PROJECT REPORT

BIOMETRIC SECURITY FOR VOTING PLATFORM

Date	**28 October 2023**
Team ID	**NM2023TMID11230**
Project Name	**BIOMETRIC SECURITY FOR VOTING PLATFORM**

TEAM MEMBERS

T. AROCKIA ROOPAN	**814620105305**
S. REENA	**814620105008**
D. SUGANTHI	**814620105315**
S. THAKIR NISHA	**814620105316**

ABSTRACT

Presently voting is performed using ballot paper and the counting is done manually, hence it consumes a lot of time. There can be possibility of invalid votes. All these make election a tedious task. In recent times in India, due to elections the second wave of COVID transmission also made huge loss of human lives. In our proposed system voting and counting is done with the help of computer in Online. It saves time, avoid error in counting and there will be no invalid votes. It makes the election process easy. It also avoids the process of physical touching or visiting any places and so in the time of pandemic too it will be more helpful to conduct elections.

The system deals with the online voting and its details. Allows the user to vote for the candidate online. Can get the details of the candidate and voter as well. Without the wastage of time the citizen can vote the respective candidate. In present existing system we are using ballot paper and counting the number of votes, it takes the lot of time to for the existing process, to overcome the drawbacks in the existing system this particular system was proposed to mark our work much easier and to reduce wastage of time. And more over us doesn’t get the accurate results in the present existing system. So, there is a need for Online Voting Systems.

1. INTRODUCTION

Elections are fundamental pillar of a democratic system enabling the general public to express their views in the form of a vote. Due to their significance to our society, the election process should be transparent and reliable so as to ensure participants of its credibility. Within this context, the approach to voting has been an ever-evolving domain. This evolution is primarily driven by the efforts to make the system secure, verifiable and transparent. In view of its significance, continuous efforts have been made to improve overall efficiency and resilience of the voting system. Electronic voting or e-voting has a profound role in this. Since its first use as punched-card ballots in 1960's, e-voting systems have achieved remarkable progress with its adaption using the internet technologies (Gobel et al, 2015). However, e-voting systems must adhere to specific benchmark parameters so as to facilitate its widespread adoption. These parameters include anonymity of the voter, integrity of the vote and non-repudiation among others. Blockchain is one of the emerging technologies with strong cryptographic foundations enabling applications to leverage these abilities to achieve resilient security solutions.

A Blockchain resembles a data structure which maintains and shares all the transactions being executed through its genesis. It is primarily a distributed decentralized database that maintains a complete list of constantly germinating and growing data records secured from unauthorized manipulating, tampering and revision. Blockchain CORE Metadata, citation and similar papers at core.ac.uk Provided by UWL Repository allows every user to connect to the network, send new transactions to it, verify transactions and create new blocks (Rosenfeld, 2017; Kadam et al, 2015; Nakamoto, 2009). Each block is assigned a cryptographic hash (which may also be treated as a finger print of the block) that remains valid as long as the data in the block is not altered. If any changes are made in the block, the cryptographic hash would change immediately indicating the change in the data which may be due to a malicious activity. Therefore, due to its strong foundations in cryptography, blockchain has been increasingly used to mitigate against unauthorized transactions across various domains (Nakamoto, 2009; Kraft, 2015; Narayanan et al, 2015). Bitcoin remains the most distinguished application of blockchain however researchers are keen to explore the use of blockchain technology to facilitate applications across different domains leveraging benefits such as non-repudiation, integrity and anonymity. In this paper, we explore the use of blockchain to facilitate e-voting applications with the ability to assure voter anonymity, vote integrity and end-to verification.

We believe e-voting can leverage from fundamental blockchain features such as self-cryptographic validation structure among transactions (through hashes) and public availability of distributed ledger of records. The blockchain technology can play key role in the domain of electronic voting due to inherent nature of preserving anonymity, maintaining decentralized and publicly distributed ledger of transactions across all the nodes. This makes blockchain technology very efficient to deal with the threat of utilizing a voting token more than once and the attempt to influence the transparency of the result. The focus of our research is to investigate the key issues such as voter anonymity, vote confidentiality and end-to-end verification.

1.1 Project Overview

The Biometric Vote project aims to enhance the security and integrity of the voting process by implementing a biometric security system in a voting platform. Traditional voting methods often suffer from issues such as identity fraud, duplicate voting, and the inability to verify the identity of voters accurately. By integrating biometric technology into the voting system, this project seeks to address these challenges and ensure a secure, transparent, and tamper-proof voting process.

1.2 Purpose

The purpose of implementing a biometric security system for a voting platform project is to enhance the security, integrity, and accessibility of the voting process in elections. Biometric security systems utilize unique physical or behavioral characteristics of individuals to verify their identity.

2. LITERATURE SURVEY

Raspberry Pi and image processing based on Electronic Voting Machine (EVM) [1], provides a small computer capable of image processing and controls the entire voting system. A photo of the national ID card of citizens is taken with the help of a camera which indicates a valid voter of that zone. If the person is legitimate and has not voted, the person will be allowed to cast his or her ballot. Each voting www.ijcrt.org © 2022 IJCRT | Volume 10, Issue 4 April 2022 | ISSN: 2320-2882 IJCRT2204455 International Journal of Creative Research Thoughts (IJCRT) www.ijcrt.org d917 machine is locked with a module of fingerprint access. When the user gets verified, the fingerprints gets submitted to a particular system for voting. Each voting system is connected for identification to a voting system of central raspberry pi. The Impressive Smart Card Based Electronic Voting System [2], introduces a voting system that gives voters confidence in elections by using fingerprint methods and providing a smart card to every user to promise diversity in the voting system and reduce the work of the Indian election committee. At the same time the outcome of the election process will be automatically announced to the public. With the help of this method, one can easily vote in any polling station. With the data sets available, this paper manages and integrates test and effect. All possible guidelines were discussed in this paper. An Electronic Voting Machine that uses Biometric Fingerprint and Aadhar Card Verification [4], has a voting system that uses biometric fingerprints with Aadhar certification. In this program, the aadhar number is stored on a small ARM7 microcontroller that verifies based on the available information. This will be used to take fingerprints of Indian citizens. If that person is eligible to vote they are entitled to submit their votes. Smart Voting System [6], introduces a system where people who are Indian citizens and over the age of 18 can give their vote. Even though they don't have to go to their hometown on the allotted day. The purpose of voting system based on Aadhar is that, the electoral elections will allow people to vote in their current city electronically. The Smart Voting System using RFID [9], provides a RFID (Radio Frequency Identification) approach by which from anywhere a user can vote safely using his or her computer or mobile phone and no need to go to the polls by using following two-step verification by recognizing a face and authenticating the OTP. The offline voting system is extemporized using RFID tags instead of voter id. This program allows the voters to see results at any time which may prevent consequences which opens the way for disruptive voting.

2.1 Existing problem

The voting system currently being used by the association is a paper-based system, in which the voter simply picks up ballot’s sheets from electoral officials, tick off who they would like to vote for, and then cast their votes by merely handing over the ballot sheet back to electoral official. The electoral officials gather all the votes being cast into a ballot box. At the end of the elections, the electoral officials converge and count the votes cast for each candidate and determine the winner of each election category.

2.2 References

1.Md. Maminul Islam, Md. Sharif Uddin Azad, Md.Asfaqul Alam, Nazmul Hassan, “Raspberry Pi and image processing based Electronic Voting Machine (EVM)”, 2014 International Journal of Scientific & Engineering Research, Volume 5, Issue 1, pp. 1506-1510, January-2014.

2. G. Keerthana, P. Priyanka, K. Alise Jenifer, R.Rajadharashini, Aruna Devi. P, “Impressive Smart Card Based Electronic Voting System”, 2015 IJRET: International Journal of Research in Engineering and Technology, Volume 4, Issue 3, pp. 284-288, March2015.

3. Ms.Ashwini Ashok Mandavkar, Prof. Rohini Vijay Agawane, “Mobile Based Facial Recognition Using OTP Verification for Voting System”, 2015 IEEE International Advance Computing Conference (IACC), pp.644-649, 2015

4. Shekhar Mishra, Y. Roja Peter, Zaheed Ahmed Khan M. Renuka, Abdul Wasay, S.V. Altaf, “Electronic Voting Machine using Biometric Finger Print with Aadhar Card Authentication”, 2017 International Journal of Engineering Science and Computing, Volume 7, Issue 3, pp. 5897-5899, March-2017.

5. L. Vetrivendan, Dr. R. Viswanathan, J. Angelin Blessy,“Smart Voting System Support through Face Recognition”, 2018 International Journal of Engineering Research in Computer Science and Engineering (IJERCSE) Vol 5, Issue 4, pp. 203-207, April-2018.

6. Gowtham R , Harsha K N, Manjunatha B, Girish H S ,Nithya Kumari R, “Smart Voting System”, 2019 International Journal of Engineering Research &Technology (IJERT), Volume 8 Issue 4, pp. 294-296, April-2019.

7. Ch. Chandra Mouli, M. Laasya Priya, J. Uttej, G. Pavan Sri Sai, DR. R. Vijay Kumar Reddy, “Smart Voting System”, 2020 International Journal for Innovative Engineering and Management Research”, Volume 9 Issue 9, pp. 115-119, Sept 2020.

2.3 Problem Statement Definition

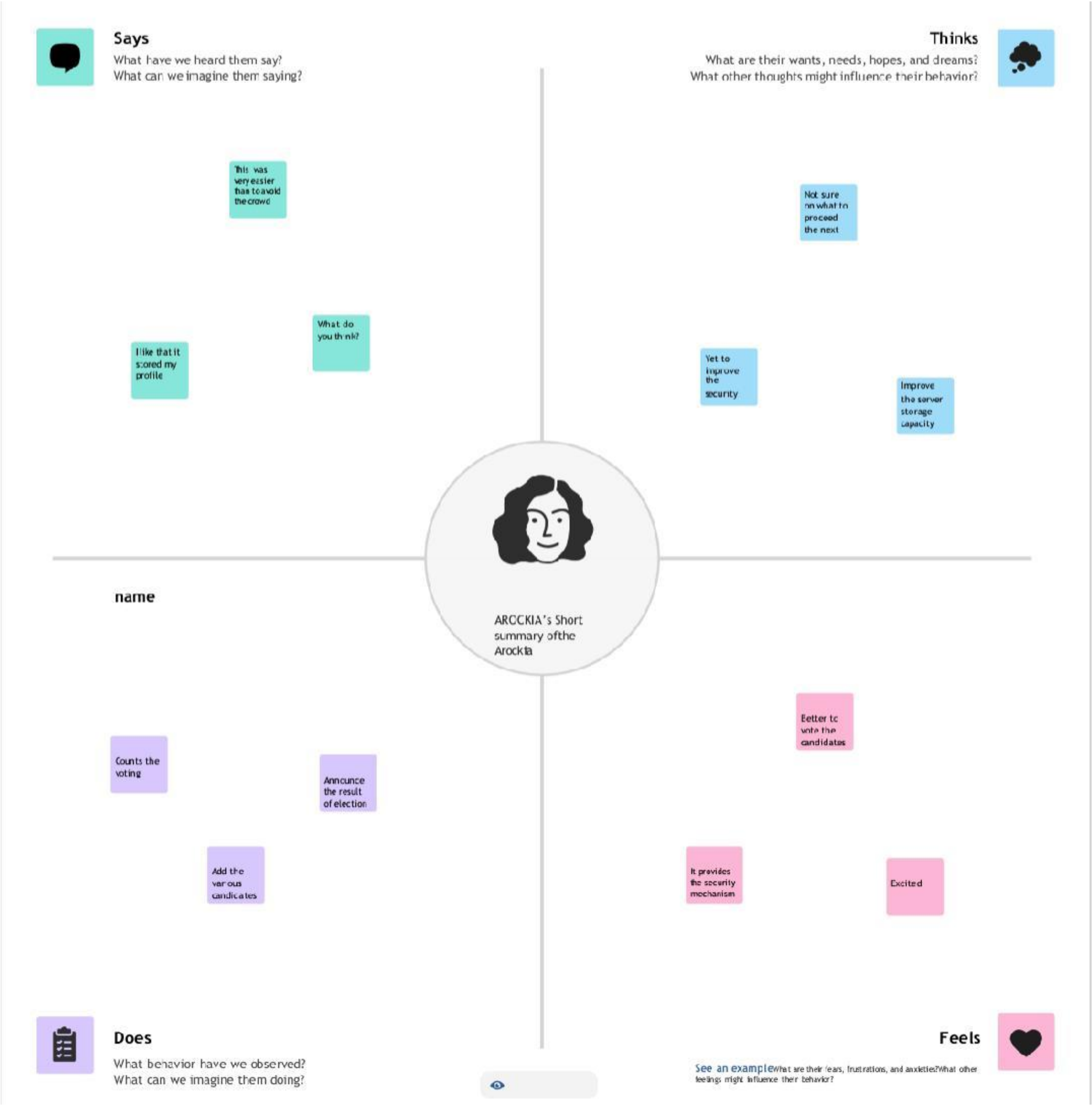
The existing voting systems often rely on paper-based or electronic methods that are susceptible to various issues, such as identity fraud, ballot tampering, and data breaches. To overcome these challenges, the project's primary objective is to develop a biometric security system that can enhance the security and accuracy of the voting process. The proposed system will leverage biometric data, such as fingerprint or facial recognition, for voter authentication.

Challenges to Address:

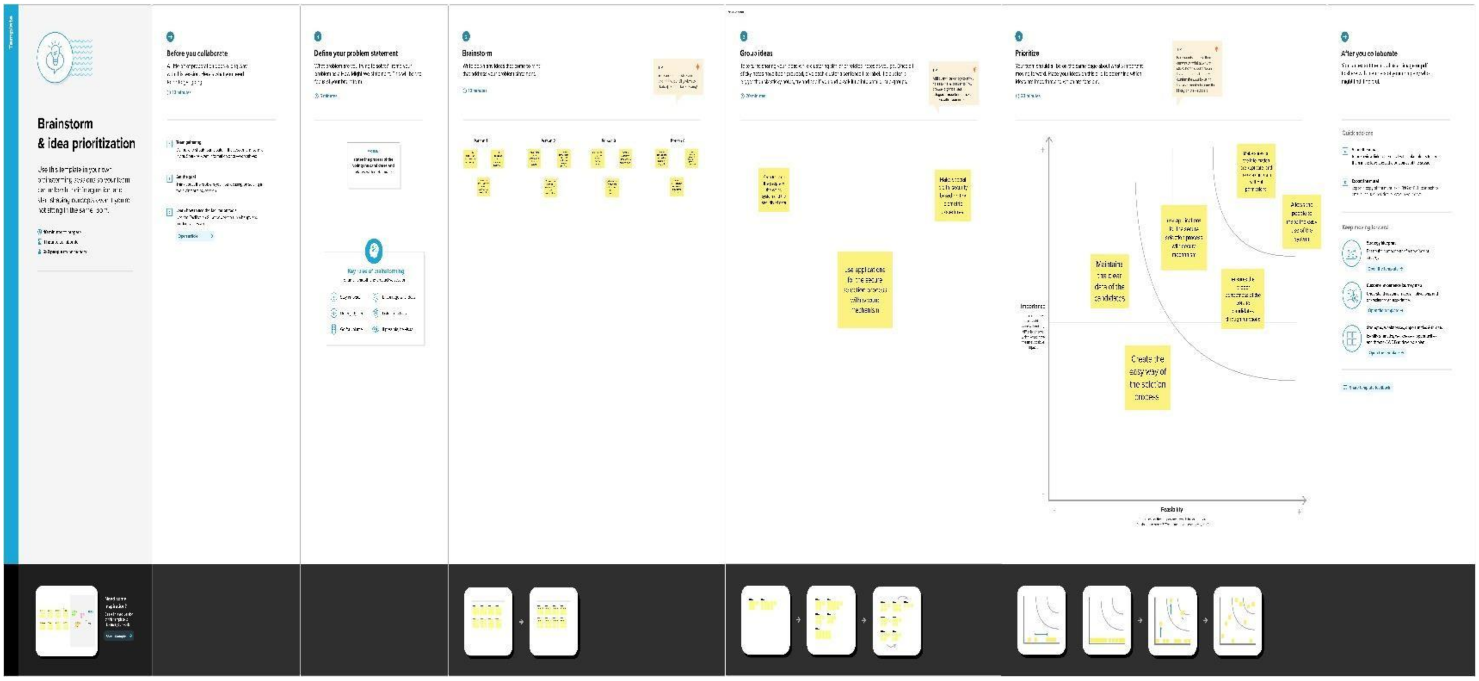
1. Voter Authentication: Developing a reliable method to authenticate voters using biometric data, ensuring that only eligible voters can participate in the election.
2. Data Privacy and Security: Ensuring the protection of biometric data, as well as the election data, against unauthorized access, hacking, or misuse.
3. System Accuracy: Ensuring that the biometric system is accurate, with a low false acceptance rate (FAR) and a low false rejection rate (FRR), to prevent both unauthorized access and legitimate voters from being denied.
4. Robustness Against Attacks: Developing mechanisms to defend against various forms of attacks, such as spoofing, replay attacks, and denial-of-service attacks.
5. Backup and Contingency Plans: Preparing for contingencies, such as network failures, equipment malfunctions, or other unexpected issues, to ensure the continuity of the voting process.

3. IDEATION & PROPOSED SOLUTION

3.1 Empathy Map Canvas


Says
What have we heard them say?
What can we imagine them saying?
This was very easier than to avoid the crowd
What do you think?
I like that it stored my profile
Thinks
What are their wants, needs, hopes, and dreams?
What other thoughts might influence their behavior?
Not sure on what to proceed the next
Yet to improve the security
Improve the server storage capacity
name
AROCKIA's Short summary ofthe Arockia
Counts the voting
Announce the result of election
Add the various candidates
Better to vote the candidates
It provides the security mechanism
Excited
Does
What behavior have we observed?
What can we imagine them doing?
Feels
See an exampleWhat are their fears, frustrations, and anxieties?What other feelings might influence their behavior?

3.2 Ideation & Brainstorming


Brainstorm
& idea prioritization
Before you collaborate
Define your problem statement
Brainstorm
Group ideas
Prioritize
After you collaborate
Key rules of brainstorming
Make a good data security based on the complete candidates
Use applications for the secure selection process with secure mechanism
Maintains the clear data of the candidates
Create the easy way of the selection process
Allows the people to make the data use of the system
Importance
Feasibility

REQUIREMENT ANALYSIS

4.1 Functional requirement

Designing a biometric security system for a voting platform is a complex task that involves ensuring the integrity, security, and fairness of the voting process. The functional requirements for such a system should cover various aspects of the voting process, from voter registration to ballot casting and result tabulation. Here are some functional requirements for a biometric security system for a voting platform:

Voter Registration:

- Registration process for eligible voters, including biometric data capture (fingerprint, facial recognition, etc.).
- Verification and validation of voter identity during registration.
- A secure database to store voter information and biometric data.

Voter Authentication:

- Biometric authentication of voters at polling stations.
- Voter ID verification using biometric data.
- Real-time validation of voter eligibility.

Ballot Casting:

- Secure and user-friendly interface for casting votes.
- Confirmation mechanisms to ensure voters cast their votes correctly.
- The ability to prevent multiple votes by the same individual.

4.2 Non-Functional requirements

Non-functional requirements for a biometric security system for a voting platform project are crucial for ensuring the system's overall performance, reliability, and security. Here are some non-functional requirements to consider:

Security:

- **Authentication Security:** The system should provide a high level of security to ensure that only eligible voters are allowed to cast their votes.
- **Data Encryption:** All data transmitted and stored should be encrypted to protect against unauthorized access.
- **Biometric Data Protection:** Biometric data should be securely stored and transmitted to prevent identity theft and fraud.
- **Redundancy:** The system should have redundancy and failover mechanisms to prevent service disruptions due to security breaches or technical failures.

Scalability:

- The system should be capable of handling a large number of concurrent users, especially during peak voting periods.
- It should scale easily to accommodate an increasing number of voters and polling locations.

Availability:

- The system should have high availability, ensuring that voters can access and use it at any time during the voting period.
- It should include backup and disaster recovery measures to ensure continued operation in case of system failures.

5. PROJECT DESIGN

5.1 DATA FLOW DIAGRAM

A two-dimensional diagram explains how data is processed and transferred in a system. The graphical depiction identifies each source of data and how it interacts with other data sources to reachcommon output. Individuals seeking to draft a data flow diagram must identify external inputs and outputs, determine how the inputs and outputs relate to each other, and explain with graphics how these connections relate and what they result in. This type of diagram helps business development and teams visualize how data is processed and identify or improve certain aspects.

LEVEL 0

The Level 0 DFD shows how the system is divided into 'sub-systems' (processes), each of which deals with one or more of the data flows to or from an external agent, and which together provide all of the functionality of the system as a whole. It also identifies internal data stores that must be presentin order for the system to do its job, and shows the flow of data between the various parts of the system.

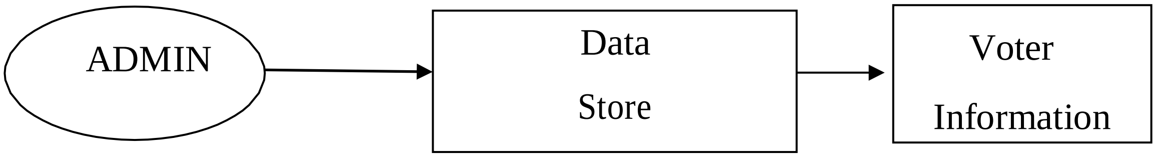


Figure No.5.1.1: Data Flow Diagram (level 0)

LEVEL 1

The next stage is to create the Level 1 Data Flow Diagram. This highlights the main functions carried out by the system. As a rule, to describe the system was using between two and seven functions two being a simple system and seven being a complicated system. This enables us to keep the model manageable on screen or paper.

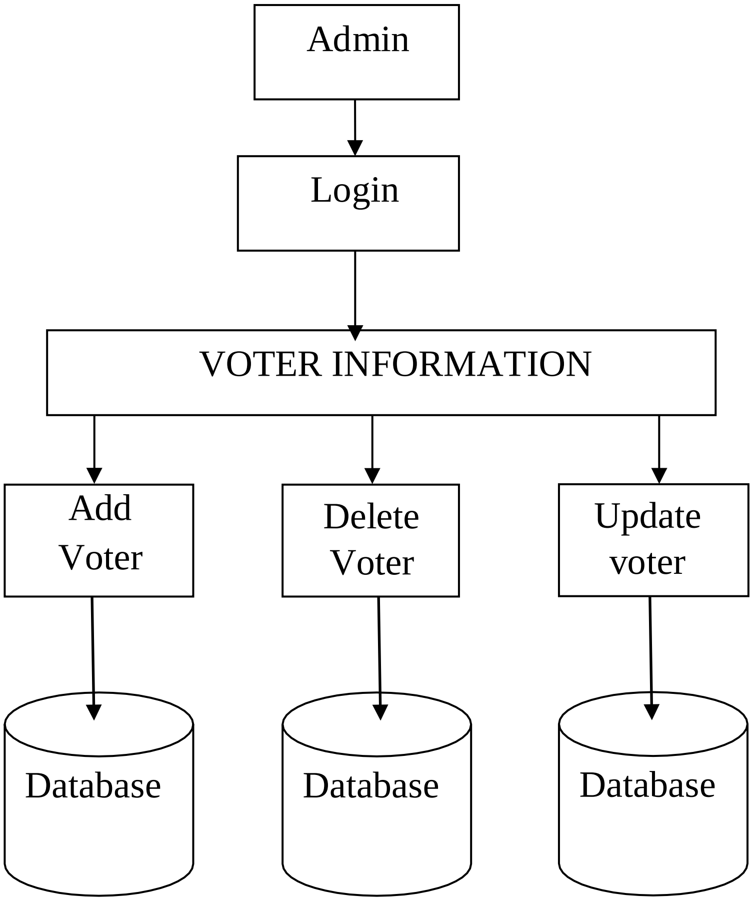
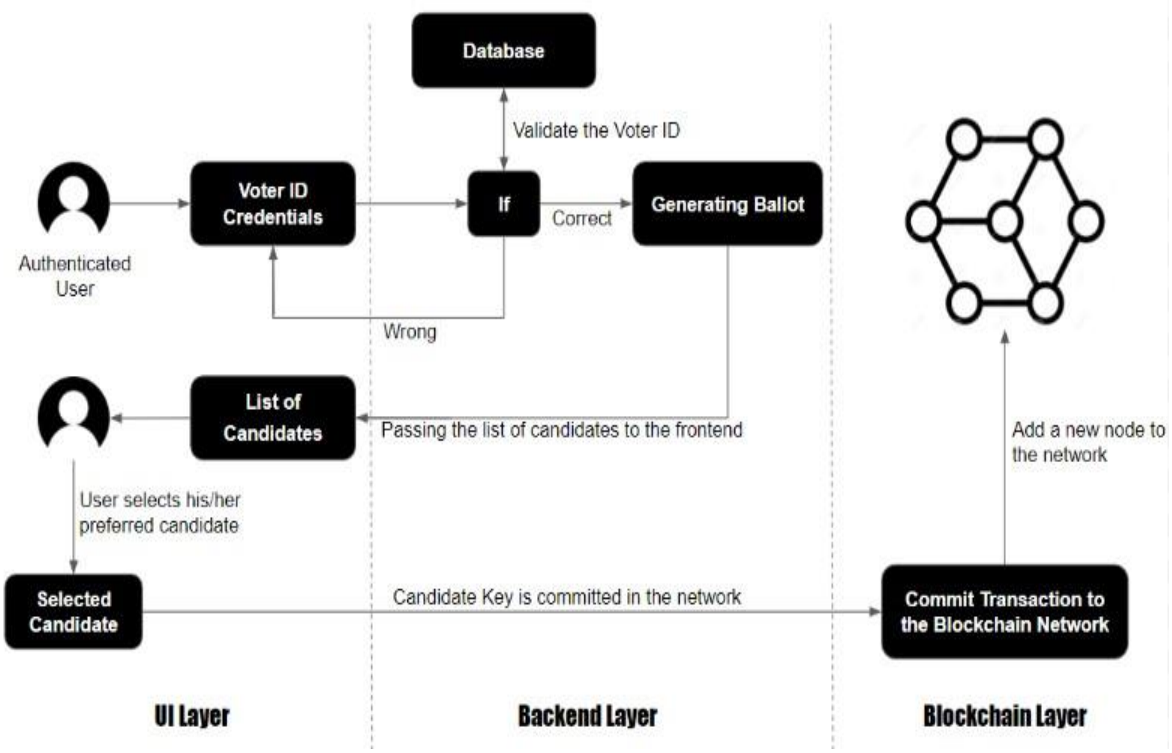


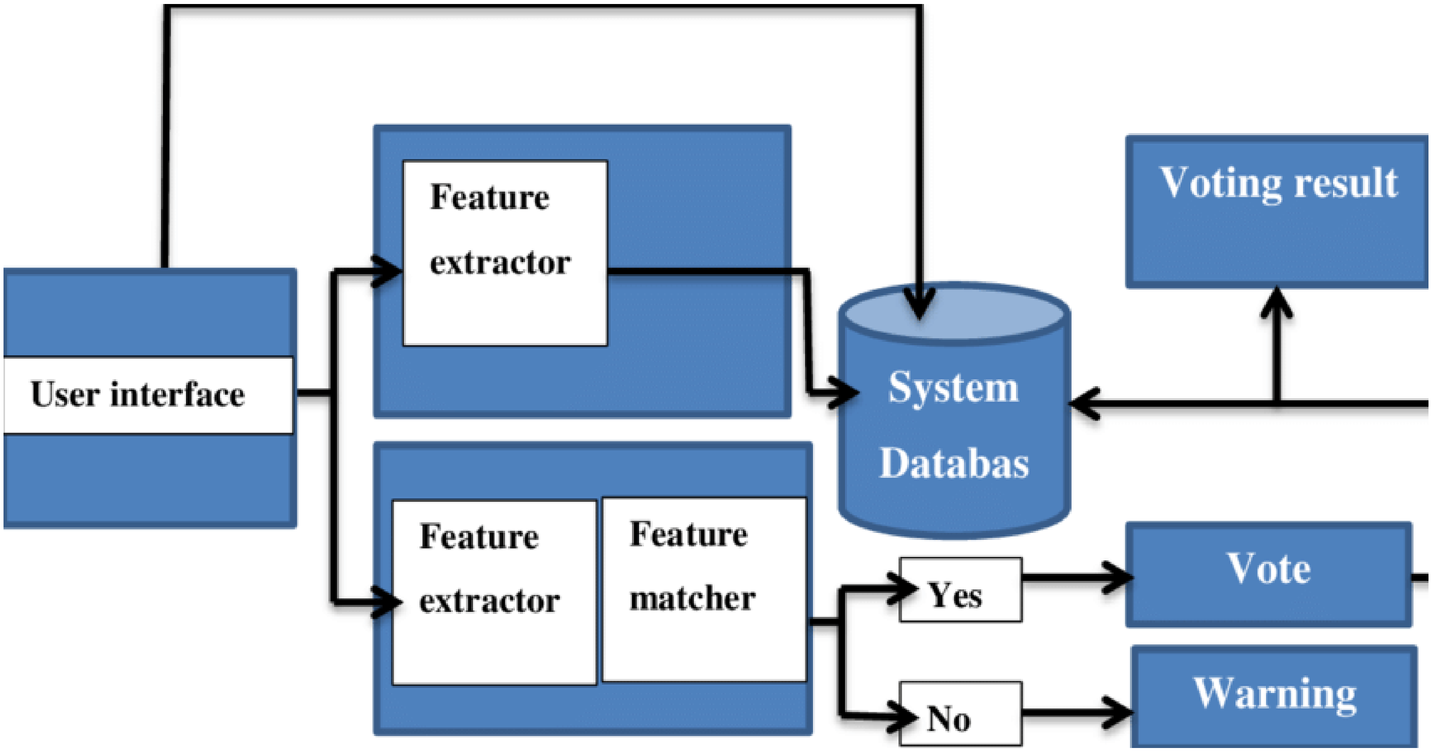
Figure No.5.1.2: Data Flow Diagram (Level 1)

5.2 Solution Architecture

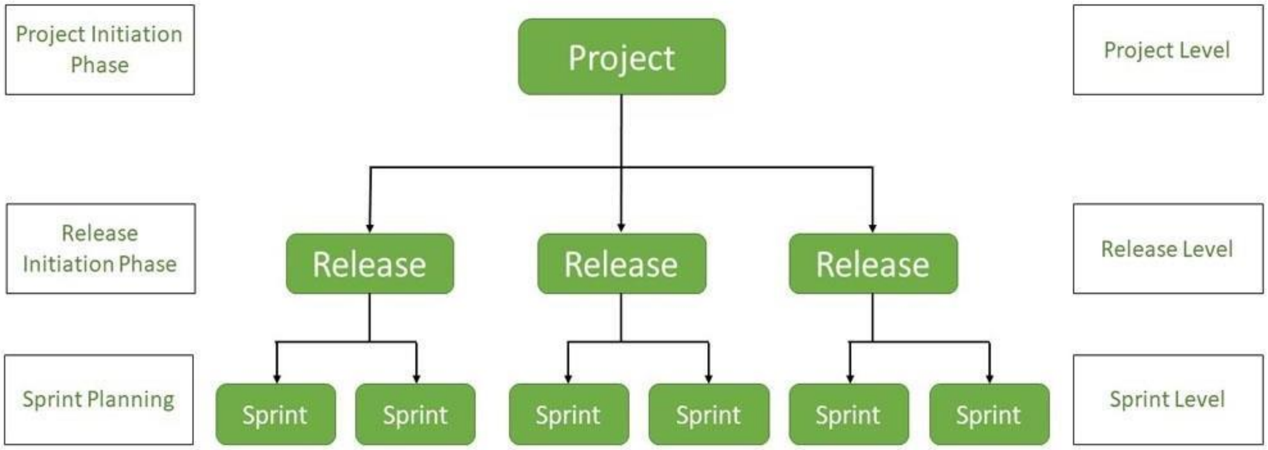

Database
Validate the Voter ID
Authenticated User
Voter ID Credentials
If
Correct
Generating Ballot
Wrong
List of Candidates
Passing the list of candidates to the frontend
Add a new node to the network
User selects his/her preferred candidate
Selected Candidate
Candidate Key is committed in the network
Commit Transaction to the Blockchain Network
UI Layer
Backend Layer
Blockchain Layer

6. PROJECT PLANNING & SCHEDULING

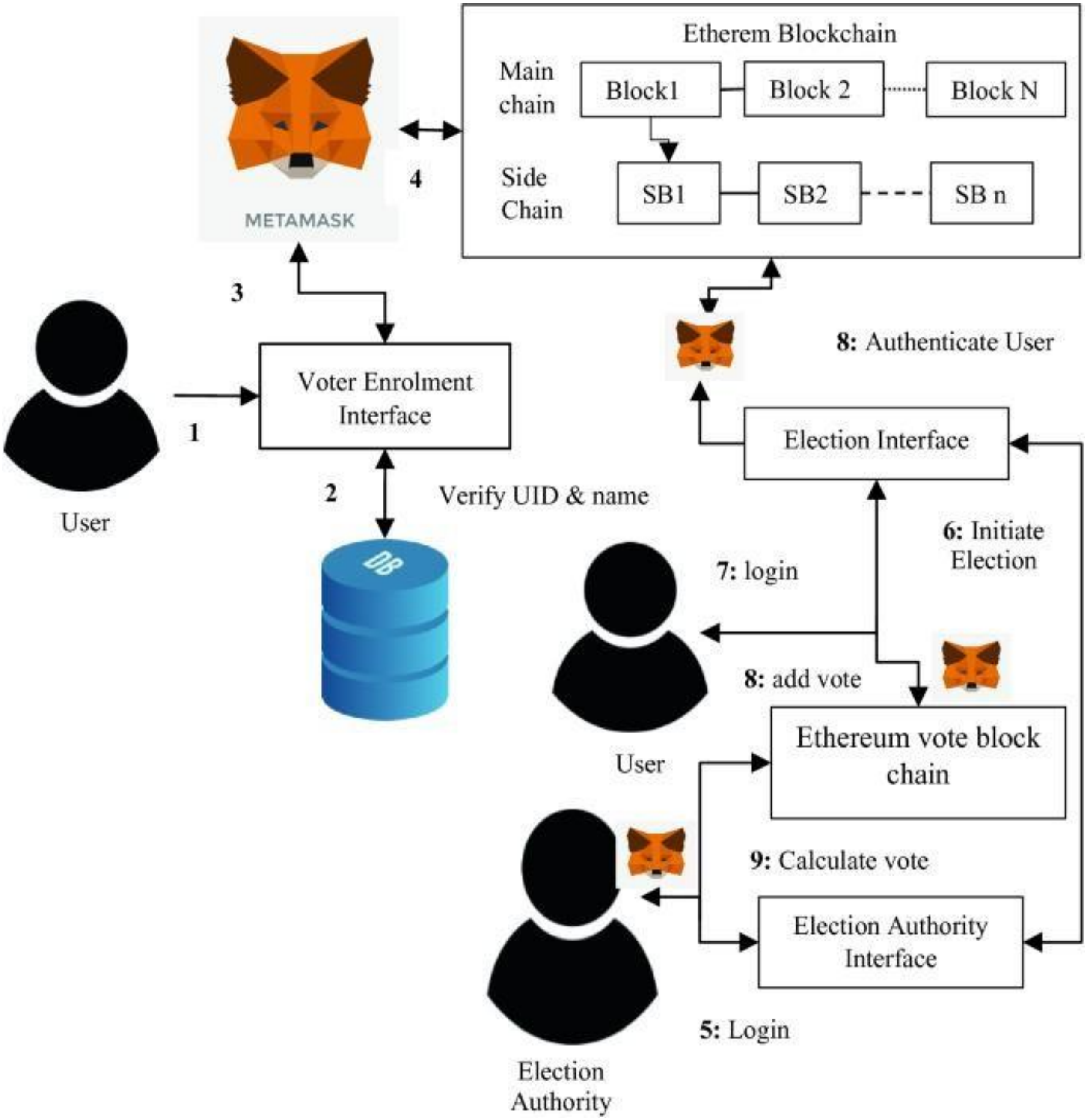
6.1 Technical Architecture



6.2 Sprint Planning & Estimation



6.3 Sprint Delivery Schedule



7. CODING & SOLUTIONING

7.1 Feature1

A biometric security system for a voting platform project is designed to enhance the security and integrity of the voting process by verifying the identity of voters using unique physiological or behavioral characteristics. Here are some key features of such a system:

Biometric Enrollment:

Voter registration process involves capturing and storing biometric data (e.g., fingerprints, iris scans, facial recognition) of eligible voters.

Ensure secure storage and encryption of biometric templates to protect against data breaches.

Biometric Verification:

Voters are required to authenticate themselves using their biometric data at the polling station.

Real-time verification compares the presented biometric data with the enrolled templates to confirm the voter's identity.

Multi-Modal Biometrics:

Support multiple biometric modalities to increase accuracy and accommodate voters with disabilities or conditions that may affect certain biometrics.

7.2 Feature 2

Data Privacy and Protection:

Strict data privacy measures to ensure that biometric data is not misused or accessed by unauthorized personnel.

Compliance with data protection regulations and encryption protocols.

Voter Database Management:

Centralized database management to update and maintain voter records, ensuring accuracy and eliminating duplicate entries.

Anti-Spoofing Measures:

Implement anti-spoofing mechanisms to detect fraudulent attempts to use fake biometric data, such as liveness detection.

Audit Trail:

Maintain an audit trail of all biometric verifications for transparency and accountability.

Redundancy and Fail-Safe Mechanisms:

Implement backup systems to ensure the continuity of the voting process in case of system failures or biometric authentication issues.

Secure Transmission:

Ensure that biometric data is securely transmitted between polling stations and the central database to prevent interception or tampering.

Accessibility:

Provide accommodations for individuals with disabilities, ensuring that the biometric system is accessible to all eligible voters.

7.3 Database Schema

1. Users Table

user_id (Primary Key): Unique identifier for each user.

username: User's username for login.

password: User's password (hashed and salted).

email: User's email address.

role: User's role (e.g., voter, administrator, etc.).

2. Voters Table

voter_id (Primary Key): Unique identifier for each registered voter.

user_id (Foreign Key): References the Users table.

full_name: Full name of the voter.

date_of_birth: Voter's date of birth.

national_id: Voter's national ID or passport number.

biometric_data: Storage for biometric data

3. Elections Table

election_id (Primary Key): Unique identifier for each election.

start_date: Date and time when the election starts.

end_date: Date and time when the election ends.

description: A brief description of the election.

4. Candidates Table

candidate_id (Primary Key): Unique identifier for each candidate.

election_id (Foreign Key): References the Elections table.

full_name: Full name of the candidate.

party_affiliation: The political party the candidate represents.

position: The candidate's position in the election (e.g., presidential, senatorial).

5. Votes Table

vote_id (Primary Key): Unique identifier for each vote cast.

voter_id (Foreign Key): References the Voters table.

election_id (Foreign Key): References the Elections table.

candidate_id (Foreign Key): References the Candidates table.

vote_time: Timestamp when the vote was cast.

6. BiometricLogs Table

log_id (Primary Key): Unique identifier for each biometric log entry.

voter_id (Foreign Key): References the Voters table.

timestamp: Timestamp when the biometric data was captured.

biometric_type: Type of biometric data (e.g., fingerprint, facial recognition).

device_id: Identifier for the biometric capture device.

7. AuditLogs Table

log_id (Primary Key): Unique identifier for each audit log entry.

user_id (Foreign Key): References the Users table.

action: Description of the action performed (e.g., login, logout, data modification).

timestamp: Timestamp when the action occurred.

8. PERFORMANCE TESTING

8.1 Performance Metrics

When developing a biometric security system for a voting platform project, it's important to establish performance metrics to ensure the system's reliability, security, and usability. Here are some key performance metrics to consider:

False Acceptance Rate (FAR):

FAR measures the percentage of unauthorized users who are incorrectly granted access. In the context of voting, this would indicate the percentage of fraudulent votes that go undetected.

False Rejection Rate (FRR):

FRR measures the percentage of authorized users who are incorrectly denied access. In a voting system, this would indicate the percentage of legitimate voters who face difficulties with the biometric authentication.

Equal Error Rate (EER):

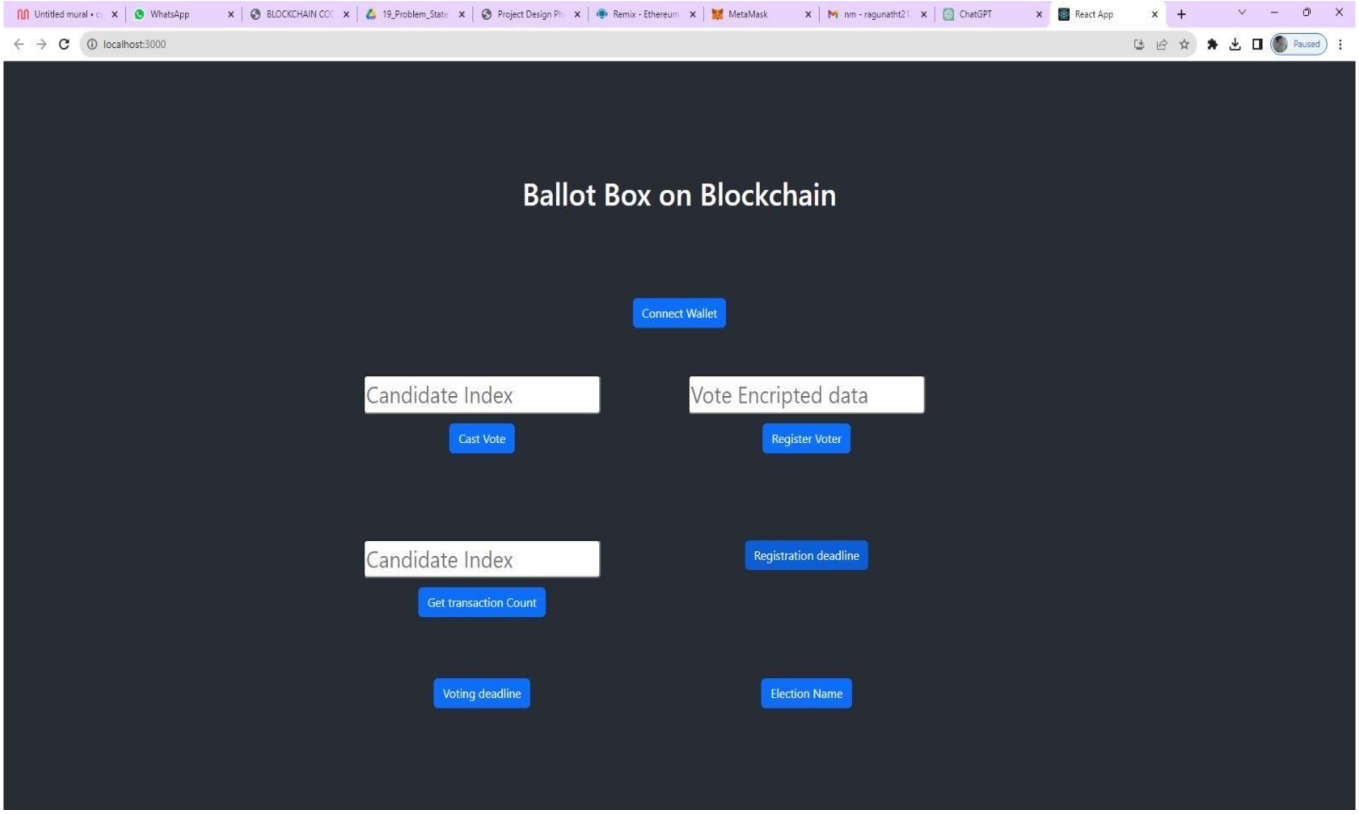
EER is the point at which the FAR and FRR are equal. This is a critical metric for balancing security and usability.

Accuracy:

This is a more straightforward measure of the system's correctness, calculated as the ratio of the number of correct authentications to the total number of authentication attempts.

9. RESULTS

9.1 Output Screenshot



10. ADVANTAGES & DISADVANTAGES

Advantages:

Implementing a biometric security system in a voting platform project can offer several advantages. Biometric authentication relies on unique physical or behavioral characteristics of an individual to verify their identity. Here are some advantages of using biometric security in a voting platform:

Enhanced Security:

Biometric data is highly unique and difficult to fake, making it a robust security measure against impersonation and voter fraud.

Reduced Voter Fraud:

Biometric authentication helps prevent multiple voting by the same person or individuals assuming false identities.

Accuracy and Reliability:

Biometric systems are highly accurate, reducing the risk of errors and ensuring that only eligible voters can cast their ballots.

Increased Trust:

The use of biometrics can enhance public trust in the voting process, as it provides a transparent and secure way to verify voter identities.

Prevention of Voter Suppression:

Biometric systems can help prevent voter suppression tactics, as eligible voters are less likely to be turned away or denied the right to vote.

Convenience:

Biometric authentication can streamline the voting process by eliminating the need for physical ID cards or paper-based verification methods.

Faster Voting Process:

Biometric systems can speed up the voting process, reducing wait times at polling stations and improving overall efficiency.

Accessibility:

Biometric systems can be designed to accommodate individuals with disabilities, ensuring inclusivity in the voting process.

Tamper Resistance:

Biometric data is difficult to tamper with, reducing the risk of data manipulation or interference with the voting system.

Audit Trail:

Biometric systems can provide an audit trail of who voted and when, improving transparency and accountability in the electoral process.

Disadvantages:

While a biometric security system for a voting platform may seem appealing, it also comes with several disadvantages and challenges that need to be carefully considered. Some of the key disadvantages include:

Privacy Concerns:

Biometric data is highly sensitive, and its collection and storage raise significant privacy concerns. Citizens may be uncomfortable with their biometric information being stored in a government database, as it can be vulnerable to misuse or data breaches.

Vulnerability to Hacking:

Biometric data can be stolen or hacked, just like any other form of data. If biometric data is compromised, it can have long-lasting consequences for individuals, as it is not easy to change or replace biometric characteristics like fingerprints or irises.

False Positives and Negatives:

Biometric systems are not infallible and can produce false positives (granting access to an unauthorized individual) or false negatives (denying access to an authorized individual). This can result from factors such as poor image quality, variations in biometric traits, or hardware limitations.

Technical Challenges:

Implementing a biometric system for voting requires robust technology infrastructure, including high-quality scanners, databases, and specialized software. These systems are costly to set up and maintain.

Inclusivity and Accessibility:

Biometric systems may not work well for all individuals, including those with disabilities or certain medical conditions. It's essential to ensure that the voting system remains inclusive and accessible to all citizens.

Enrollment Challenges:

Enrolling citizens into the biometric system can be a time-consuming and resource-intensive process. Not all citizens may have access to enrollment centers, especially in remote areas, which can lead to unequal access to voting.

Long Lines and Delays:

Biometric verification can slow down the voting process, as it requires additional steps for authentication. This can lead to long lines at polling stations and discourage voter participation.

Legal and Ethical Issues:

The use of biometric data in voting systems can raise legal and ethical questions regarding consent, data ownership, and the right to anonymity. Developing a legal framework for biometric voting can be complex and contentious.

Maintenance and Upkeep:

Biometric systems require regular maintenance and updates to remain secure and accurate. This adds ongoing costs and logistical challenges to the voting platform.

Cost:

Implementing biometric security systems can be expensive, requiring significant financial resources for both initial setup and ongoing maintenance.

11. CONCLUSION

The implementation of a biometric security system for a voting platform is a significant advancement in ensuring the integrity and trustworthiness of the electoral process. This project has aimed to address the following objectives: enhancing security, increasing accessibility, and improving overall transparency in the voting process.

The introduction of biometric authentication in a voting platform offers several advantages. It reduces the risk of identity fraud, as it is considerably more challenging to fake biometric information compared to traditional identification methods. This results in a more secure and tamper-proof voting system, which is essential for upholding the democratic process.

Additionally, the incorporation of biometrics can enhance the accessibility of the voting platform. It can make it easier for individuals with disabilities to participate in the electoral process, as the technology can be adapted to accommodate a range of physical impairments. This inclusive approach is essential for ensuring that every eligible citizen can exercise their right to vote.

Despite the potential benefits, it's crucial to consider some challenges associated with biometric voting systems. Privacy concerns must be addressed, as the collection and storage of biometric data raise important ethical and legal questions. Safeguards, including stringent data protection measures and secure storage protocols, must be in place to mitigate these concerns.

12. FUTURE SCOPE

Implementing a biometric security system for a voting platform is a significant step towards enhancing the security and integrity of elections. This project has a wide range of potential future scopes and implications. Here are some key points to consider:

Improved Security: Biometric authentication can help in ensuring that only eligible voters participate in elections. Future developments could focus on refining biometric algorithms, making them even more secure and tamper-resistant.

Reducing Voter Fraud: The system can help reduce voter fraud, such as multiple voting or impersonation. Ongoing developments could focus on further reducing these risks.

Enhanced Accessibility: Future versions of the system could incorporate accessibility features to make it inclusive for people with disabilities. This could involve voice recognition or other accessible biometric modalities.

13. APPENDIX

Source Code

```
import React, { useState } from "react";
import { Button, Container, Row, Col } from 'react-bootstrap';
import 'bootstrap/dist/css/bootstrap.min.css';
import { contract } from "./connector";

function Home() {
  const [Wallet, setWallet] = useState("");

  const [CandidateIndex, setCandidateIndex] = useState("");

  const [VoterData, setVoterData] = useState("");

  const [CandidateIndexed, setCandidateIndexed] = useState("");

  const [CandidatesData, setCandidatesData] = useState("");

  const [RegDeadline, setRegDeadlne] = useState("");

  const [VoteDeadlne, setVoteDeadlne] = useState("");

  const [Election, setElection] = useState("");



  const handleCandidateIndex = (e) => {
    setCandidateIndex(e.target.value)
  }

  const handleCastVote = async () => {
    try {
      let tx = await contract.castVote(CandidateIndex.toString())

      let wait = await tx.wait()
      console.log(wait);
      alert(wait.transactionHash)
    } catch (error) {
```

```
    alert(error)
  }
}

const handleVoterBiometricData = (e) => {
  setVoterData(e.target.value)
}


const handleRegisterVoter = async () => {
  try {
    let tx = await contract.registerVoter(VoterData)
    let wait = await tx.wait()
    console.log(wait)
    alert(wait.transactionHash)

  } catch (error) {
    alert(error)
  }
}

const handleCandidateIndexs = (e) => {
  setCandidateIndexed(e.target.value)
}

const handleCandidate = async () => {
  try {
    let tx = await contract.candidates(CandidateIndexed.toString())
    setCandidatesData(tx)
    console.log(tx);
    // alert(wait.transactionHash)
  } catch (error) {
    alert(error)
  }
}

const handleRegdeadline = async () => {
  try {
    let tx = await contract.registrationDeadline()
    setRegDeadlne(tx)
    console.log(tx);
    // alert(wait.transactionHash)
  } catch (error) {
    alert(error)
  }
}

const handleVoteDeadline = async () => {
  try {
    let tx = await contract.votingDeadline()
    setVoteDeadlne(tx)
    console.log(tx);
    // alert(wait.transactionHash)
  } catch (error) {
    alert(error)
  }
}

const handleElecName = async () => {
  try {
    let tx = await contract.electionName()
    setElection(tx)
    console.log(tx);
    // alert(wait.transactionHash)
  } catch (error) {
    alert(error)
  }
}


const handleWallet = async () => {
  if (!window.ethereum) {
    return alert('please install metamask');
  }

  const addr = await window.ethereum.request({
    method: 'eth_requestAccounts',
  });

  setWallet(addr[0])
```

```
   }

 return (
  <div>
   <h1 style={{ marginTop: "30px", marginBottom: "80px" }}>Ballot Box on
Blockchain</h1>
      {!Wallet ?

         <Button onClick={handleWallet} style={{ marginTop: "30px", marginBottom: "50px"
}}>Connect Wallet </Button>
         :
         <p style={{ width: "250px", height: "50px", margin: "auto", marginBottom: "50px",
border: '2px solid #2096f3' }}>{Wallet.slice(0, 6)}. ..{Wallet.slice(-6)}</p>
      }
   <Container>
    <Row>


     <Col style={{marginRight:"100px"}}>
      <div>

      <input style={{ marginTop: "10px", borderRadius: "5px" }}
onChange={handleCandidateIndex} type="number" placeholder="Candidate Index"
value={CandidateIndex} /> <br />
      <Button onClick={handleCastVote} style={{ marginTop: "10px" }}
variant="primary">Cast Vote</Button>

      </div>
     </Col>

      <Col style={{ marginRight: "100px" }}>
        <div>
          <input style={{ marginTop: "10px", borderRadius: "5px" }}
onChange={handleVoterBiometricData} type="string" placeholder="Vote Encripted data"
value={VoterData} /> <br />
          <Button onClick={handleRegisterVoter} style={{ marginTop: "10px" }}
variant="primary">Register Voter</Button>

        </div>
      </Col>


   </Row>
   <Row style={{marginTop:"100px"}}>
              <Col style={{ marginRight: "100px" }}>
                 <div>
                  <input style={{ marginTop: "10px", borderRadius: "5px" }}
onChange={handleCandidateIndexs} type="number" placeholder="Candidate Index"
value={CandidateIndexed} /> <br />
                    <Button onClick={handleCandidate} style={{ marginTop: "10px" }}
variant="primary"> Get transaction Count</Button>
                  {CandidatesData ? CandidatesData?.map(e => <p>{e.toString()}</p>) : <p></p>
                    }
                 </div>
              </Col>

              <Col style={{ marginRight: "100px" }}>
                 <div>
                  <Button onClick={handleRegdeadline} style={{ marginTop: "10px" }}
variant="primary">Registration deadline</Button>
                  {RegDeadline ? <p>{RegDeadline.toString()}</p> : <p></p>}


                 </div>
              </Col>

       </Row>
          <Row style={{ marginTop: "50px" }}>
            <Col style={{ marginRight: "100px" }}>
               <div>
                  <Button onClick={handleVoteDeadline} style={{ marginTop: "10px" }}
variant="primary">Voting deadline</Button>
                  {VoteDeadlne ? <p>{VoteDeadlne.toString()}</p> : <p></p>}

               </div>
            </Col>

            <Col style={{ marginRight: "100px" }}>
               <div>
            <Button onClick={handleElecName} style={{ marginTop: "10px" }} variant="primary">Election Name</Button>
            {Election ? <p>{Election.toString()}</p> : <p></p>}

          </div>
        </Col>
  </Row>
  </Container>

 </div>
 )
}

export default Home;
```

GitHub Link:

https://github.com/au8146814620105305/Project-Name-BIOMETRIC-SECURITY-FOR-VOTING-PLATFORM.git

Project Demo Link:

https://youtu.be/HXdrYYrFydQ?si=VrsGwNU-AHwb7Ydo