting ends, results are automatically calculated
- Dashboard displays:
  - Total votes
  - Participation rate
  - Final results

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

5.3 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

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

6.1 Hardware Requirements

Table 2: 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

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

6.2 SOFTWARE REQUIREMENTS

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

These software tools work together to provide a complete full-stack solution for secure online voting.

6.3 SYSTEM MODULES

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

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. The frontend provides an interactive interface for users, while the backend handles authentication, vote processing, and data storage.

The main user dashboard of the VoteChain system is shown in Fig. 1, which provides access to active elections, user profile details, and recent activities.

Fig. 2: Welcome Dashboard Interface

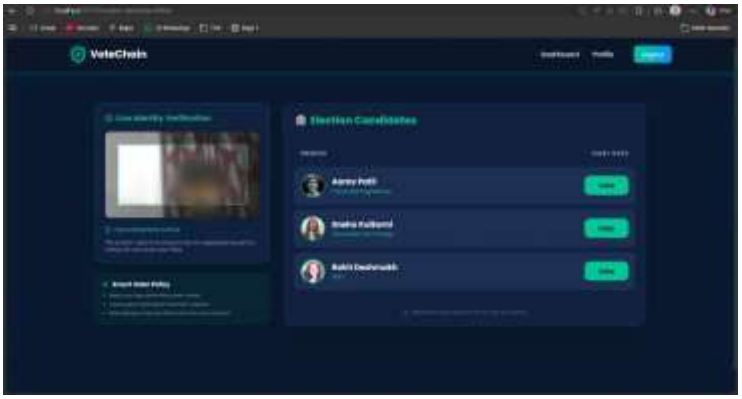

Fig. 3: Voting Interface with AI-Based Face Verification and Candidate Selection

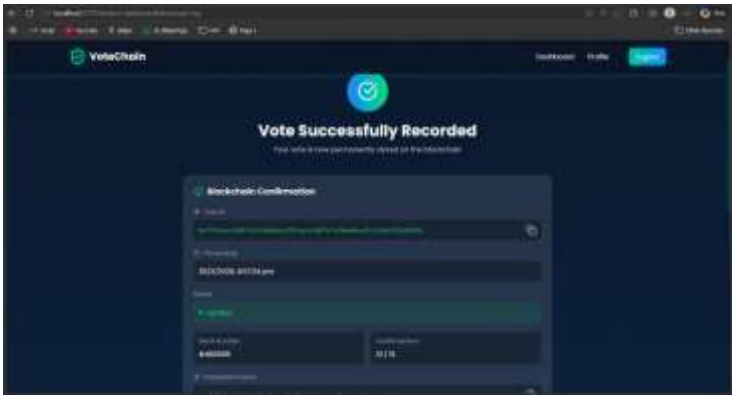

Fig. 4: KYC Verification Interface with Biometric Authentication

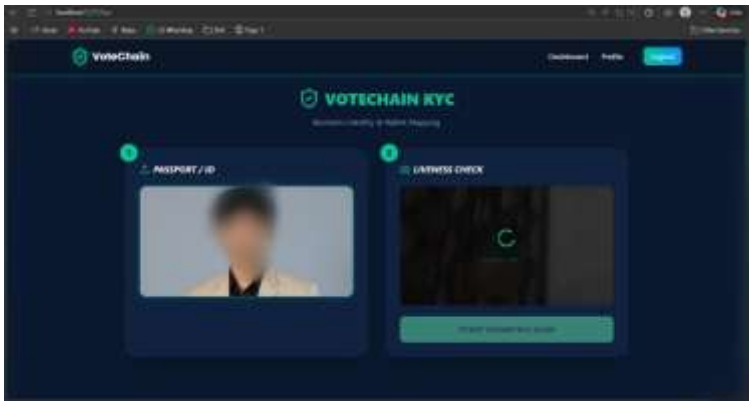

Fig. 5: Blockchain Vote Confirmation Interface

Figures 2 to 5 illustrate the key functional interfaces of the VoteChain system, demonstrating its secure and user-centric design. Fig. 2 presents the voting interface, where users are authenticated through AI-based face verification before selecting their preferred candidate, ensuring that only legitimate voters can participate. Fig. 3 shows the blockchain confirmation interface, where each vote is successfully recorded with transaction details, ensuring transparency and immutability of the voting process. Fig. 4 represents the system performance comparison, highlighting the improved efficiency, security, and accuracy of the proposed VoteChain system over traditional voting methods. Fig. 5 illustrates the distribution of valid votes and detected fraudulent attempts, demonstrating the effectiveness of real-time fraud detection mechanisms. Together, these interfaces validate the reliability, security, and practical implementation of the proposed system.

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.

6.5 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.

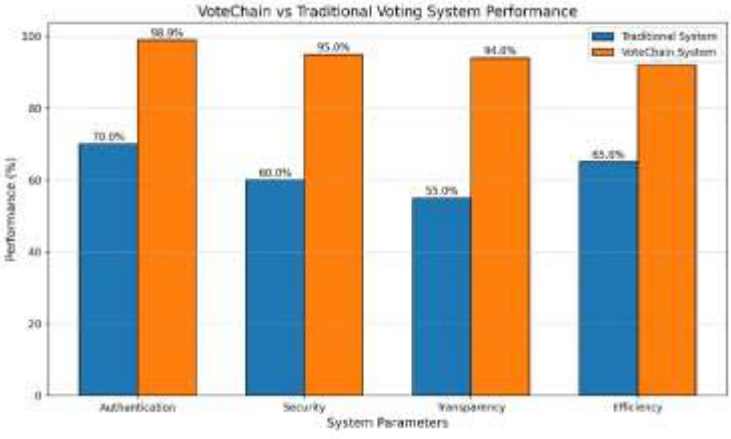

Fig. 2: Performance Comparison between Traditional Voting System and Proposed VoteChain System

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.

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

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

7.3 FRAUD DETECTION PERFORMANCE

The machine learning module continuously monitors system activity to detect suspicious behavior. During testing, the system successfully identified and flagged abnormal activities such as:

- Multiple login attempts from different devices
- Duplicate voting attempts
- Unusual voting patterns

These features enable real-time prevention of fraud instead of post-election analysis, making the system more secure and proactive.

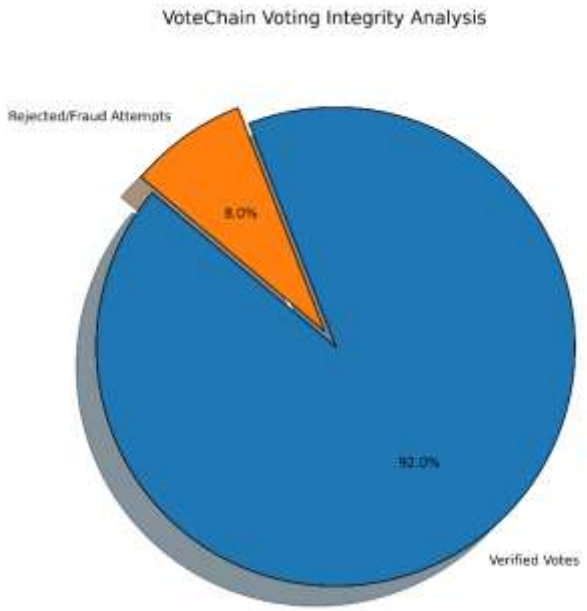

Fig. 3: Distribution of Valid Votes and Detected Fraudulent Attempts in VoteChain System

7.4 SYSTEM USABILITY

The user interface was designed to be simple and intuitive, allowing students to easily navigate through the system. The voting process requires minimal steps, reducing the chances of user errors.

- Easy login and authentication process
- Clear voting interface
- Quick response time

This improves overall user experience and encourages higher participation.

7.5 RESPONSE TIME AND EFFICIENCY

The system demonstrated efficient performance during testing, with minimal delays in authentication, vote submission, and result generation.

- Fast authentication process
- Immediate vote recording
- Instant result computation after voting ends

This eliminates the need for manual counting and significantly reduces the time required to declare results.

7.6 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.

Compared to conventional systems, VoteChain offers:

- Stronger authentication through facial recognition
- Real-time fraud detection instead of post-analysis
- Tamper-proof vote storage using ledger mechanisms
- Faster and more accurate result generation

Furthermore, the system minimizes human intervention, reducing the chances of errors and bias during the election process. The combination of these features enhances trust among users and ensures fairness in the election.

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

In this paper, a secure and intelligent digital voting system named **VoteChain** has been presented to address the limitations of traditional and existing online voting methods used in educational institutions. Conventional election systems often suffer from issues such as identity fraud, vote duplication, lack of transparency, and vulnerability to data manipulation. These challenges reduce trust in the election process and affect the reliability of results. To overcome these problems, the proposed system integrates modern technologies including Artificial Intelligence, Machine Learning, and a blockchain-inspired ledger mechanism. The use of AI-based facial recognition ensures that only authorized users can participate in the election, effectively preventing impersonation and enforcing the "one-student-one-vote" principle. In addition, machine learning techniques enable real-time detection of suspicious activities, making the system proactive in handling fraud rather than relying on post-election analysis. The system also ensures data security and integrity through encryption techniques and immutable vote storage. Each vote is securely recorded in a tamper-resistant ledger, guaranteeing transparency and trustworthiness. Furthermore, the automated result generation process eliminates manual errors and significantly reduces the time required to declare election outcomes. The experimental results demonstrate that VoteChain enhances election reliability, improves efficiency, and provides a user-friendly experience for both voters and administrators. Overall, the proposed system successfully transforms the traditional voting process into a modern, secure, and transparent digital solution suitable for academic environments.

8.2 Future Scope

1. **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.
2. **Advanced Biometric Authentication**
Future versions can include more advanced biometric methods such as deep learning-based facial recognition or multi-modal biometrics (face + fingerprint).
3. **Mobile Application Development**
A dedicated mobile app can be developed to increase accessibility and allow users to participate in elections from anywhere.
4. **Multi-Factor Authentication (MFA)**
Additional security layers like OTP, device verification, or biometric combinations can be integrated for stronger authentication.
5. **Scalability for Large-Scale Elections**
The system can be expanded to support large-scale elections such as university-wide, corporate, or government voting systems.
6. **Cloud-Based Deployment**
Deploying the system on cloud infrastructure can improve performance, scalability, and availability for a large number of users.
7. **Real-Time Analytics Enhancement**
Advanced analytics and visualization tools can be added for better insights into voting patterns and participation.
8. **Improved Fraud Detection Models**
More sophisticated machine learning models can be implemented to enhance the accuracy of anomaly and fraud detection.
9. **Offline Voting Support (Hybrid Mode)**
Future systems can include hybrid models that support both online and offline voting integration.
10. **Legal and Policy Integration**
The system can be adapted to comply with government regulations and standards for use in official elections.

9. 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 arXiv:2111.05096*, 2021.

[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, "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.

[16] S. Patel and D. Singh, "Application of Machine Learning for Election Data Analysis and Fraud Detection," *IEEE Conference*, 2024.

[17] L. Thomas, R. Joseph and P. Fernandes, "Cloud-Based Voting Application for Digital Campuses," *International Journal of Cloud Computing*, 2023.

[18] D. Chaum, "Secret-Ballot Receipts: True Voter-Verifiable Elections," *IEEE Security & Privacy*, vol. 2, no. 1, pp. 38–47, 2004.

[19] K. Karame, E. Androulaki and S. Capkun, "Double-Spending Fast Payments in Bitcoin," *ACM Conference on Computer and Communications Security*, 2012.

[20] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," 2008.