INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.379

Online Voting System

Sakshi Salve[1], Ruchita Dhawale[1], Priyanka Kamble[1], Dia Koul[1], Kritika Mishara[1]

Prof. Vishakha jadhav[2]

Student, Department of Information Technology, Dhole Patil College of Engineering Pune, Maharashtra, India[1]

Professor, Department of Information Technology, Dhole Patil College of Engineering Pune, Maharashtra, India[2]

ABSTRACT: We are developing an on-line voting system by taking advantage of centralized database with a web interface. The main concept of this project is to build a website , which will be able to allow people to cast their vote through on-line. Time saving , working load reduced , information available at time and it provides security for data. In a democratic country like India we are not getting 100% of voting. People are not ready to poll their vote because of many factors like people can't go to the polling stations to cast their vote(especially aged persons and physically challenged people). People may be at remote places . There are several issues with traditional paper based voting like ridging votes during election , insecure or inaccessible polling stations , inadequate polling materials and also inexperienced personnel. This On-line Voting System seeks to address the above issues. With this system , the citizens may get ample time during the voting period. Every citizen is registered first and all the details are managed at centralized database. And at the time of elections the citizens will be login through their credentials and cast their vote

I. INTRODUCTION

Elections allow the populace to choose their representatives and express their preferences for how they will be governed . The election system must be sufficiently robust to withstand a variety of fraudulent behaviours and must be sufficiently transparent and comprehensible that voters and candidates can accept the results of an election. The voting system must be tamper-resistant Online voting systems are software platforms used to securely conduct elections.

As a digital platform , they eliminate the need to cast votes using paper or having to gather in person . Presently voting is performed by using ballot paper and the counting is done manually , hence it consumes a lot of time . There can be possibility of invalid votes. In our proposed systems , voting and counting is automated . It makes the election process easy and secure It also protect the integrity of every vote by preventing voters from being able to vote multiple times . Voting services helps to save time , stick to best practices , and meet internal requirements and/or external regulations , such as third-party vote administration needs.

II. RELATED WORK

1. Designing an online voting system involves various considerations, including security, accessibility, scalability, and user experience. Here are some related works and concepts in the field of online voting systems:

2. Helios Voting: Helios is an open-source online voting system that employs advanced cryptographic techniques like homomorphic encryption to ensure security and privacy in the voting process. It allows voters to verify that their vote is correctly recorded and counted without compromising anonymity.

3. Scantegrity: Scantegrity is another open-source voting system that integrates cryptographic methods with traditional paper-based voting. It enables voters to verify that their votes are accurately tallied through a verification code printed on their ballots.

4. Election Guard: Developed by Microsoft, Election Guard is a free and open-source software development kit (SDK) designed to make voting more secure, transparent, and accessible. It utilizes homomorphic encryption and zero-knowledge proofs to enable voters to verify that their votes are counted correctly.

5. Blockchain-based Systems: Some online voting systems leverage blockchain technology to enhance transparency and tamper resistance. By storing votes on a decentralized ledger, these systems aim to prevent fraud and manipulation.

6. Usability Studies: Various research studies have focused on the usability aspects of online voting systems, exploring user interfaces, accessibility features, and the overall user experience to ensure that voting platforms are intuitive and accessible to all voters.

7. Risk Assessment and Mitigation: Researchers and practitioners also conduct risk assessments and propose mitigation strategies to address potential vulnerabilities and threats in online voting systems, including cyberattacks, insider threats, and system failures.

8. Legal and Policy Frameworks: Developing legal and policy frameworks for online voting is crucial to ensure compliance with electoral regulations and to address concerns related to privacy, security, and voter authentication.

9. Pilot Projects and Case Studies: Some jurisdictions have conducted pilot projects or case studies to evaluate the feasibility and effectiveness of online voting in real-world elections, providing valuable insights and lessons learned for future implementations.

10. By exploring these related works and concepts, researchers and developers can gain valuable insights into the design, implementation, and evaluation of online voting systems, ultimately contributing to the advancement of secure, transparent, and inclusive democratic processes.

III. PROPOSED ALGORITHM

Designing an algorithm for an online voting system involves several key considerations to ensure security, accuracy, and efficiency. Here's a proposed algorithm outline:
1. Voter Authentication:
  - Voters need to be authenticated before casting their votes. This can be done using various methods such as username/password, biometrics, or two-factor authentication.

2. Ballot Generation:
  - The system generates a unique, encrypted ballot for each voter based on their authentication credentials. This ensures that each voter can only cast one vote and that their vote remains confidential.
3. Voting Process:
  - Voters access the online voting platform and securely cast their votes using the provided ballot. The system verifies the eligibility of the voter and records their vote.
4. Vote Recording:
  - Each vote is recorded in a secure and tamper-proof database. The system should ensure that the recorded votes cannot be altered or tampered with once they are submitted.
5. End-to-End Encryption:
  - All communications between the voter's device and the voting system should be encrypted to prevent interception and tampering.
6. Vote Tallying:
  - Once the voting period ends, the system tallies the votes and generates the final results. This process should be transparent and auditable to ensure the integrity of the election.
7. Result Verification:
  - The final results are made available for verification by independent observers and auditors to ensure accuracy and fairness.
8. Security Measures:
  - Implement robust security measures such as firewalls, intrusion detection systems, and regular security audits to protect the voting system from cyber attacks and unauthorized access.
9. Anonymity:
  - The system should ensure the anonymity of voters by separating their identity from their vote, preventing anyone, including system administrators, from linking votes back to specific individuals.
10. Accessibility:
  - The online voting platform should be accessible to all eligible voters, including those with disabilities, by providing alternative voting methods such as accessible interfaces and assistance options.

11. Contingency Planning:
- Have contingency plans in place to address any technical issues, disruptions, or attempts at tampering with the voting system during the election process.

12. Legal and Regulatory Compliance:
- Ensure that the online voting system complies with relevant laws, regulations, and standards governing elections and data privacy.

This proposed algorithm provides a high-level overview of the key components and considerations involved in designing an online voting system. Implementing such a system requires careful planning, rigorous testing, and collaboration with experts in cybersecurity, cryptography, and election administration.

IV. PSEUDO CODE

1. Initialize the system : Initialize list of candidates
                            Initialize list of voters

2. Registering process: for each new voter:
        Prompt voter to register with personal information
    Verify eligibility (age, citizenship, etc.)
    Generate a unique voter ID for the registered voter
    Store the voter information securely

3. Voting process: for each registered voter:
    Display list of candidates
    Prompt voter to select their choice
    Record the vote
    Ensure each voter can only vote once
    Verify the validity of the vote
    Store the vote securely

4. Counting votes: Initialize count for each candidate to zero
    for each recorded vote: Increment the count for the corresponding candidate

5. Displaying results: Display the total count for each candidate
    Declare the winner based on the highest count
    Ensure transparency and security in displaying results

6. Security measures: Implement encryption to secure voter information and votes. Protect against unauthorized access
    Regularly audit the system for vulnerabilities
    Implement measures to prevent tampering with votes or results

7. Accessibility: Ensure the system is user-friendly for voters with disabilities
    Provide multiple languages for accessibility
    Offer technical support for users encountering difficulties

8. Handling errors and disputes:Implement a process for handling errors, discrepancies, and disputes
    Allow for recounts or investigations if necessary
    Ensure transparency in addressing issues

9. Post-election procedures: Securely store all voter information and voting data for auditing purposes. Ensure the integrity of the voting records
    Review the performance of the system and make improvements as necessary

This is a basic outline and would need to be expanded upon with more detailed logic and error handling depending on the specific requirements and complexity of the voting system. Additionally, it's important to consider legal and regulatory requirements when implementing an online voting system.

V. SIMULATION RESULTS

1. Authentication Simulation:
- Simulate the authentication process where users log in with their credentials. Generate a set of dummy user accounts with different authentication scenarios (successful login, failed login due to incorrect credentials, etc.).

2. Ballot Generation Simulation:
- Simulate the generation of unique, encrypted ballots for each authenticated user. These ballots should correspond to the available voting options.

3. Voting Simulation:
- Simulate the voting process where users securely cast their votes using the provided ballots. Generate simulated voting data for each user, including their chosen candidate or option.

4. Vote Recording Simulation:
- Simulate the recording of votes in a secure database. Store the simulated voting data securely to prevent tampering.

5. End-to-End Encryption Simulation:
- Simulate the encryption of communication between users' devices and the voting system. Ensure that all communication channels are encrypted to maintain security.

6. Vote Tallying Simulation:
- Simulate the tallying of votes once the voting period ends. Aggregate the simulated voting data to calculate the total votes for each candidate or option.

7. Result Verification Simulation:
- Simulate the verification of final results by independent observers and auditors. Compare the simulated tally results with the recorded votes to ensure accuracy.

8. Security Measures Simulation:
- Simulate various security measures such as firewall protection, intrusion detection, and encryption to assess the system's resilience against cyber attacks.

9. Anonymity Simulation:
- Ensure that the simulated voting data maintains the anonymity of users, separating their identity from their vote.

10. Accessibility Simulation:
- Ensure that the simulated voting platform is accessible to all users, including those with disabilities.

11. Contingency Planning Simulation:
- Simulate contingency scenarios such as technical issues or disruptions during the election process. Evaluate the effectiveness of contingency plans in addressing these scenarios.

12. Legal and Regulatory Compliance Simulation:
- Ensure that the simulated voting system complies with relevant laws, regulations, and standards governing elections and data privacy.

VI. CONCLUSION AND FUTURE WORK

In conclusion, the development of an online voting system presents both opportunities and challenges in modernizing the electoral process. Through the proposed algorithm and simulation results, we've outlined a framework for designing and evaluating such a system. However, there are several considerations for future work and improvements:

1. Enhanced Security Measures: Future work could focus on further strengthening the security measures of the online voting system. This includes robust encryption techniques, advanced authentication methods, and proactive measures against cyber threats.
2. Usability and Accessibility: Improving the usability and accessibility of the voting platform is essential to ensure that it is intuitive and accessible to all voters, including those with disabilities or limited technical proficiency.
3. Trust and Transparency: Future efforts should prioritize enhancing trust and transparency in the electoral process. This includes implementing mechanisms for independent verification, conducting regular audits, and increasing public awareness of the system's integrity.
4. Scalability and Reliability: As the online voting system scales to accommodate larger populations or elections, future work should focus on ensuring scalability and reliability. This involves optimizing the system's performance, minimizing downtime, and implementing redundancy measures.
5. Legal and Regulatory Framework: Developing a comprehensive legal and regulatory framework is crucial for the widespread adoption of online voting. Future work should involve collaboration with policymakers, election officials, and legal experts to address legal and regulatory challenges.
6. Continued Research and Innovation: Continued research and innovation are essential to address emerging threats and leverage advancements in technology. This includes exploring new cryptographic techniques, improving user authentication methods, and integrating blockchain technology for enhanced security and transparency.

REFERENCES

1. Election Assistance Commission (EAC):

Website: eac.gov

The EAC provides resources, guidelines, and best practices for election administration in the United States. It offers insights into the legal and regulatory aspects of online voting.

2. International Foundation for Electoral Systems (IFES):

Website: ifes.org

IFES provides resources and expertise on electoral processes worldwide. Their publications and research can offer insights into online voting systems' design, security, and implementation.

3. National Institute of Standards and Technology (NIST):

Website: nist.gov

NIST offers cybersecurity guidelines, standards, and best practices. Their publications on voting system security and cryptographic protocols can be valuable for designing secure online voting systems.

4. GitHub:

Website: github.com

Explore open-source voting system projects and related repositories on GitHub. You can find code samples, libraries, and frameworks that can be useful for building and securing your online voting system.

5. Scholarly Journals and Conferences:

Websites like IEEE Xplore, ACM Digital Library, and SpringerLink host academic research papers on topics related to online voting systems, cryptography, and cybersecurity.

6. Online Courses and Tutorials:

Platforms like Coursera, Udemy, and edX offer courses on cybersecurity,   cryptography, and software development. These courses can provide valuable knowledge and practical skills for building secure online voting systems.

7. Government Election Websites:

Websites of government election authorities in your country or region may provide guidelines, regulations, and reports related to online voting systems and election technology.

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

Scan to save the contact details