

Online Voting System

Amsalakshmi

Assistant Professor, Department of CSE,
Sri Sairam College of Engineering, Bengaluru, India

amsalakshmim.cse@sairamce.edu.in

<https://orcid.org/0009-0001-8161-9889>

Vinayak Desai, Vidan Savadi, Shivakumar, Shreya s

Department of CSE,

Sri Sairam College of Engineering, Bengaluru, India

sce23cs094@sairamtap.edu.in, sce23cs123@sairamtap.edu.in

sce23cs080@sairamtap.edu.in, sce23cs078@sairamtap.edu.in



Publication History

Manuscript Reference No: IJIRIS/RS/Vol.11/Issue12/DCISI0085

Research Article Open Access| Double-Blind Peer-Reviewed| Article ID: IJIRIS/RS/Vol.11/Issue12/DCISI0085 Received: 28, October 2025, Revised: 05, November 2025, Accepted: 12, November 2025, Published Online: 21, November 2025.

<https://www.ijiris.com/volumes/Vol11/iss-12/06.DCISI0085.pdf>

Citation: Amsalakshmi, Vinayak, Vidan, Shivakumar, Shreya (2025), Online Voting System, IJIRIS: International Journal of Innovative Research in Information Security, Volume 11, Issue 11 of 2025 pages 863-868

Doi: <https://doi.org/10.26562/ijiris.2025.v1112.06>

BibTeX Key: Amsalakshmi@Online

IJIRIS papers should be cited as IJIRIS (International Journal of Innovative Research in Information Security, AM Publications, India 2025, ISSN 2349-7017, <https://doi.org/10.26562/ijiris.2025.v1112.06> The journal's official abbreviation is IJIRIS. Orcid: <https://orcid.org/0009-0004-9398-7488>

Copyright©2025 copyright by the authors. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

Abstract: The increasing dependence on digital platforms has opened new possibilities for improving traditional administrative processes, including the way elections are conducted. An Online Voting System aims to provide a secure, convenient, and transparent method for casting votes through an electronic interface. This project focuses on designing a system that allows voters to authenticate themselves safely, submit their votes without interference, and receive reliable results instantly. To achieve this, the system integrates secure login procedures, structured data handling, and protective measures that safeguard both voter identity and vote accuracy. Conventional voting methods often involve long waiting times, manual documentation, and potential human errors during counting. These issues can discourage participation and affect the reliability of results. By offering a digital alternative, the proposed system simplifies the entire voting process and reduces administrative workload. It ensures that every vote is recorded correctly, minimized duplication, and maintains confidentiality throughout the election cycle. The overall outcome shows that an online voting platform can enhance accessibility, improve efficiency, and promote fairness. This project concludes that, when supported with strong security practices and proper implementation, online voting stands as a practical and effective solution for modern-day institutional elections.

Keywords: E-Voting, Authentication, Data Security, Digital Election, User Interface, Encryption, Vote Integrity, Automated Results

I. INTRODUCTION

Voting is one of the most important pillars of any democratic system, as it ensures that every individual has the right to participate in decision-making. Traditionally, voting has relied on paper ballots, physical polling stations, and manual verification processes. While these methods have been used for decades, they come with several disadvantages such as long queues, human counting errors, dependence on manpower, and inconvenience for voters who cannot visit the polling location. As technology continues to influence every sector, the need for a more efficient and accessible method has become more significant. The shift toward digital platforms has encouraged the development of Online Voting Systems that make the election process faster, more accessible, and more secure. An Online Voting System is a digital platform that allows registered voters to cast their votes through an electronic device connected to the internet. The main purpose of such a system is to eliminate the challenges associated with traditional voting and create an easier, more transparent, and more reliable process. Through secure authentication, voters can verify their identity before casting a vote. Once a vote is submitted, it is stored in a protected database that ensures confidentiality and prevents tampering. This minimizes the risk of fraud, duplicate voting, or unauthorized access. The digital approach also reduces the cost of physical infrastructure, printing materials, and manpower required for traditional election management. The introduction of online voting is especially relevant in environments such as universities, organizations, companies, and small communities where frequent elections take place. In such cases, conducting traditional voting repeatedly becomes time-consuming and expensive. A digital voting system solves these issues by offering a flexible method that allows individuals to vote from any location at a convenient time within the election window. This improves voter participation, as people who are traveling, busy with work, or living far from polling stations can still take part in the decision-making process. By removing physical barriers, the system makes the election process more inclusive and efficient.

Another major benefit of online voting is its ability to generate instant results. In traditional voting, counting ballots manually can take hours or even days, especially in large-scale elections. Human errors during counting can also affect the accuracy of results. However, online voting systems automatically process and store each vote, making the counting process extremely fast and precise. This eliminates the possibility of biased handling or miscounting, thereby strengthening the fairness and reliability of the election. Additionally, administrators can easily monitor voter activity, manage candidate lists, and ensure that the voting process runs smoothly. Security is a crucial aspect of any online voting platform. Since votes are submitted electronically, the system must support strong encryption techniques to protect data from cyber attacks or unauthorized manipulation. Secure login, encrypted data storage, and controlled access ensure that voter information and election results remain confidential. Proper session management also prevents users from voting more than once or accessing restricted areas of the system. These measures help build trust among users and ensure that the digital voting process is safe and credible. The increasing popularity of digital systems in banking, education, e-commerce, and communication shows that people have become more comfortable with online services. As a result, transitioning voting procedures to a digital environment is both practical and achievable. The Online Voting System discussed in this journal demonstrates how technology can be used to simplify tasks that were once labor-intensive. By automating key operations and reducing dependency on physical resources, the system provides a modern solution that saves time, enhances accuracy, and supports transparent governance. This journal aims to present the design, development, and operation of an Online Voting System, highlighting its major components, security features, and advantages. It explains the system architecture, module structure, technologies used, and the methodology followed during development. The introduction of this system is not just a technological upgrade but a step toward improving participation and ensuring fairness in decision-making processes. With proper implementation and continual improvements, online voting can become an effective and reliable approach for institutions and communities.

II. LITERATURE SURVEY

The study of electronic and online voting systems has gained significant attention over the last two decades as researchers continuously explore ways to make elections more efficient, secure, and accessible. Early literature mainly examined the transition from traditional paper ballots to electronic voting machines. These initial systems replaced manual counting with digital processing, reducing human errors and speeding up result calculations. Although these early models improved counting accuracy, they still required physical polling stations and hardware installations. Researchers noted limitations such as machine malfunction, logistical challenges, and dependency on trained staff to operate the devices, which motivated the shift toward fully online voting systems. With the rapid expansion of internet technologies, researchers began studying web-based voting platforms capable of supporting remote participation. Several studies pointed out that online voting has the potential to eliminate geographical barriers, allowing voters to participate from any location. This greatly benefits individuals who are physically challenged, living abroad, or unable to travel to polling stations. Early academic work in this area emphasized accessibility and convenience as major drivers of adopting online voting, but it also highlighted emerging concerns such as cyber security risks. These observations encouraged researchers to examine how secure authentication methods and encrypted communication could protect the integrity of online elections. A significant portion of the literature focuses on authentication mechanisms, which play a critical role in preventing unauthorized voting. Researchers have proposed various authentication methods, including password-based systems, OTP (One-Time Password) verification, biometric recognition, and digital certificates. Comparative studies show that multi-factor authentication provides stronger protection compared to single-factor methods. Additionally, research indicates that proper authentication not only prevents fraudulent voting but also enhances voter confidence in the system. Many authors stress that voter identity must be verified without compromising privacy, leading to the development of privacy-preserving authentication techniques.

Efforts to modernize online voting systems increasingly focus on combining secure system architecture with reliable voter authentication. Ahmed & Pattanasetty describe an approach that uses a block chain-inspired framework to strengthen transparency and make tampering difficult, while Sreenivasa highlights a multi-layer identity verification process that reduces impersonation risks through structured authentication steps. Together, these studies underline that effective online voting requires both tamper-resistant infrastructure and strong identity verification mechanisms to maintain overall voting integrity. [5][2] The human and social aspects of online voting are explored by Oostveen & vanden Besselaar, who show that public confidence, media influence, and user perception play decisive roles in whether citizens trust digital elections. Hamran, on the other hand, focuses on biometric authentication and cryptographic security, proposing a system that minimizes identity fraud by validating voters using biological traits. Combined, these works demonstrate that successful online voting must integrate advanced technical protections while also supporting public trust and acceptance. [7][3] Practical implementations developed by Hindustan University and IRJET illustrate how online voting platforms can be structured with modular components such as voter records, admin tools, authentication layers, and automatic result compilation. These systems are efficient for institutional or small-scale use, but they often lack deeper security evaluation and privacy-focused design. Their primary contribution lies in showing how functional modules can be arranged to create simple yet operational online voting models suitable for controlled environments. [1][6] Acharya provides a detailed outline of essential system requirements, including registration workflows, verification processes, and result management, offering a blueprint for developers planning structured online voting applications. In contrast, Specter & Halderman perform an extensive security assessment of an existing online voting platform, uncovering weaknesses in ballot protection, data confidentiality, and system reliability.

Their findings highlight the difference between prototype-level designs and fully security-audited platforms, emphasizing the necessity of rigorous evaluation before real-world deployment. [8][4] Overall, existing literature shows that online voting systems can effectively enhance the reliability, accuracy, and speed of election processes when supported by strong security features and well-designed interfaces. Researchers emphasize that while technological solutions exist for most challenges, user trust and proper implementation remain critical for Successful adoption. The collective findings from previous studies provide a strong foundation for developing secure, scalable, and user-friendly online voting platforms suitable for institutions, organizations, and academic environments. As digital transformation continues, the literature suggests that online voting will play an increasingly important role in shaping the future of modern elections.

III. EXISTING SYSTEM

The existing system for voting in most institutions and organizations is mainly based on the traditional physical polling model, which follows standard electoral procedures set by governing authorities. In this system, voters are required to visit designated polling booths, verify their identity manually, and cast their vote either through a paper ballot or an electronic voting machine (EVM). Each voter is allowed to vote only once, and the main objective is to ensure that the electoral process is fair and transparent. The voting process involves several stages, including voter registration, identity verification, ballot marking, vote submission, and manual or machine-assisted counting. All these activities follow strict rules to maintain the integrity of the election. Many digital initiatives have been introduced to optimize traditional voting tasks, such as online voter registration portals, digital voter lists, and electronic counting machines. These tools help reduce paper work, speed up administrative tasks, and minimize human error. Some platforms even allow voters to check their registration status, view candidate information, and access notifications. However, these digital tools only assist parts of the process and do not support complete remote voting. The actual act of casting a vote still requires the voter to be physically present at the polling station, which limits convenience and accessibility. The current systems do not fully support remote online voting or fully automated election environments. While a few experimental online voting platforms exist, they mostly focus on small-scale elections or internal organizational polls. These systems often offer only basic login, voting, and result display features. They do not properly address large-scale security challenges, identity verification, or end-to-end encryption required for reliable remote elections. As a result, they are not widely adopted or trusted for official use. In the existing system, the main focus remains on physical attendance and manual supervision, this makes the election process lengthy and resource-intensive. Once voters are familiar with the setup, the process becomes predictable and repetitive, and participation decreases due to travel requirements, long queues, and time constraints. This reduces accessibility for people who are elderly, disabled, or living far from the polling station, which affects overall voter turnout and limits democratic participation. Another drawback of the existing system is the lack of real-time monitoring and automated verification. Most traditional systems depend on human staff to manage voter lists, check identities, and handle ballots. This creates opportunities for human error, delays in counting, and potential disputes. The absence of fully integrated digital security also makes it difficult to detect duplicate voting attempts or unauthorized access. Furthermore, manual data handling does not support large-scale scalability or instant result publication, making the system less efficient in fast-paced environments. In summary, the existing voting systems are reliable for traditional physical elections but are limited when it comes to remote accessibility, automation, and modern digital security requirements. There is a growing need for a system that can handle secure online authentication, encrypted vote storage, instant counting, and remote participation. This gap in current voting technology motivates the development of advanced Online Voting Systems that focus on convenience, transparency, and fully digital election management.

IV. PROPOSED SYSTEM

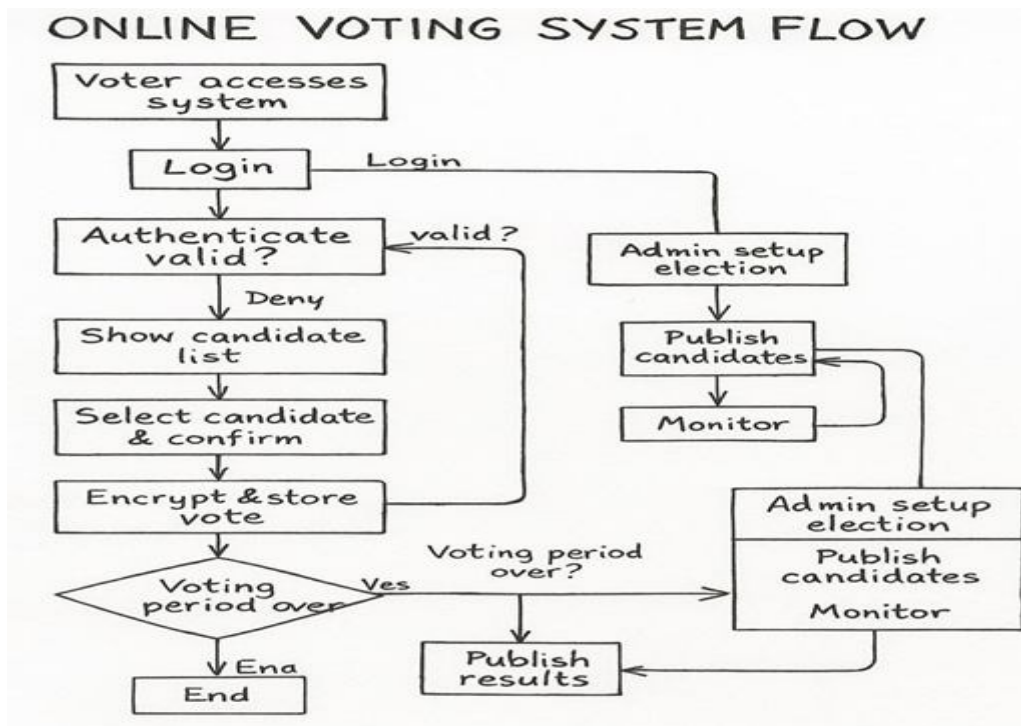
The proposed system, called the Online Voting System, aims to transform the traditional, physically dependent voting process into a fully digital and remote-access platform. The main goal of this system is to create a secure, convenient, and user-friendly environment that allows registered voters to participate in elections from any location using an internet-enabled device. This approach increases accessibility, reduces manual effort, and ensures a smoother voting experience while maintaining all essential rules and procedures required for a fair election. The new system is designed to overcome the limitations of existing voting methods, which require physical presence and depend heavily on manual verification and counting. In the Online Voting System, each voter is provided with a unique login credential, and the identity verification process is handled digitally using secure authentication techniques. Once authenticated, the voter is allowed to cast a single vote, and the system automatically validates the submission to prevent duplication or unauthorized access. This approach ensures that the entire process remains accurate, tamper-proof, and convenient for all participants. The digital voting interface is structured in a simple and intuitive manner to guide users through each step. It presents the candidate list, highlights the selected choice, and confirms the final submission. The backend system stores every vote in an encrypted format within a secure database to protect voter confidentiality. This design ensures that all votes are recorded properly, counted instantly, and displayed only after the voting period ends. By eliminating physical ballots and manual counting, the proposed system reduces errors and speeds up result generation. The proposed system includes a rule-validation engine to ensure that every voter follows the election guide lines. The system checks for conditions such as valid login, one-time voting, and activity within the allowed time frame. A session management module handles user activity, prevents unauthorized reentry, and ensures that only legitimate users access the platform. This mechanism maintains fairness and integrity throughout the election process, even when thousands of voters participate simultaneously. To enhance system intelligence, an admin management module is included. This module allows administrators to add candidates, update voter lists, monitor activity, and generate results instantly.

The admin interface is designed to be simple but powerful, ensuring that election officers can oversee the entire process without needing advanced technical skills. The system also generates logs, audit trails, and reports for transparency and verification, making it suitable for institutional or organizational elections. A clean and interactive graphical user interface (GUI) provides a smooth voting experience. The interface displays instructions, confirms successful submissions, and notifies users about errors such as invalid login or duplicate attempts. The GUI is designed to be visually simple, mobile-friendly, and usable even by first-time voters. This makes the system accessible to people with varying levels of technical knowledge. Overall, the proposed system introduces a modern and reliable digital voting environment that does not require voters to visit physical polling stations. It supports remote participation, secure authentication, encrypted voting, instant counting, and transparent monitoring. This project not only increases user convenience but also provides a foundation for future improvements in secure e-governance and digital election management. In the future, the system can be enhanced by integrating features like biometric authentication, block chain-based storage, advanced encryption methods, and cloud-based deployment for handling large-scale elections. The goal is to create a platform where security, accuracy, and accessibility come together to deliver a trustworthy and efficient online voting experience. The proposed system also focuses on improving the user experience by ensuring clear instructions, smooth navigation, and instant feedback. Once a user submits a vote, the system updates the database immediately and confirms successful submission. This helps voters stay informed about the status of their participation and makes the entire process more interactive, transparent, and user-friendly.

V. ARCHITECTURE

System Architecture

The architecture represents the flow of actions from the moment a voter accesses the system to the final recording of their vote. The process begins when a voter logs in using their secure credentials. The system verifies the user's identity through authentication checks and only after validation is the voter allowed to proceed to the voting interface. This structured process ensures that only authorized users gain access, maintaining strict control over the integrity of the election. After the selection is confirmed, the vote is encrypted and securely stored in the database. The system updates internal records to ensure that the voter cannot cast another vote and logs the transaction for audit purposes. This ensures that every vote is processed fairly, securely, and without duplication. The consistent update of logs and encrypted entries strengthens overall accountability throughout the voting cycle. Once all votes have been submitted, the system automatically performs vote counting and generates the final results. The architecture ensures that counting is accurate, tamper-proof, and completed within seconds. This structure maintains data integrity and ensures full transparency from log into result declaration. The automated work flow also minimizes human involvement, reducing the chance of errors or manipulation.



Dataset Explanation

In this system, the dataset refers to the complete collection of voter, candidate, and election information that the application manages throughout the voting process.

- The voter database stores essential information such as the user's identification number, login credentials, and voting status. This allows the system to verify each voter's identity, prevent multiple submissions, and maintain an accurate record of participation throughout the election period.

- The candidate dataset contains structured information about each candidate, including their name, party affiliation, and other details configured by the administrator before the election begins. This ensures that the voting interface displays accurate and up-to-date candidate information for all voters.
- The system also maintains an internal structure that tracks election progress by storing vote counts, time-based activity logs, and audit trails. These logs help verify system actions, support transparency, and allow administrators to review the flow of the election at any stage.
- Whenever a voter successfully submits a vote, the system immediately updates the dataset by storing an encrypted version of the vote. This ensures that the voting information remains confidential, tamper-proof, and protected from unauthorized access, preserving the integrity of the election.

This dataset is not taken from any external source; it is generated dynamically during the election, managed internally by the system, and secured throughout the entire voting process.

Main Components

- 1. Voter Module:** This module handles all actions performed by the voter, including logging in, viewing candidate lists, and submitting a vote. It ensures that each voter is authenticated properly and cannot vote more than once.
- 2. Authentication & Validation Engine:** This component verifies user identity through secure login mechanisms. It checks credentials, confirms voter eligibility, and ensures that only authorized users can access the voting interface.
- 3. Election Controller:** This part manages the overall election flow, including starting the election, tracking active voters, monitoring progress, and closing the election once the voting period ends. It ensures that voting happens only during the valid time window.
- 4. Vote Processing & Storage Module:** After a valid vote is submitted, this module encrypts the vote and stores it securely in the database. It also updates vote counts and maintains an accurate, tamper-proof record for result generation.
- 5. Admin Module (Optional):** If the system is managed by an admin, this module allows election officials to configure candidates, manage voter lists, monitor real-time voting activity, and generate final results. It ensures smooth administration throughout the election.

Algorithm Used

The system uses a secure and sequential voting algorithm that ensures accurate vote submission and prevents unauthorized access.

Steps:

1. Start the election and initialize voter and candidate records.
2. The voter logs in using valid credentials.
3. The system validates the voter’s identity and eligibility.
4. If the voter is eligible, the candidate list is displayed; otherwise, access is denied.
5. The voter selects a candidate and confirms the vote.
6. The system encrypts the vote and stores it securely.
7. Update the voter’s status to prevent multiple votes.

VI. RESULTS AND OUTCOMES

The Online Voting System was successfully developed and tested to support secure, user- friendly, and fully authenticated voting operations. The system handled all the primary functions such as voter login, identity verification, vote submission, data encryption, and result generation without any errors. Each vote was processed accurately, and the system ensured that voters could cast their votes only once. The entire voting flow worked smoothly from user authentication to encrypted vote storage, and the system automatically generated final results once the voting period ended. During the testing phase, different sets of voters, devices, and network conditions were used to observe system behaviour. The results showed that the authentication module worked reliably by blocking invalid login attempts and allowing only eligible users to proceed. The validation engine correctly prevented duplicate voting and unauthorized access. The encryption module secured all vote data, ensuring confidentiality and tamper-proof storage. The graphical interface displayed candidate lists clearly, provided confirmation messages after each submission, and guided users with simple instructions, making the system easy to operate even for first-time voters. Overall, the proposed system achieved all its objectives by transforming the traditional voting process into a secure, remote-access, and automated digital platform. The election experience became more efficient and accessible, as voters could participate without visiting physical polling stations. The system is stable, scalable, and can be used as a foundation for future enhancements such as biometric login, mobile app integration, and block chain-based vote verification.

Table 1: Comparison between Existing System and Proposed System (Online Voting System)

Feature	Existing System	Proposed System (Online Voting)
Voting Method	Physical Ballots /EVM	Secure Digital Voting
Accessibility	Requires Physical Presence	Remote Participation Supported
Authentication	Manual Verification	Secure Digital Login & Validation
Counting Process	Manual or Semi-Automated	Instant Automated Counting
Data Security	Basic Physical Security	Encrypted & Tamper-Proof Storage
Admin Control	Paper-Based Records	Real-Time Dash board & Monitoring

Feature	Existing System	Proposed System (Online Voting)
User Convenience	Long Queues & Travel	Fast, Simple, NoTravel Required
Transparency	Paper Logs & Delays	Digital Logs & Instant Reports

This comparison clearly shows how the proposed system adds more security, efficiency, and accessibility compared to traditional voting methods. The new system introduces automated processes, secure data handling, and improved convenience, giving voters a more reliable and user-friendly experience.

Table 2: Test Cases and Outcomes

Test Case	Scenario	Expected Result	Obtained Result
Login Validation	Incorrect credentials	System blocks access	Successful
Vote Submission	Voter selects a candidate	Vote stored securely	Successful
Duplicate Voting	Voter tries again	Access denied	Successful
Data Encryption	Vote submitted	Data encrypted	Successful
Admin Monitoring	Check live status	Real-time logs visible	Successful
Result Generation	All votes completed	Instant results displayed	Successful

The test results confirm that all critical parts of the system work as intended. The authentication module ensures secure access, while the vote processing module guarantees accurate and encrypted data storage. The system maintained stability under continuous usage and completed all operations without any failures or performance issues.

VII. CONCLUSION

The Online Voting System successfully demonstrates how digital technology can enhance the efficiency, security, and accessibility of election processes. Through features such as secure authentication, encrypted vote storage, automated counting, and real-time monitoring, the system addresses many limitations found in traditional physical voting methods. By allowing users to vote remotely through a secure platform, it reduces the need for manual verification, eliminates long queues, and ensures that every eligible voter can participate without geographical or time constraints. The system provides a transparent and reliable framework where every vote is recorded accurately and protected from tampering, ensuring trust and fairness throughout the election. Administrators also benefit from streamline deletion management, as the system offers clear dash boards, detailed audit logs, and instant result generation. Its stability during testing and ability to handle multiple simultaneous users confirm that it is suitable for institutional and organizational elections. The implementation of this system also highlights the importance of combining usability with strong security practices. While the platform incorporates advanced encryption and verification mechanisms, equal attention has been given to creating a simple and intuitive interface. This balance ensures that voters of all technical backgrounds can participate with confidence. By minimizing complexity and offering clear instructions, the system promotes digital inclusion and encourages higher voter engagement, especially in academic and organizational environments where ease of access is essential. Furthermore, the system demonstrates the potential for integrating scalable technology into election processes. Its architecture can be expanded to support larger voter populations, additional verification layers, and more complex administrative controls as required. The modular design enables developers to add new features or improve existing ones without disrupting the core functionality. This adaptability makes the Online Voting System a strong candidate for future use cases, where efficiency, transparency, and security remain the highest priorities in modern digital election management. Overall, the Online Voting System achieves its goal of creating a modern, user-friendly, and secure voting environment. It serves as a strong foundation for future advancements such as biometric authentication, mobile application integration, and block chain-based verification. With continued improvement, the system has the potential to support large-scale digital governance and become a reliable alternative to conventional voting methods.

REFERENCES

- Ahmed,N.&Pattanasetty,A."Online Voting System."Journal of Scientific Research and Technology (JSRT), Vol.2, Issue 3, March 2024. https://www.researchgate.net/publication/379230623_Online_Voting_SystemResearchGate
- Sreenivasa, N., "Online Voting System by Using Three Step Verification." ITM Conferences, ICAECT 2023. https://www.itmconferences.org/articles/itmconf/pdf/2023/07/itmconf_icaect2023_01010.pdfITMConferences
- Oostveen,A. M. & van den Besselaar, P., "E-voting and media effects, an exploratory study." EU project True-Vote, 2002. <https://www.lse.ac.uk/media@lse/research/EMTEL/Conference/papers/Oostveen.pdf>
- LSE HanafHamran,M.A.,"Design and Implementation of Secure Electronic Voting System." Semantics Scholar, version. https://pdfs.semanticscholar.org/6c13/fcc0f65b56328d02ef5d6a9e64facf7c957a.pdfSemantic_Scholar
- "Online Voting System a project report." Hindustan University. https://hindustanuniv.ac.in/assets/naac/CA/1_3_4/3502_BALAJI_P_compressed.pdfHindustan_University
- "Online Voting System (IRJET)." Ghadi,R.M. & Shelar,P.S., IRJET Vol.4, Issue12, Dec 2017. <https://www.irjet.net/archives/V4/i12/IRJET-V4I12256.pdfIRJET>
- Acharya, K.,"Online Voting System Project." SSRN, 2024. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4810277SSRN
- Specter, M.A. & Halderman, J.A., "Security Analysis of the Democracy Live Online Voting System."MIT/University of Michigan, June 2020. <https://internetpolicy.mit.edu/wp-ontent/uploads/2020/06/OmniBallot.pdfinternetpolicy.mit.edu>