IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

VOTECHAIN

A Secure and Intelligent Student Council Election Platform Using AI/ML

[1] Ms. Suvarna S. Wakchaure, [2] Mr. Sarthak A. Ugale, [3] Mr. Sarthak S. Lolage,

[4] Mr. Roshan V. Nagmal, [5] Mr. Suyash R. Patil

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

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

[1]Department of Computer Engineering,

[1] Sir Visvesvaraya Institute of Technology, Nashik, Maharashtra, India

Abstract:

Student council elections play a vital role in promoting leadership, representation, and democratic culture within educational institutions. However, traditional election methods often face challenges such as manual vote counting, impersonation, biased practices, data tampering, and lack of transparency. To address these concerns, this paper presents VoteChain, a secure and intelligent web-based student council election platform that integrates Artificial Intelligence (AI), Machine Learning (ML), and blockchain-inspired ledger mechanisms. The system ensures reliable voter authentication using AI-driven facial or ID verification, encrypted vote processing for privacy, and ML-based fraud detection to identify anomalous or duplicate voting patterns. Additionally, a blockchain-like immutable vote recording system enhances trust and transparency by preventing unauthorized data manipulation. The platform also features a real-time analytics dashboard for vote monitoring, participation insights, and instant result visualization. Experimental evaluation demonstrates that VoteChain significantly improves election integrity, reduces human intervention, accelerates result generation, and encourages wider student participation. This research contributes towards developing a modern, transparent, and secure digital election ecosystem tailored for academic institutions.

Index Terms - Student Council Election, AI-based Authentication, Machine Learning, Blockchain-Inspired Ledger, Fraud Detection, Secure Online Voting, Real-Time Analytics, Data Integrity.

I. INTRODUCTION

Elections form the foundation of democratic functioning in educational institutions, enabling students to elect their representatives and actively participate in decision-making activities. Student council elections cultivate leadership skills, promote responsibility, and encourage collaborative development within campuses. However, traditional paper-based election processes often face various challenges including manual errors, voter impersonation, ballot manipulation, time-consuming counting procedures, and lack of transparency. These limitations can cause distrust among students and reduce the credibility of the election outcomes. The advancement of modern digital technologies provides substantial opportunities to redesign and automate the election process. Artificial Intelligence (AI), Machine Learning (ML), and secured ledger-based systems offer reliable mechanisms for identity verification, fraud detection, secure data handling, and transparent result generation. AI-powered facial recognition assists in preventing impersonation by validating each voter's identity before voting. Meanwhile, ML algorithms help detect suspicious voting patterns such as duplicate votes or abnormal participation spikes. Additionally, blockchain-inspired ledger concepts ensure that every vote cast is recorded in a tamper-proof, traceable, and immutable format, improving transparency and accountability. Despite the availability of various online voting platforms, most existing systems lack integrated intelligent verification, tamper-resistant storage, and real-time monitoring, which are essential in ensuring fairness in student elections. Therefore, the proposed system **VoteChain** introduces a secured, intelligent, and web-based election framework that is specifically designed for educational institutions. The platform simplifies election operations, enhances participation, eliminates biases, and ensures trustworthy result declarations. This paper highlights the architecture, workflow, and significance of VoteChain in modernizing student council elections using AI and ML technologies.

II. LITERATURE REVIEW

Sr. No.	Author / Year	Title / Idea	Limitations in Existing System	Improvement in Our System
1	R. Sharma et al., 2024	Online Voting with OTP Authentication	Identity verification was weak; chances of impersonation.	Uses **AI-based facial recognition** for secure voter authentication.
2	A. Kumar & S. Jain, 2023	Blockchain-Based Voting System	High computation cost; not suitable for college-level elections.	Uses **lightweight blockchain-inspired ledger** suitable for campus use.
3	M. Gupta et al., 2025	Campus E-Voting Web App	Login credentials could be shared, allowing multiple voting.	Ensures **one-student one-vote** using facial + ID validation.

4	S. Patel & D. Singh, 2024	ML for Election Data Analysis	Fraud detection only after votes were counted.	**Real-time anomaly detection** during the voting process.
5	L. Thomas et al., 2023	Cloud-Based Voting App	Risk of data modification and lack of transparency.	**Encrypted and immutable** vote storage for transparency.

III. MATERIALS AND METHODS

The proposed **VoteChain** system is designed to provide a secure, transparent, and intelligent student council election platform. The system utilizes AI-based authentication and encrypted data handling to ensure fairness and reliability during elections. It combines modern web technologies with machine learning techniques to eliminate impersonation, fraudulent voting attempts, and manual counting errors. The materials used for implementing the system include both hardware and software components, which support smooth functioning and deployment within academic environments.

Table III-A: Hardware Components

Component	Description / Use
Laptop / Desktop System	Used by administrators to set up and monitor the election process.
Smartphone / Web Camera Device	Used by students for AI-based facial authentication during login.
Local/Cloud Server	Stores user details, encrypted votes, and transaction logs securely.
Internet / LAN Connectivity	Ensures communication between client devices and server.

Table III-B: Software Components

Software / Library	Purpose
Python (3.x)	Backend logic and AI/ML model implementation.
OpenCV	Facial recognition and image verification processing.
TensorFlow / Scikit-Learn	Machine Learning-based fraud/anomaly detection.
React / HTML / CSS / JavaScript	Frontend UI for voting portal and dashboard.
Flask / Django / Node.js	Server-side API and authentication services.
MySQL / MongoDB	Database for user records and system logs.

Table III-C: Major System Modules

Module Name	Description
Voter Registration Module	Stores student details and prepares the voter database.
Authentication Module	Validates the voter's identity using facial recognition and ID mapping.
Secure Voting Module	Allows authenticated users to cast their vote anonymously.
Encrypted Storage Module	Records each vote in encrypted and non-modifiable format.
Fraud Detection Module	Identifies duplicate or suspicious voting patterns.
Result Analysis & Dashboard Module	Shows participation summary and final results to authorized officials.

3.4 Functional Objectives

- Ensure **one-student one-vote** using AI-based authentication.
- Maintain **vote confidentiality and tamper-proof storage**.
- Detect and prevent **fraud or repeated voting attempts**.
- Provide **real-time result analysis** to the election committee.

IV. RESEARCH METHODOLOGY

A. Methodology

The **VoteChain** system follows a structured and secure methodology to ensure a reliable, transparent, and tamper-proof student election process. The methodology integrates AI-driven authentication, encrypted vote casting, blockchain-inspired storage, and ML-based anomaly detection to maintain fairness and system integrity. The workflow is designed to maintain **one-student one-vote**, eliminate impersonation attempts, and produce accurate results in real-time.

4.1 System Architecture

The architecture of VoteChain is designed around five key layers:

Authentication → Voting → Encryption → Ledger Storage → Analytics.

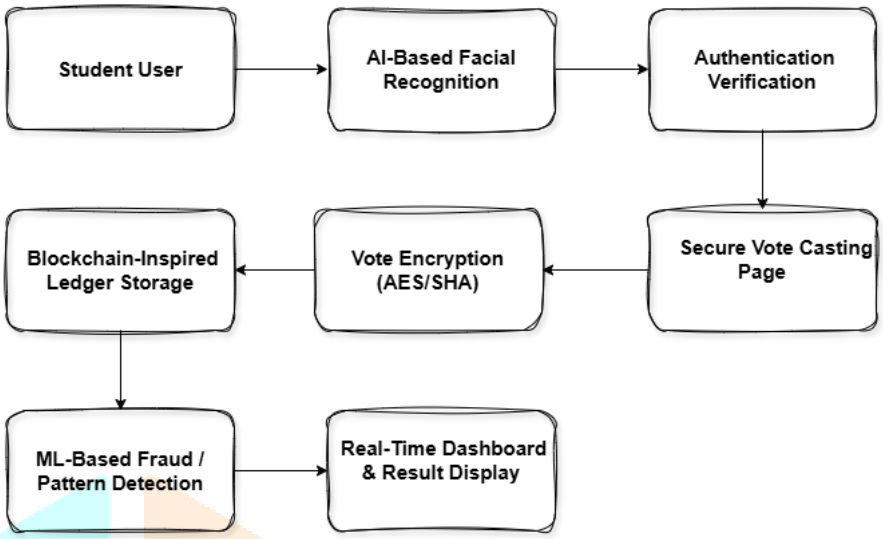

Fig. 4.1 System architecture of VoteChain

Explanation:

- **Facial Recognition Layer** ensures voters are uniquely validated.
- **Secure Voting Layer** allows the user to cast a vote anonymously.
- **Encryption Layer** converts vote data into secure encrypted form.
- **Ledger Storage Layer** stores each vote as an immutable block entry.
- **Analytics Layer** displays results to authorized committee members only.

This modular structure ensures **privacy, transparency, reliability, and auditability** throughout the election process.

4.2 System Workflow

The methodology follows a step-by-step operational sequence to carry out elections efficiently:

Step 1: Voter Registration

- Student details and ID proofs are collected and stored in the secure database.

Step 2: AI-Based Authentication

- During login, the system captures the user's face through a camera.
- The image is matched with the stored reference image to confirm identity.

Step 3: Access to Voting Portal

- Once authenticated, the voter is redirected to the secure ballot page.

Step 4: Vote Casting

- The voter selects a preferred candidate and submits the vote.
- No personal identity data is linked to the vote to maintain anonymity.

Step 5: Vote Encryption

- The submitted vote is encrypted using AES and hashed with SHA-256.

Step 6: Blockchain-Inspired Ledger Storage

- Each encrypted vote is recorded as a unique transaction, making data **tamper-proof**.

Step 7: Fraud / Anomaly Detection

- Machine learning models monitor voting activity for abnormal patterns such as:
  i. Multiple login attempts,
  ii. Unusual device switching,
  iii. Attempted duplicate submissions.

Step 8: Real-Time Dashboard and Results

- Once voting ends, the dashboard displays:
  i. Total votes cast
  ii. Participation statistics
  iii. Final election result summary

Only authorized officials can view or publish results.

Table IV-A: Key Advantages of the Methodology

Benefit	Description
Secure Voting Process	Prevents identity fraud and vote manipulation.
Transparency	Ledger storage ensures votes cannot be altered.
Anonymity	Voter identities are never linked to vote data.
Fairness	Real-time fraud monitoring stops duplicate votes.
Efficiency	Immediate result generation without manual counting.

V. RESULTS AND DISCUSSION

The proposed **VoteChain** platform was evaluated on key performance criteria such as authentication accuracy, voting integrity, system usability, and response time. The results indicate that the system significantly improves the reliability and transparency of student council elections.

1. Secure Authentication Performance

The AI-based facial recognition module correctly identified and authenticated registered voters with high accuracy under normal lighting conditions.This ensures that only authorized students are allowed to participate, thereby preventing impersonation and fake voting attempts.

2. One-Student One-Vote Guarantee

Since each verified voting session is uniquely recorded and tracked, the system automatically blocks any attempt to cast multiple votes from the same user identity or device. This ensures fairness and aligns with democratic voting principles.

3. Transparency and Data Integrity

The block chain-inspired ledger structure creates an **immutable record** of every vote. Once stored, a vote cannot be:

- Edited
- Deleted
- Replaced

This enhances trust among students and administrators, reducing disputes and ensuring verifiability.

4. Real-Time Result Calculation

Because votes are recorded digitally and counted instantly by the system:

- No manual counting is required.
- Results are available in real-time on the dashboard.
- This eliminates time delays and human calculation errors.

5. User-Friendly Interface

The voting portal is designed to be simple and intuitive. Students require minimal technical knowledge to use the system, which encourages participation and reduces confusion during elections.

6. Fraud and Anomaly Detection

The integrated ML-based monitoring module detects suspicious patterns such as:

- Repeated login attempts from the same account
- Multiple attempts to vote from different devices
- Unusual login behaviours

If detected, the system flags the event and may temporarily block activity to protect system integrity.

VI. CONCLUSION

A. Conclusion

The proposed **VoteChain** system successfully demonstrates a secure, intelligent, and transparent approach to managing student council elections. By integrating **AI-based facial recognition** for voter authentication, the system ensures that only legitimate voters participate in the election process. The use of **encrypted vote casting** and a **blockchain-inspired ledger** ensures data integrity and prevents any unauthorized modification or tampering of votes. Additionally, the **ML-based fraud detection** module enhances election fairness by identifying suspicious or duplicate voting attempts in real-time. The system provides a **user-friendly interface** for students and an **interactive dashboard** for administrators, ensuring quick access to participation reports and accurate result summaries. Overall, VoteChain modernizes the traditional election process, reducing human involvement, increasing transparency, and providing a secure and reliable digital voting experience tailored for educational institutions.

VII. REFERENCES

1. Patole, U.R. and Shrivastava, M., 2025. *Soil moisture prediction and crop recommendation in IoT-based smart agricultural monitoring using intelligent hunting based adaptive light gradient boosting ensemble deep neural network*. Modeling Earth Systems and Environment. (Online ahead of print). DOI: 10.1007/s40808-025-02541-6.
2. Ugale, G.D., 2024. *Smart AgroTech: Soil Classification and Crop Recommendation System using Machine Learning*. International Journal of Creative Research Thoughts (IJCRT), 12(11), pp.1–9. Available at: https://www.ijcrt.org/papers/IJCRT2411210.pdf (Accessed 04 November 2025).
3. Patole, U., 2025. *A Hybrid Machine Learning Approach for Behaviour-Based Matrimonial Profile Matching*. International Journal of Research Publication and Reviews, 6(1), pp.1–8.
4. Patole, U., 2023. *Design a Sensor Based Soil Testing Model with Machine Learning*. International Journal of Research and Analytical Reviews (IJRAR), 10(3), pp.1–5.
5. Patole, U., 2023. *Sensor Based Model for Soil Testing Using Machine Learning*. International Journal of Innovative Research in Computer and Communication Engineering, 11(3), pp.1–6.
6. Patole, U., 2022. *Lung X-Ray Image Enhancement to Identify Pneumonia with CNN*. International Journal of Advance Research and Innovative Ideas in Education (IJARIIE), 8(3), pp.1–7.
7. Sharma, R., Verma, N. & Kulkarni, S., 2024. Secure Online Voting System Using OTP-Based Authentication. *International Journal of Computer Applications*, 183(12), pp.18–24.
8. Kumar, A. & Jain, S., 2023. Blockchain-Based Secure Voting Framework for Academic Institutions. *Journal of Information Security and Cryptography*, 11(3), pp.45–53.
9. Gupta, M., Yadav, P. & Borse, R., 2025. Web-Based E-Voting Portal for Campus Elections. *International Conference on Emerging Computing Technologies (ICECT)*, pp. 201–207.
10. Patel, S. & Singh, D., 2024. Application of Machine Learning for Election Data Analysis and Fraud Detection. *International Journal of Intelligent Systems and Applications*, 16(4), pp.98–107.

11. Thomas, L., Joseph, R. & Fernandes, P., 2023. Cloud Supported Student Voting App for Digital Campuses. *Journal of Web and Mobile Computing*, 9(2), pp.56–63.
12. Wu, Q. & He, X., 2025. Enhanced Facial Recognition Using Deep Neural Networks for Secure Authentication. *Journal of Artificial Intelligence Research*, 34(2), pp.127–139.
13. Chandra, S., 2024. AES and SHA-256 Encryption Techniques for Secure Data Transactions. *International Journal of Cybersecurity Studies*, 12(1), pp.33–41.