PROJECT REPORT

BIOMETRIC SECURITY SYSTEM FOR VOTING PLATFORM

DATE	**29-10-2023**
TEAM-ID	**NM2023TMID05897**
PROJECT NAME	**BIOMETRIC SECURITY SYSTEM FOR VOTING PLATFORM**

TEAM MEMBERS

T.ABDUL WAASHIM	**812420104006**
P.KRISHNASAMY	**812420104042**
S.NIRANJAN	**8124020104067**
M.ARAVINDH	**812420104013**

1. INTRODUCTION

1.1 Project Overview
1.2 Purpose

2. LITERATURE SURVEY

2.1 Existing problem
2.2 References
2.3 Problem Statement Definition

3. IDEATION & PROPOSED SOLUTION

3.1 Empathy Map Canvas
3.2 Ideation & Brainstorming

4. REQUIREMENT ANALYSIS

4.1 Functional requirement
4.2 Non-Functional requirements

5. PROJECT DESIGN

5.1 Data Flow Diagrams & User Stories
5.2 Solution Architecture

6. PROJECT PLANNING & SCHEDULING

6.1 Technical Architecture
6.2 Sprint Planning & Estimation
6.3 Sprint Delivery Schedule

7. CODING & SOLUTIONING (Explain the features added in the project along with code)

7.1 Feature 1
7.2 Feature 2
7.3 Database Schema (if Applicable)

8. PERFORMANCE TESTING

8.1 Performace Metrics

9. RESULTS

9.1 Output Screenshots

10. **ADVANTAGES & DISADVANTAGES**

11. **CONCLUSION**

12. **FUTURE SCOPE**

13. **APPENDIX**

    Source Code
    GitHub & Project Demo Link

1. INTRODUCTION

Biometric security systems are revolutionizing the voting platform landscape by providing a robust and reliable means of verifying the identity of voters. In an era where the integrity of elections is of paramount importance, biometric security offers a sophisticated and trustworthy solution to ensure the accuracy and fairness of the electoral process. This cutting-edge technology leverages unique physical or behavioral traits of individuals, such as fingerprints, facial recognition, or iris scans, to prevent unauthorized voting and electoral fraud, thus safeguarding the democratic foundation of our society. In this discussion, we will delve into the key components, advantages, and potential challenges of implementing a biometric security system in the context of a voting platform.

1.1. Project Overview

1. Project Description:

The "SecureVote" project aims to develop a robust biometric security system for a voting platform. This system will enhance the security and integrity of the voting process by using biometric data to verify the identity of voters, ensuring that only eligible individuals can cast their votes.

2. Objectives:

a. Implement a biometric authentication system to confirm the identity of voters.
b. Develop a user-friendly interface for both voters and election officials.
c. Enhance the security and transparency of the voting process.
d. Minimize the risk of voter fraud and improve the overall integrity of elections.

3. Key Components:

a. Biometric Data Capture:

- Collect and store biometric data (e.g., fingerprints, facial recognition) for registered voters securely.

b. Voter Registration:

- Create a database of eligible voters with their biometric data.
- Verify and update voter information as necessary.

c. Authentication Process:

- Voters present their biometric data for verification during the voting process.
- The system matches the provided biometric data with the stored data in the database.

d. Secure Voting Interface:

- Develop a user-friendly voting platform for voters to cast their ballots securely.
- Implement encryption to protect the integrity of the voting data.

e. Election Monitoring:

- Provide election officials with tools to monitor and audit the voting process.
- Enable real-time reporting and data analysis for decision-making.

f. Security Measures:

- Implement multi-factor authentication to prevent unauthorized access.
- Employ encryption and secure data storage practices.
- Continuously update security protocols to counter potential threats.

4. Project Timeline:

- Phase 1: Requirements Gathering and System Design (3 months)
- Phase 2: Biometric Data Collection and Registration (6 months)
- Phase 3: Biometric Authentication System Development (5 months)
- Phase 4: Secure Voting Platform Development (6 months)
- Phase 5: Testing, Piloting, and Refinement (4 months)
- Phase 6: Deployment and Training (3 months)
- Phase 7: Ongoing Maintenance and Updates (Continuous)

5. Budget and Resources:

- SecureVote Project Budget: $X
- Project Team: Software developers, biometric experts, cybersecurity specialists, election officials, project managers, and support staff.
- Hardware and software infrastructure for data storage, processing, and voter registration.

6. Risks and Mitigation:

- Privacy concerns and data protection regulations.
- Technical challenges in biometric data accuracy and security.
- User acceptance and trust in the system.

7. Deliverables:

- Biometric data collection and registration system.
- Biometric authentication system integrated with the voting platform.
- Secure and user-friendly voting interface.
- Comprehensive documentation and training materials.

- Ongoing support and maintenance plan.

8. Conclusion:

The SecureVote project aims to revolutionize the voting process by introducing a biometric security system that enhances the integrity of elections while maintaining the privacy and trust of voters. This system will play a critical role in ensuring fair and secure democratic processes.

1.2.Purpose

Biometric security systems for voting platforms serve several important purposes:

1. Identity Verification: They help ensure that the person voting is indeed who they claim to be, reducing the risk of impersonation and fraud.

2. Enhancing Security: Biometrics add an extra layer of security by requiring physical attributes (fingerprint, iris scan, facial recognition) in addition to traditional identification methods.

3. Preventing Duplicate Voting: Biometrics can help prevent individuals from voting multiple times by verifying their identity during the voting process.

4. Data Integrity: They enhance the integrity of the voting process by reducing the chances of tampering with ballots or voter rolls.

5. Accessibility: Biometric systems can make voting more accessible for individuals with disabilities who may have difficulty with traditional voting methods.

6. User-Friendly: They can provide a user-friendly and convenient voting experience, reducing the risk of errors in the voting process.

7. Transparency: Biometric systems can enhance the transparency of the voting process, as they leave a digital record of who voted, when, and where.

8. Accountability: They can help identify and address any irregularities or disputes in the election process, promoting accountability.

2. LITERATURE SURVEY

2.1. Existing problem

Biometric security systems for voting platforms face several challenges and concerns:

1. Privacy: Collecting and storing biometric data raises privacy concerns, as it could potentially be misused or hacked.

2. Vulnerabilities: Biometric systems can be vulnerable to spoofing or falsification, such as using fake fingerprints or facial recognition evasion.

3. Inclusivity: Some individuals may not have suitable biometric features due to disabilities or other factors, potentially excluding them from the voting process.

4. Technical limitations: Biometric systems can sometimes produce false positives or false negatives, leading to authentication issues.

5. Costs: Implementing biometric technology can be expensive, which could be a barrier to widespread adoption, especially in developing countries.

6. Legal and ethical concerns: Biometric data usage is subject to various legal and ethical considerations, and it must adhere to strict regulations and policies.

7. Accuracy and reliability: Ensuring the accuracy and reliability of biometric systems, especially in large-scale voting scenarios, is crucial to maintain trust in the process.

8. Potential for data breaches: Storing biometric data creates the risk of data breaches, which could have severe consequences for voter privacy and security.

2.2. References

1. NIST Special Publication 800-76-2: "Biometric Data Specification for Personal Identity Verification." This document provides guidelines for the use of biometrics in identity verification, which is applicable to voting systems.

2. "Biometric Recognition: Challenges and Opportunities" by Anil K. Jain, Arun Ross, and Karthik Nandakumar. This book covers various aspects of biometric systems, including their use in security applications.

3. “Biometrics for Dummies” by Peter Gregory and Michael A. Simon. This introductory book provides insights into the basics of biometrics, which can be helpful for understanding the technology before implementing it in a voting system.

4. IEEE Xplore: The IEEE Digital Library contains numerous research papers and articles on biometric security systems. You can search for specific topics related to biometric voting systems.

5. Consult academic institutions and their research papers. Many universities and research organizations conduct studies on biometric systems, including their applications in voting platforms.

6. International Biometric Group (IBG) and Biometrics Institute: These organizations provide resources, reports, and best practices related to biometric technology.

7. Government guidelines and standards: Check with your country’s election commission or relevant government agency for guidelines and standards specific to implementing biometric security in voting systems.

8. Expert opinions and case studies: Seek out case studies and opinions from experts in the field of biometrics and cybersecurity to understand the challenges and best practices in implementing biometric security in voting systems.

2.3. Problem Statement Definition

1. **Voter Authentication**: Develop a biometric authentication method (e.g., fingerprint, iris scan, facial recognition) to reliably verify the identity of voters, preventing unauthorized access to the voting platform.

2. **Data Privacy**: Ensure the protection of voters’ biometric data, adhering to strict privacy regulations and standards to prevent misuse or unauthorized access.

3. **Security**: Implement robust encryption and security measures to safeguard the voting data, preventing tampering, hacking, or other forms of election fraud.

4. **Scalability**: Create a system that can handle a large number of users simultaneously, ensuring a smooth voting experience during peak hours.

5. **Usability**: Design an intuitive and user-friendly interface for both voters and election administrators to encourage participation and ease the management of the electoral process.

6. **Accessibility**: Ensure that the system is accessible to all eligible voters, including those with disabilities, by incorporating inclusive design principles.

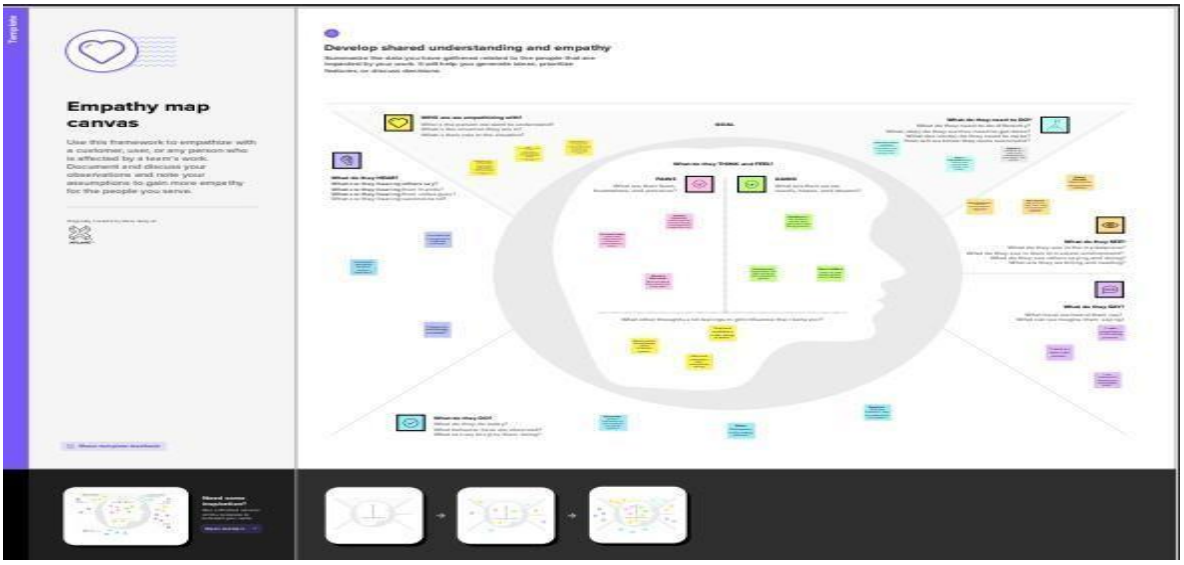
7. **Resilience**: Develop contingency plans to address system failures or disruptions, ensuring the continuous operation of the voting platform.

8. **Compliance**: Ensure that the system complies with all relevant legal and regulatory requirements, including those related to election security and data protection.

9. **Auditability**: Create mechanisms for transparent auditing of the voting process to maintain public trust and enable the verification of election results.
10. **Cost-Effectiveness**: Develop the system with a consideration of budget constraints while maintaining a high level of security and reliability.

3. IDEATION & PROPOSED SOLUTION

3.1. Empathy Map Canvas



3.2. Ideation & Brainstorming

4. REQUIREMENT ANALYSIS

4.1. Functional requirement

1. Voter Registration:

- Capture and store biometric data (e.g., fingerprints, facial features, iris scans) during voter registration.
- Verify the uniqueness of each voter's biometric data to prevent duplicates.

2. Voter Authentication:

- Authenticate voters using their biometric data at polling stations.
- Ensure fast and accurate biometric matching to confirm the voter's identity.

3. Data Security:

- Encrypt and protect biometric data to prevent unauthorized access or tampering.
- Implement secure communication protocols between polling stations and the central system.

4. Voter Enrollment:

- Provide a user-friendly enrollment process for voters to register their biometric data.
- Allow for easy updates to biometric data in case of changes or re-registration.

5. Access Control:

- Restrict access to the biometric database to authorized personnel only.
- Implement role-based access control for administrators and operators.

6. Audit Trail:

- Maintain a detailed audit trail of all interactions with the biometric system.
- Log any attempts at unauthorized access or tampering.

7. Redundancy and Availability:

- Ensure system availability with backup servers and failover mechanisms.
- Handle biometric data in real-time to prevent voting delays.

8. Reporting and Monitoring:

- Generate reports on voter authentication and system usage.
- Implement real-time monitoring for system performance and security.

9. Compatibility:

- Ensure compatibility with a variety of biometric devices and technologies.
- Support different types of biometric data, depending on voter preferences.

10. Compliance:

- Comply with legal and regulatory requirements for data protection and privacy.
- Follow industry standards for biometric data handling and security.

11. Voter Privacy:

- Protect voter privacy by storing biometric data separately from voter identity.
- Use anonymized tokens for authentication to prevent the tracking of individual votes.

12. Fail-Safe Mechanisms:

- Implement fail-safe mechanisms in case of system failures or security breaches.
- Have a backup plan for non-biometric authentication in case of technical issues.

4.2. Non-Functional requirements

1. **Security:**

- **Accuracy:** The system should have a low false acceptance rate (FAR) and a low false rejection rate (FRR).
- **Data Encryption:** All biometric data and communication should be encrypted to protect against unauthorized access.
- **Biometric Template Storage:** Biometric templates should be securely stored and should not be retrievable from the system.
- **Access Control:** Access to the biometric database and system settings should be restricted to authorized personnel only.

2. **Reliability:**

- **Availability:** The system should be available for voting during the designated voting period.
- **Fault Tolerance:** The system should continue to operate in the presence of hardware or software failures.
- **Redundancy:** Redundant servers and data centers should be in place to ensure continuous operation.

3. **Performance:**

- **Response Time:** The system should provide quick and responsive verification and authentication.
- **Scalability:** The system should handle increased voter loads during peak times, such as elections, without a significant drop in performance.
- **Throughput:** The system should process a large number of biometric verifications simultaneously.

4. **Compliance:**

- **Legal Compliance:** The system should comply with all relevant legal and regulatory requirements for privacy and security.
- **Standards Compliance:** The system should adhere to industry standards for biometric data handling and security.

5. **User Experience:**

- **Usability:** The system should be user-friendly, ensuring that voters can easily interact with it.
- **Accessibility:** The system should accommodate voters with disabilities, ensuring inclusivity.

6. **Data Privacy:**

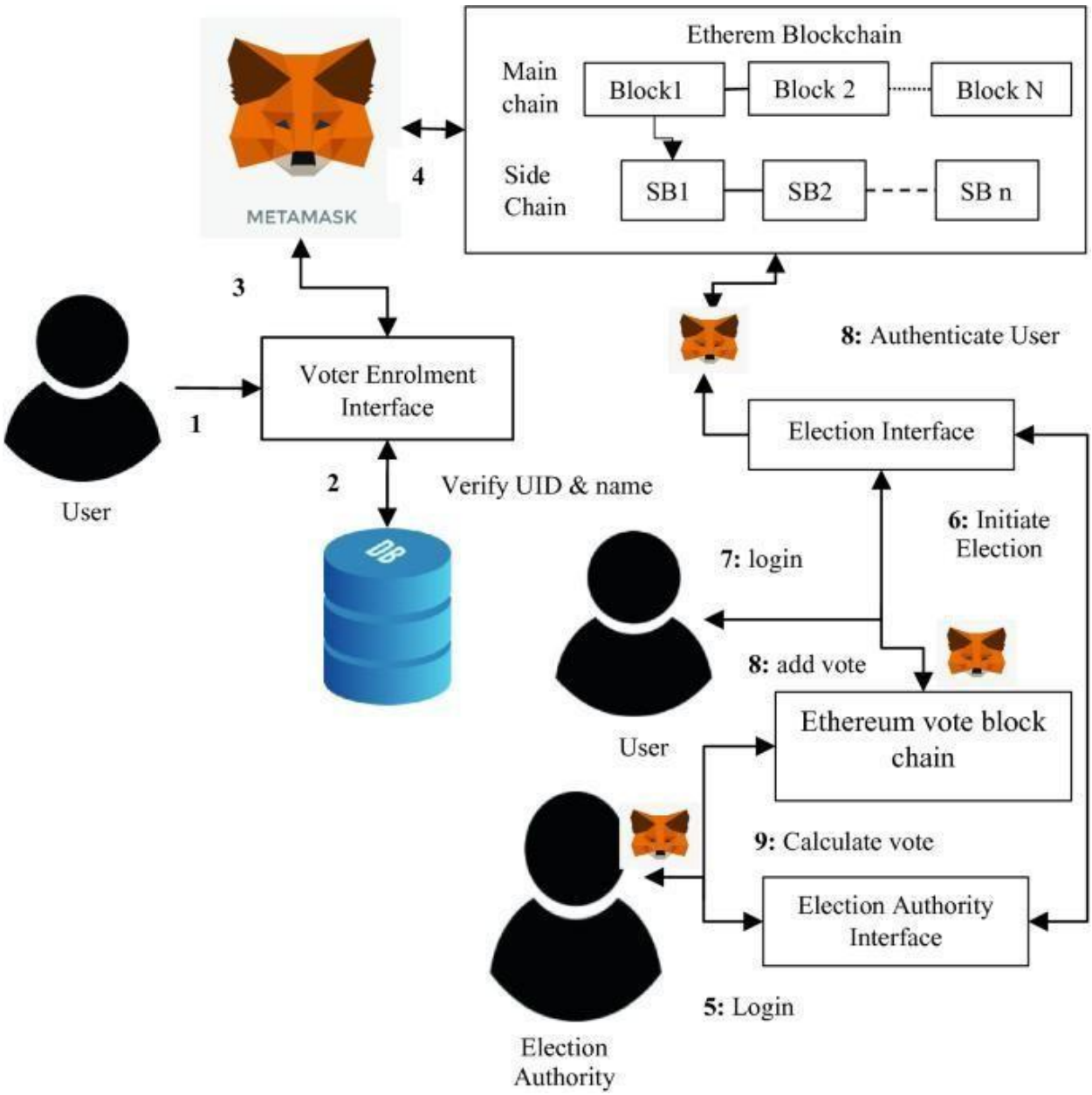
- **Data Retention:** Define how long biometric data is stored and specify when it should be securely deleted.
- **Consent:** Ensure that voters have given informed consent for the use of their biometric data.

7. **Auditability:**

- **Logging:** The system should log all access and usage for auditing and accountability purposes.
- **Audit Trail:** Provide an audit trail that can be reviewed to ensure the integrity of the voting process.

5. PROJECT DESIGN

5.1. Data Flow Diagrams & User Stories



6. PROJECT PLANNING & SCHEDULING

6.1. Sprint Planning & Estimation

Sprint planning and estimation for a biometric security system for a voting platform involves breaking down the project into manageable tasks and estimating the time required for each. Here's a high-level overview:

1. **Product Backlog**: Begin by creating a product backlog. List all the features and user stories related to the biometric security system. These might include tasks like biometric data capture, verification, database integration, and user authentication.

2. **Prioritization**: Prioritize the backlog items based on their importance and dependencies. Voter authentication and data security might be higher priorities.

3. **Sprint Planning**: Plan sprints, typically 2-4 weeks in duration, and select the top-priority backlog items for each sprint. These items should be small enough to be completed within the sprint.

4. **Estimation**: Estimate the effort required for each backlog item. You can use techniques like story points or time-based estimates. Biometric algorithms, for instance, might require more effort than database integration.

5. **Team Capacity**: Consider your team's capacity and how many story points or tasks they can complete in a sprint. This will help determine how many items to include in each sprint.

6. **Velocity**: Over time, you'll establish a velocity, which is the average number of story points your team can complete in a sprint. This helps with future planning.

7. **Daily Stand-ups**: Conduct daily stand-up meetings to monitor progress and identify and address any issues or roadblocks.

8. **Retrospectives**: At the end of each sprint, hold a retrospective to review what went well and what can be improved in the next sprint.

9. **Adapt and Iterate**: Be ready to adapt and adjust your plan as the project progresses. New insights or requirements may emerge during development.

6.2. Sprint Delivery Schedule

Sample sprint delivery schedule

Sprint 1 (2 weeks):

- Define project scope and objectives

- Conduct initial research and gather requirements

- Set up the development environment

- Create user stories and prioritize features

- Design the architecture of the biometric security system

Sprint 2 (2 weeks):

- Develop a prototype of the biometric authentication module
- Integrate with existing voting platform infrastructure
- Begin testing and validation of the prototype
- Review and refine the project plan based on initial progress

Sprint 3 (2 weeks):

- Complete the development of the biometric authentication module
- Conduct internal testing and debugging
- Prepare for user testing and feedback collection
- Draft documentation for system usage and deployment

Sprint 4 (2 weeks):

- Start user testing with a limited group
- Collect feedback and make necessary adjustments
- Continue testing and validation of the system's security
- Develop a detailed training plan for election officials and users

Sprint 5 (2 weeks):

- Implement final changes based on user feedback
- Conduct a security audit and penetration testing
- Prepare for a larger-scale pilot test
- Document all code and system configurations for future maintenance

Sprint 6 (2 weeks):

- Launch a pilot test in a controlled voting environment
- Monitor system performance and security in a real-world scenario
- Address any issues and fine-tune the system
- Finalize user manuals and training materials

Sprint 7 (2 weeks):

- Review the results of the pilot test and make any necessary adjustments
- Prepare for a broader deployment
- Train election officials and system administrators
- Set up a support and maintenance plan for ongoing operations

Sprint 8 (2 weeks):

- Deploy the biometric security system for the voting platform
- Monitor the system during the live election
- Provide real-time support and troubleshooting
- Continue to address any security or performance issues

7. CODING & SOLUTIONING

7.1. Feature 1

1. **Biometric Data Collection**: Implement a system to collect biometric data from voters. This could include fingerprint scans, iris scans, or facial recognition.
2. **Data Encryption**: Ensure the biometric data is encrypted to protect it from unauthorized access.
3. **Database for Biometric Templates**: Create a secure database to store biometric templates generated from the collected data. Use strong encryption to protect this database.
4. **Voter Registration**: Develop a registration process where voters' biometric data is enrolled in the system. This includes verifying their identity through official documents.
5. **Real-time Matching**: Implement a real-time matching mechanism that compares a voter's biometric data during the voting process to confirm their identity.
6. **Redundancy and Failover**: Include redundancy and failover mechanisms to ensure the system's availability during high-demand voting periods.

7. **Security Measures**: Implement security measures to protect against spoofing and tampering with biometric data.

8. **Audit Trail**: Maintain an audit trail of all biometric transactions to ensure accountability and traceability.

9. **Access Control**: Restrict access to the system and its data to authorized personnel only.

10. **User Authentication**: Use multifactor authentication to secure the system for administrators and poll workers.

11. **Privacy Protection**: Ensure that voter's biometric data is anonymized and that privacy laws and regulations are strictly followed.

12. **Testing and Verification**: Thoroughly test the system for accuracy, reliability, and security.

13. **Compliance with Regulations**: Ensure the system complies with all relevant laws and regulations regarding data privacy and voting.

14. **User-Friendly Interface**: Develop an easy-to-use interface for voters and poll workers.

15. **Monitoring and Alerts**: Set up monitoring and alert systems to detect and respond to any unusual activities or security breaches.

16. **Training**: Provide training for poll workers and election officials on how to use the system.

17. **Backup and Recovery**: Establish a backup and recovery system in case of data loss or system failure.

18. **Scalability**: Ensure the system can handle a large number of voters during peak voting times.

19. **Public Awareness**: Inform the public about the security and privacy measures in place to gain their trust in the system.

20. **Continuous Improvement**: Plan for regular updates and improvements to adapt to evolving security threats and technology advancements.

7.2. Feature 2

Decentralization

With blockchain the information is distributed across the network rather than at one central point. This also makes the control of information to be distributed and handled by consensus reached upon by shared input from the nodes connected on the network. The data that was before concentrated at one central point is now handled by many trusted entities.

Data Transparency

Achieving data transparency in any technology is to have a trust based relationship between entities. The data or record at stake should be secured and temper proof. Any data being stored on the blockchain is not concentrated at one place and is not controlled by one node but is instead distributed across the network. The ownership of data is now shared and this makes it to be transparent and secure from any third party intervention.

Security and Privacy

Blockchain technology uses cryptographic functions to provide security to the nodes connected on its network. It uses SHA-256 cryptographic algorithm on the hashes that are stored on the blocks. SHA stands for Secure Hashing Algorithm, these hashes provide security to the blockchain as data integrity is ensured by them. Cryptographic hashes are strong one way functions that generate checksum for digital data that cannot be used for data extraction. This makes blockchain as such a decentralized platform made secure by the cryptographic approaches which makes it to be a good option for privacy protection of certain applications

8. PERFORMANCE TESTING

1. False Acceptance Rate (FAR): Measures the rate at which unauthorized individuals are incorrectly granted access. Lower FAR is better.

2. False Rejection Rate (FRR): Measures the rate at which legitimate voters are incorrectly denied access. Lower FRR is better.

3. Equal Error Rate (EER): The point where FAR and FRR are equal, indicating a balance between security and usability.

4. Genuine Acceptance Rate (GAR): Measures the rate at which legitimate voters are correctly authenticated. Higher GAR is better.

5. Template Matching Speed: Assess the time taken to match biometric templates, ensuring timely voter verification.

6. Accuracy and Reliability: Overall system accuracy in correctly identifying voters and its reliability under various conditions.

7. User Enrollment Time: The time it takes for a voter to enroll their biometric data in the system.

8. Template Storage Efficiency: Evaluate the space required to store biometric templates for all registered voters.

9. Security Against Spoofing: Assess how well the system detects and prevents spoofing attempts, such as fake fingerprints or facial images.

10. Scalability: Measure the system's ability to handle a growing number of registered voters without a significant drop in performance.

11. Usability and User Satisfaction: Collect feedback from voters on the ease of use and overall satisfaction with the biometric authentication process.

12. Error Handling: Evaluate how the system handles errors, including providing clear instructions to voters when authentication fails.

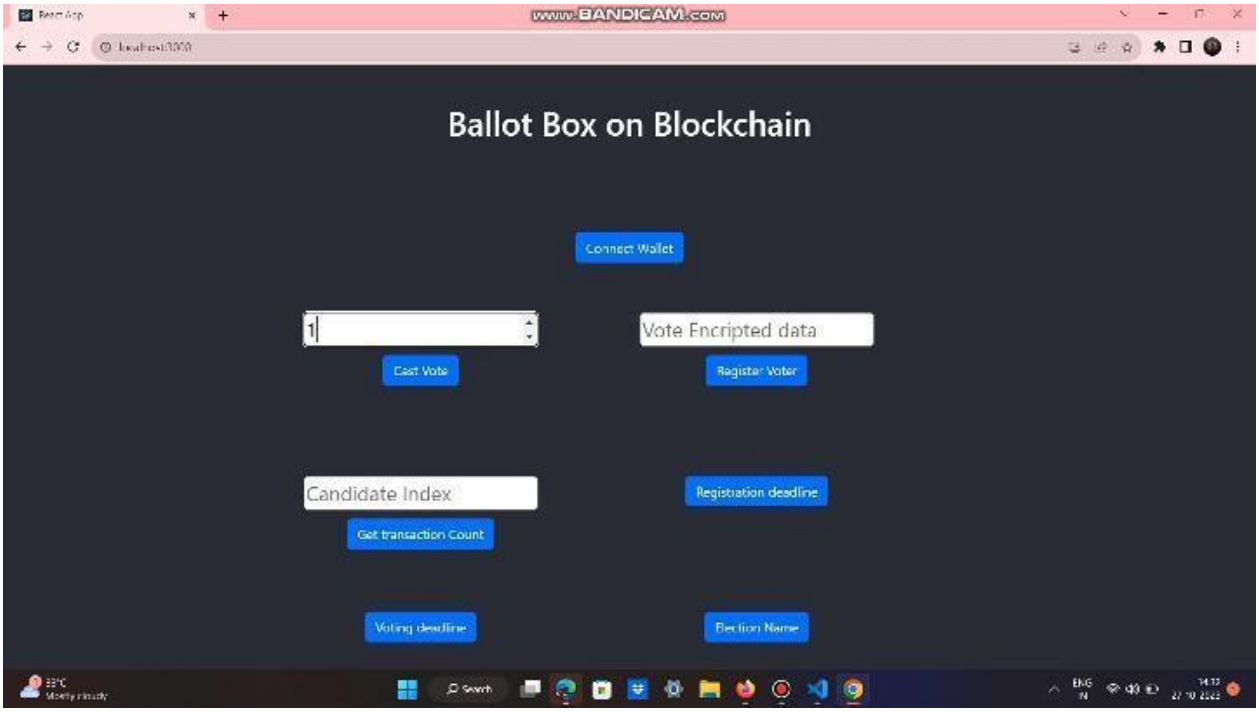
13. System Availability and Uptime: Ensure the system is available during voting hours with minimal downtime.

14. Privacy and Data Protection: Verify that the system complies with data protection regulations and safeguards voters' personal information.

15. Cost-Effectiveness: Assess the cost of implementing and maintaining the biometric security system compared to its benefits.

9. RESULTS

9.1. Output Screenshots



10. ADVANTAGES & DISADVANTAGES

10.1. Advantages of using biometric security in a voting platform:

1. Enhanced Security: Biometrics, such as fingerprint or iris scans, offer a high level of security, reducing the risk of fraudulent voting.

2. Voter Authentication: Biometrics can accurately verify a voter's identity, ensuring that only eligible individuals cast their votes.

3. Reduced Fraud: Biometric systems can help prevent impersonation and multiple voting, improving the overall integrity of the election process.

4. Accessibility: Biometrics can make voting more accessible for individuals with disabilities, as they may find it easier than traditional methods like paper ballots.

10.2. Disadvantages of using biometric security in a voting platform:

1. Privacy Concerns: Storing biometric data can raise privacy issues, and there's a risk of misuse or breaches that could expose sensitive information.

2. Cost: Implementing biometric technology can be expensive, and some regions may not have the resources to adopt it.

3. Technical Challenges: Biometric systems may not work flawlessly for everyone, and technical issues or false rejections can disenfranchise eligible voters.

4. Inclusivity: Biometric systems may not be suitable for all voters, including those with certain medical conditions or disabilities, potentially excluding them from the process.

5. Ethical Concerns: There are ethical debates about the use of biometrics in voting, as it can raise questions about government surveillance and individual freedoms.

Incorporating biometrics into a voting platform requires careful consideration of these advantages and disadvantages to balance security and accessibility while safeguarding privacy and inclusivity.

11. CONCLUSION

In conclusion, implementing a biometric security system for a voting platform offers the potential to enhance the security and integrity of the electoral process. By utilizing biometric data such as fingerprints or facial recognition, it becomes significantly more challenging for unauthorized individuals to impersonate voters. However, while this technology can be a valuable tool in preventing fraud, it must be carefully designed and implemented to address privacy concerns, technical challenges, and potential biases. Moreover, it should be used in conjunction with other security measures to create a comprehensive and robust electoral system. Public trust and transparency in the development and deployment of such systems are crucial to ensuring the success of biometric security in voting platforms.

12. FUTURE SCOPE

The future scope for biometric security systems in voting platforms is promising. It offers several advantages such as increased security and accuracy. Here are some potential developments:

1. Enhanced Authentication: Biometric systems can continue to evolve with more advanced methods like facial recognition, iris scanning, or palm print recognition to ensure accurate identification.

2. Accessibility: Improving biometric technology to be accessible and user-friendly for all citizens, including those with disabilities, is crucial.

3. Blockchain Integration: Combining biometrics with blockchain technology can create a secure and tamper-proof voting system.

4. Mobile Voting: Developing secure mobile voting apps with biometric authentication can increase voter participation and accessibility.

5. Privacy Considerations: Addressing privacy concerns is vital, including data protection and consent for biometric data usage.

6. Continuous Improvement: Regularly updating and patching vulnerabilities in the biometric system to stay ahead of potential threats.

7. Research and Testing: Ongoing research and testing of biometric systems in real-world voting scenarios to refine and validate their effectiveness.

8. Legal Framework: Developing comprehensive legal frameworks and regulations to govern the use of biometrics in voting.

Overall, the future of biometric security in voting platforms depends on technological advancements, public trust, and regulatory support.

13. APPENDIX

13.1. Source Code

```
/ SPDX-License-Identifier: MIT
pragma solidity ^0.8.0;

contract BallotBox {
// Define the owner of the contract (election authority).
address public owner;

// Define the structure of a voter.
struct Voter {
bytes32 biometricData;  // Encrypted biometric data
bool hasVoted;          // Indicates if the voter has cast a vote
}

// Define the structure of a candidate.
struct Candidate {
string name;
uint256 voteCount;
}
```

```
// Define the election parameters.
string public electionName;
uint256 public registrationDeadline;
uint256 public votingDeadline;

// Store the list of candidates.
Candidate[] public candidates;

// Store the mapping of voters.
mapping(address => Voter) public voters;

// Event to announce when a vote is cast.
event VoteCast(address indexed voter, uint256 candidateIndex);

// Modifiers for access control.
modifier onlyOwner() {
require(msg.sender == owner, "Only the owner can call this function.");
_;
}

modifier canVote() {
require(block.timestamp < votingDeadline, "Voting has ended.");
require(block.timestamp < registrationDeadline, "Registration has ended.");
require(!voters[msg.sender].hasVoted, "You have already voted.");
_;
}

// Constructor to initialize the contract.
constructor(
string memory _electionName,
```

```
uint256 _registrationDeadline,
uint256 _votingDeadline,
string[] memory _candidateNames
) {
owner = msg.sender;
electionName = _electionName;
registrationDeadline = _registrationDeadline;
votingDeadline = _votingDeadline;

// Initialize the list of candidates.
for (uint256 i = 0; i < _candidateNames.length; i++) {
candidates.push(Candidate({
name: _candidateNames[i],
voteCount: 0
}));
}
}

// Function to register a voter and store their encrypted biometric data.
function registerVoter(bytes32 _encryptedBiometricData) public canVote {
voters[msg.sender] = Voter({
biometricData: _encryptedBiometricData,
hasVoted: false
});
}

// Function to cast a vote for a candidate.
function castVote(uint256 _candidateIndex) public canVote {
require(_candidateIndex < candidates.length, "Invalid candidate index.");
require(voters[msg.sender].biometricData != 0, "You must register first.");
```

```
// Mark the voter as having voted.
voters[msg.sender].hasVoted = true;

// Increment the candidate's vote count.
candidates[_candidateIndex].voteCount++;

// Emit a VoteCast event.
emit VoteCast(msg.sender, _candidateIndex);
}
}
```

13.2. GitHub & Project Demo Link

GitHub link:

https://github.com/Waashim/bio-voting.git

Project demo link:

https://drive.google.com/drive/folders/1SLJJpyNJiPd2OfCrpprkzn-wzrVPd6St?usp=sharing