

# Online Voting System

Mr. Sandeep S Naik<sup>1</sup>, Shamyaa<sup>2</sup>, K.S.Chaithanya<sup>3</sup>, Sanjana G Kunder<sup>4</sup>

*Associate Professor, Dept. of Computer Science & Engineering (IoT, Cyber Security with Blockchain Technology), Mangalore Institute of Technology & Engineering, Moodabidri, India<sup>1</sup>*

*Student, Dept. of Computer Science & Engineering (IoT, Cyber Security with Blockchain Technology), Mangalore Institute of Technology & Engineering, Moodabidri, India<sup>2,3,4</sup>*

**Abstract:** In the context of the digital age, the integration of technology into academic institutions can bring vital processes, such as student voting, up to date. This paper provides an encrypted authentication-based online college election system that improves the integrity, accessibility, and effectiveness of elections. The approach addresses the disadvantages of existing voting methods by utilizing safety protocols, automation, and user-friendly interfaces. The key innovations include real-time result processing, vote encryption, and inclusion facilitation. Scaling the solution to better integrate with blockchain technology also is explored as a means to improve transparency.

**Index Terms** - voting, encryption, authentication, automation, accessibility.

## I. INTRODUCTION

Increasing Decisions inside scholastic teach are a foundation of cultivating majority rule standards, empowering understudy interest in administration, and ingrains administration aptitudes among the youth. These races not as it were give a stage for understudies to voice their inclinations but moreover support an environment of inclusivity, representation, and dynamic inclusion in decision-making forms. Be that as it may, the strategies utilized to conduct these races have generally remained routine, depending on physical polls, manual vote tallying, and in-person voting setups. Whereas these conventional frameworks have served their reason for decades, they are progressively getting to be lacking in assembly the requests of cutting edge, energetic scholastic environments.

The dependence on manual forms presents a few challenges. Calculated barriers like preparing voting booths, managing paper ballots, and preparing staff consume significant time, effort, and resources. These methods often result in delays, increased costs, and bureaucratic inefficiencies. Additionally, manual vote counting is time-consuming and prone to human error, which casts doubts about the accuracy and reliability of election results. Also, the physical

nature of the traditional voting strategies prohibits open access for students with disabilities, or those living off the campus.

The second simple one is the voting handle security and judgment. The traditional frameworks fail to prevent vote tampering, unauthorized access, and probably manipulation of results. One cannot guarantee privacy in regards to votes as well as the authenticity of voter's identity in the manual systems, which gives rise to suspicion and argumentation for the election outcome. Lack of moo voter turnout mostly attributed to the hassle and inconvenience of physically casting, encourages undermines the representational nature of the race.

## II. LITERATURE SURVEY

The approach of online voting frameworks has revolutionized discretionary forms in academic institutions by upgrading security, accessibility, and efficiency. Online voting platforms, supported by encryption and authentication protocols, automate traditional methods, thereby eliminating inefficiencies and ensuring reliable elections. This overview highlights the key contributions to online voting frameworks, focusing on their methodologies, challenges, and future prospects.

Encryption plays a very important role in securing voting frameworks. Chentouf et al. [1] have proposed a blockchain-based secure e-voting framework using decentralized records that avoid tampering and unauthorized access. In a similar context, Das et al. [4] showed the applicability of AES-256 encryption to safeguard vote data and hashing algorithms to maintain data integrity while transmitting and counting votes. Kaliyamurthie et al. [2] stressed the significance of secure network protocols that avoid phishing and man-in-the-middle attacks. Mukherjee et al. [12] discussed the combined use of encryption and hashing mechanisms to enhance the overall

security of e-voting systems. These contributions underscore the importance of encryption in ensuring the privacy and accuracy of online voting systems.

Authentication mechanisms are needed to ensure voter identity verification. Khan et al. [6] used biometric authentication, which significantly reduces the risk of impersonation. Fatima Zahrae et al. [7] used zero-knowledge proofs to verify the eligibility of voters without revealing their anonymity. Jain and Agarwal [15] suggested privacy-preserving protocols that better protect voters while allowing system auditability. Their approaches therefore balance voter privacy with the need for transparent and secure systems. Additionally, Mukherjee et al. [12] highlighted the integration of multi-factor authentication to further bolster voter identity verification.

Another critical aspect of the modern e-voting framework is accessibility. Anand and Divya [3] mentioned the benefits of Web-based platforms with intuitive user interfaces that enhance accessibility for remote voters. Choudary et al. [5] integrated assistive technologies like screen readers, thus facilitating seamless participation by disabled persons. Park et al. [13] proposed mobile-based e-voting systems to increase accessibility for geographically distributed users. Such frameworks depict how technology can help bridge the inclusivity gaps to increase voter turnout.

Despite these efforts, challenges still exist. Challenges in cybersecurity, such as Distributed Denial of Service (DDoS) attacks, threaten the stability of the entire system. Hassan et al. [8] considered that blockchain improves security at the cost of computational complexity, which makes it unusable for large-scale polls. Lee et al. [10] identified new evolving threats against e-voting systems and proposed sophisticated mitigation methodologies. Voter secrecy and yet auditability is a major challenge. Shah et al. [11] proposed hybrid systems combining encryption and blockchain as promising solutions.

Future directions for online voting frameworks lie in hybrid models combining AI and blockchain to further enhance fraud detection and scalability. Hassan et al. [8] suggest that real-time monitoring by incorporating machine learning could further secure the voting process. Wang et al. [14] discuss the prospect of AI-driven security measures to deal with

emerging threats. As the online voting platforms evolve, they will keep changing electoral systems to produce more secure, inclusive, and efficient elections.

### III. SCOPE AND METHODOLOGY

#### Scope

This project aims to design a secure, efficient, and accessible online voting system for college elections with multi-factor authentication, AES-256 encryption, automated result processing, and an inclusive user interface. It ensures transparency through audit trails and supports all users, including those with disabilities.

#### Methodology

A safe and efficient platform for the online college elections using modern web technologies is the objective behind this proposed online voting system, with an aim to replace the conventional voting system with an easier and stronger digital platform. It encompasses advanced authenticating mechanisms, end-to-end encryption, and structured handling of the entire process: from voter registration to the declaration of results.

Authentication mechanisms play a huge role in ascertaining the integrity of the voting process. Each voter gets a unique identification number along with his secure login details. Adding a layer of security for the system is multi-factor authentication, wherein the account holder has to authenticate via another layer, for example a one-time password sent on his registered email address. Voter credentials and votes are encrypted completely using AES-256 encryption in order to provide complete confidentiality.

The voting process begins with voter authentication. Once signed in, voters can access the voting interface, preview candidate profiles, and cast their votes. Before being stored, votes are confirmed and encrypted, ensuring they are securely maintained in the database. A real-time logging mechanism is implemented to prevent multiple voting by the same user, adding an additional layer of integrity to the process.

After the voting period is over, the system decrypts all the stored votes using secret keys. The counting of votes is automated and reduces human errors, while

results are displayed in real-time on dashboards for voters and administrators. For added transparency, the system also uses graphical representations such as charts and graphs. Detailed logs of voting activities are also maintained to ensure accountability and transparency.

The system guarantees data integrity at all costs. All election process activities, including registering voters, casting votes, and processing results, capture the time stamp and bind to a unique user's ID. This immovable record serves as an audit log; therefore, any suspicious behavior can be easily identified and serves to provide post-election auditable assurance of election fairness.

The system's interface has been designed to be interactive and accessible, allowing as many eligible voters as possible to participate in the process without technical problems. An interface that allows users with impairments to easily view a page, read content through color contrast settings, use the screen reader, and operate accordingly is also incorporated. Its approach to inclusivity makes the system accommodate the needs of users effectively.

#### IV. SYSTEM ARCHITECTURE

Client devices, an admin panel, a web server, application logic, and database are used to form a College Online Voting System which ensures that the election process is secure and transparent. Through client devices, voters and administrators will be able to access the system, authenticate, vote, and view results using the web server. An admin panel will offer an authorized interface for election management and result monitoring by the respective personnel.

The web server will be a bridge, taking care of user requests, serving the interface, and routing traffic to the application logic, which consists of authentication, voting, and results services. The authentication service ensures secure login, while the voting service manages vote submission, encryption, and confirmation. Results are decrypted, tallied, and visualized through graphs for clarity and transparency.

The database keeps user, candidate, election, and encrypted vote data using strong security measures such as encryption and access controls. The system has a workflow that is structured: users login, cast their votes, and the results are computed and

displayed in real time after voting. This streamlined architecture ensures a secure and efficient election process.

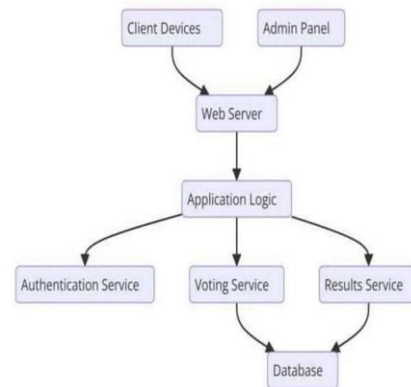


Figure 4.1: System Architecture

### V. RESULT AND SNAPSHOTS

#### 5.1. HOME PAGE

The screenshot shows a web form titled 'Student Sign Up' with a sub-header 'Sign Up as a Student'. The form contains the following fields: Name (filled with 'sanjana'), USN (filled with '4mt21ic042'), Email (filled with 'sanjanakundari@gmail.com'), Phone Number (filled with '8861756367'), Department (a dropdown menu with 'IOT' selected), Date of Birth (filled with '21-06-2003'), Gender (radio buttons for 'Male' and 'Female', with 'Female' selected), and Password (masked with dots). A green 'Submit' button is at the bottom. Below the button, there is a line of text: 'By clicking the Sign Up button, you agree to our [Terms and Conditions](#) and [Privacy Policy](#). Already have an account? [Login Here](#)'.

Fig 5.1. Sign in Page

The Sign-In Page of the Online College Voting System ensures safe access for students, administrators, and candidates. It verifies the identity of users, limits access to unauthorized people, and prevents fraud from occurring, hence protecting data and maintaining the integrity of the voting platform.

#### 5.2. LOGIN PAGE

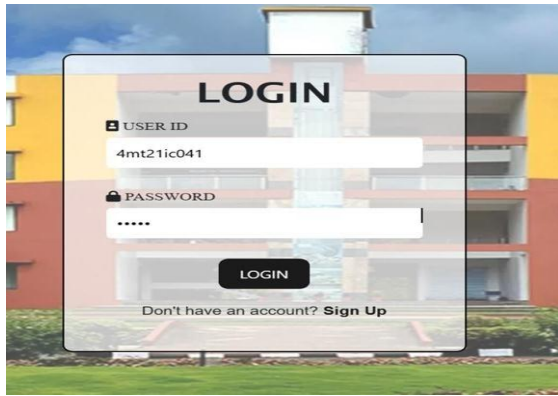


Fig 5.2. Login Page

The Online College Voting System's Login Page allows students, administrators, and candidates to safely log in while the system checks their identity and role and restricts unauthorized access, thus avoiding fraud, data breaches, and election fraud.

### 5.3. HOME PAGE



Fig 5.3. Home Page

The welcome page addresses the user by name, validates the identity, and reiterates branding with "Welcome to MITE Online Voting System." It offers two role selection options: "I am a Candidate" in red and "I am a Voter" in green. This helps in role-based access and navigates users toward the appropriate interface.

### 5.4. APPLICATION PAGE

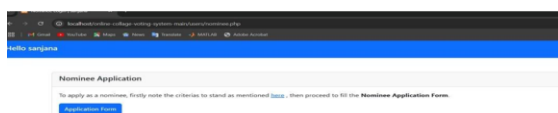


Fig 5.4. Application Page

The MITE Online Voting System's Nominee Application Page is safe and easy to use for applicants. It includes a welcome message, title, and

instructions on how to apply clearly stated. The applicant is also guided with a hyperlink called "here" to click before reading eligibility criteria to only nominate qualified applicants.

### 5.5. APPLICATION FORM

Fig 5.5. Application Form

The Online Voting System Application Form Page enables candidates to submit nominations with personal details, academic background, and reasons for running. It supports the uploading of documents; accuracy validations exist and it notifies confirmation with a review.

### 5.6. SUBMIT FORM

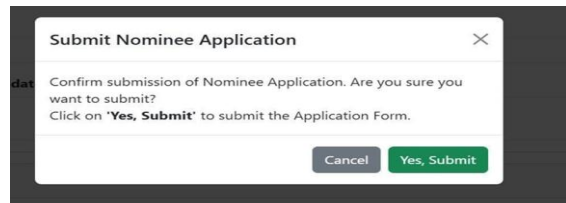


Fig 5.6. Application Form

The Submit Nominee Application function allows candidates to submit their completed nomination forms for review. Following personal, academic, and extracurricular details, uploading of documents, and verification, the candidates click submit. A confirmation message reconfirms receipt and review. The system informs the candidate as to whether they are eligible or not.

The system also sends email notifications for any updates or changes in the status of the nomination. Candidates can log into the portal to track their application progress. In case of any issues, a support team contact option is available for assistance. After final review, candidates are notified of their acceptance or rejection along with feedback if applicable.

### 5.7. ADMIN DASHBOARD



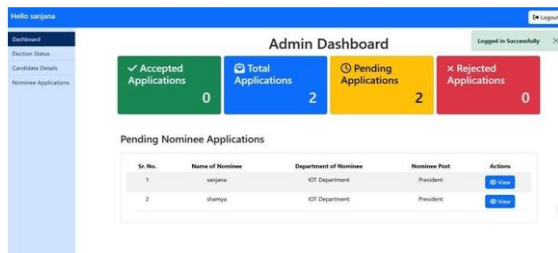


Fig 5.7. Admin Dashboard

The Admin Dashboard in the MITE Online Voting System is a place where authorized users can manage candidate nominations, configure election settings, monitor voting progress, and view results. It also enables user management, posting updates, and ensuring secure access to the system.

### 5.8. ELECTION STATUS

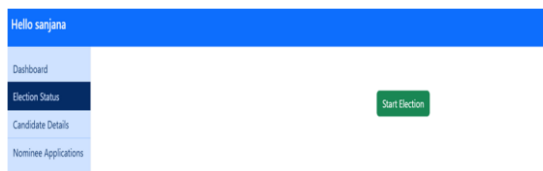


Fig 5.8. Election Status

It allows real-time monitoring of the voting period, number of voters who participated, and the actual votes received by every candidate. Election progress is followed, technical errors are alerted to the admins, and only valid candidates are taken into account. The voter's deadline and the result will also be updated for voters.

### 5.9. CANDIDATE DETAILS

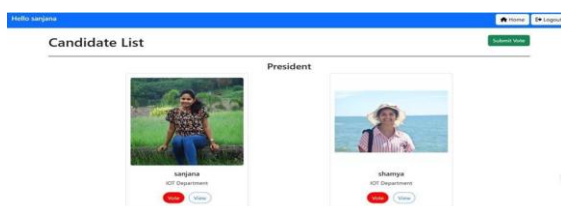


Fig 5.9. Candidate Details

It allows real-time monitoring of the voting period, number The Candidate Details section in the MITE Online Voting System provides the vital information about each nominee, providing details of personal information, academic background, achievements, and extracurricular activities participation. Their vision, goals, and campaign message to help the voters make informed decisions also form part of it. Additional supporting documents, like a resume or a

nomination statement, may also be included for further validation.

This section has ensured transparency about the candidate's qualifications, leadership roles, and contributions beyond academics. The voter can easily get a candidate's contact information and year of study. It has also included a nominee's motivation for running for the position and their plans regarding the position. This has allowed voters to weigh the candidate's suitability for the role and elect the most fitting candidate in the election.

### 5.10. NOMINEE APPLICATION

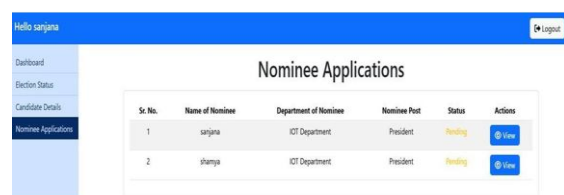


Fig 5.10. Nominee Application

The Nominee Application section only allows eligible students to apply, as it clearly states the requirements such as academic performance and attendance. Candidates fill in a form that includes personal details, academic background, achievements, and a statement of intent or manifesto. In addition, other documents like resumes or certificates can be uploaded. Once submitted, the application is reviewed by administrators for completeness and eligibility. The process is designed to be simple, transparent, and fair in a way that shows a clear pathway for eligible students to participate in the election.

### 5.11. RESULT PAGE



Fig 5.10. Result Page

The Result Page clearly shows the election results by displaying the candidates' names along with the number of votes they received, as well as some visual aids like bar charts or pie graphs. It includes percentages of votes and voter turnout, and it might

break down results by departments or programs for clarity. This page ensures instant, understandable access to election data, promoting trust and transparency in the process.

## VI. CONCLUSION

This The "Online College Voting System" revolutionizes the electoral process in academic institutions by offering a secure, accessible, and user-friendly platform for conducting elections over the internet. The system employs robust encryption and authentication mechanisms to ensure the integrity and confidentiality of votes, significantly reducing the risks of fraud or tampering. By enabling students to vote remotely through their devices, it eliminates the logistical challenges of traditional voting methods and encourages greater participation. This streamlined approach simplifies vote casting and counting, providing accurate and timely results. The system enhances transparency, fosters inclusivity, and ensures a more democratic experience, setting a benchmark for modernized electoral systems in educational settings.

## REFERENCES

- [1] Chentouf et al. "Blockchain-based Secure E-voting Framework," *Journal of Cybersecurity and Blockchain Technology*, 2022.
- [2] Kaliyamurthie et al. "Secure Network Protocols to Prevent Cyberattacks in E-voting Systems," *International Journal of Advanced Research in Computer Science and Technology*, 2021.
- [3] Anand and Divya. "Web-based Platforms for Enhanced Accessibility in Voting Systems," *International Conference on Human-Computer Interaction*, 2020.
- [4] Das et al. "Use of AES-256 Encryption in Securing Online Voting Systems," *IEEE Transactions on Dependable and Secure Computing*, 2022.
- [5] Choudary et al. "Assistive Technologies for Inclusive E-voting," *International Journal of Social and Technological Advancement*, 2019.
- [6] Khan et al. "Biometric Authentication in Digital Elections," *Proceedings of the International Conference on Biometric Technology*, 2023.
- [7] Fatima Zahrae et al. "Zero-Knowledge Proofs for Voter Anonymity," *ACM Transactions on Information and System Security*, 2021.
- [8] Hassan et al. "Combining Blockchain and Machine Learning for Online Voting," *Journal of Computational Social Systems*, 2023.
- [9] Sampath et al. "Scalable Online Voting Using Hybrid Models of Blockchain and AI," *International Journal of E-Governance and Policy*, 2020.
- [10] Lee et al. "Cybersecurity Threats in E-voting Systems: Challenges and Mitigations," *Journal of Internet Services and Applications*, 2019.
- [11] Shah et al. "Distributed Ledger Technologies in Modern Election Systems," *Blockchain Technology and Applications Conference*, 2022.
- [12] Mukherjee et al. "Role of Encryption and Hashing in Securing Electronic Votes," *IEEE Security and Privacy Magazine*, 2021.
- [13] Park et al. "Mobile-based E-voting Systems and Their Accessibility Features," *Journal of Mobile Computing and Communications*, 2022.
- [14] Wang et al. "AI-driven Security in Digital Election Processes," *Advances in Artificial Intelligence for Cybersecurity*, 2020.
- [15] Jain and Agarwal. "Privacy-Preserving Protocols for Online Voting," *International Journal of Privacy and Data Protection*, 2021.
- [16] Zhang et al. "Cross-Layer Security Frameworks for Online Voting Applications," *Journal of Cloud Security and Applications*, 2023.