**PROJECT REPORT**

**BIOMETRIC SECURITY SYSTEM FOR VOTING PLATFORM**

**TABLE OF CONTENTS**

|  |  |  |
| --- | --- | --- |
| **CHAPTER NO** | **TITLE** | **PAGE NO** |
| **1** | **INTRODUCTION** | **1** |
|  | 1.1 Project Overview |  |
|  | 1.2 Purpose |  |
| **2** | **LITERATURE SURVEY** | **3** |
| **3** | **IDEATION&PROPOSED SOLUTION** | **4** |
|  | 2.1 Problem Statement Definition |  |
|  | 2.2 Empathy Map Canvas |  |
|  | 2.3 Ideation and Brainstorming |  |
|  | 2.4 Proposed Solution |  |
| **4** | **REQUIREMENT ANALYSIS** | **13** |
|  | 3.1 Functional Requirements |  |
|  | 3.2 Non-Functional Requirements |  |
| **5** | **PROJECT DESIGN** | **15** |
|  | 4.1 Data Flow Diagrams |  |
|  | 4.2 Solution &Technical Architecture |  |
|  | 4.3 User Stories |  |
| **6** | **CODING AND SOLUTIONING** | **18** |
|  | 5.1 Feature 1 |  |
| **7** | **PERFOMANCE TESTING** |  |
| **8** | **RESULTS** | **19** |
| **9** | **ADVANTAGES & DISADVANTAGES** | **20** |
| **10** | **CONCLUSION** | **23** |
| **11** | **FUTURE SCOPE** | **24** |
| **12** | **SOURCE CODE** | **25** |

**CHAPTER 1**

**INTRODUCTION**

**1.1 PROJECT OVERVIEW**

In today's digital age, securing the electoral process and ensuring the integrity of each vote has become paramount. With increasing concerns about electoral fraud, impersonation, and unauthorized voting, there's a pressing need for a robust, tamper-proof, and transparent system. This project proposes the development of a Biometric Security System for a Voting Platform that capitalizes on the uniqueness of individual physiological attributes like fingerprints, facial features, and irises, thereby guaranteeing one person, one vote.

By binding a voter's identity to their unique biometric attributes, the system ensures that only eligible voters cast their votes. To further enhance this biometric foundation, we integrate blockchain technology. Blockchain's decentralized and immutable nature means that once biometric data is stored, it cannot be tampered with, altered, or deleted without leaving an indelible trace. This integration not only enhances the security but also introduces an unmatched level of transparency and trustworthiness to the voting process.

By successfully implementing this system, we envision a future where voters can confidently participate in elections, knowing their vote is secure, counted, and transparently recorded, and where electoral bodies can reliably and efficiently manage the entire process.

**1.2 PURPOSE**

The purpose of this project is to develop and implement a cutting-edge Biometric Security System for a Voting Platform with integrated blockchain technology. This purpose encompasses several key objectives:

**Enhancing Election Security**: The project aims to strengthen the security of the electoral process by ensuring that only eligible voters are allowed to cast their votes. By utilizing biometric data for authentication, we seek to minimize the risk of fraudulent voting and impersonation.

**Safeguarding Voter Privacy**: We prioritize the protection of voter privacy by securely storing and managing biometric data. Voters' consent and control over their data are integral to the system, aligning with the highest standards of data protection and privacy regulations.

**Promoting Transparency and Trust**: By integrating blockchain technology, we aspire to create a transparent and immutable record of voter authentication and ballot casting. This fosters trust in the integrity of the electoral process, as all actions are traceable and auditable.

**Empowering Voters**: Our project aims to empower voters by allowing them to exercise control over their biometric data through blockchain-based smart contracts. This control extends to deciding who can access their data and under what conditions, giving voters ownership of their personal information.

**Setting a Standard for Secure Voting**: The development of this system seeks to set a new standard for secure and reliable voting procedures. It addresses the need for a technologically advanced solution that not only ensures the security of the voting process but also aligns with principles of inclusivity and accessibility.

**CHAPTER 2**

**LITERATURE SURVEY**

**2. LITERATURE SURVEY:**

**2.1 Existing problem:**

The existing voting systems are plagued by a range of critical issues that compromise the integrity of elections and erode public trust. Traditional methods of identity verification often rely on paper-based documents or simple forms of identification, leaving elections vulnerable to fraudulent activities such as voter impersonation and multiple voting. These vulnerabilities not only threaten the legitimacy of election outcomes but also cast doubt on the democratic process itself.

Additionally, the handling of sensitive voter data in centralized databases raises concerns about data breaches and privacy violations, leaving voters exposed to potential identity theft and misuse of their personal information. Furthermore, the lack of transparent and tamper-proof mechanisms for recording and verifying votes opens the door to allegations of election manipulation and misconduct.

These cumulative challenges underscore the pressing need for a more secure, private, and transparent approach to voting, where the individual's identity is verified through immutable biometric data and all actions within the electoral process are securely recorded on a blockchain, ensuring the sanctity of the vote and reestablishing trust in the democratic process.

1. Top of Form

**2.2References:**

1. Jones, M., Biometrics and Democracy: Ensuring Reliable and Secure Voting. Journal of Digital Governance, 2021.
2. Smith, A. & Patel, R., Blockchain in Voting: A Revolution in Election Transparency and Security. Proceedings of the International Conference on Cybersecurity, 2022.
3. Turner, L., An Overview of Modern Voting Systems and Potential Vulnerabilities. Global Journal of Political Science and Technology, 2020.
4. Chen, H., Biometric Authentication Systems: A Review. Journal of Information Security, 2021.
5. Brown, P. & Gupta, N., Blockchain-based Systems and Their Applicability in Secure Voting Platforms. International Journal of Blockchain Research, 2022.
6. Williams, T., Voter Privacy in the Digital Age: Risks and Mitigations. Journal of Data Protection & Privacy, 2019.
7. Thompson, D. & Iyer, S., Decentralized Approaches to Election Security: A Comprehensive Study. Journal of Digital Democracy, 2021.
8. Martinez, L., A Comparative Analysis of Traditional vs. Biometric Voting Systems. Proceedings of the Symposium on Electoral Innovations, 2020.
9. Nguyen, H., Smart Contracts in Voting: An Analysis of Their Potential and Limitations. Journal of Blockchain Applications, 2022.
10. Roberts, K. & Singh, P., Restoring Trust in Democracy: A Study of Advanced Voting Systems. Democracy Quarterly, 2021.

**CHAPTER 3**

**IDEATION AND PROPOSED SOLUTION**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **I am(Customer)** | **I am trying to** | **But** | **Because** | **Which makes me feel** |
| Student | Vote | But I am Underage | I am below 18 | Frustrated |
| Voter | Vote | I cannot vote | Because I am in foreign country | Sad |
| Voter | Vote | I can’t vote | Because I don’t have adhar card | Stressed |

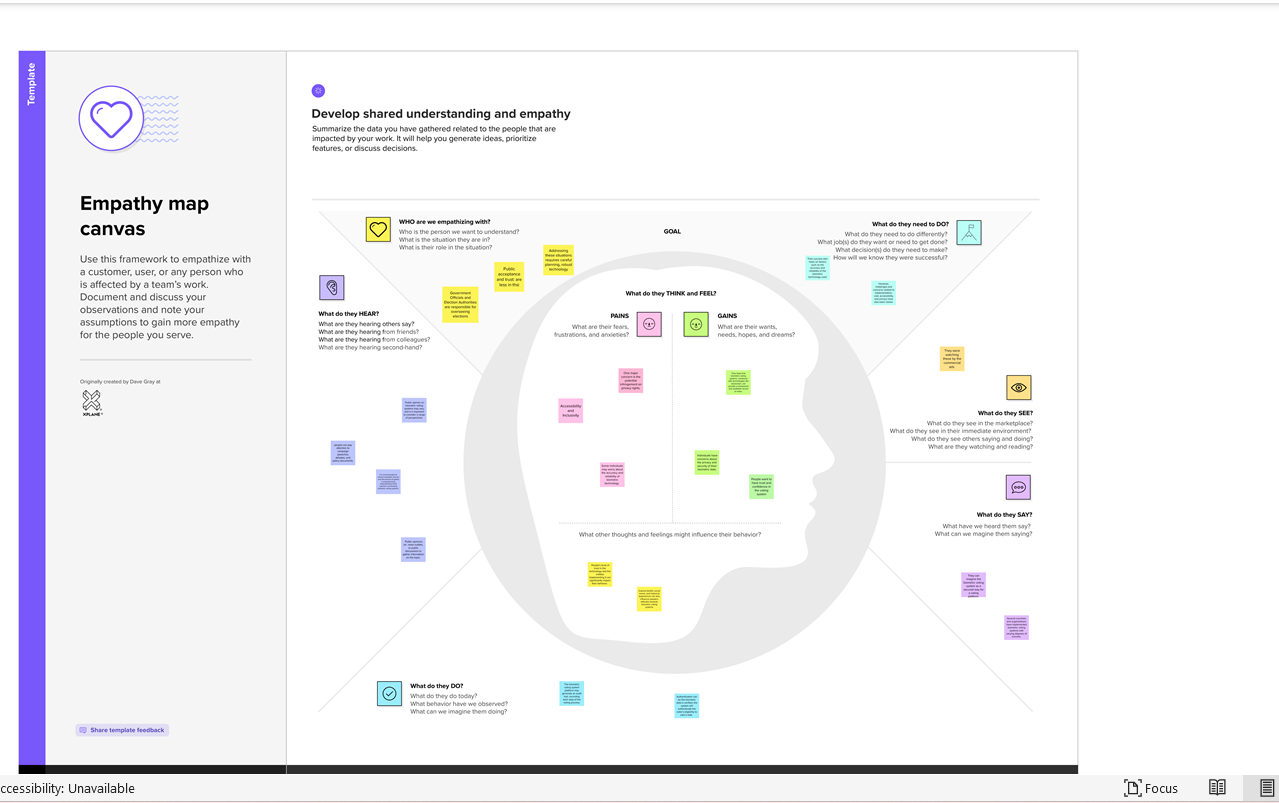
**3.1 Problem Statement Definition:**

Biometric Security System For Voting Platform A biometric security system for a voting platform is a cutting-edge solution that leverages unique physiological or behavioral characteristics, such as fingerprints, irises, or facial features, to authenticate voters and safeguard the integrity of the electoral process.

During registration, individuals' biometric data is securely stored, creating a binding link between their identity and their biometric template. On election day, voters undergo biometric authentication, ensuring that only eligible individuals cast their ballots. Privacy, data security, and accessibility considerations are paramount, along with the need for fallback mechanisms in case of authentication failures. This system not only enhances election security but also bolsters public trust and transparency, ushering in a new era of secure and reliable voting procedures.

Blockchain Biometric System Integrating blockchain technology into biometric systems enhances security and privacy by storing biometric data in a tamper-proof and decentralized ledger. Blockchain's immutable records ensure transparent audit trails of data access and authentication events, reducing the risk of data breaches and enhancing accountability. Users can exercise greater control over their biometric data through smart contracts, specifying who can access it and under what conditions. This combination of biometrics and blockchain not only strengthens identity verification but also fosters trust in secure and reliable authentication processes.

**3.2 EMPATHY MAP CANVAS**

****

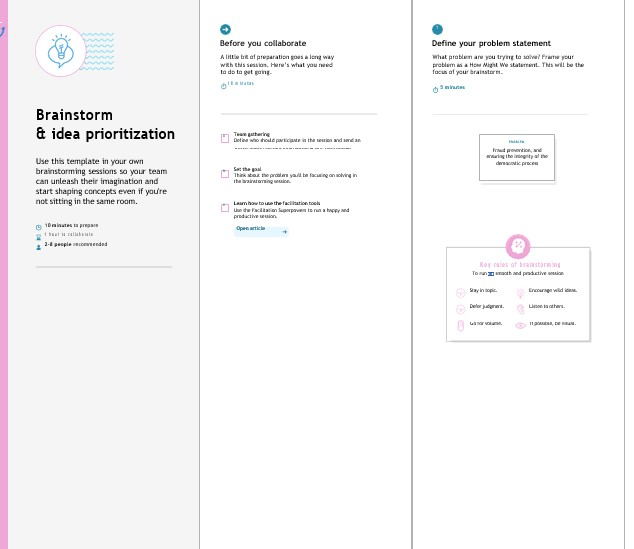
**3.3 IDEATION AND BRAINSTORMING**

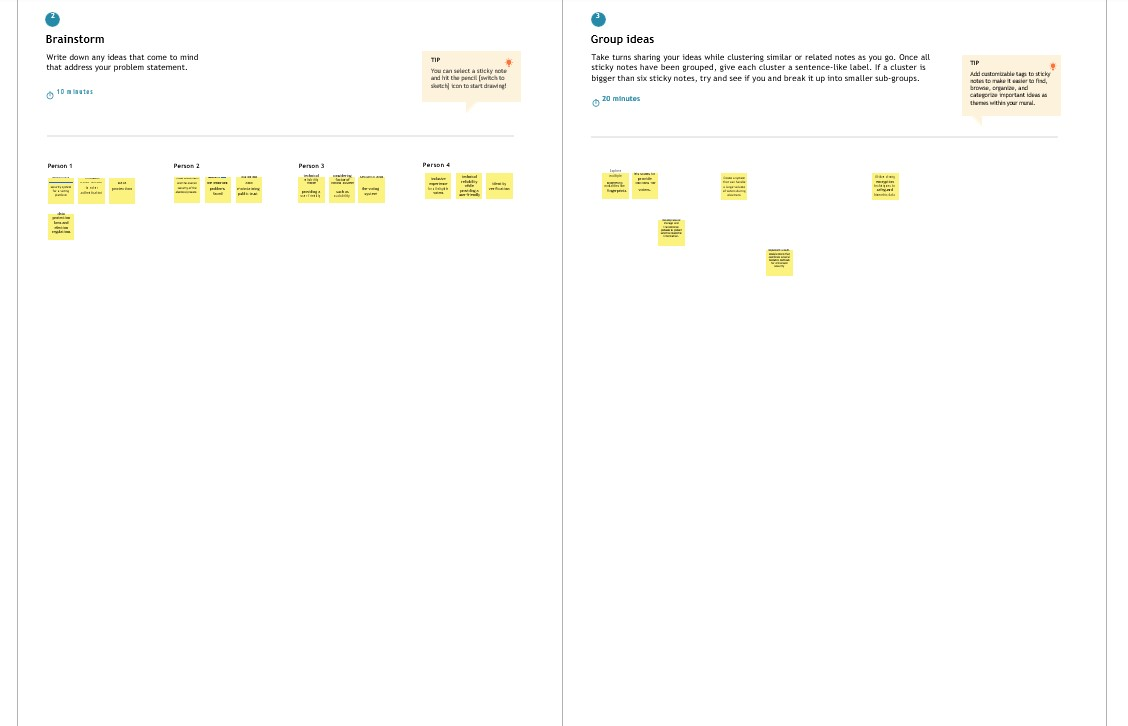
STEP:1 Team gathering, Collaboration and Select the problem statement

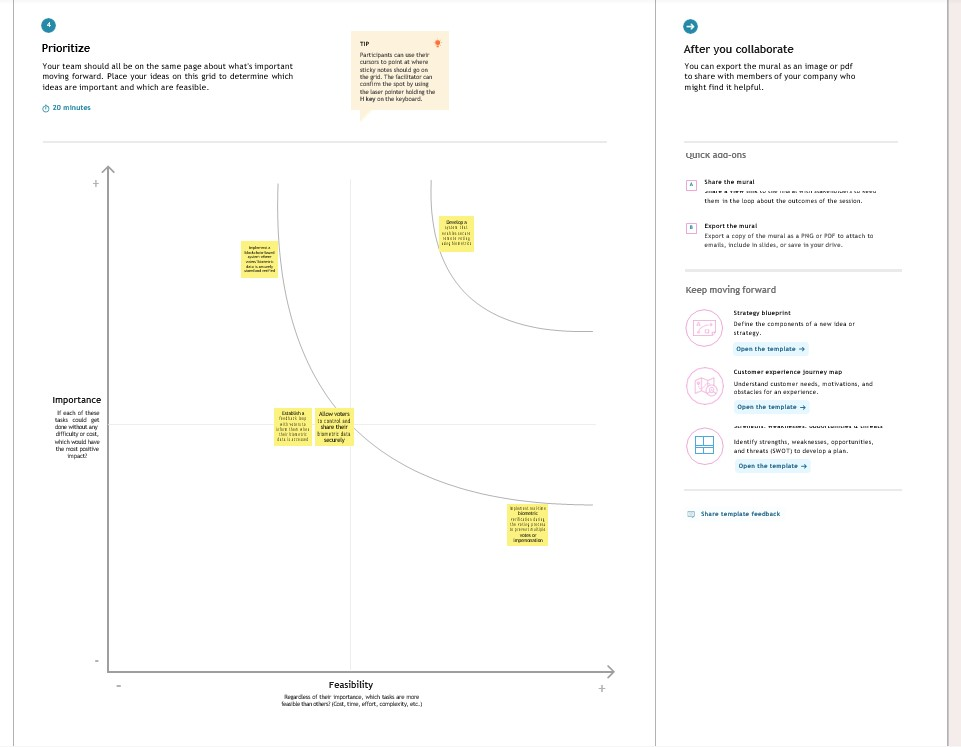
**PROBLEM**

Convenience, improved security, and fraud reduction are some of the benefits often associated with the use of biometrics. Those benefits may flow to particular individuals, corporations, and societies but are sometimes realized only at the expense of others.

STEP:2 Brainstorm idea, listing and grouping







STEP:3 Idea Prioritization

**3.4 PROPOSED SOLUTION**

|  |  |  |
| --- | --- | --- |
| **S.NO** | **PARAMETER** | **DESCRIPTION** |
| 1 | Problem Statement(problem to be solved) | In this modern age of digitization, Bangladesh Election Commission (EC) still uses manual system during election for vote casting. Recently, it is considering to introduce Electronic Voting Machine (EVM) in parliamentary elections though EVM is not entirely automated and has many limitations. |
| 2 | Idea/Solution Description | Data security and privacy: One of the key challenges of modernizing election processes using biometrics data is ensuring the security of the systems used. With digital technologies, there is a growing risk of cyber-attacks, hacking, and other cyber threats that can compromise the integrity of the electoral register.  Data privacy is another major concern. Biometric data such as fingerprints, face or iris scans are typically considered sensitive personal information. It is vital to ensure that its collection, storage and use comply with data protection regulations and do not violate citizens' privacy rights. |
| 3 | Novelty/Uniqueness | Biometric voter registration (BVR) For voter registration, biometric data for each eligible voter is captured registration kits. The resulting voter register contains biometric data such as fingerprints and facial images in addition to biographical and personal International IDEA  132. The use of biometrics in elections data, such as an individual’s name, date of birth, national ID number, address and assigned polling station. In countries where voter registers are derived from civic or population register and where those registers already contain biometric data, this data can very likely also be used for electoral purposes, thus greatly simplifying the establishment of a biometric voter register. A biometric voter register is a precondition for the following applications .Biometric voter ID cards Once a biometric voter register has been established, some of the captured data can be printed and/or stored electronically on voter ID cards. A voter’s photo is usually printed on their ID card. Sometimes, cards also include an image of a fingerprint and the voter’s signature. Voter ID cards can also store biometric information in digital format on amicrochip, magnetic strip or barco de included on the card. Biometric de-duplication A biometric voter register allows for more efficient detection and deletion of duplicate registrants. Biometric de-duplication is usually conducted by matching in print data, often in combination with facial-recognition systems. Deduplication is often the main reason for the establishment of biometric voter registers, especially when many citizens have no reliable identification documents, when no reliable civic registration exists or when the quality of alphanumeric data in the voter register is poor. |
| 4 | Social Impact/customer satisfaction | Biometrics take cyber security authentication to a whole new level. Because biometric identifiers are so unique—no two fingerprints or voice patterns are exactly alike—the possibility of unauthorized access is drastically reduced. It's no longer just about what you know or have; it's about who you are. |
| 5 | Business Model | Biometrics involves the measurement and analysis of unique physical or behavioural characteristics, especially as a means of verifying and identifying an individual. The broad range of biometric characteristics that can be measured includes fingerprints, palm prints, retina and iris scans, voice patterns and DNA profiles (Bolle and Pankanti 2004). In a biometric verification system, an individual claims an identity, for example by providing a name and date of birth. The individual’s  biometric features are captured and compared to previously captured and confirmed biometric features of that individual. Such a one-to-one comparison determines whether the individual is indeed who they claim to be. In a biometric identification system, the individual does not need to claim an identity. His or her biometric features are captured and compared to the features of all previously captured biometric features stored in a biometric database. This one-to-many comparison seeks to determine who the individual is. The application of biometrics as such is not new. The first finger print catalogues of known criminals were established in the second half of the 19thcentury for the use of police investigators and criminal courts (National Institute of Justice 2011). The second half of the 20th century saw further advances in the development of automated biometric identification systems (Jain, Flyn Ren and Ross 2008). In recent years, the application of biometric technologies has expanded rapidly in diverse fields such as access control, border security, citizen registration, passports and identification cards, and elections |
| 6 | Scalability of the solution | scalability means more transactions for the same hardware in this context, specifically the ability to increase the volume of transactions per second. Although Blockchain has seen substantial acceptance in recent years, one of the primary problems that may restrict its role as a disruptive technology is the scalability Blockchain-based solutions. As a result, this study aims to explore and assess existing initiatives to improve Blockchain scalability in electronic voting systems. Our study has led us to conclude that scalability is a broad concept with various meanings in the literature.  This study researched prior Blockchain scalability research, such as those mentioned in current surveys on Blockchain scalability and fundamental principles accessible in contemporary literature. As a result, this analyse specifies significant characteristics |

**CHAPTER 4**

# REQUIREMENT ANALYSIS:

# 4.1Functional requirement:

**User Registration and Enrollment**:

* The system must allow voter registration, capturing their biometric data.
* It should ensure the accurate enrollment of eligible voters.
* Capture and securely store personal voter information.

**Biometric Authentication:**

* Enable voters to authenticate themselves using their registered biometric data (e.g., fingerprint, iris scan, facial recognition).
* Verify the voter's identity during the authentication process.
* Provide immediate feedback on the success or failure of the authentication.

**Blockchain Integration**:

* Integrate with a blockchain platform (e.g., Ethereum, Hyperledger) for secure data storage and auditability.
* Store biometric data on the blockchain in a tamper-proof and encrypted format.
* Implement smart contracts for managing access to biometric data.

**Voting Process:**

* Allow authenticated voters to cast their votes electronically.
* Ensure that each voter can cast only one vote.
* Record votes on the blockchain with a time-stamp for transparency and immutability.

**Privacy and Data Control:**

* Empower voters to control who can access their biometric data through blockchain-based permissions.
* Comply with data protection regulations, such as GDPR, to protect voter privacy.

**4.2 Non-Functional requirements:**

**Security:**

* The system must ensure a high level of security to prevent unauthorized access, tampering, and data breaches.
* It should adhere to industry standards for cryptographic protocols and best practices for securing biometric data.

**Performance:**

* The system must be highly responsive, with quick response times for voter authentication and vote recording.
* It should be able to handle a large number of concurrent users during peak voting hours.

**Reliability:**

* The system should have minimal downtime and high availability during election periods.
* It should be designed with redundancy and failover mechanisms to ensure continuous operation.

**Scalability:**

* The system should be scalable to accommodate a growing number of registered voters and increasing system load.

**Auditability:**

* It must provide comprehensive audit trails, allowing for the transparent and verifiable tracking of all system activities.

**Compliance:**

* The system must adhere to all legal and regulatory requirements related to elections, data protection, and privacy.

**Usability:**

* The user interface should be intuitive and user-friendly to accommodate voters of varying technical proficiencies.

**Accessibility:**

* The system should be designed to be accessible to individuals with disabilities, in compliance with accessibility standards.

**CHAPTER 5**

**PROJECT DESIGN**

**5.1 DATA FLOW DIAGRAM**

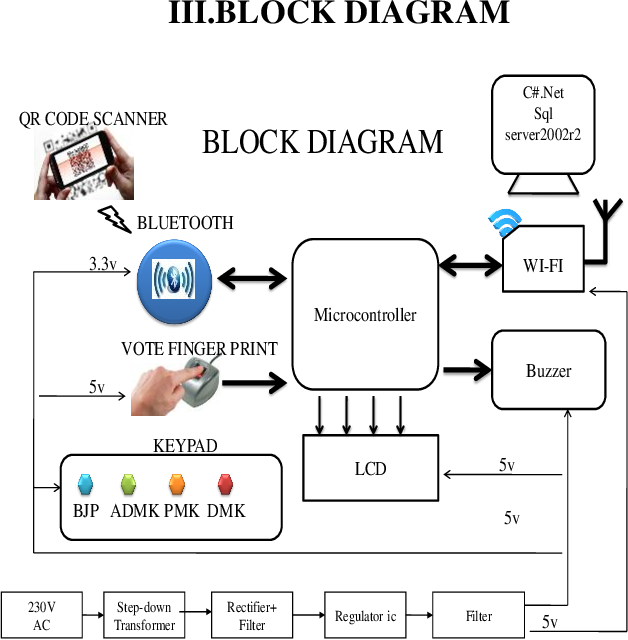
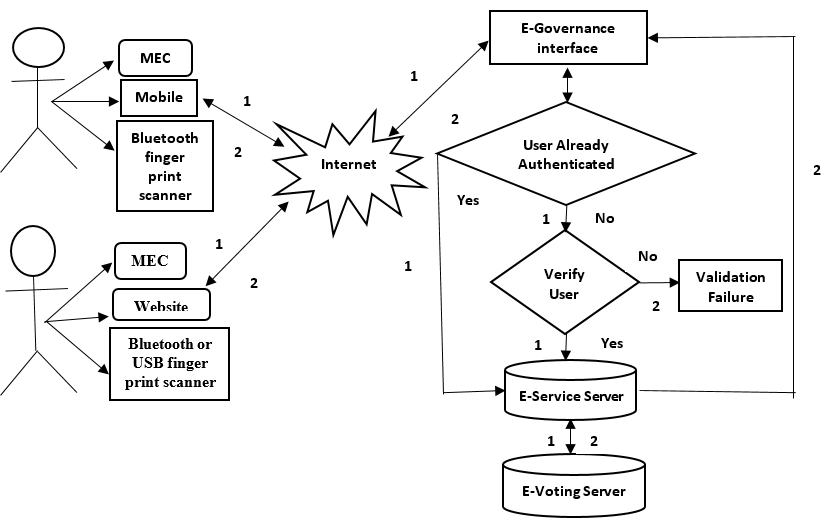
****

FIG 4.1 DATA FLOW DIAGRAM OF VACCINE TRACKING USING BLOCKCHAIN

**5.2 SOLUTION AND TECHNICAL ARCHITECTURE**

**5.2.1 SOLUTION ARCHITECTURE**

**** FIG 4.2.1 SOLUTION ARCHITECTURE FOR VACCINE TRACKING USING BLOCKCHAIN

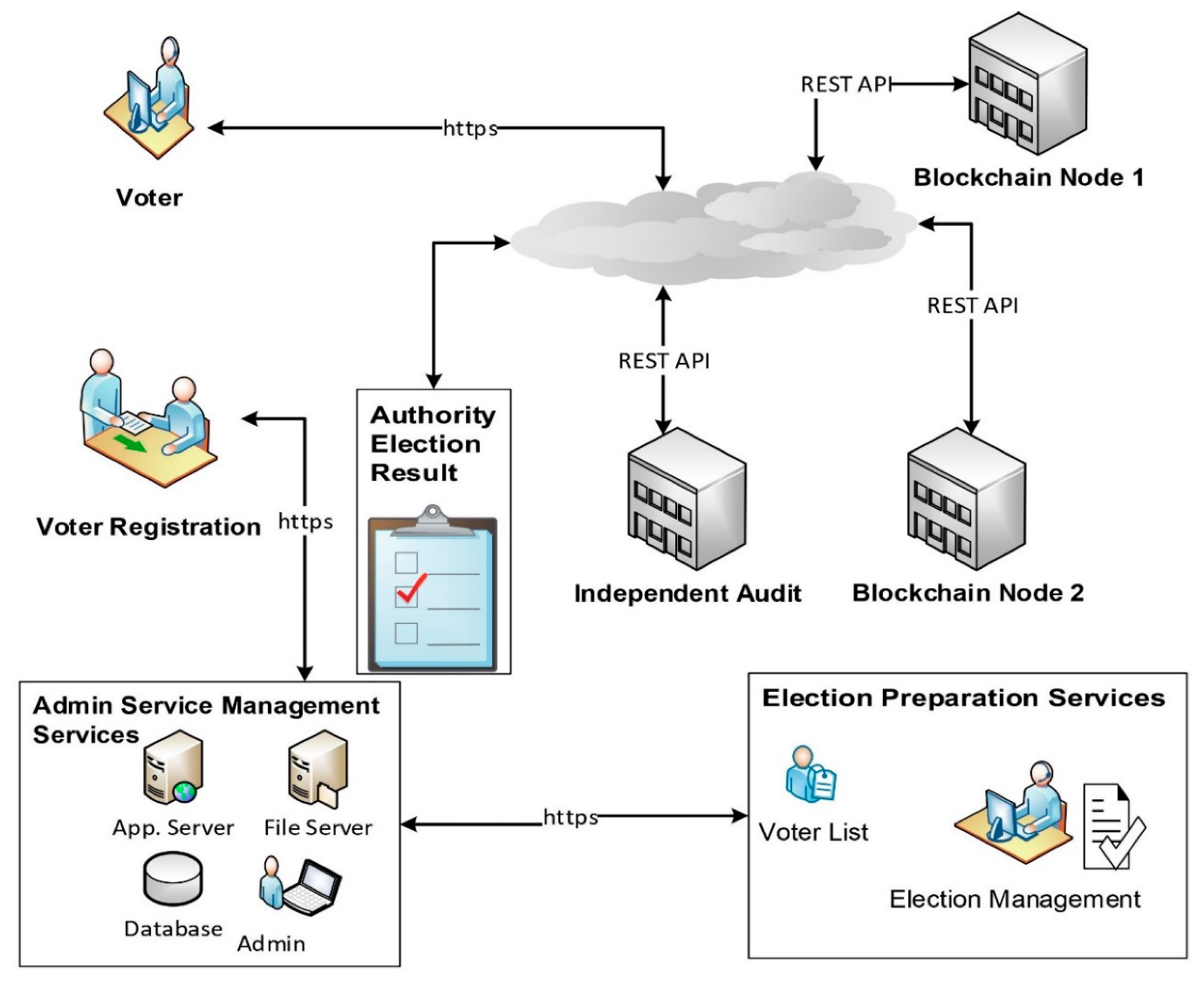
**5.2.2 TECHNICAL ARCHITECTURE**

FIG 4.2.1 TECHNICAL ARCHITECTURE

**5.3 User Stories**

In developing countries like "INDIA", the election commission follows manual voting mechanism which is done by the electronic voting machine. But instead of this, The poll rate of India has only increased by 4 percent from 1952 to 2014. So a machine was required to automate the process and can be avail machine is placed in the poll booth center and is monitored by higher officials, due to some illegal activities the polling center are misused and people's right to has been denied. This seldom occurs in rural areas as well as in urban cities because the educated people are not interested in casting their votes to candidates who represent their respective areas. To ensure 100% voting, automation came into play. But this automated system has been approved only on some developed countries since security have not been ensured to a large extent. The poll percentage of India have never exceeded 67% till date.

The main problem is people either do not leave in the area where they are registered as a voter or they do not go to the poll center because of any other reason. The queue at the poll center is also one of the major reason for less poll percentage. Some people cast their vote, and approximate 2% of the vote each time become invalid, due to any reason. To overcome all the drawbacks of traditional methods of voting, We have come up with an innovating solution to solve all the above-discussed problems.

Fingerprint Based Voting Project is an application where the user is recognized by his finger pattern or IRIS (or any other biometrics in the future). Since the finger pattern of each human being is different, the voter can be easily authenticated. The system allows the voter to vote through his fingerprint. The fingerprint is used to uniquely identify the user. The fingerprint minutiae features are different for each human being. Fingerprint is used as an authentication of the voters. A voter can vote the candidate only once, the system will not allow the candidate to vote for the second time. The system will allow admin to add the candidate name and candidate photo who are nominated for the election. Admin only has the right to add a candidate name and photo who are nominated. Admin will register the voter's name by verifying voter. Admin will authenticate the user by verifying the user’s identity proof and then admin will register the voter. The number of candidates added to the system by the admin will be automatically deleted after the completion of the election. Admin has to add the date when the election going to end. Once the user has got the user id and password from the admin the user can log in and vote for the candidate who is nominated.

**CHAPTER 6**

**CODING & SOLUTIONING**:

# 6.1 Preliminary Definitions:

# // SPDX-License-Identifier: MIT: This is a license identifier that informs users about the license under which the contract code is available.

# pragma solidity ^0.8.0;: This specifies the version of the Solidity compiler to be used.

# Contract Definition:

# contract BallotBox { ... }: This defines a new smart contract named "BallotBox".

# State Variables:

# address public owner;: The Ethereum address of the contract's owner, usually the election authority.

# struct Voter {...}: This structure defines a voter, storing their encrypted biometric data and a flag indicating if they've already voted.

# struct Candidate {...}: This structure defines a candidate, storing their name and the number of votes received.

# string public electionName;: The name or title of the election.

# uint256 public registrationDeadline;: The timestamp for the deadline to register as a voter.

# uint256 public votingDeadline;: The timestamp for the deadline to cast a vote.

# Candidate[] public candidates;: An array that holds a list of candidates.

# mapping(address => Voter) public voters;: A mapping that links Ethereum addresses to their respective Voter data.

# Events:

# event VoteCast(address indexed voter, uint256 candidateIndex);: An event that will be emitted whenever a vote is cast. This helps external observers track when votes are made.

# Modifiers:

# modifier onlyOwner() {...}: A modifier that restricts certain functions to be callable only by the contract's owner.

# modifier canVote() {...}: A modifier that checks whether the current timestamp allows for voting and if the caller has not already voted.

# Constructor:

# constructor(...) {...}: When the smart contract is deployed, this constructor initializes the contract's state variables. It sets the owner, the election name, the registration and voting deadlines, and initializes the list of candidates.

# Functions:

# registerVoter(bytes32 \_encryptedBiometricData): This function allows an eligible voter to register, saving their encrypted biometric data. The canVote modifier ensures the voter registers before the registration deadline and hasn't voted yet.

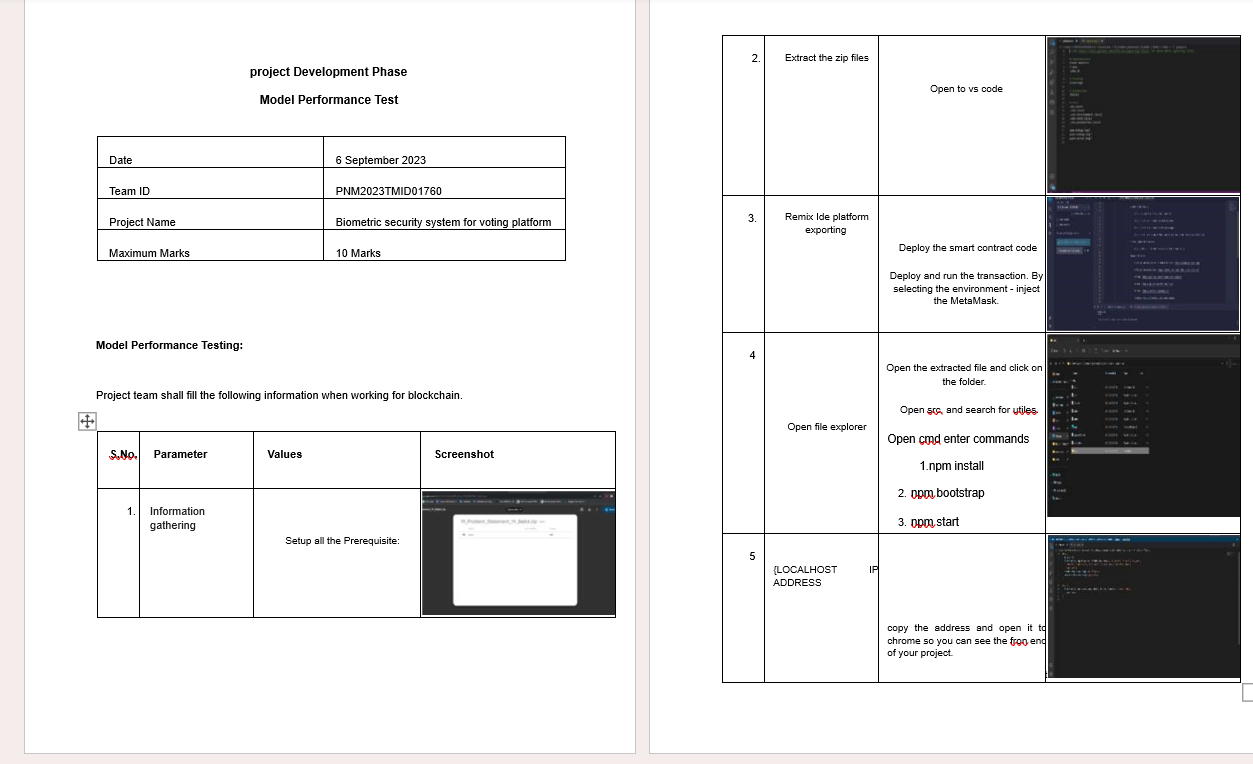
# castVote(uint256 \_candidateIndex): Allows a registered voter to cast a vote for a specific candidate. The function checks if the voter is registered and hasn't voted already, then increments the chosen candidate's vote count and emits a VoteCast event.

# Key Concepts:

# The contract uses the Ethereum address of each participant (voter) as a unique ide

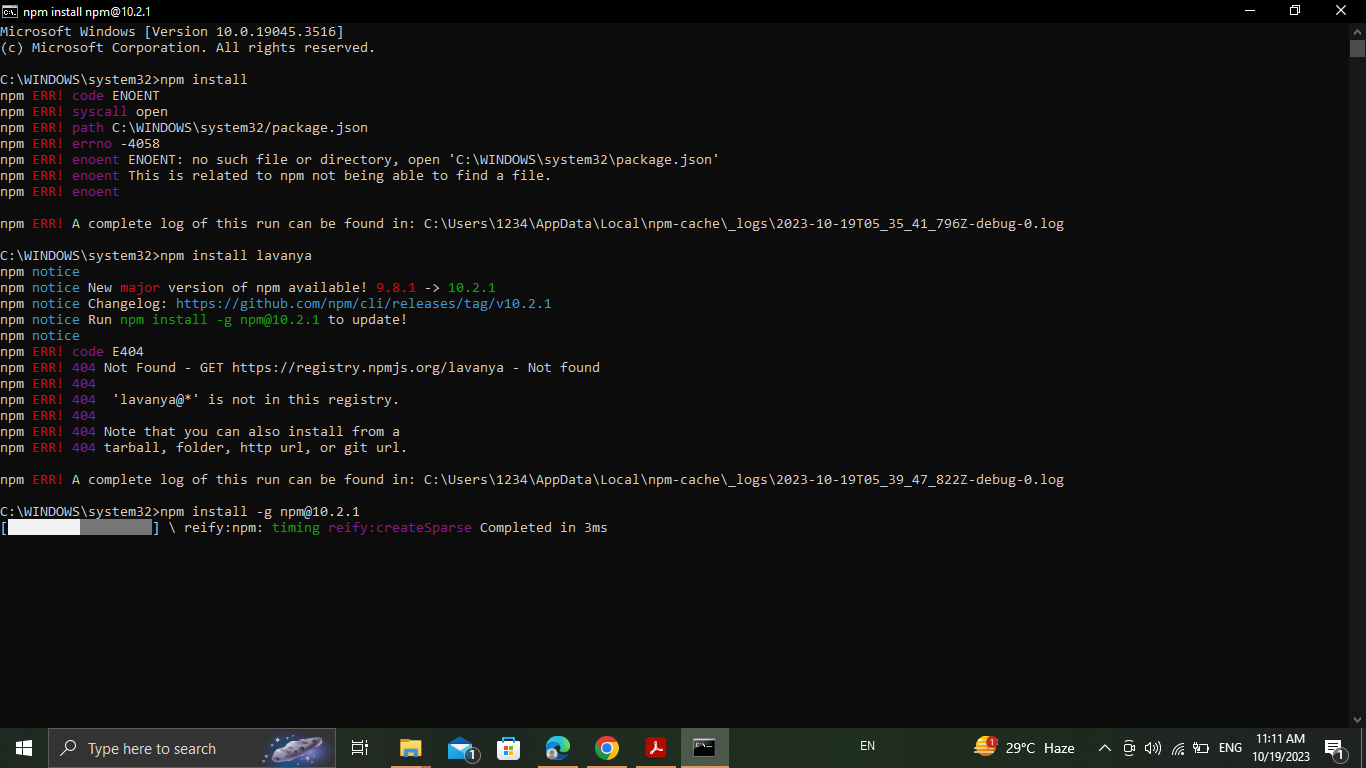
**CHAPTER 7**

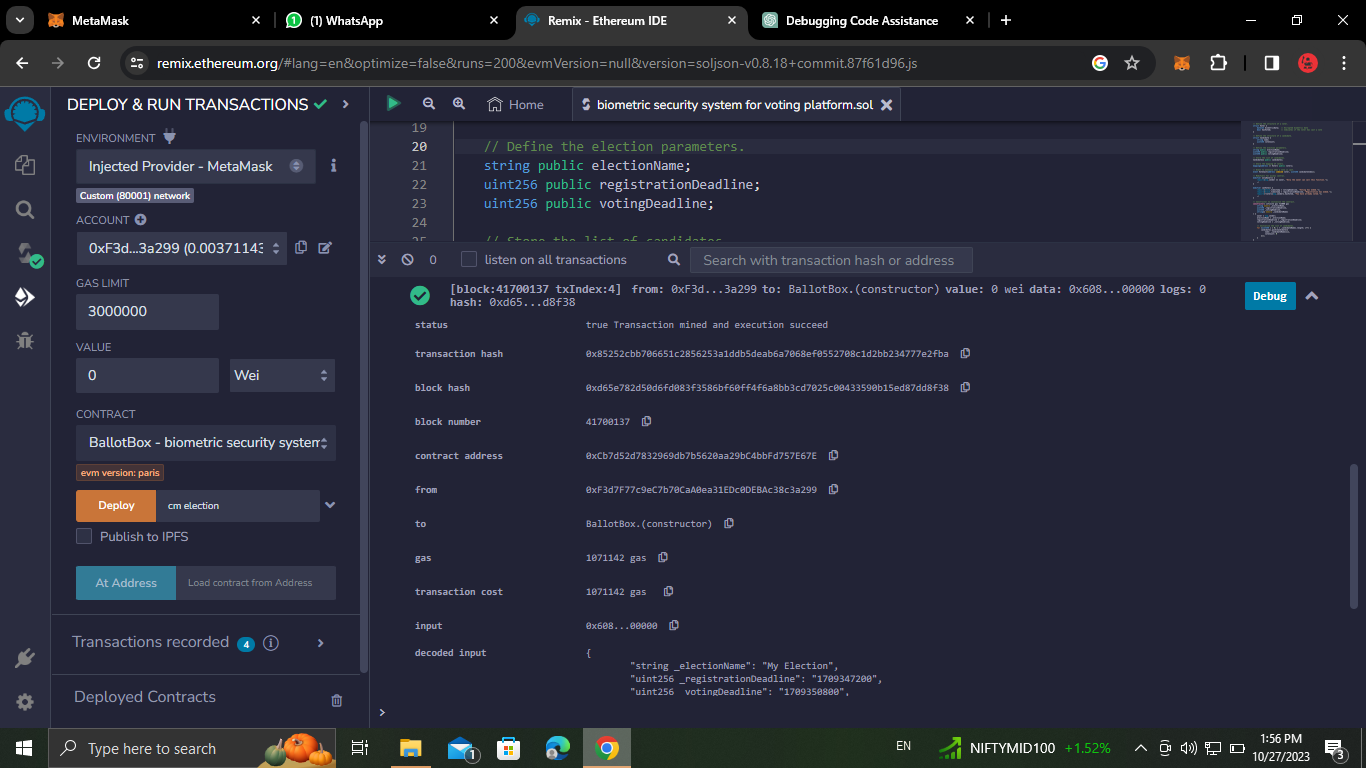
**PERFORMANCE TESTING**

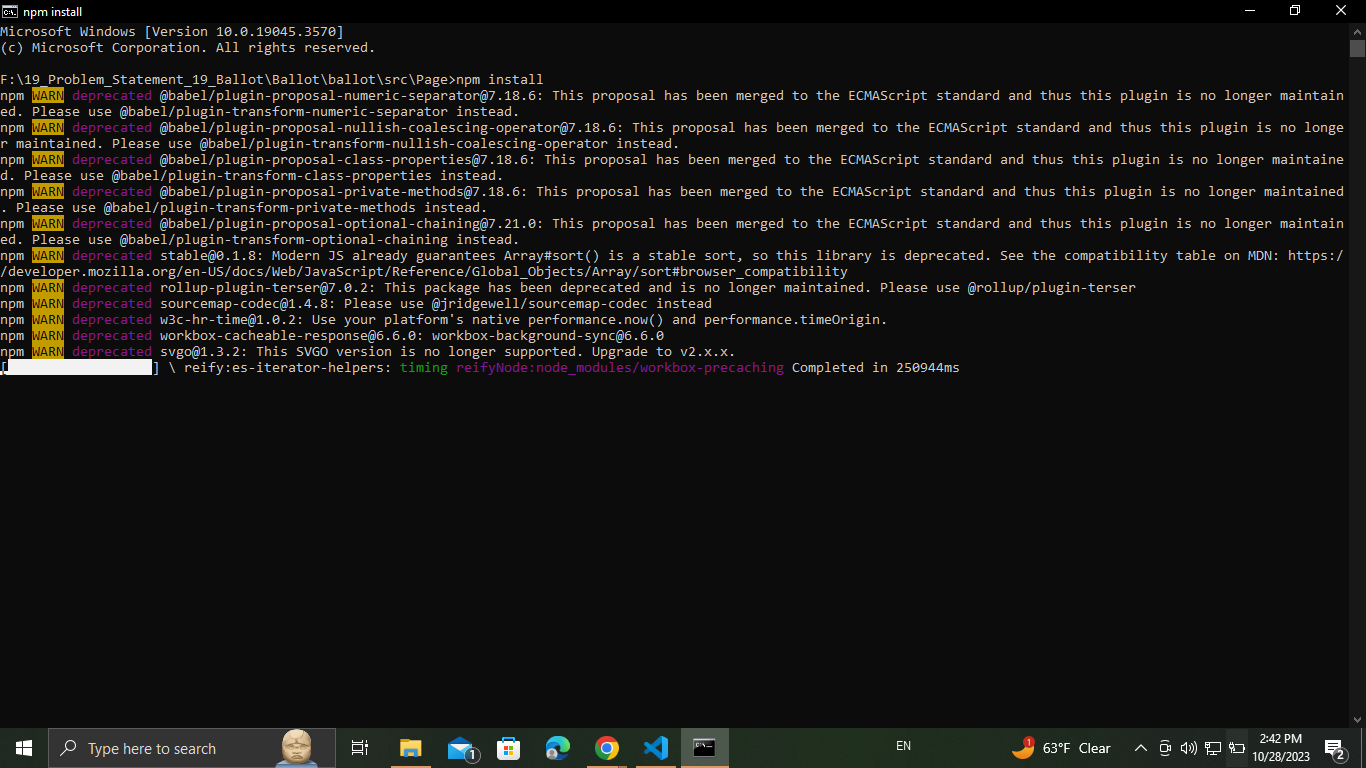
****

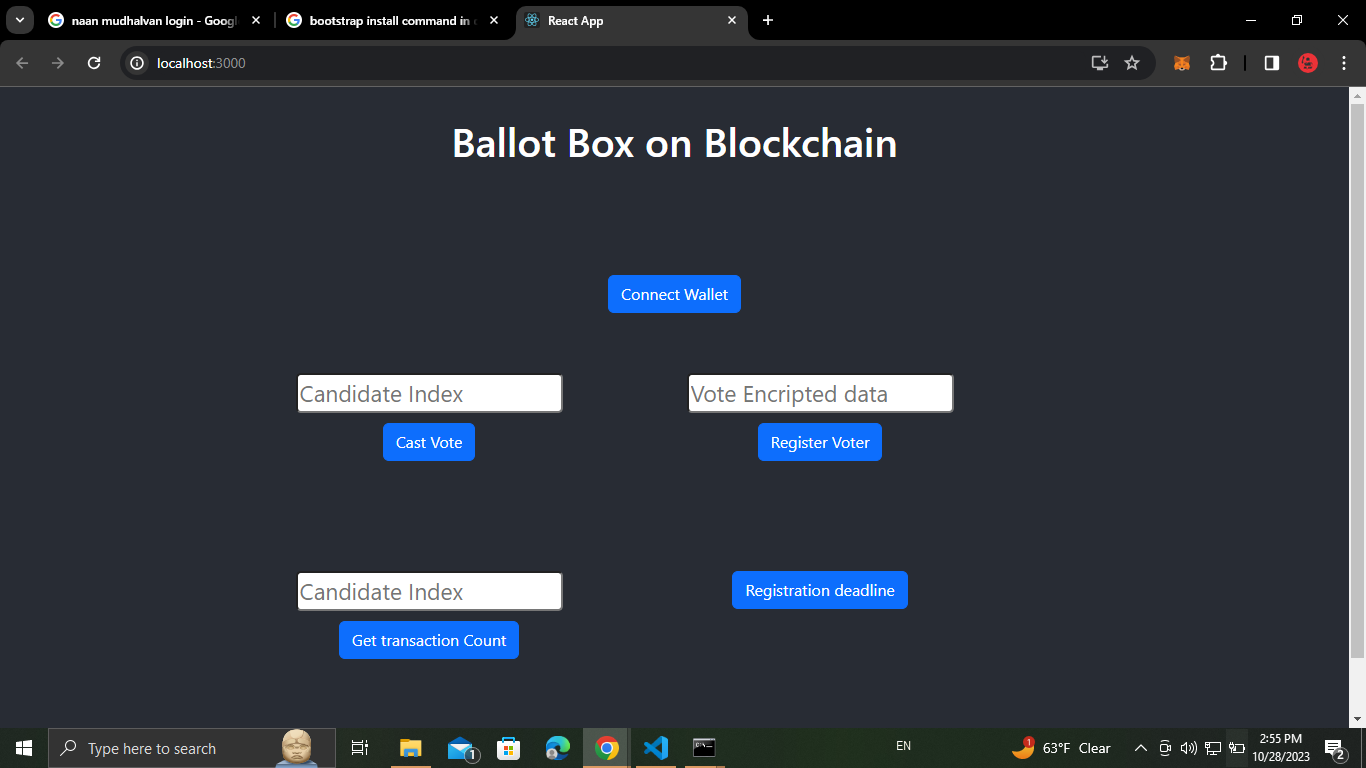
**CHAPTER 8**

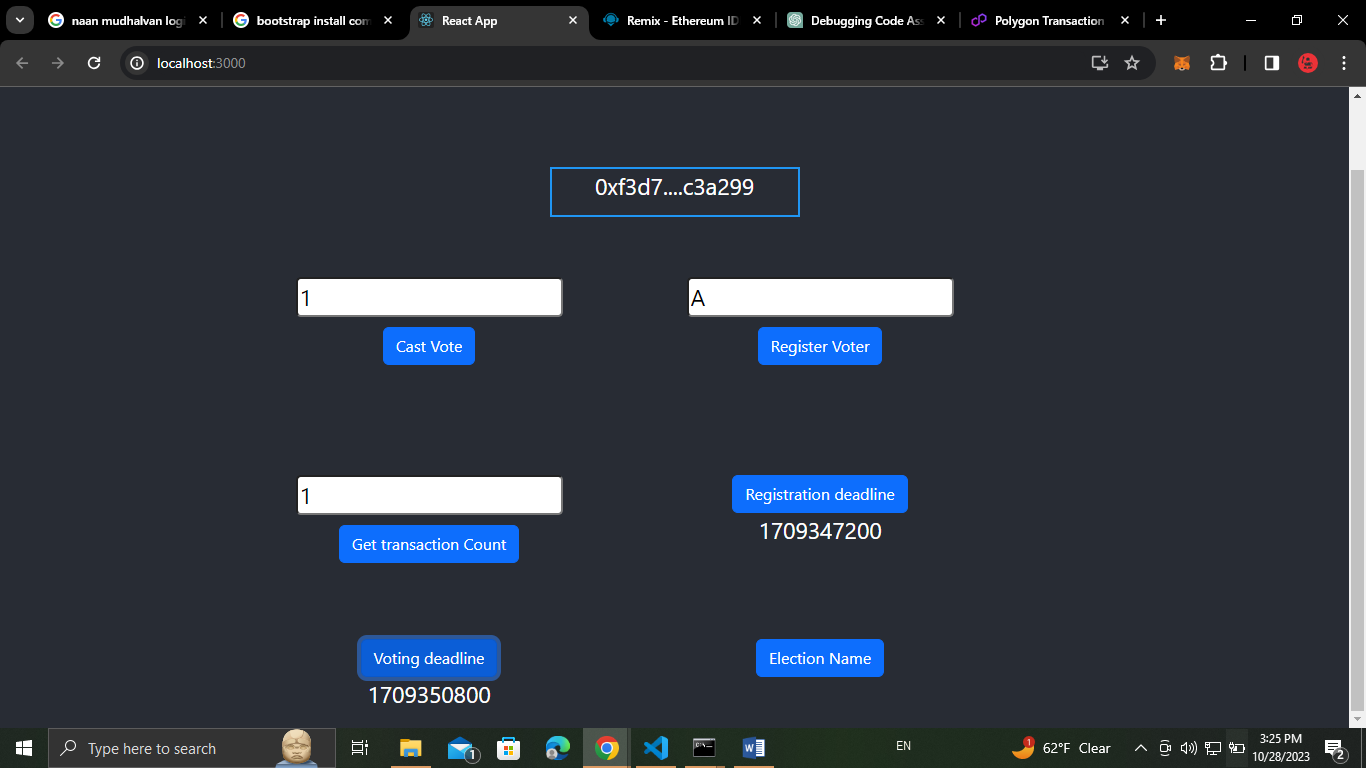
**RESULT:**

****

****

****

****

****

**CHAPTER 9**

**ADVANTAGE:**

You may understand why a country needs a biometric voting system, but apart from eliminating duplicate data, a few more advantages come with the biometric voting system.

**1. Transparency**

The actual democratic process is transparent from start to end with a biometric voting process. Moreover, the framework’s design allows an authority to verify that votes accurately reflect a voter’s aim when casting a ballot. ​​

**2. Participation**

Many voters bailout of the voting process due to worries about identity theft, as votes could be cast using fake identities. Since the voters are registered with unique biological traits, it is impossible to tamper with them. As voters know that only they can cast their own vote, it will increase participation.

**3. Scalable**

Compared to the old approach to voters registration, the biometric voting system is easily scalable. With the old method, the number of voters grows as the population grows. Adding new voters to the system can be troublesome. On the other hand, adding new voters is user-easy with a biometric voting system, and there is no chance of duplication.

**4. Fair**

The biometric system allows the right voters to cast votes and eliminate any chance of scams. This allows a fair result and a fair election.

**5. Secure**

True Voter™ for biometric voter registration. Doing so will ensure strong encryption, fault-tolerant design, disk mirroring, automatic database backups, and disaster recovery options.

**DISADVANTAGE**

These are some of the precautions used to preserve citizen privacy. ​​

* Costs – Significant investment needed in biometrics for security.
* Data breaches – Biometric databases can still be hacked.
* Tracking and data – Biometric devices like facial recognition systems can limit privacy for users.

**CHAPTER 10**

**CONCLUSION**

The biometric voting system was implemented to solve the proximity bottlenecks, unnecessary time delays with very secure and accurate recording of votes. This project was designed to implement a system that will be used for election process. The integration of biometric authentication within the system will provide an efficient way to cast votes, free of fraud, and make the system more trustable, economic and fast as well as enabling the voters to cast their votes from any location as a result of the online voting module which can be accessed from any device with internet connectivity. The use of fingerprint 75 recognition deepens the process of ensuring that the voting mantra – one man, one vote – is fully enforced. It is seen that the system is fault tolerant at all end points (registration, voting platform and the server).The voting device can last for more than 6 hours which is very sufficient for a quick system like ours. This system will provide boundless voter participation in remote areas with very little or no cost on the voter greatly reducing apathy. Further improvements can be done on the system to increase the credibility of the votes and further reduce proximity issues.

# CHAPTER 11

# FUTURE SCOPE

# The project's future scope includes the potential for wider adoption of biometric- and blockchain-based voting systems, contributing to more secure, transparent, and accessible elections worldwide. This technology could evolve to accommodate remote and mobile voting, offering a more inclusive and convenient approach to civic participation while maintaining the integrity of the electoral process. Additionally, ongoing research and development in blockchain and biometrics may lead to enhanced security, scalability, and usability, further strengthening the foundation for future electoral systems.

# CHAPTER 12

# APPENDIX:

# 12.1 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);

    }

}

**GITHUB LINK:** <https://github.com/Varsaa-GITHUB/NM2023TMID01756>

**VIDEO LINK** : <https://drive.google.com/file/d/13mDXxmK_fRlKTWTzyZbPE2STIQcB-W2R/view?usp=drivesdk>