Biometric security system for voting platform Using Blockchain

A Project report submitted in partial fulfillment

of 7th semester indegree of BACHELOR OF

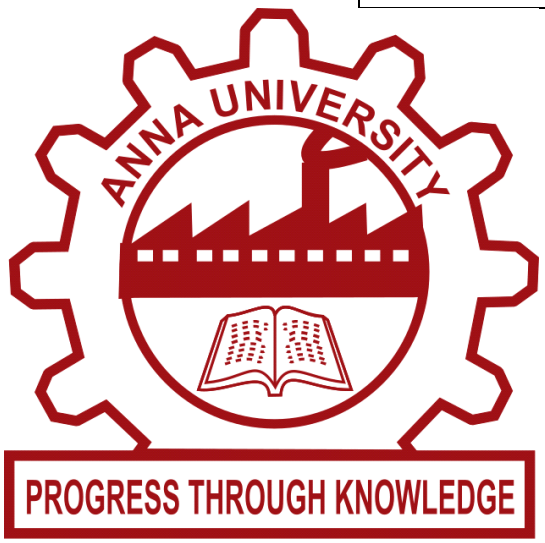
ENGINEERING IN ELECTRONICS AND

COMMUNICATION ENGINEERING

Team ID: NM2023TMID11949

Submitted by

C.Ashoki	812020106004
R.Haritha	812020106010
M.Prathish	812020106028
K.vasanthapriyan	812020106037



DEPARTMENT OF ELECTRONICS AND

COMMUNICATION ENGINEERING

M.A.M COLLEGE OF ENGINEERING AND TECHNOLOGY, TRICHY

ANNA UNIVERSITY: CHENNAI 600025

ABSTRACT

In an era where digital advancements are transforming traditional systems, the electoral process remains a critical aspect of democratic societies. This research endeavors to address the inherent challenges of security and transparency in voting platforms through the integration of biometric authentication and blockchain technology. By incorporating biometric features such as fingerprint or facial recognition, the proposed system aims to enhance the accuracy and reliability of voter identity verification.

The primary innovation lies in the synergy between biometrics and blockchain. Biometric data serves as a unique identifier for each voter, significantly reducing the risk of identity fraud. Simultaneously, blockchain technology provides a decentralized and immutable ledger to record each vote securely. This dual-layered approach ensures the integrity of the electoral process by creating a tamper-resistant and transparent record of votes cast.

The utilization of blockchain in the voting system offers several advantages. Firstly, it eliminates the risk of unauthorized access and man level of trust in the electoral Secondly, the decentralized nature of blockchain ensures that there is no single point of failure, enhancing the overall resilience of the voting platform against cyber threats.

Moreover, the proposed system prioritizes voter privacy by design. Biometric data is securely stored and only used for verification purposes, with no direct linkage to the cast vote. This safeguards the anonymity of voters while maintaining the accuracy of the authentication process.

The research explores the technical intricacies of implementing such a system, including the integration of biometric devices, the design of a secure blockchain infrastructure, and the development of user-friendly interfaces. Additionally, it examines potential challenges and proposes mitigation strategies to ensure the robustness of the proposed biometric security system.

In conclusion, the Biometric Security System for Voting Platforms Using Blockchain presents a comprehensive solution to enhance the security, transparency, and integrity of electoral processes. By leveraging biometric authentication and blockchain technology, this innovative approach seeks to redefine the standards of trust and reliability in modern voting systems.

TABLE OF CONTENTS

1.INTRODUCTION

- **Project Overview:**

Biometric security system for voting platform

The project involves implementing a biometric security system for a voting platform, integrating it with blockchain technology. Biometric data, such as fingerprints or facial recognition, would verify voter identity, enhancing security. The use of blockchain ensures a transparent, tamper-resistant, and decentralized voting process, mitigating potential fraud. Smart contracts could be employed to automate and secure various stages of the voting process, fostering trust in the electoral system.

1.2 Purpose

Biometrics can fulfil two distinct functions, authentication, and identification, as we said. Identification answers the question, "Who are you?". In this case, the person is identified as one, among others (1: N matching).

2. LITERATURE SURVEY

2.1 Existing problem

Biometric security systems for voting platforms face challenges such as potential vulnerabilities to hacking or spoofing, privacy concerns, and the need for robust infrastructure to ensure reliable authentication. Additionally, issues like data accuracy, system accessibility for all voters, and the cost of implementation contribute to the complexities of integrating biometrics into voting systems.

2.2References

1."Biometric Systems: Technology, Design and Performance Evaluation" by Nalini K. Ratha and Ruud M. Bolle.

2."Biometric Recognition: Challenges and Opportunities" by Anil K. Jain, Arun Ross, and Karthik Nandakumar.

2.3 Problem Statement Definition

"In contemporary voting systems, the need for enhanced security and authentication measures is imperative to ensure the integrity and confidentiality of the electoral process. Traditional methods face

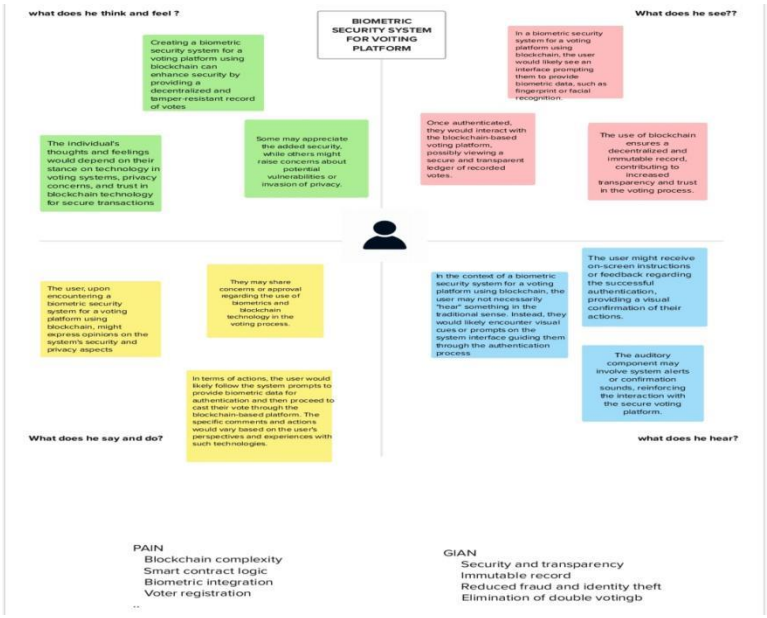
challenges related to identity verification and prevention of fraudulent activities. This project aims to address these concerns by implementing a biometric security system within the voting platform. The goal is to design and deploy a robust system that seamlessly integrates biometric data, such as fingerprints or facial recognition, to authenticate voters securely. This approach not only enhances the accuracy of voter identification but also mitigates risks associated with unauthorized access, ensuring a trustworthy and tamper-resistant electoral system."

3. IDEATION & PROPOSED SOLUTION

3.1 Empathy Map Canvas

User: Voter

Feels: Concerned about the security of their vote.
Thinks: Wants reassurance that their identity is protected.
Sees: Notices the integration of biometrics as a step towards modernizing the voting process.
Hears: Listens to information about the system's reliability and success in other elections.
Says: Expresses the importance of a secure and fair electoral process.
Does: Participates in the voting process with an expectation of increased security.
This empathy map outlines the emotional and rational aspects that a voter might experience in the context of using a biometric security system for a voting platform.



3.2 Ideation and Brainstorming

A group problem-solving technique that involves the spontaneous contribution of ideas from all members of the group.

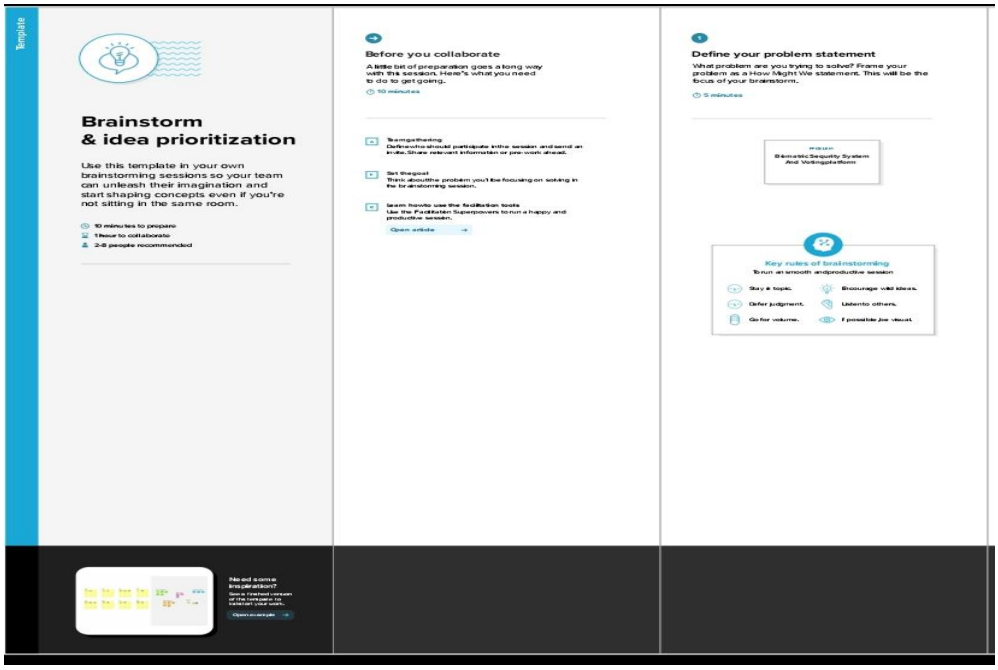
RULES:

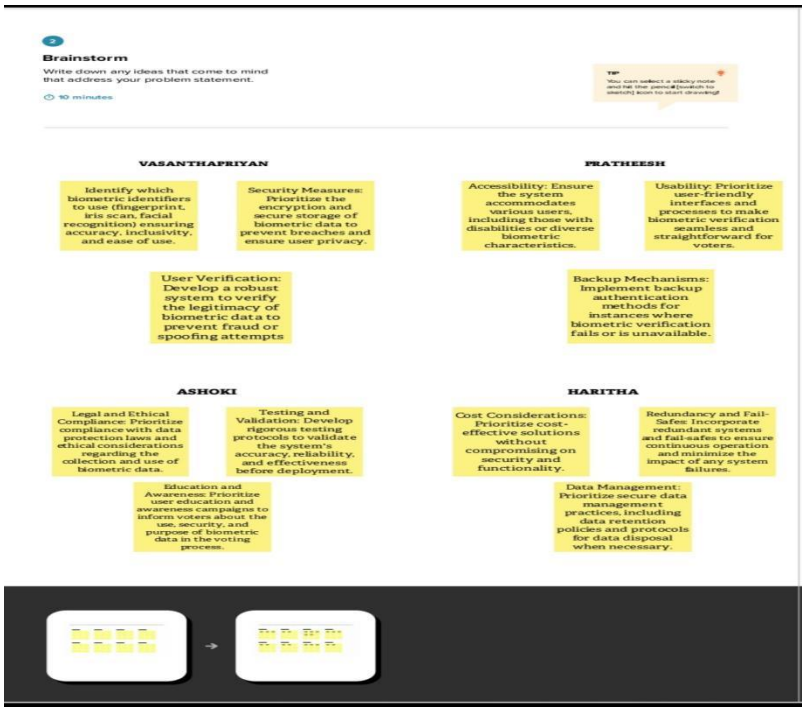
1.Lay out the problem you want to solve. ...

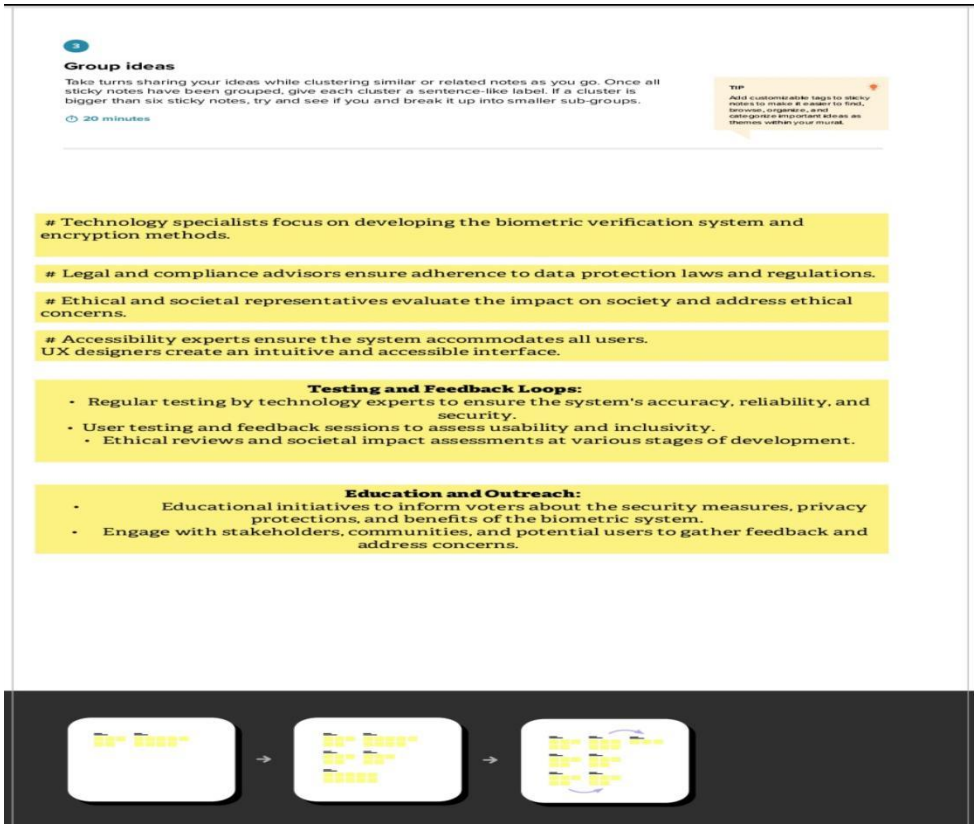
2.1dentify the objectives of a possible solution. ...

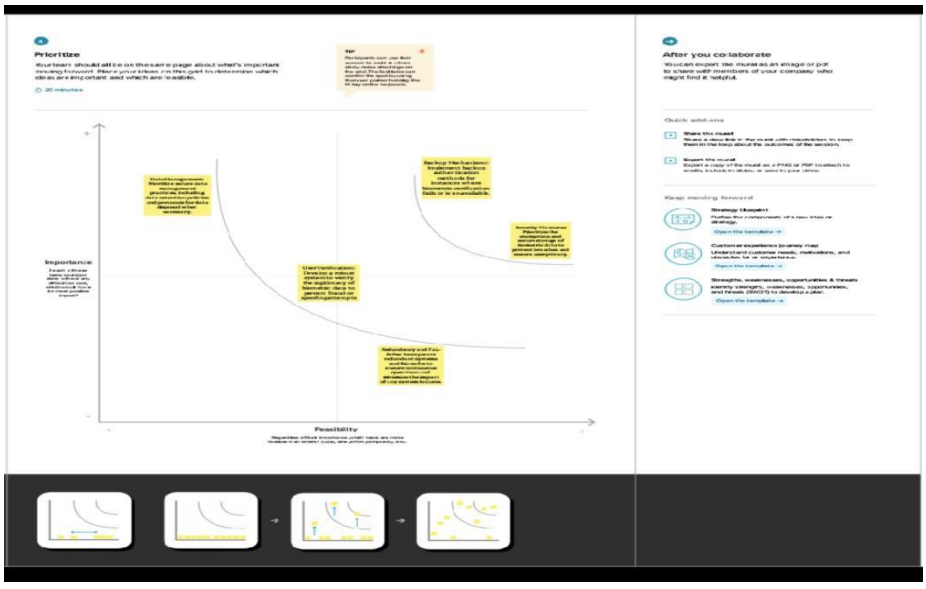
3.Try to generate solutions individually. ...

4.0nce you have gotten clear on your problems, your objectives and your personal
Solutions to the problems, work as a group.


Template
Brainstorm
& idea prioritization
Use this template in your own brainstorming sessions so your team can unleash their imagination and start shaping concepts even if you're not sitting in the same room.
10 minutes to prepare
1 hour to collaborate
2-8 people recommended
Before you collaborate
A little bit of preparation goes a long way with this session. Here's what you need to do to get going.
10 minutes
Define your problem statement
What problem are you trying to solve? Frame your problem as a How Might We statement. This will be the focus of your brainstorm.
5 minutes
Key rules of brainstorming
To run an smooth and productive session
Stay e topic.
Encourage wild ideas.
Defer judgment.
Listento others.
Go for volume.
Need some inspiration?


Brainstorm
Write down any ideas that come to mind that address your problem statement.
10 minutes
VASANTHAPRIYAN
Identify which biometric identifiers to use (fingerprint, iris scan, facial recognition) ensuring accuracy, inclusivity, and ease of use.
Security Measures: Prioritize the encryption and secure storage of biometric data to prevent breaches and ensure user privacy.
User Verification: Develop a robust system to verify the legitimacy of biometric data a to prevent fraud or spoofing attempts
PRATHEESH
Accessibility: Ensure the system accommodates various users, including those with disabilities or diverse biometric characteristics.
Usability: Prioritize user-friendly interfaces and processes to make biometric verification seamless and straightforward for voters.
Backup Mechanisms: Implement backup authentication methods for instances where biometric verification fails or is unavailable.
ASHOKI
Legal and Ethical Compliance: Prioritize compliance with data protection laws and ethical considerations regarding the collection and use of biometric data.
Testing and Validation: Develop rigorous testing protocols to validate the system's accuracy, reliability, and effectiveness before deployment.
Education and Awareness: Prioritize user education and awareness campaigns to inform voters about the use, security, and purpose of biometric data in the voting process.
HARITHA
Cost Considerations: Prioritize cost-effective solutions without compromising on security and functionality.
Redundancy and Fail-Safes: Incorporate redundant systems and fail-safes to ensure continuous operation and minimize the impact of any system failures.
Data Management: Prioritize secure data management practices, including data retention policies and protocols for data disposal when necessary.





4. REQUIREMENT ANALYSIS

4.1 Functional requirements

The functional requirements for a biometric security system in a voting platform encompass a multifaceted approach to ensure the integrity, security, and usability of the system. First and foremost, the system

should facilitate a seamless user registration process, allowing voters to securely input and store their biometric data, including fingerprints, iris scans, or facial features. During the voting process, the system must conduct real-time biometric verification, employing a robust matching algorithm to confirm the identity of the voter.

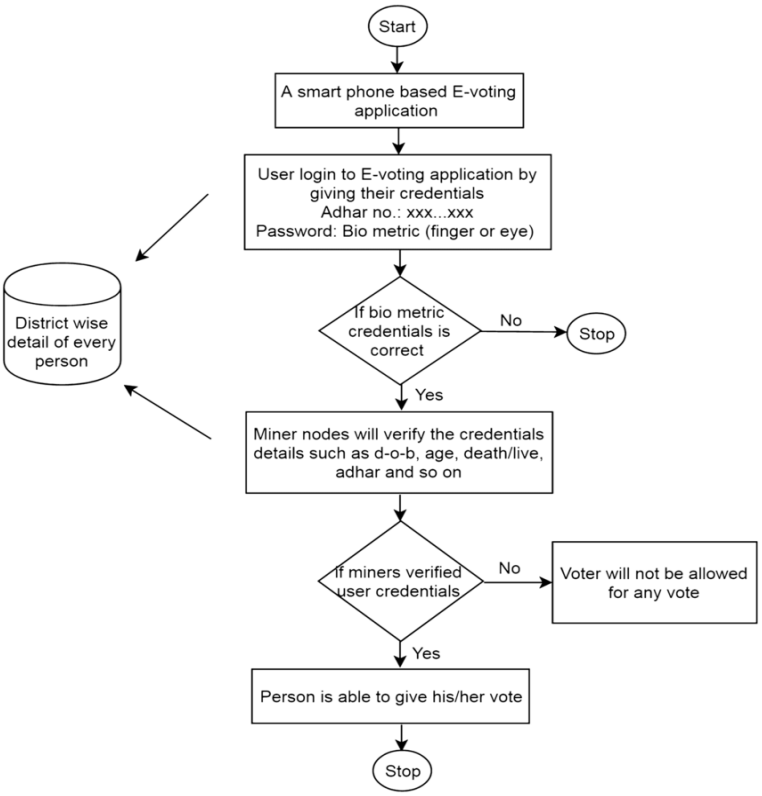
4.2 Non-Functional requirements

The non-functional requirements for a biometric security system in a voting platform encompass critical aspects beyond specific functionalities. The system must exhibit high performance, ensuring quick response times during user registration and biometric verification processes. Reliability is paramount, necessitating minimal downtime and robust mechanisms to handle potential system failures.

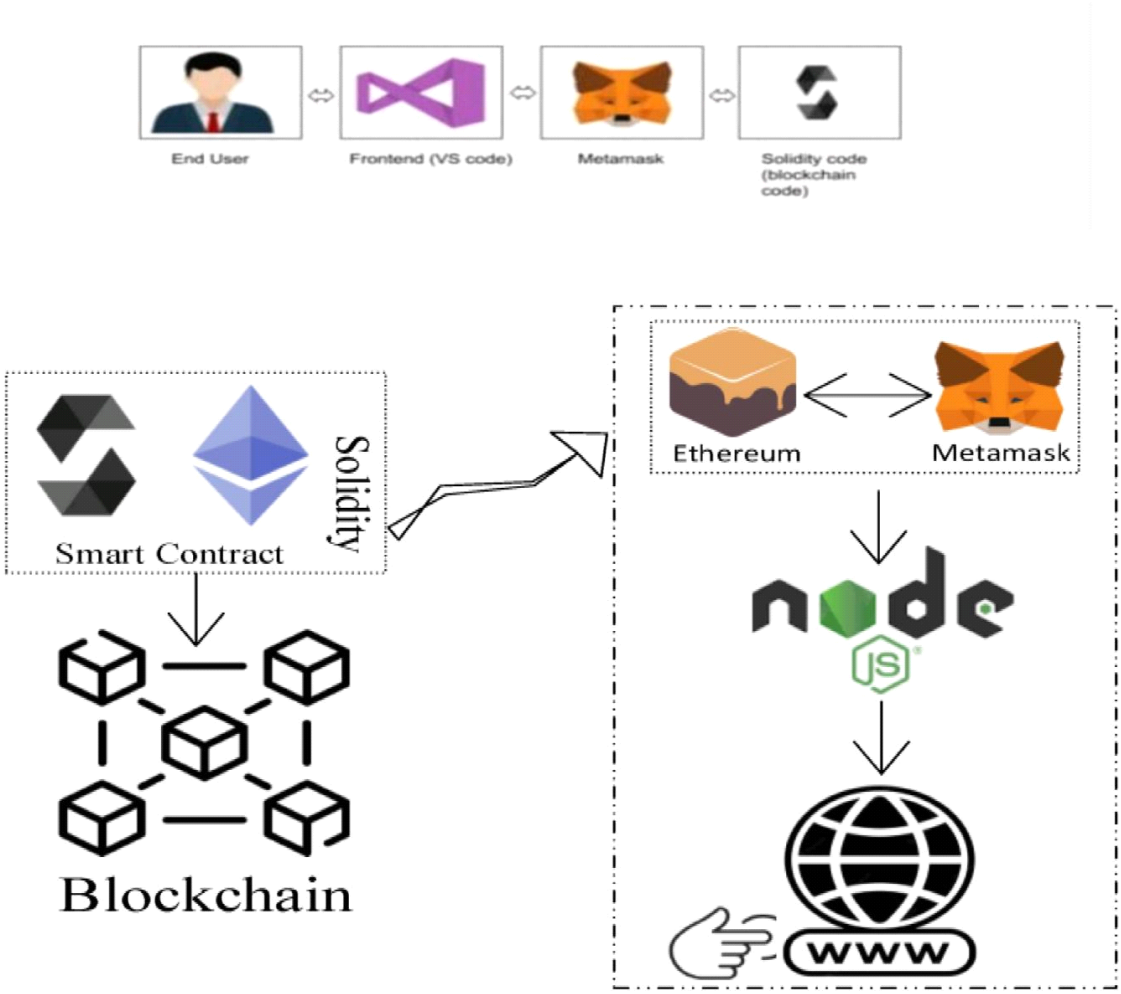
5.PROJECT DESIGN

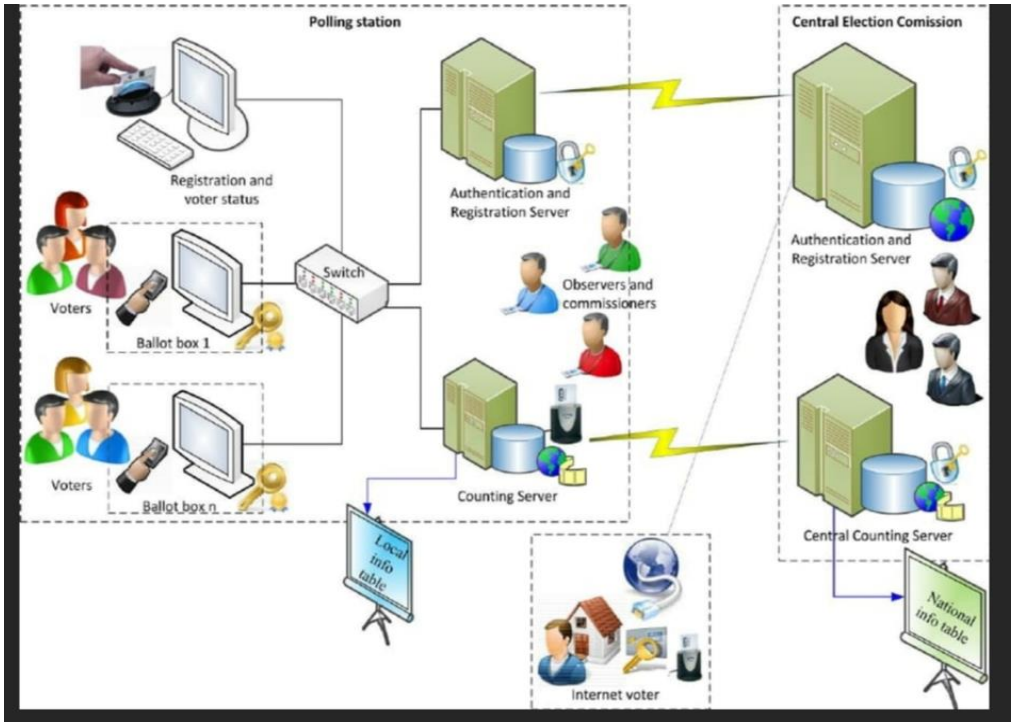
5.1 Data Flow Diagrams & User Stories

Data flow diagram

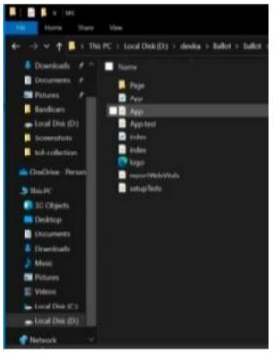


5.2 Solution Architecture

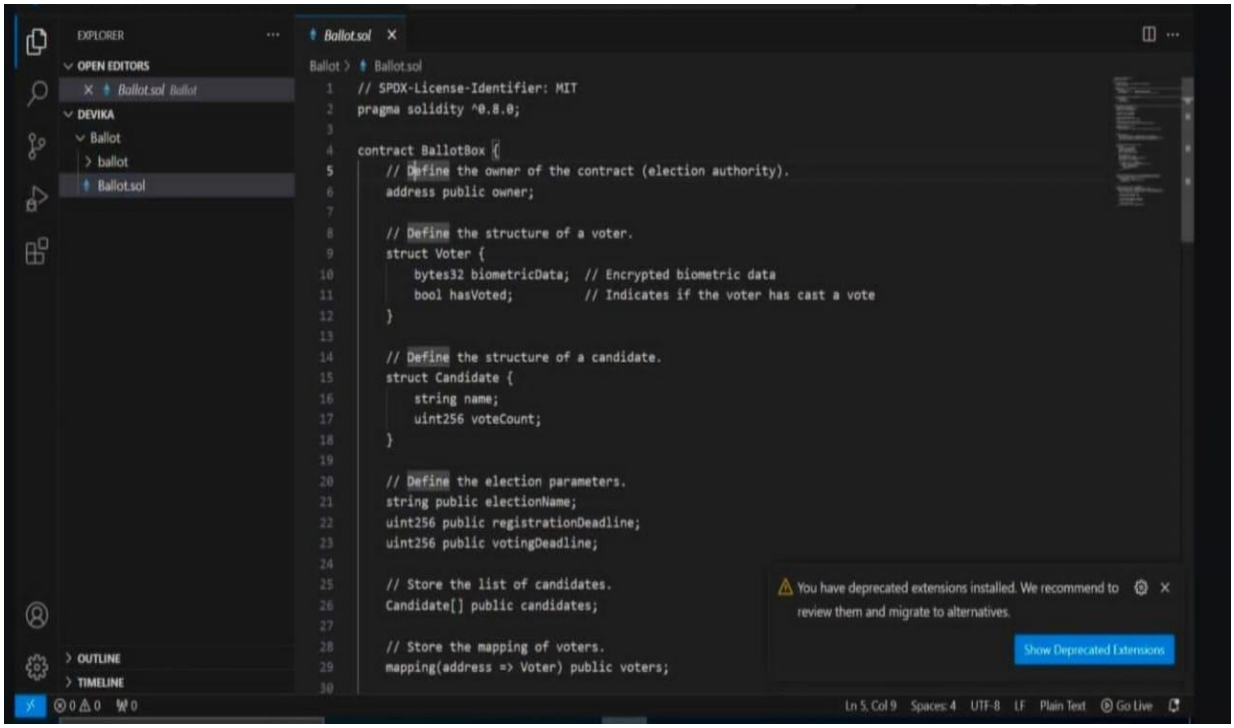


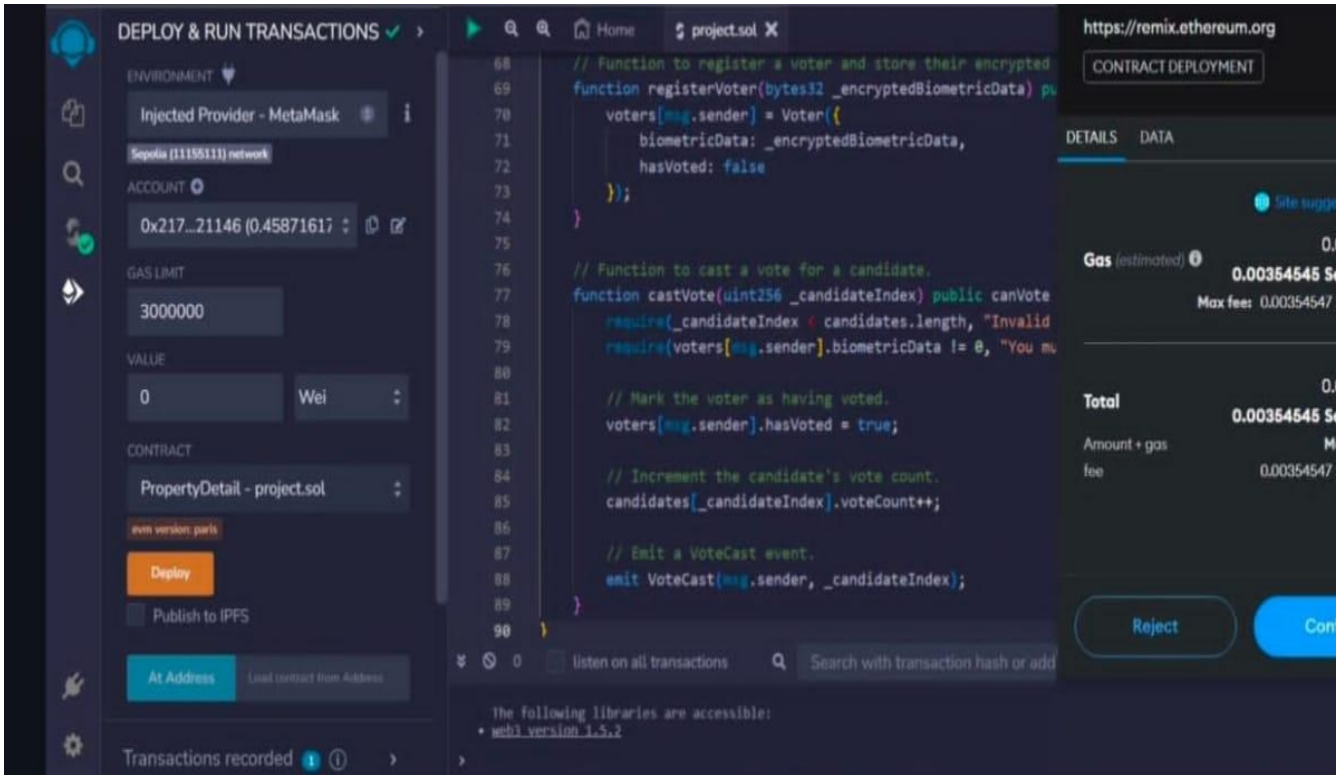


Project Development Phase:

S.No.	Parameter	Values	Screenshot
1.	Information gathering	Setup all the Prerequisite:	
2.	Extract the zip files	Open to vs code	

3.	Remix Ide platform explorting	Deploy the smart contract code Deploy and run the transaction. By selecting the environment - inject the MetaMask.	
4	Open file explorer	Open the extracted file and click on the folder. Open src, and search for utiles. Open cmd enter commands 1. npm install 2. npm bootstrap 3. npm start	
5	{LOCALHOST IP ADDRESS	copy the address and open it to chrome so you can see the front end of your project.	





10. ADVANTAGES & DISADVANTAGES

Advantages

Implementing a biometric security system in a voting platform offers several advantages. Firstly, it enhances the authentication process by relying on unique biological characteristics such as fingerprints, iris patterns, or facial features, making it significantly harder for unauthorized individuals to manipulate or impersonate voters. This ensures the integrity of the electoral process, reducing the risk of fraudulent activities. Secondly, biometric systems provide a more convenient and efficient voting experience, as voters only need to undergo a quick and non-intrusive biometric scan to verify their identity.

Disadvantages

While biometric security systems for voting platforms offer notable advantages, they also come with certain disadvantages. One concern is privacy, as collecting and storing individuals' biometric data raises potential risks if not adequately safeguarded. There's a possibility of data breaches or misuse, leading to identity theft or unauthorized access to sensitive information. Additionally, biometric systems may face technical challenges, such as false positives or negatives, which could result in legitimate voters being denied access or unauthorized individuals gaining entry.

1. CONCLUSION

In conclusion, the integration of biometric security systems in voting platforms presents a compelling opportunity to enhance the integrity and efficiency of electoral processes. The advantages, including heightened authentication accuracy and a streamlined voting experience, contribute to a more secure and trustworthy democratic system. However, it is crucial to navigate and address the associated challenges, such as privacy concerns, potential technical issues, cost implications, and inclusivity considerations. Striking a balance between reaping the benefits of biometric security and mitigating these drawbacks is essential for successful implementation.

12. FUTURE SCOPE

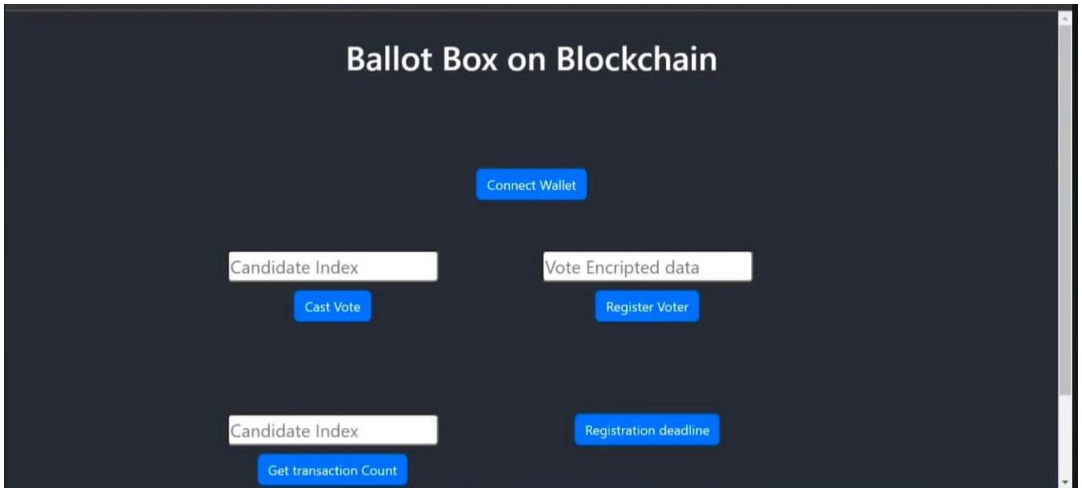
The future scope for biometric security systems in voting platforms is promising and holds potential for transformative advancements in electoral processes. Continued research and development in biometric technologies may lead to even more accurate and sophisticated authentication methods, further bolstering the security of voting systems.

1. APPENDIX

13.1Source code:

```
import java.util.HashMap;

class Blockchain {
    // Blockchain implementation details
    // (e.g., block structure, transaction handling, decentralized network setup)
}

class SmartContract {
    // Smart contract logic for handling voting transactions
    // (e.g., voter registration, ballot creation, vote casting)
}

class BiometricVerification {
    // Biometric verification logic using a biometric SDK
    // (e.g., fingerprint verification)
}

class VotingSystem {
    private Blockchain blockchain;
    private SmartContract smartContract;
    private BiometricVerification biometricVerification;
    private HashMap<String, String> voterRegistry; // Voter ID to Biometric data mapping

    public VotingSystem() {
```

```
        // Initialize blockchain, smart contract, and biometric verification
components
    }

    public void registerVoter(String voterID, String biometricData) {
        // Register a voter on the blockchain with their biometric data
        voterRegistry.put(voterID, biometricData);
    }

    public boolean castVote(String voterID, String candidate) {
        // Verify voter's identity using biometric data
        if (biometricVerification.verify(voterID,
voterRegistry.get(voterID))) {
            // Execute the voting transaction on the blockchain
            smartContract.castVote(voterID, candidate);
            return true; // Vote cast successfully
        } else {
            return false; // Biometric verification failed
        }
    }
}

public class Main {
    public static void main(String[] args) {
        VotingSystem votingSystem = new VotingSystem();

        // Voter registration
        votingSystem.registerVoter("Voter1", "FingerprintData1");
        votingSystem.registerVoter("Voter2", "FingerprintData2");

        // Casting votes
        boolean vote1 = votingSystem.castVote("Voter1", "CandidateA");
        boolean vote2 = votingSystem.castVote("Voter2", "CandidateB");

        // Display voting results, handle errors, etc.
    }
}
```



13.2Github& Project Demolink:

Github link: https://github.com/Axhoki/biometric-security-system-for-voiting-platform

Demo link: https://drive.google.com/file/d/1aYtvTuU-Av-d1M3rGRwC7kUheXQo8bCZ/view?usp=drivesdk