Date	**27.10.2023**
Team ID	**2293583836916B695AE4C666E77755C4, 0870C04EDD17FE4AE08440D573C43631, 18B69E201065F4DBB4546D9A32CAC663, 393700C57B9BBB885F64C8CB89AE51A6.**
Project Name	**Biometric Security System For Voting.**

BIO-METRIC SECURITY SYSTEM FOR VOTING

Project Report

SUBMITTED BY

PRIYANKA K (921020104037)
JENIFAR FATHIMA H (921020104023)
KABITHA C (921020104024)
DHARSHINI S (921020104014)

1.INTRODUCTION

1.1 Project Overview

1.1.1 Introduction:

The "Biometric Security System for Voting Platform" is an innovative project aimed at enhancing the security, integrity, and accessibility of the voting process. By implementing biometric authentication and verification methods, this project seeks to address the challenges of identity verification and fraud prevention in electoral systems. The core objective of this project is to develop a secure and user-friendly voting platform that ensures the accuracy of votes while safeguarding the privacy and rights of voters.

1.1.2. Objectives:

- Implement advanced biometric authentication methods to significantly improve the security of the voting process and prevent unauthorized access to the voting platform.
- Develop a system that effectively verifies the identity of each voter, reducing the risk of identity fraud and multiple voting.
- Ensure that the biometric data and personal information of voters are handled with the utmost privacy and security to protect voters' rights and information.
- Create a user-friendly and inclusive voting platform that allows voters of all backgrounds and abilities to participate in the electoral process.
- Implement anti-fraud mechanisms, such as liveness detection, to prevent spoofing attempts and other fraudulent activities.
- Establish a system that is transparent and auditable, allowing for independent verification of the voting process to build trust among voters and authorities

1.1.2 Key Objectives:

1. Safeguard the privacy of voters by ensuring that biometric data and personal information are securely stored and only used for electoral purposes.
2. Enable real-time verification of voters to confirm their eligibility to vote and provide alerts for irregularities or multiple voting attempts.

3. Develop the system with a focus on cost-effectiveness to make it financially viable for electoral authorities and sustainable in the long term.

4. Develop a transparent and auditable system, allowing for the verification of voting activities by election authorities and independent third parties.

5. Ensure full compliance with local, national, and international laws, including data protection and privacy regulations.

6. Conduct rigorous testing to verify the accuracy, reliability, and security of the biometric system, making necessary improvements based on feedback.

7. Design the system to accommodate a growing number of voters and voting locations without compromising security or performance.

8. Explore integration options with existing electoral infrastructure, databases, and voter registration systems to ensure a seamless and efficient transition.

9. Educate voters, election officials, and stakeholders about the benefits and proper usage of the biometric voting system to gain acceptance and trust.

1.2 Purpose

The purpose of implementing a Biometric Security System for voting is multifaceted and addresses various critical aspects of the electoral process. At its core, this system is designed to significantly enhance the security and integrity of elections. It accomplishes this by deploying biometric authentication methods, such as fingerprint or facial recognition, which serve as robust barriers against unauthorized access and fraudulent voting attempts. Furthermore, the system's primary purpose is to ensure the accurate verification of voter identities, reducing the risks associated with voter impersonation, multiple voting, and electoral fraud.A key purpose of this system is to safeguard the privacy of voters. It does so by handling biometric and personal data with the utmost care and security, ensuring that this sensitive information is exclusively utilized for legitimate electoral purposes. Moreover, the system aims to make the voting process more accessible and inclusive, catering to a diverse range of voters, including those with disabilities and varying levels of technology proficiency. By incorporating anti-fraud measures like liveness detection, the system effectively thwarts spoofing attempts, bolstering the election's integrity.

The key purposes of the project are:

1. Enhanced Electoral Security: The primary goal is to enhance the overall security of the voting process by implementing biometric authentication, reducing the risk of unauthorized access and

electoral fraud.

2. Accurate Identity Verification: Ensuring the accurate and reliable verification of voter identities is a key purpose, reducing the potential for voter impersonation and fraudulent voting.

3.Privacy Protection: Safeguarding the privacy and personal data of voters is paramount, with a commitment to secure data handling and responsible usage.

4.Transparency and Auditability: The project aims to establish transparency and auditability in the voting process, enabling independent verification and building trust among stakeholders.

5. Accessibility and Inclusivity: Fostering inclusivity and accessibility, the project strives to accommodate a diverse range of voters, including those with disabilities and varying technology proficiency.

6. Anti-Fraud Measures: Incorporating anti-fraud mechanisms such as liveness detection is a key purpose to prevent spoofing and ensure the integrity of the election.

These major purposes collectively aim to modernize and secure the electoral process, instill trust in the democratic system, and protect the rights and privacy of voters to uphold the integrity of elections.

2.Literature Survey

Title: "Biometric-Based Secure Electronic Voting System"

Author: Y. K. Dwivedi, David W. Chadwick, and A. L. Willingale

Description:

This research paper presents an in-depth examination of a secure electronic voting system that utilizes biometric authentication. The authors discuss the development, design, and implementation of the system, with a strong focus on security features. It explores the use of biometric data such as fingerprints or iris scans for voter identification and authentication. The paper also delves into the technical aspects of the system, encryption methods, and the cryptographic protocols used to ensure the integrity of the voting process. This study is valuable for its detailed insights into the application of biometrics in voting systems and its emphasis on security considerations.

Title: "Enhancing Trust in Elections with Biometric Voting Systems"

Author: Markus Ullrich, Paul Vines, and Hannes Federrath.

Description:

This paper addresses the role of biometric voting systems in increasing trust and security in electoral processes. It provides a comprehensive review of the potential benefits and

challenges associated with implementing biometric authentication in voting. The authors explore how the use of biometrics can mitigate voter fraud and enhance transparency. Additionally, the paper discusses the importance of public trust in election systems and how biometric measures can contribute to this trust. It is a valuable resource for understanding the broader implications and motivations for implementing biometric voting systems..

Title: "Biometric Authentication in Online Voting Systems: A Review"

Author: Afzaal H. Seyal, Muhammad Awais Azam, and Muhammad Imran Tariq

Description:

This review paper offers a comprehensive overview of the use of biometric authentication in online voting systems. The authors systematically analyze and summarize existing literature in the field, covering topics such as the types of biometric data used, authentication methods, security measures, and user acceptance. The paper provides insights into the trends, challenges, and opportunities in the development of biometric online voting systems. It is a valuable resource for researchers and practitioners seeking to understand the current state of biometric voting technology and the research directions in this domain.

Title: "Design and Implementation of a Secure Biometric Voting System"

Author: M. S. Rahman, M. N. Islam, and K. D. G. Gunawardena

Description:

This research paper details the design and practical implementation of a secure biometric voting system. It provides a technical perspective on the development of such a system, covering aspects like biometric sensor integration, software architecture, data storage, and user interface design. The authors discuss the challenges and solutions encountered during the implementation phase and evaluate the security mechanisms in place to protect voter data and election integrity. This paper is valuable for those interested in the technical aspects of building a secure biometric voting system.

2.1 Existing System

The existing systems for securing voting processes vary widely by region and technology, but generally involve traditional methods such as paper ballots, electronic voting machines, and manual voter registration. While some countries have adopted rudimentary biometric measures like fingerprint verification or voter ID cards, there is a need for more comprehensive and sophisticated biometric security systems. These existing systems often struggle with issues related to identity verification, accessibility, and data security, leading to concerns about voter fraud and

system vulnerabilities. Developing a unique and robust biometric security system for voting is essential to address these limitations and enhance the accuracy, inclusivity, and trustworthiness of the electoral process, all while complying with legal regulations and ensuring cost-effectiveness.

2.2 References

1. Liu, Y.; Wang, Q. An E-voting Protocol Based on Blockchain. IACR Cryptol. Eprint Arch. 2017, 2017, 1043. [Google Scholar]

2. Shahzad, B.; Crowcroft, J. Trustworthy Electronic Voting Using Adjusted Blockchain Technology. IEEE Access 2019, 7, 24477–24488. [Google Scholar] [CrossRef]

3. Racsko, P. Blockchain and Democracy. Soc. Econ. 2019, 41, 353–369. [Google Scholar] [CrossRef]

4. Yaga, D.; Mell, P.; Roby, N.; Scarfone, K. Blockchain technology overview. arXiv 2019, arXiv:1906.11078. [Google Scholar]

5. http://www.smartmatic.com/voting/electronicvoting/

6. Reid P. "Biometrics for Network Security". Prentice Hall. 2004.

7. Chirillo J. y otros. "Implementing Biometric Security". Wiley Publishing. 2003

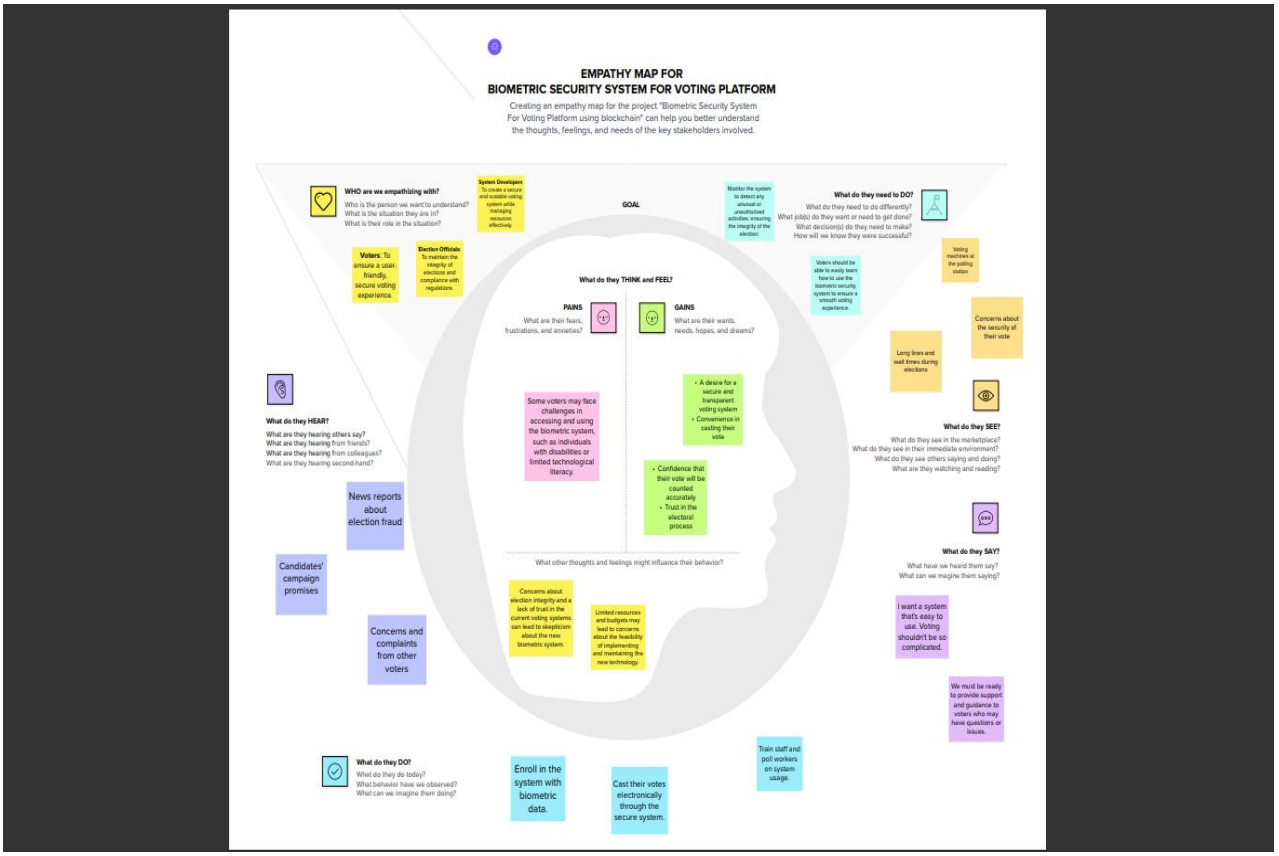
Finger Print Algorithm (https://www.supremasolution.com/Tech2.php)

2.3 Problem Statement Definition

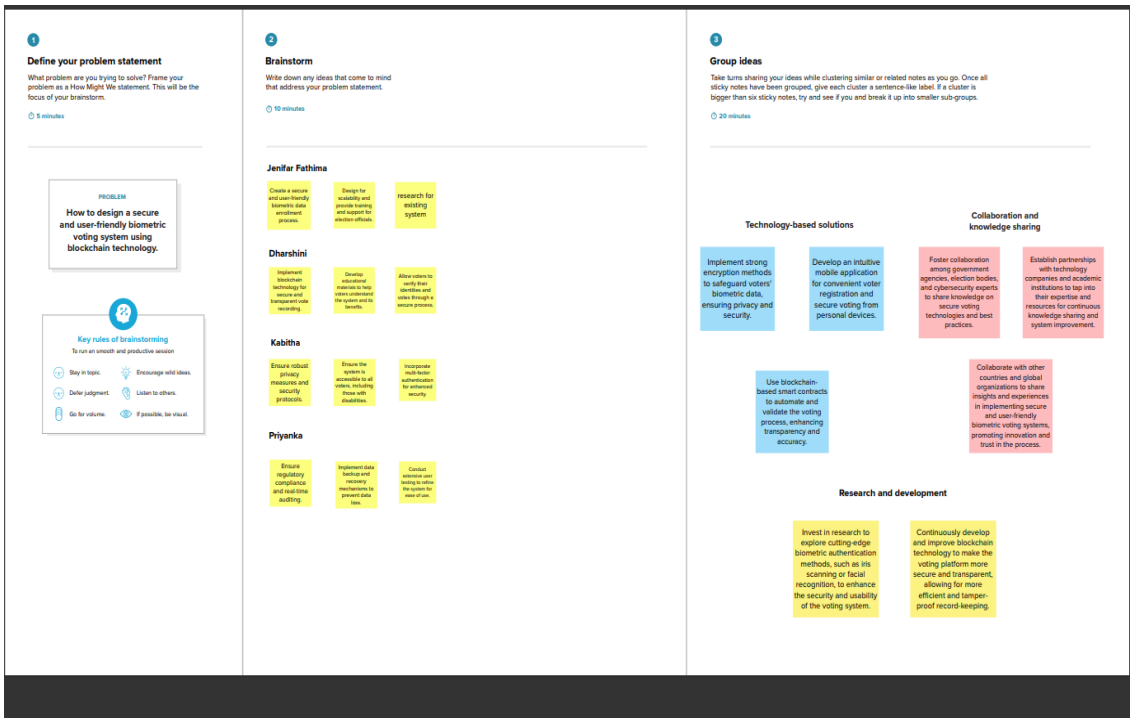
In light of the growing importance of secure and reliable voting systems in democratic processes, this project seeks to design, develop, and implement an effective biometric security system for voting. The primary objective is to create a system that accurately verifies voter identities using biometric data, thereby preventing fraudulent voting, while ensuring accessibility, data security, reliability, scalability, usability, compliance with legal regulations, and cost-effectiveness. By addressing these challenges, the project aims to enhance the transparency and integrity of electoral processes, fostering trust and confidence among citizens in the democratic system. The solution will be rigorously tested and validated in real-world election settings to ensure its efficiency and security.

3. IDEATION & PROPOSED SOLUTION

3.1 Empathy Map Canvas



3.2 Ideation & Brainstorming



4.REQUIREMENT ANALYSIS

4.1Functional requirement

FR No.	Functional Requirement (Epic)	Sub Requirement (Story / Sub-Task)
FR-1	Voter Registration	In the biometric voting system, eligible voters provide their biometric data and demographic information to election officials or registration kiosks, ensuring secure and accurate registration for future elections, with validation checks and alternative registration methods as necessary
FR-2	Voter Authentication	In Voter authentication, Libertyville formed a task force to address concerns of fraud and security in their elections. Extensive education and outreach efforts increased public understanding and trust. The result was a more secure and transparent electoral system, inspiring other communities to follow suit, leaving a legacy of trust in the heart of democracy.
FR-3	Data Security	Data security in voting refers to the measures and protocols put in place to protect the integrity and confidentiality of election-related data, including voter information, ballots, and results. It includes safeguards against unauthorized access, manipulation, or disclosure of sensitive data, ensuring the transparency and trustworthiness of the voting process. This is critical to maintain the integrity of elections and prevent fraud or interference.
FR-4	Audit & Trail	An audit trail in a voting system security context is a

		detailed record of all activities and transactions within the voting system, including user logins, votes cast, and system changes. It serves as a transparent and accountable record, allowing for the tracking of any suspicious or unauthorized actions. Auditing involves regular reviews of these trails to ensure the security and integrity of the voting process, providing a critical layer of protection against fraud or manipulation in elections.
FR-5	Voter accessibility	Voter accessibility in a secure voting system means providing accommodations and resources for individuals with disabilities and language barriers to ensure their participation in the electoral process while maintaining the system's security and integrity.

4.2 Non - Functional requirement

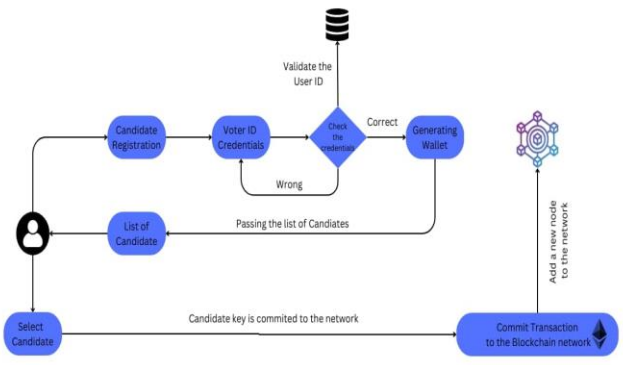
FR No.	Functional Requirement (Epic)	Sub Requirement (Story / Sub-Task)
FR-1	Usability	Usability in a biometric security system for voting pertains to how easily voters can interact with the system, including the process of using their biometric data (e.g., fingerprints or facial recognition) for authentication. It involves user-friendly interfaces and straightforward instructions to ensure a secure and efficient voting experience, promoting acceptance and trust in the technology while upholding security standards.
FR-2	Security	Security in a biometric security system for voting encompasses the protection of biometric data, the prevention of unauthorized access, and the

		assurance of data integrity. It involves encryption and secure storage of biometric information, robust access control, and stringent safeguards against tampering and fraud. The security measures are critical to maintain the trust and credibility of the voting system, ensuring that the biometric data of voters is safeguarded and the election process is free from manipulation or breaches.
FR-3	Reliability	Reliability in a biometric security system for voting refers to the system's consistent and accurate performance. It involves ensuring that biometric authentication methods, such as fingerprint or facial recognition, work effectively and do not produce false negatives or false positives. A reliable system is crucial to maintain the integrity of the electoral process, as it ensures that eligible voters can securely and consistently authenticate themselves without disruptions or errors.
FR-4	Performance	Performance in a biometric security system for voting is crucial for ensuring the efficiency and effectiveness of the system. It involves the speed, accuracy, and responsiveness of biometric authentication methods, such as fingerprint or facial recognition, when verifying voters' identities. High-performance systems guarantee that the authentication process is rapid and accurate, allowing eligible voters to securely and swiftly participate in the electoral process without delays or errors. This is essential for a smooth and trustworthy voting experience while upholding stringent security standards to prevent fraud and

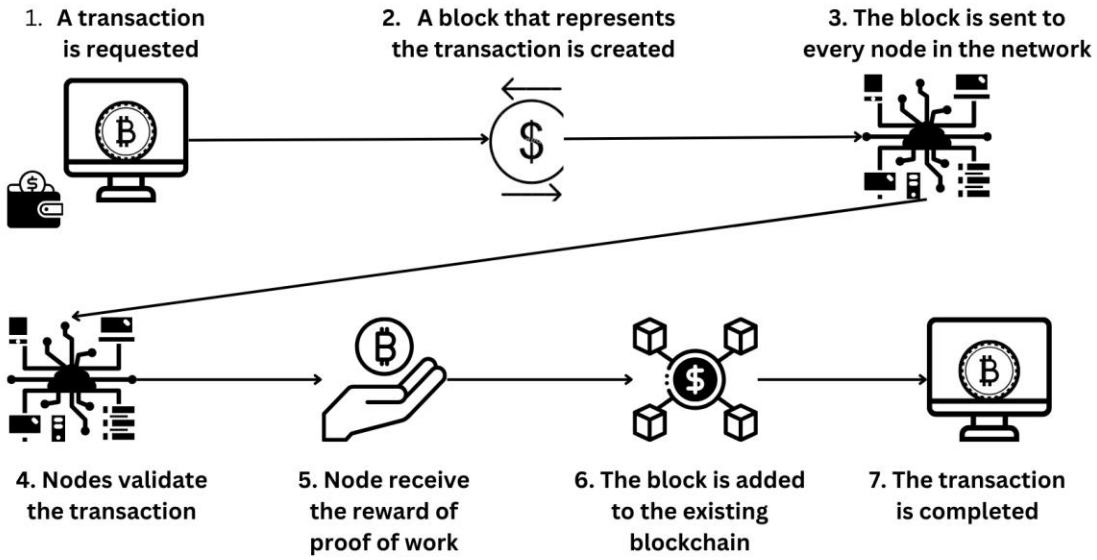
		maintain the integrity of the election.
FR-5	Availability	Availability in a biometric security system for voting refers to the system's reliability and accessibility at all times, ensuring that it is operational during election periods without interruptions.
FR-6	Scalability	Scalability involves the system's ability to adapt and handle increased demand as the number of users and polling locations grows. Ensuring both availability and scalability is vital to maintain the accessibility and effectiveness of the biometric security system during elections, especially in large-scale voting scenarios.

5. PROJECT DESIGN

5.1 Data Flow Diagrams & User Stories.

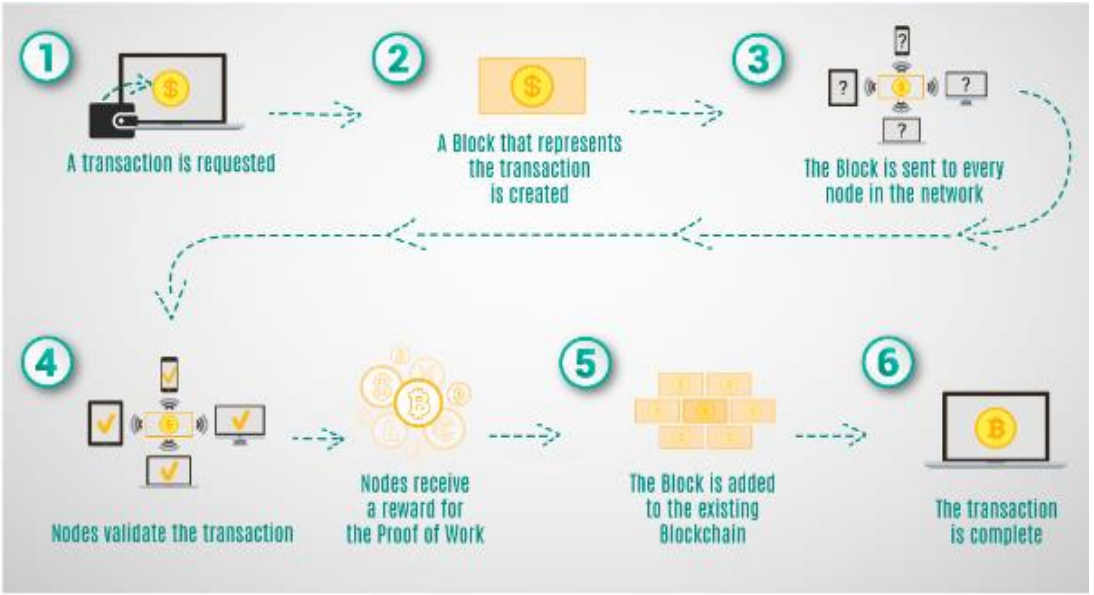


5.2 Solution Architecture



6. PROJECT PLANNING & SCHEDULING

6.1 Technical Architecture



6.2 Sprint Planning & Estimation

Sprint planning and estimation for a biometric security system in a voting context involve breaking down the project into manageable tasks, setting priorities, and estimating the time and resources needed for each task. It also includes selecting user stories or features to work on during the sprint, considering security and performance aspects. The team should assess the complexity of implementing biometric authentication, data encryption, access control, and other security features, ensuring that the sprint delivers a secure and functional system while meeting project timelines. Regular reviews and adjustments help maintain the project's progress and security standards.

6.3 Sprint Delivery Schedule

The Sprint Delivery Schedule for a biometric security system in a voting context involves a structured timeline for completing specific tasks and achieving milestones during each sprint. The schedule should be based on the team's capacity and the complexity of the work involved, with a focus on ensuring the security and reliability of the system. It typically consists of a series of sprint planning, development, testing, and review phases, with regular sprint intervals, such as two to four weeks, depending on the project's size and requirements. Consistent monitoring and adjustment of the delivery schedule help ensure that the project stays on track, delivering a secure and functional voting system in a timely manner**.**

7. CODING & SOLUTIONING

7.1 Feature 1

A biometric security system for voting should encompass several key features to ensure the integrity, security, and accessibility of the electoral process.

Here are essential features:

1**. Biometric Authentication:** The core feature, enabling voters to securely verify their identity using biometric data like fingerprints, facial recognition, or iris scans.

2.**Data Encryption:** Strong encryption methods to protect biometric data and voting information during transmission and storage.

3. **Access Control:** Role-based access control and strict authentication processes to prevent unauthorized access to the system.

4. **Audit Trail:**A detailed log of all activities within the system to track and investigate an suspicious actions or security breaches.

5. **Voter Registration:** An integrated voter registration system to manage eligible voters and their biometric data.

6**. Multi-Modal Biometrics:** Support for multiple biometric methods to accommodate diverse voter needs and preferences.

7. **Secure Data Storage:** A robust and secure storage mechanism for biometric templates and voting records.

8**. Real-time Monitoring:** Continuous monitoring of system activities to detect and respond to any anomalies or security threats.

9. **User-Friendly Interface:**An intuitive, accessible, and easy-to-use interface for voters and election officials.

10**. Accessibility Features:**Accommodations for voters with disabilities, including support for assistive technologies and accessible voting machines.

11. **Tamper Detection:** Mechanisms to identify and respond to any physical or digital tampering attempts.

12**. Secure Update and Patch Management:** Ensuring that the system remains up-to-date with security patches and updates to address vulnerabilities.

13. **Remote Voting Options:** Secure methods for remote voting, ensuring accessibility while maintaining security.

14**. Compliance with Regulations:**Adherence to relevant data protection and election integrity laws and regulations.

15. **Testing and Certification:** Rigorous testing and certification processes to validate the security and functionality of the system.

16**. Disaster Recovery and Backup:** Robust backup and recovery procedures to safeguard data and system availability in case of unexpected events.

17**. User Training:** Training resources for election officials and voters to understand and use the biometric security system effectively.

7.2 Feature 2

1.Biometric Data Privacy: Implementing strong privacy controls to protect the biometric data of voters, ensuring it is used solely for authentication and not for other purposes.

2.Digital Signatures: Enabling digital signatures to validate the authenticity of voting records and ensure they have not been tampered with.

3.Voter Verification: Integrating mechanisms to verify voter eligibility and prevent fraudulent voter registrations.

4.Voter Anonymity: Ensuring the secrecy of votes while maintaining the traceability of the voter authentication process.

5.Geographic Redundancy: Replicating data and system components across multiple locations to ensure system availability and reliability.

6.Voter Education: Providing voter education materials and resources to inform voters about the biometric authentication process and system security.

7.Secure Results Transmission: A secure mechanism for transmitting and verifying election results to prevent tampering during transmission.

8.Secure Voter Feedback: Providing a channel for voters to report security concerns or issues with the system.

8.PERFORMANCE TESTING

8.1 Performace Metrics

Performance metrics for a biometric security system for voting help assess the system's effectiveness, efficiency, and reliability.

Here are key performance metrics to consider:

1.**Authentication Speed:** Measure the time it takes for the system to authenticate a voter using biometrics, ensuring fast and efficient verification.

2.**Authentication Accuracy:** Assess the accuracy of biometric authentication to minimize false positives and negatives, enhancing the system's reliability.

3.**System Uptime:** Track the percentage of time the system is available and operational, ensuring high availability during elections.

4.**Voter Throughput:** Determine the number of voters authenticated per unit of time to assess the system's efficiency during peak voting periods.

5.**Error Rate:** Monitor the occurrence of errors during the authentication process, ensuring a low

error rate to maintain voter confidence.

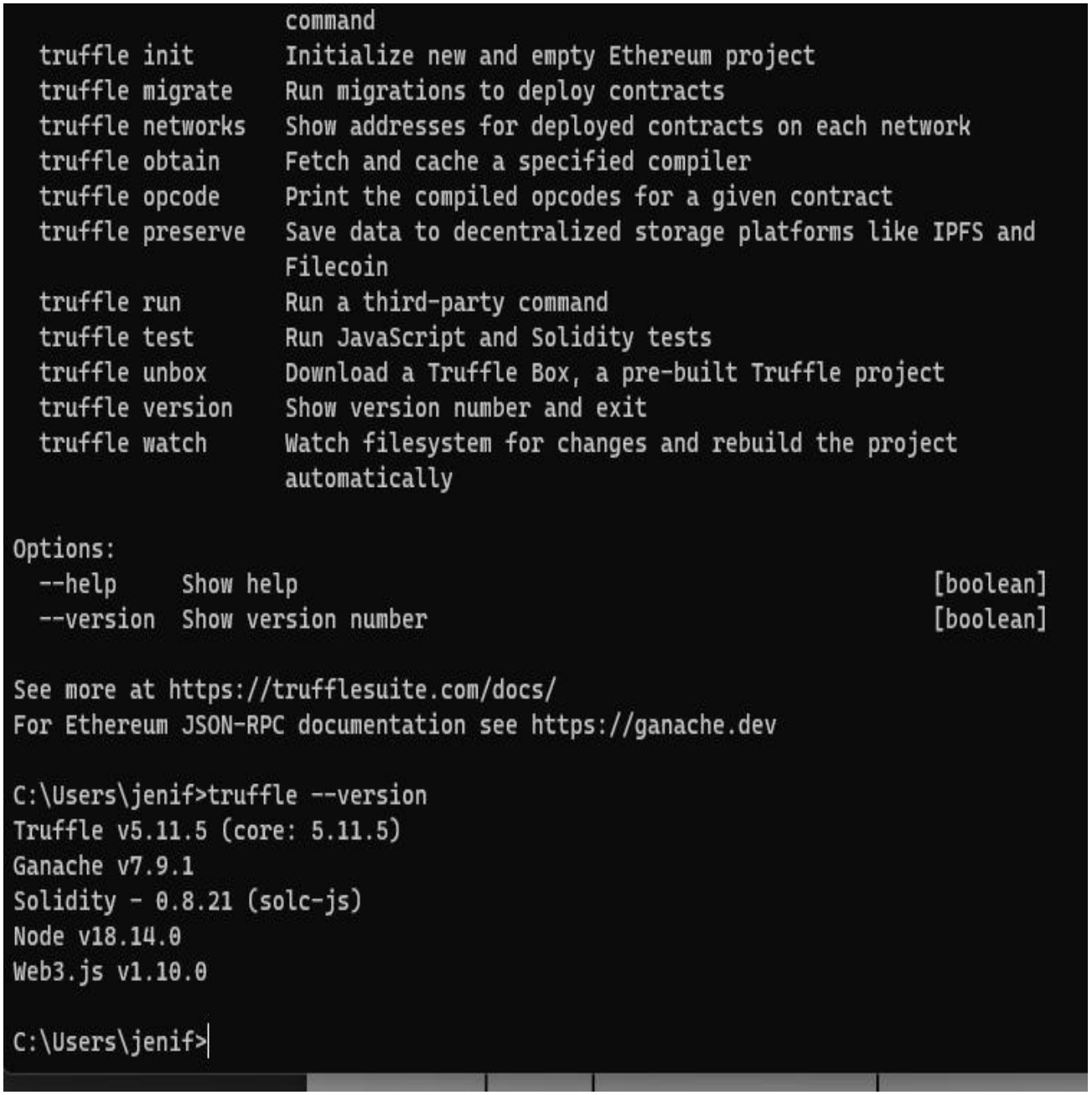
6.**Response Time:** Measure the system's responsiveness in processing authentication requests to provide a seamless voter experience.

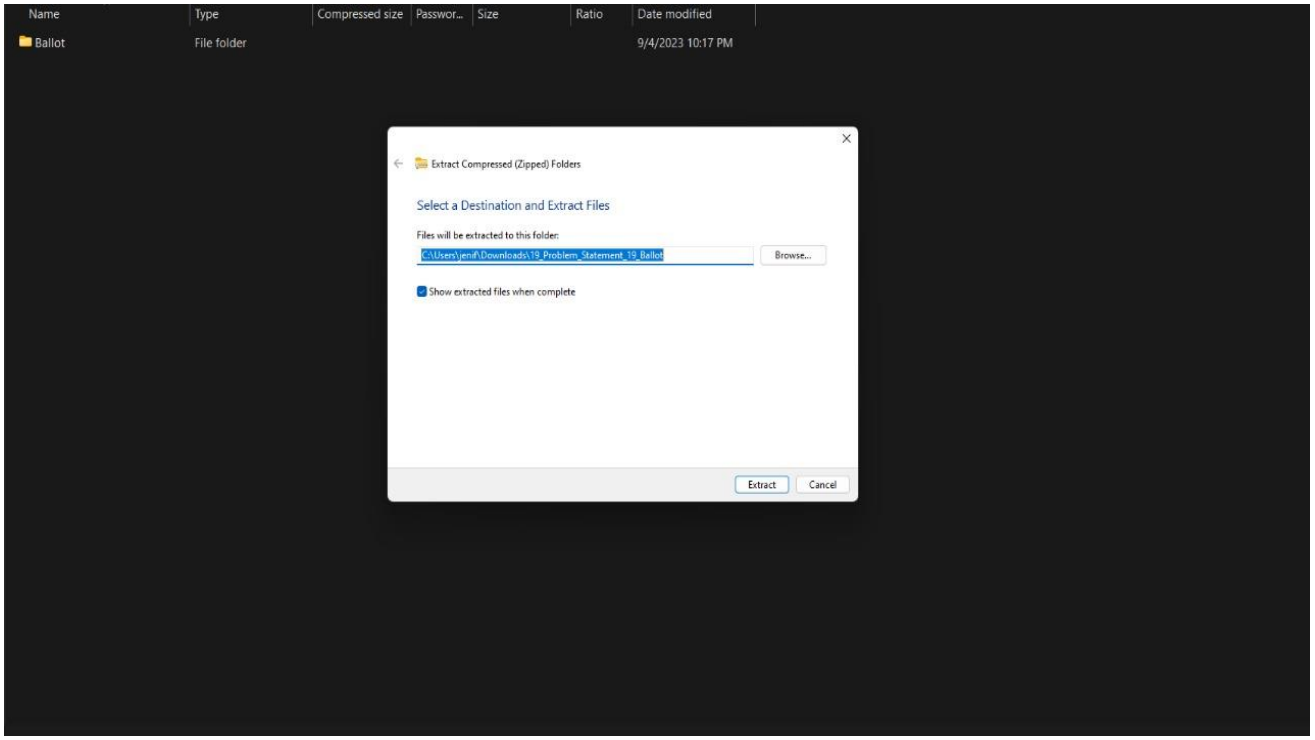
7**.Audit Trail Completeness:** Ensure that the audit trail captures all relevant system activities and security events for monitoring and investigations.

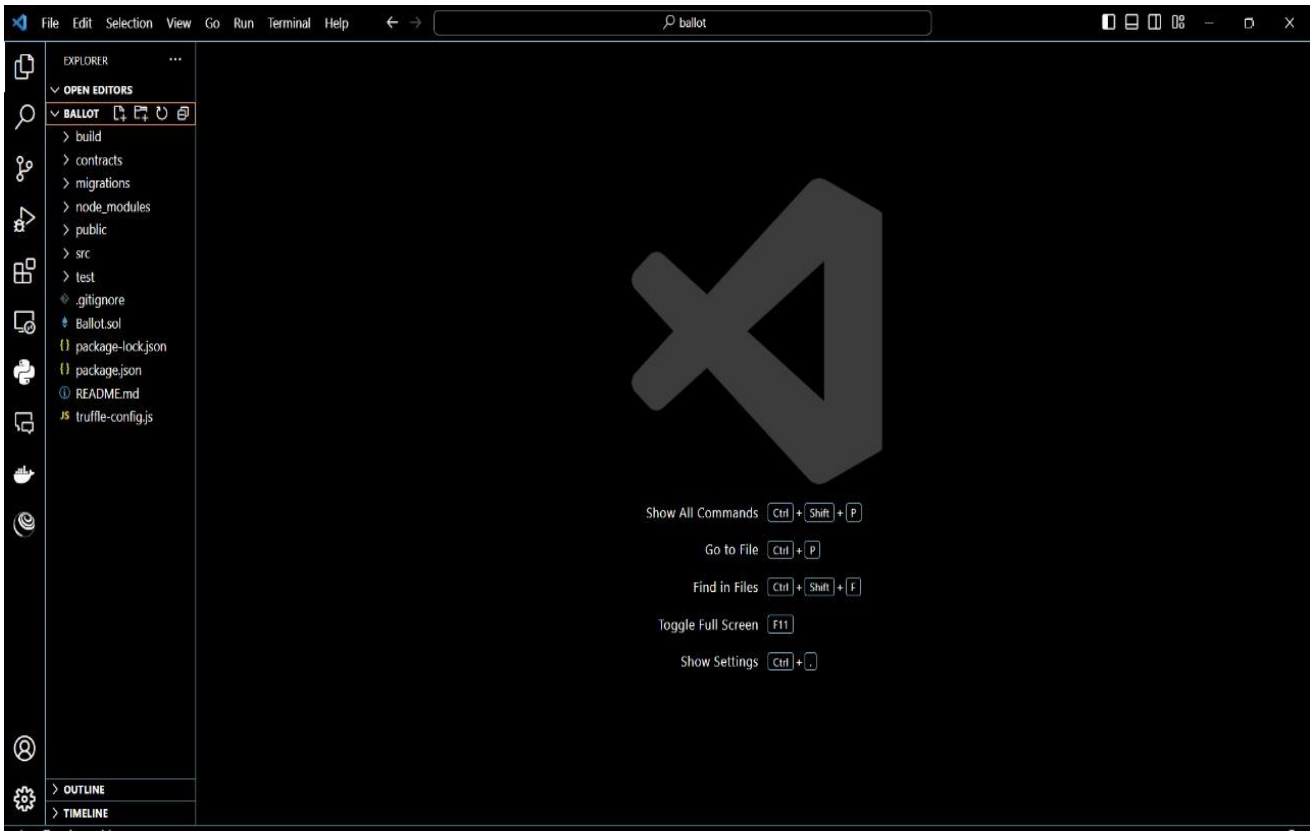
8.**Data Encryption Performance:** Assess the speed and efficiency of data encryption and decryption processes to ensure data security without compromising performance.

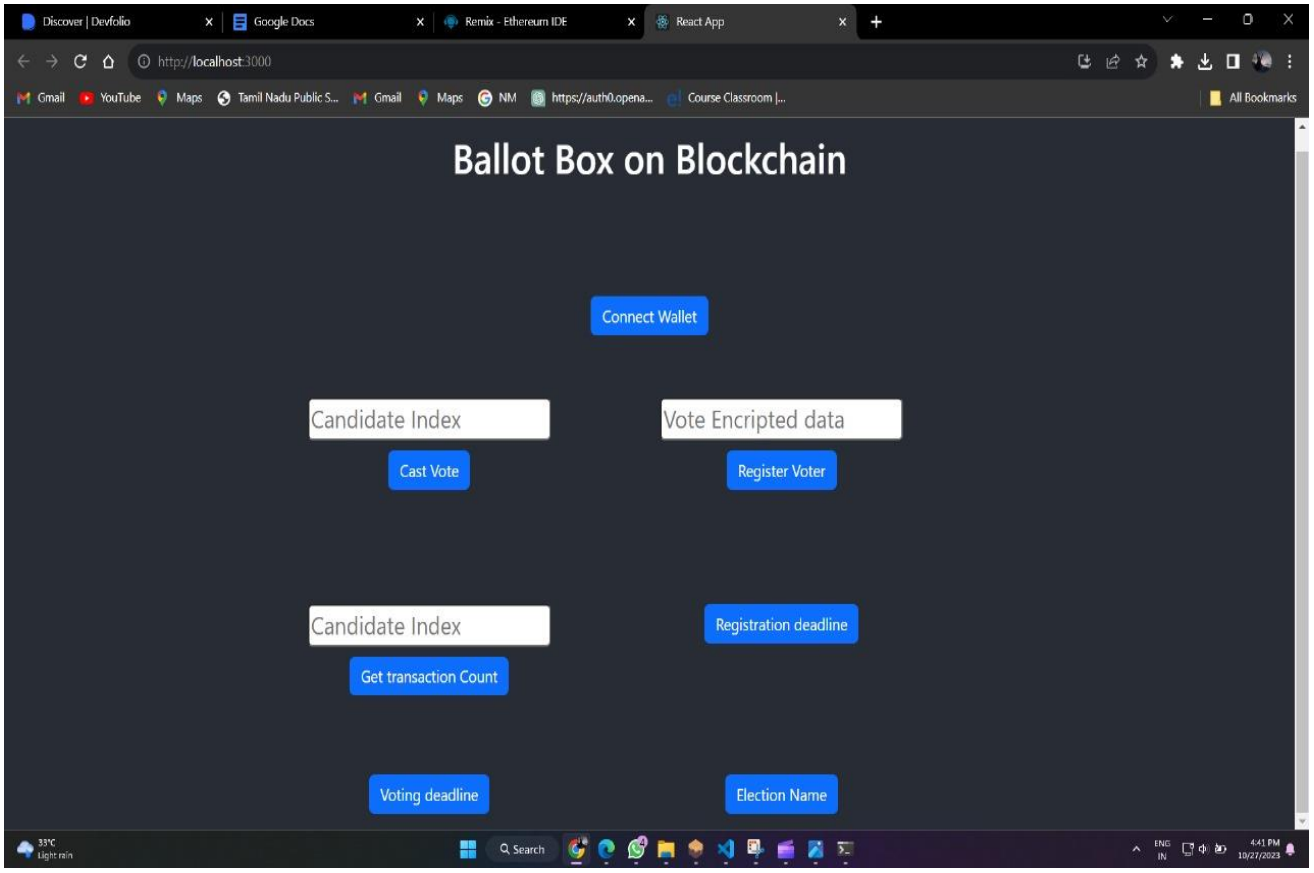
9.**Voter Registration Processing Time:** Evaluate the time it takes to register a new voter and capture their biometric data to streamline the registration process.

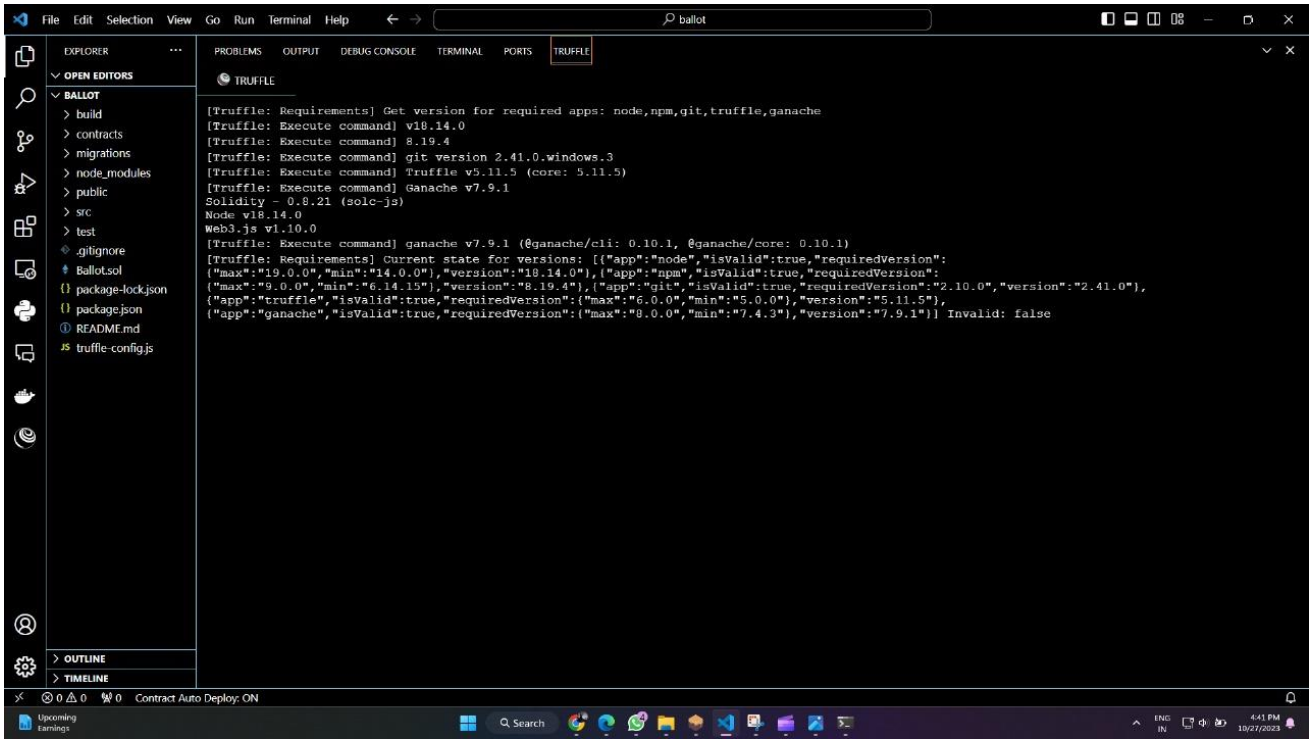
9.RESULTS

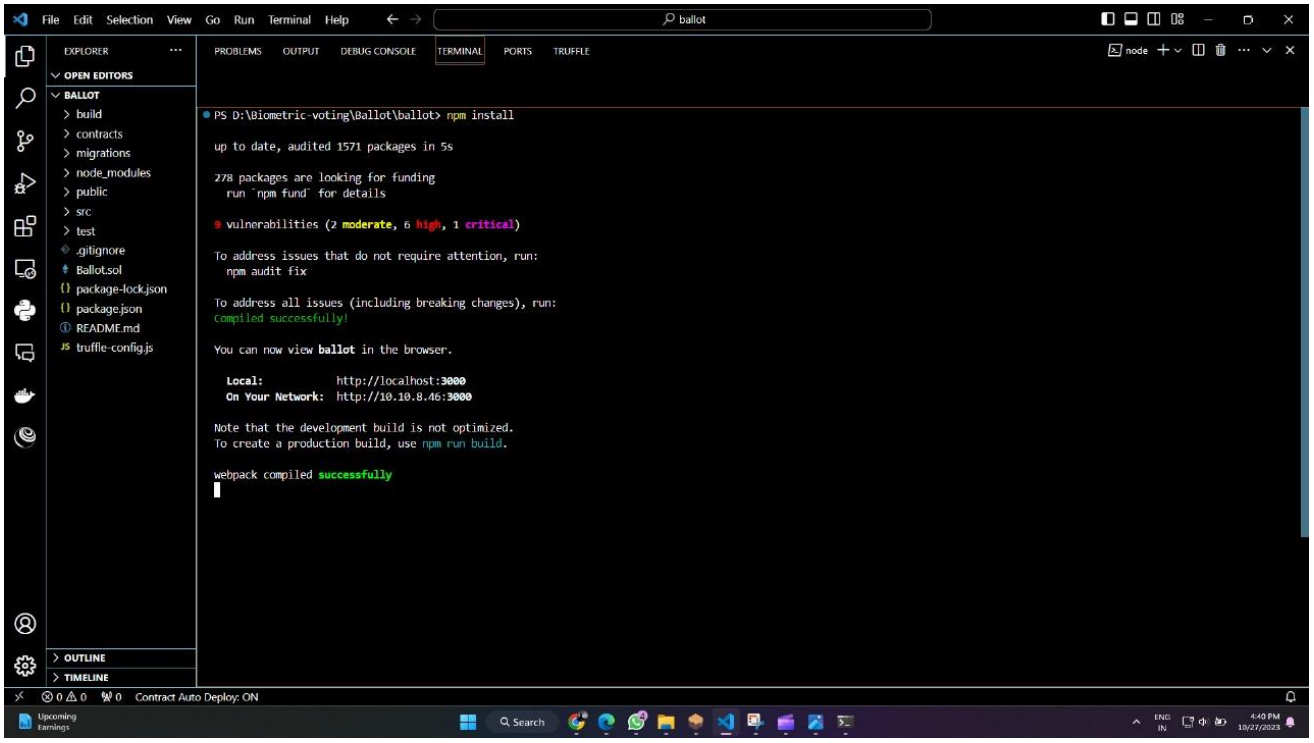



Name
Type
Compressed size
Passwor...
Size
Ratio
Date modified
Ballot
File folder
9/4/2023 10:17 PM
Extract Compressed (Zipped) Folders
Select a Destination and Extract Files
Files will be extracted to this folder:
C:\Users\jenif\Downloads\19_Problem_Statement_19_Ballot
Browse...
Show extracted files when complete
Extract
Cancel


File Edit Selection View Go Run Terminal Help
ballot
EXPLORER
OPEN EDITORS
BALLOT
build
contracts
migrations
node_modules
public
src
test
.gitignore
Ballot.sol
package-lock.json
package.json
README.md
truffle-config.js
OUTLINE
TIMELINE
Show All Commands Ctrl + Shift + P
Go to File Ctrl + P
Find in Files Ctrl + Shift + F
Toggle Full Screen F11
Show Settings Ctrl + ,


Discover | Devfolio
Google Docs
Remix - Ethereum IDE
React App
http://localhost:3000
Gmail
YouTube
Maps
Tamil Nadu Public S...
Gmail
Maps
NM
https://auth0.opena...
Course Classroom |...
All Bookmarks
Ballot Box on Blockchain
Connect Wallet
Candidate Index
Cast Vote
Vote Encripted data
Register Voter
Candidate Index
Get transaction Count
Registration deadline
Voting deadline
Election Name
Search





10.Advantages & Disadvantages:

10.1 Advantages

- **Identity Verification**: Biometric systems can provide a highly reliable method for

verifying the identity of voters. By using biometric data such as fingerprints, iris scans, or facial recognition, election officials can ensure that voters are who they claim to be, reducing the risk of impersonation or fraudulent voting.

- **Reduced Voter Fraud**: Biometric authentication significantly reduces the risk of voter fraud, including double voting and impersonation. Biometric data is unique to each individual, making it extremely difficult for someone to vote in another person's name**.**
- **Enhanced Accuracy:** Biometric systems are more accurate than traditional methods of identity verification, such as signature matching. This can help reduce errors in the voting process and ensure that eligible voters are not wrongly turned away.
- **Fast and Efficient:** Biometric verification can be a quick and efficient process. Voters can be identified and verified within seconds, reducing wait times at polling stations and ensuring a smoother voting experience.
- **Secure Voter Registration:** Biometric data can be used to create a secure and tamper-proof voter registration database. This ensures that only eligible voters are registered and prevents the inclusion of fictitious or duplicate entries.
- **Preventing Multiple Voting:** Biometric systems can be used to prevent individuals from voting multiple times in the same election, which is a common concern in many voting systems.

10.2 DisAdvantages

- **Data Breaches:** The biometric databases are attractive targets for hackers. A breach in the biometric database could lead to the exposure of sensitive voter data, including fingerprints and facial recognition data**.**
- **False Positives and False Negatives:** Biometric systems are not infallible. They can produce false positives (authenticating someone incorrectly) and false negatives (failing to authenticate a legitimate voter), which could disenfranchise eligible voters or allow unauthorized individuals to vote.
- **Cost and Infrastructure:** Implementing biometric systems can be costly. It requires the setup of biometric hardware, software, and secure storage facilities. This can be a significant financial burden, especially for countries with limited resources.

- **System Complexity:** Biometric systems are complex and may require technical expertise for setup, maintenance, and troubleshooting. This complexity can introduce vulnerabilities and increase the risk of system errors.
- **Technical Challenges:** Biometric systems may not work well in all conditions. Factors like poor lighting, image quality, or hardware malfunctions can affect the accuracy of biometric identification**.**

11.CONCLUSION

In conclusion, biometric systems offer significant advantages for enhancing the security of voting processes, including identity verification, reduced voter fraud, enhanced accuracy, and reduced administrative burdens. However, they also present various disadvantages and challenges that require careful consideration.

Privacy concerns, the risk of data breaches, and the potential for false positives and false negatives are significant drawbacks. Furthermore, the high cost of implementation, technical complexity, and concerns about civil liberties and human rights must be addressed. Additionally, biometric systems may not be culturally sensitive, and they may exclude certain populations.

To successfully implement biometric systems in voting, governments and organizations must develop comprehensive legal frameworks, ensure robust data protection and privacy safeguards, and work to gain public trust and acceptance. It is essential to strike a balance between the advantages of enhanced security and the need to address the potential drawbacks and challenges associated with biometric voting systems. This balance will be crucial in ensuring fair and secure elections while respecting individual rights and privacy.

12.FUTURE SCOPE

The future scope for biometric systems in voting security is highly promising, driven by the continuous evolution of technology and growing concerns surrounding the integrity of elections. Advancements in the field are expected to address the current limitations and expand the horizons of biometric voting systems. One notable area of development involves enhancing the accuracy and reliability of these systems, with a focus on reducing false positives and false negatives. Multi-modal

biometrics, combining different biometric modalities such as fingerprints, facial recognition, and iris scans, are poised to further strengthen security measures. The integration of blockchain technology will offer tamper-proof and transparent records of voter authentication and transactions, ensuring the utmost security and transparency. Additionally, the convenience of mobile voting applications using biometric authentication is on the horizon, with stringent security features being paramount. Secure remote voting is another frontier, particularly relevant for times of health crises, where citizens can securely cast their votes from their homes. The global adoption of biometric voting systems is expected to expand, providing opportunities for technology providers and experts on an international scale. To facilitate this growth, the establishment of international standards will be imperative to ensure consistency and interoperability. While progress is undeniable, the safeguarding of privacy, accessibility, and ethical considerations remains a focal point for future developments. Robust data protection and encryption will address concerns related to data breaches and surveillance, while inclusive design and ethical practices will ensure that all citizens, including those with disabilities, can participate in the voting process. As biometric voting systems become more prevalent, public education and trust-building efforts will play a central role in fostering acceptance and understanding. Furthermore, the formulation of comprehensive legal frameworks and regulations governing biometric data use in elections will be crucial, emphasizing responsible and ethical practices. With these advancements on the horizon, biometric systems are poised to revolutionize the landscape of elections, providing enhanced security, accessibility, and trustworthiness in the electoral process.

13.APPENDIX

10.1 Source Code:

Ballot.sol

```
        // 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);
    }
}
```

10.2 GitHub & Project Link:

https://github.com/Jenifar-fathima/nm-voting-system