### NAAN MUDHALVAN - GUIDED PROJECT DOCUMENTATION

**PROJECT TITLE: Biometric Security System for Voting Platform**

**TEAM**

**NAME:** Raghul V

**ROLL NO.:** 2020301030

**NAAN MUDHALVAN ID:** 78A4F5B26FEC85EBBB14C981E2C5C8AB

**NAME:** Sagari C

**ROLL NO:** 2020301031

**NAAN MUDHALVAN ID:** 20014FEC1C056CDBE4B4BB6E1DAA17F1

**NAME:** Sayid Zafirah A

**ROLL NO:** 2020301032

**NAAN MUDHALVAN ID:** D63E95465794E53BFCF46D96CFFE6EB3

**NAME:** Shivani S

**ROLL NO:** 2020301033

**NAAN MUDHALVAN ID:** 8BE123DC0388E64A508491F8B84AEEA7

**SEMESTER:** 7

**COLLEGE:** Alagappa College of Technology, Anna University

1. **INTRODUCTION:**

1.1 PROJECT OVERVIEW:

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. Online voting is a rising trend that reduces costs and boosts voter participation. It relies on the internet, but security concerns persist. Blockchain technology offers a decentralized solution with end-to-end verification, enhancing security. This article examines block chain-based voting, highlighting its potential to address electoral system issues. Yet, privacy and transaction speed challenges must be tackled for sustainable implementation. Improvements are needed for block chain-based voting systems to become a viable choice.

1.2: PURPOSE:

The purpose of this project is to investigate the potential of blockchain technology in revolutionizing electronic voting systems. We aim to examine the current state of blockchain-based voting research and online voting systems, as well as the associated challenges, with a view toward predicting future developments.

This research seeks to provide a conceptual framework for implementing block chain in electronic voting, emphasizing its fundamental structure and characteristics in enhancing the security and trustworthiness of the electoral process. By doing so, we aspire to contribute to the ongoing efforts to address the critical issues that plague conventional election systems, such as security, transparency, and accessibility, with the goal of advancing the development of a reliable and secure blockchain-based electronic voting system that can inspire confidence and reshape the way societies conduct their elections.

1. **LITERATURE SURVEY**

2.1: EXISTING PROBLEM:

Storing sensitive biometric data, such as fingerprints or iris scans, raises privacy issues. If not adequately protected, this data can be susceptible to theft or misuse. Biometric data can be hacked or spoofed. Fingerprint or facial recognition systems, for instance, can be tricked with high-quality replicas or manipulated images.Biometric systems may not be accessible to all. Some individuals, such as the elderly or disabled, may encounter difficulties with the technology, potentially leading to disenfranchisement. Implementing and maintaining biometric voting systems can be expensive. This cost can be a significant barrier, particularly in regions with limited resources. Biometric systems require a high level of technical infrastructure, which may not be readily available in all areas.

Power outages, connectivity issues, or system failures can disrupt the voting process.The accuracy and security of voter databases storing biometric data are critical. Errors or vulnerabilities in these databases can jeopardize the voting system's integrity. The use of biometric data in voting may raise legal and ethical issues, such as consent, data ownership, and potential misuse.Integrating biometric systems into existing voting infrastructure can be a complex and time-consuming process, requiring extensive training for election officials and voters. Building trust in biometric voting systems is a significant challenge. Voters and election authorities need to have confidence in the technology's accuracy and security. To ensure the continuity of the voting process, backup mechanisms must be in place in case the biometric system fails or faces issues.

2.2: REFERENCES:

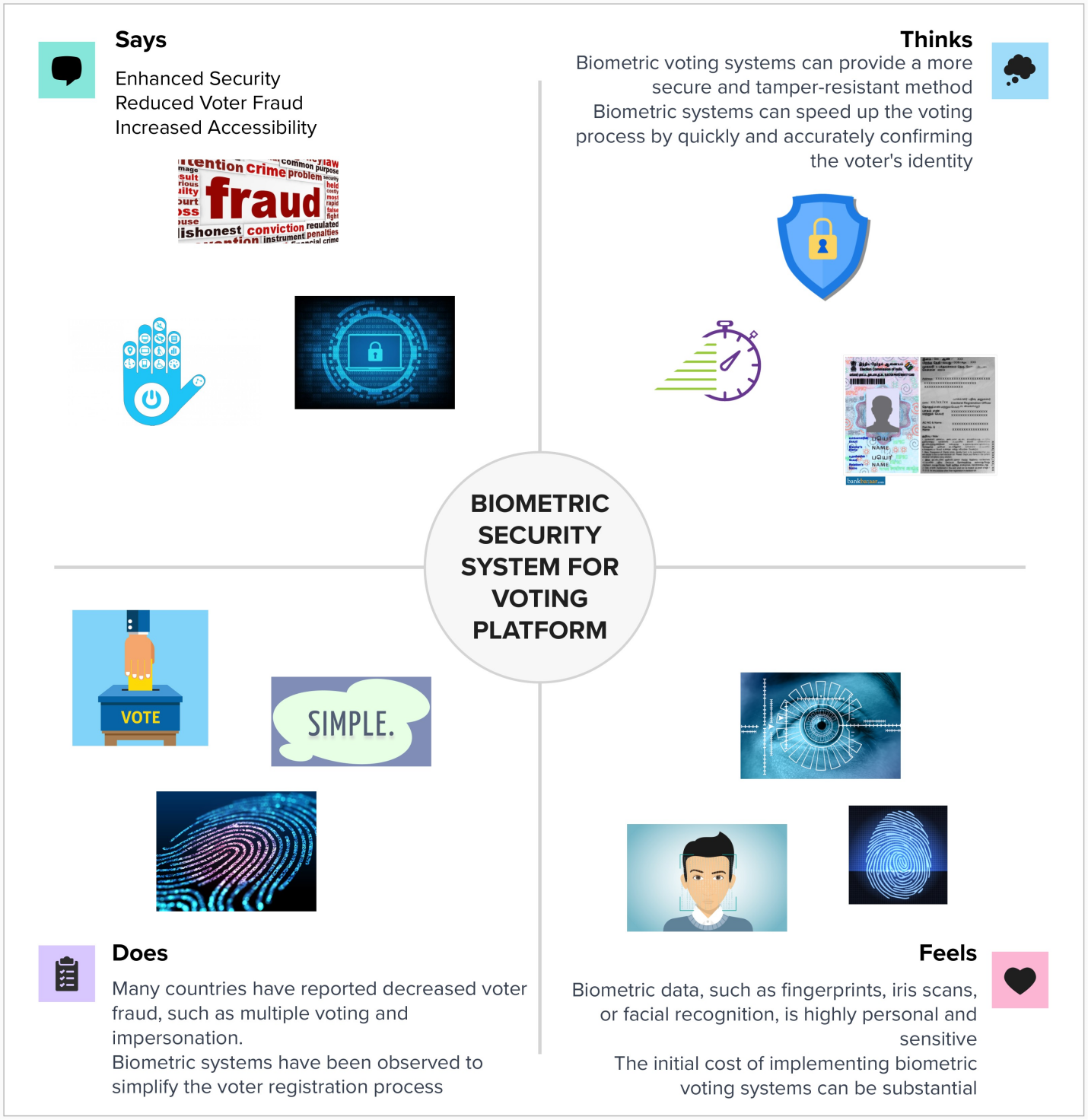
|  |  |  |
| --- | --- | --- |
| **S. No.** | **Literature** | **Author** |
| **1** | Study on security of online voting system using Biometrics and Steganography | Neha Gandhi |
| **2** | Block chain and Finger Print enabled E-Voting | Aravind P, Gokul Raj  “et al.”, |
| **3** | Study of Biometric Voting System | Parikshit Martolia , Pragati Bhojak, Shena Bisht “et al.”, |
| **4** | Biometric identification in Electronic Voting Systems | Eduardo Ibanez, Nicolas Galdamez, Cesar Estrebou “et al.”, |
| **5** | E-Voting Using Block Chain with Biometric Authentication | Sunita Suralkar, Sanjay Udasi ,Sumit Gagnani, “et al.”, |

2.3: PROBLEM STATEMENT DEFINITION:

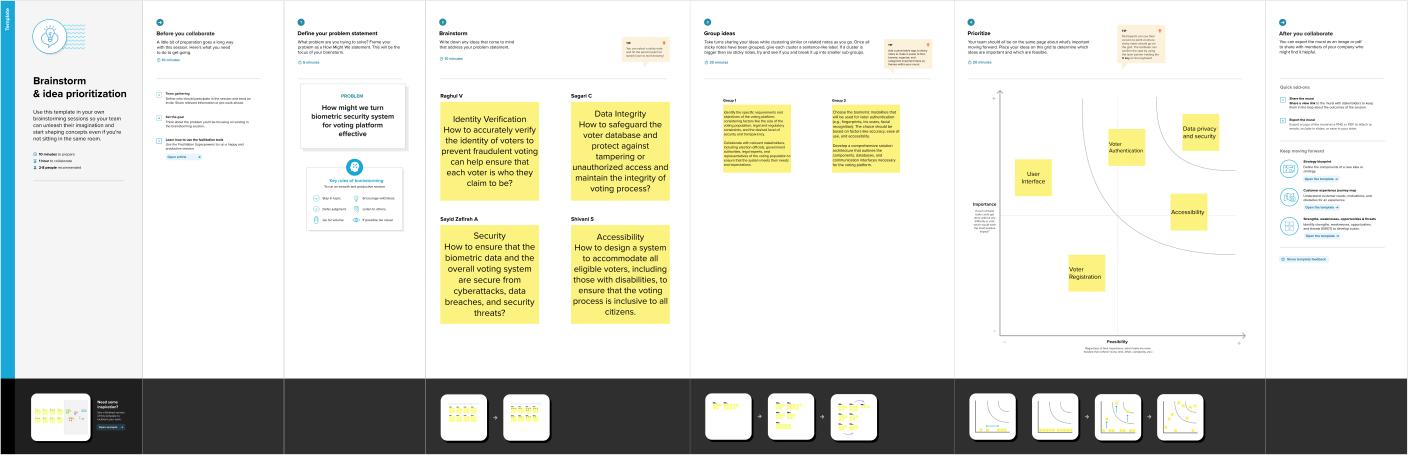
The business requirements for a Block chain Biometric System encompass the need for a highly secure and privacy-focused solution. Key elements include ensuring the robust protection of biometric data against breaches and unauthorized access, strict compliance with data protection regulations, and the development of accurate and reliable biometric authentication methods. Additionally, the system should empower users with control over their data through smart contracts, promote interoperability with other systems, maintain transparent audit trails, and be scalable to accommodate increasing user volumes. Compliance with relevant regulations and cost-effective operation are also vital to creating a trusted and efficient blockchain biometric system.

1. **IDEATION AND PROPOSED SOLUTION:**

3.1: EMPATHY MAP CANVAS



3.2: IDEATION AND BRAINSTROMING:



1. **REQUIRMENT ANALYSIS:**

4.1: FUNCTIONAL REQUIREMENTS:

The system must authenticate voters through biometric data (e.g., fingerprints, facial recognition) to ensure their eligibility to vote.Voters must be able to register their biometric data securely before an election.The system should allow voters to cast their votes electronically using their biometric identifiers. Voters must receive confirmation of their vote after casting it, which includes details of their selections.Biometric data and voting records must be securely stored using encryption and decentralized methods.The system should support multiple biometric identifiers (e.g., fingerprints, facial recognition) for added security.The system must provide accessibility features for voters with disabilities, including audio prompts and braille interfaces.Election authorities should have real-time monitoring capabilities to ensure the system's integrity and respond to any irregularities. The system should generate an audit trail of all voting activities for verification and auditing purposes. The system should provide voters with information about the candidates and issues on the ballot.

4.2: NON-FUNCTIONAL REQUIREMENTS:

The system must meet the highest standards of security, protecting biometric data and voting records from unauthorized access or tampering.Biometric data should be stored and processed with strict privacy measures to safeguard voters' sensitive information. The system should be highly reliable, with minimal downtime and robust backup systems in place. The response time of the system must be quick to ensure efficient voting processes. The system must adhere to all relevant legal and regulatory requirements for biometric data use and voting processes. The system should be capable of integrating with other election management systems and government databases Election officials and voters should receive adequate training and support to use the system effectively. The system should provide transparent mechanisms for voters to verify their votes and for authorities to audit the process, ensuring trust in the system's integrity.

**5. PROJECT DESIGN:**

5.1: DATA FLOW DIAGRAMS

CHARECTERISTICS OF BIOMETRIC SECURITY SYSTEM FOR VOTING PLATFORM

A biometric security system for a voting platform should have specific characteristics to ensure the integrity and security of the voting process. Here are some important characteristics:

1. Unique Identification: Biometric systems should use unique biometric traits such as fingerprints, iris scans, or facial recognition to identify and authenticate voters. This uniqueness helps ensure that each individual can only vote once.

2. Accuracy and Reliability: The system must be highly accurate and reliable in recognizing and verifying biometric data to prevent fraudulent attempts to vote or unauthorized access.

3. Data Protection: Biometric data must be securely stored and encrypted to protect it from unauthorized access, hacking, or data breaches.

4. User Privacy: A balance between security and privacy is crucial. The system should adhere to privacy regulations and ensure that the biometric data is used only for the purpose of voter authentication.

5. Non-repudiation: Biometric data should provide a strong level of non-repudiation, meaning that a voter cannot deny their participation in the election once their biometric data is recorded.

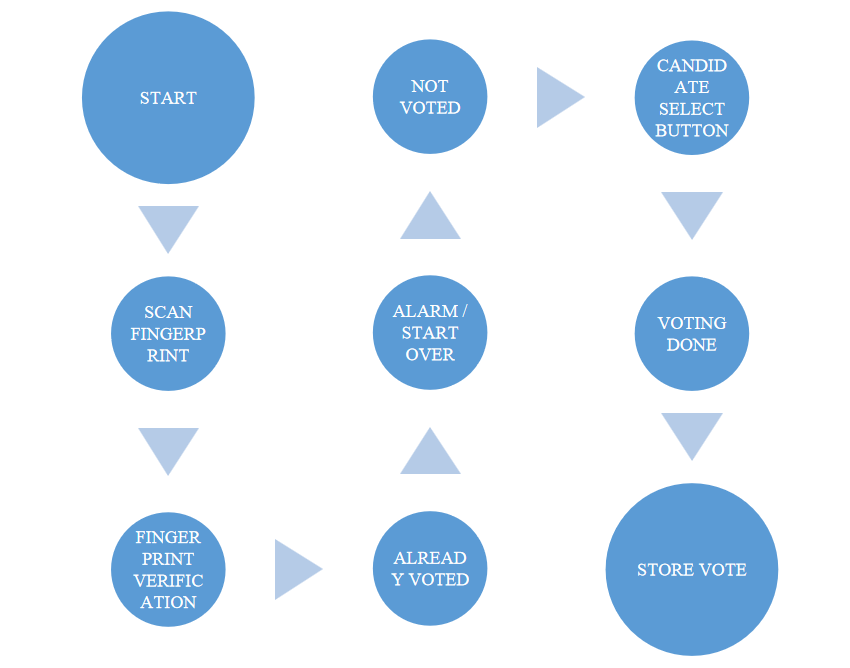
6. Scalability: The system should be able to handle a large number of voters, especially during elections when there may be a surge in participation.

7. Accessibility: The biometric system should be designed to accommodate voters with disabilities or those who may have difficulty providing certain types of biometric data. Alternative authentication methods should be available.

8. Redundancy and Fail-Safes: The system should have built-in redundancy and fail-safe mechanisms to ensure that voting can continue in case of technical failures or system malfunctions.

9. Auditability: There should be a clear audit trail for every vote, with the ability to verify and trace each vote back to the individual voter in case of disputes or recounts.

10. Secure Transmission: Ensure that biometric data and voting records are transmitted securely to prevent interception or tampering during transmission.



5.2: SOLUTION ARCHITECTURE

Designing a solution architecture for a biometric security system for a voting platform is a complex task that requires careful planning and consideration of various components and their interactions. Here's a high-level solution architecture for such a system:

1. User Interface (UI):

* Voter interface: This is where voters interact with the system to authenticate themselves, cast their votes, and review their choices.
* Admin interface: For election officials to manage and monitor the voting process.

2. Biometric Data Capture:

* Biometric devices: Fingerprint scanners, iris scanners, or facial recognition cameras for capturing and verifying voter biometric data.
* Biometric data storage: A secure database for storing biometric templates (hashed and encrypted) and ensuring data integrity.

3. Voter Registration:

* Voter registration database: Stores voter information, biometric templates, and eligibility status.
* Registration and validation services: Verify voter eligibility and ensure that each voter is registered only once.

4. Voter Authentication:

* Biometric matching service: Compares the captured biometric data with stored templates to authenticate the voter.
* Voter verification service: Cross-references biometric data with registration records to validate the voter's identity.

5. Ballot Management:

* Ballot presentation: A service that displays the appropriate ballot based on voter eligibility and location.
* Ballot configuration: Allows election administrators to design and configure electronic ballots.

6. Vote Casting:

* Electronic voting system: Enables voters to make their selections and confirm their choices.
* Voter confirmation: Ensures voters have reviewed and confirmed their selections before submitting their votes.

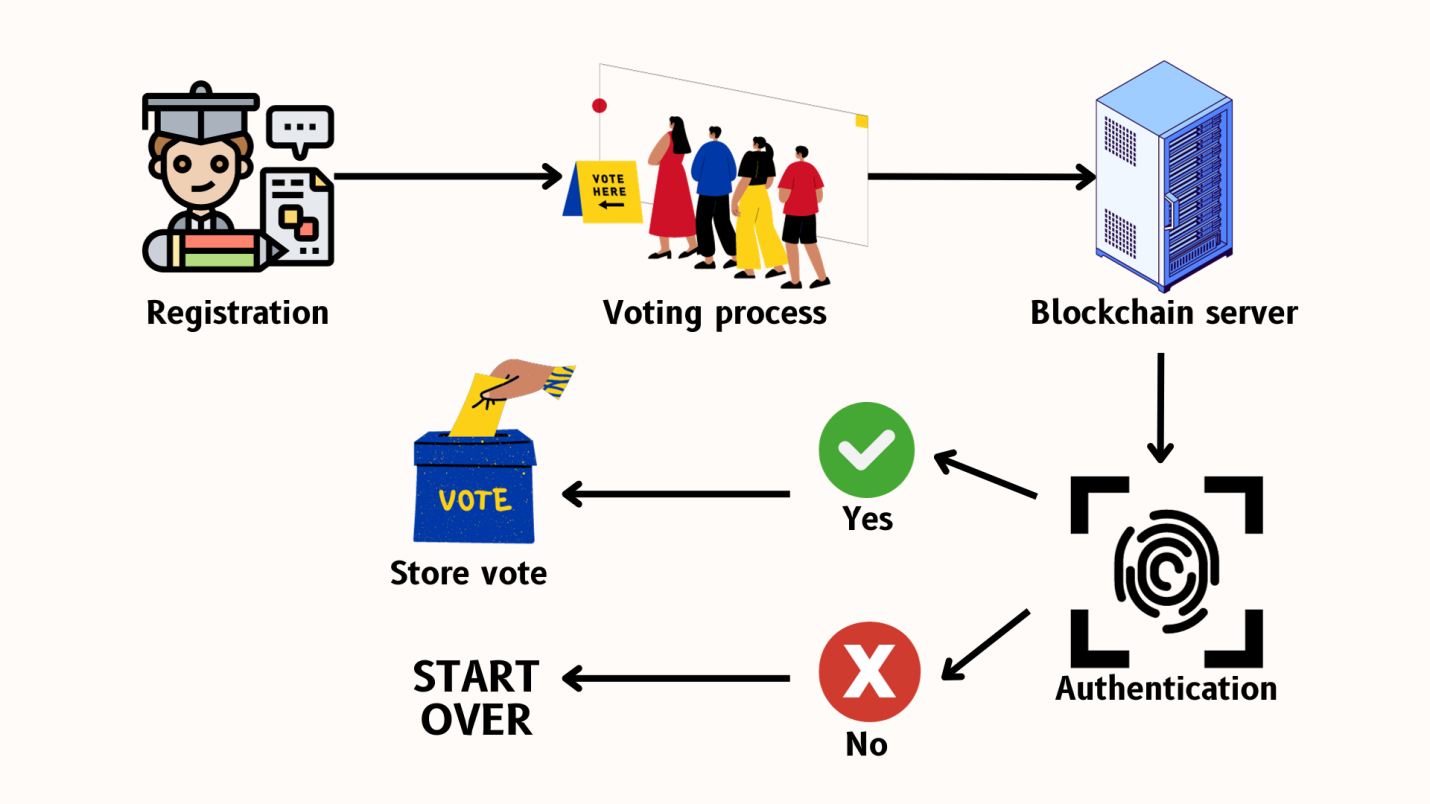
7. Security and Privacy:

* Encryption and secure communication: Ensures data protection during transmission.
* Access controls: Restricts system access to authorized users only.
* Audit trail and tamper detection: Logs all activities and detects any unauthorized changes or tampering.

8. Result Tabulation:

* Real-time vote counting: Aggregates and tallies votes in real-time.
* Reporting services: Generates election reports, results, and statistics.

**DATA FLOW DIAGRAM AND USER STORIES**



1. **PROJECT PLANNING & SCHEDULING**

Project Overview: The project aims to develop a secure and transparent blockchain-based voting system. It includes technical architecture design, sprint planning, estimation, and a sprint delivery schedule.

6.1: TECHNICAL ARCHITECTURE

**Objective**: Design the technical architecture for the blockchain voting system.

**Tasks:**

Project Kickoff (Week 1):

* Define project scope, objectives, and key stakeholders.
* Assemble project team.

Requirements Analysis(Week 2-3):

* Gather functional and non-functional requirements.
* Define the scope of blockchain integration.

Technical Design(Week 4-5):

* Create a high-level system architecture.
* Select the blockchain platform (e.g.,Ethereum, Hyperledger) and consensus mechanism.
* Design data models and smart contracts.
* Define security protocols and privacy measures.

System Prototyping(Week 6-8):

* Develop a prototype to validate the technical design.
* Conduct initial security and performance tests.

Technical Architecture Review(Week 9):

* Review the technical architecture with stakeholders.
* Address feedback and finalize the design.

6.2: SPRINT PLANNING AND ESTIMATION:

**Objective:** Plan and estimate sprints for the development of the blockchain voting system.

**Tasks:**

Sprint 1 Planning (Week 10):

* Define sprint goals, features, and priorities.
* Assign tasks and responsibilities.
* Estimate development effort.

Sprint 2 Planning (Week 12):

* Define sprint goals for the next development cycle.
* Update tasks and priorities based on feedback from Sprint 1.
* Refine development effort estimates.

Sprint 1 Development (Week 13-16):

* Develop the core blockchain components, including smart contracts, user authentication, and vote casting.

Sprint 1 Testing (Week 17):

* Conduct testing of the features developed in Sprint 1.
* Address any identified issues.

Sprint 1 Review and Sprint 3 Planning (Week 18):

* Review the outcomes of Sprint 1.
* Plan for the next development cycle, Sprint 3.

6.3: SPRINT DELIVERY SCHEDULE:

**Objective:** Implement and deliver sprints according to the schedule.

**Tasks:**

Sprint 2 Development (Week 19-22):

* Develop additional features, such as data storage, voter registration, and data encryption.

Sprint 2 Testing (Week 23):

* Conduct testing and quality assurance for features developed in Sprint 2.
* Address any issues.

Sprint 2 Review and Sprint 3 Planning (Week 24):

* Review the outcomes of Sprint 2.
* Plan for Sprint 3 based on updated priorities and feedback.

Sprint 3 Development (Week 25-28):

* Implement remaining features, like accessibility enhancements and real-time monitoring.

Sprint 3 Testing (Week 29):

* Conduct thorough testing of the complete system.
* Perform security assessments.

Final Review and Deployment (Week 30-31):

* Conduct a final system review with stakeholders.
* Prepare for system deployment.

**Conclusion:** This project plan outlines the phases, tasks, and schedules for developing a blockchain-based voting system. It covers technical architecture design, sprint planning and estimation, and a sprint delivery schedule to ensure the successful implementation of the voting system. Adaptations may be necessary based on real-world project constraints and requirements.

1. **CODING & SOLUTIONING**
   1. FEATURE 1

Biometric Security System for Voting platform

// 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);

}

}

* 1. DATABASE SCHEME

The data schema for the Transparent Education Data Management project is a crucial aspect of the database design. It defines the structure of the database and how data is organized within it.

**Students Table:**

This table stores information about individual students.

Fields may include:

* **student\_id**
* **first\_name**
* **last\_name**
* **date\_of\_birth**
* **gender**
* **contact\_email**
* **contact\_phone**

**Courses Table:**

This table holds details about the courses offered in the educational institution.

Fields may include:

* **course\_id**
* **course\_name**
* **instructor\_id**
* **start\_date**
* **end\_date**

**Enrollments Table:**

This table represents the enrollment of students in courses.

Fields may include:

* **enrollment\_id**
* **student\_id**
* **course\_id**
* **enrollment\_date**

**Grades Table:**

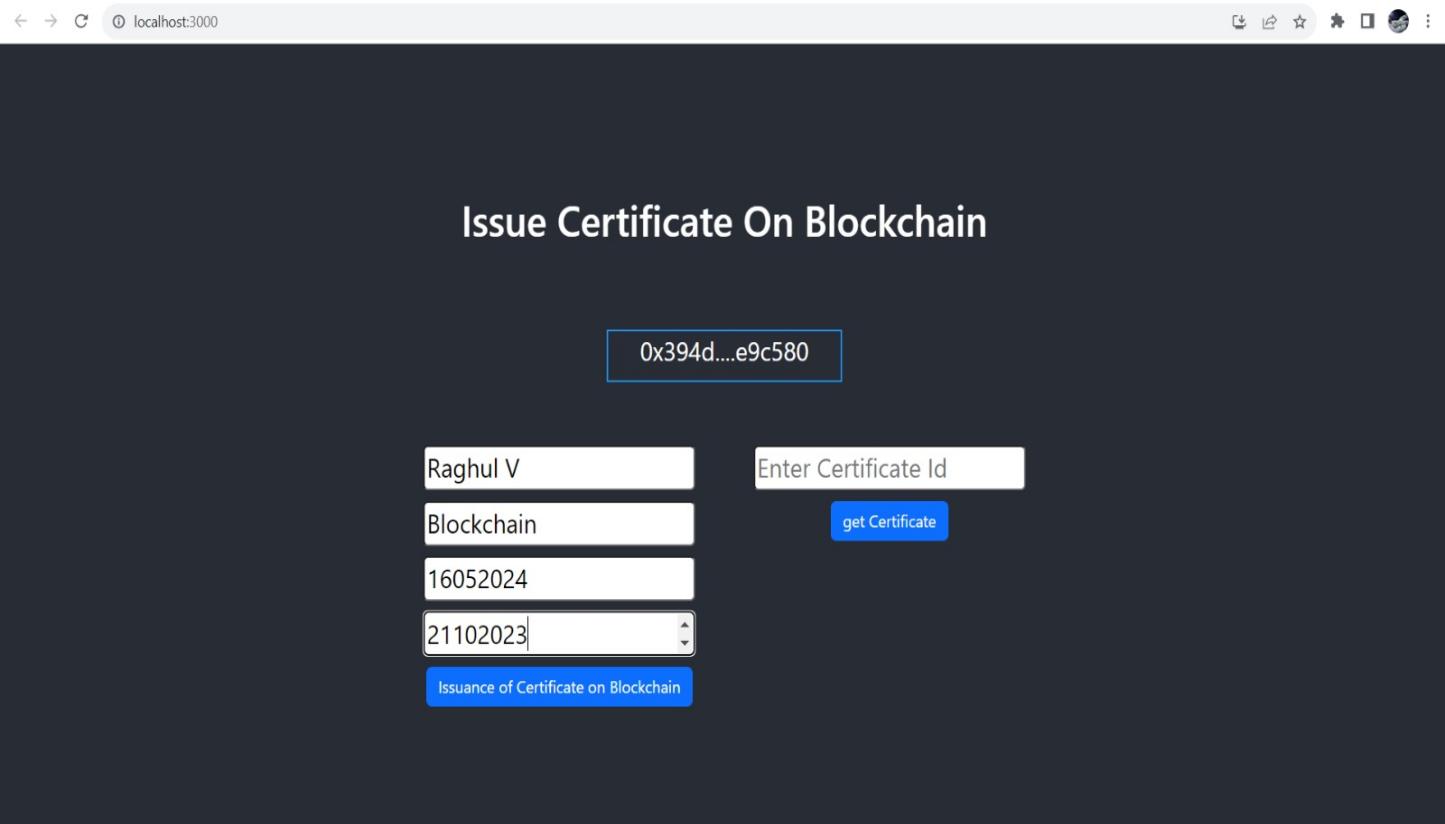
This table records students' grades for assessments within courses.

Fields may include:

* **grade\_id**
* **enrollment\_id**
* **assessment\_name**
* **score**
* **assessment\_date**

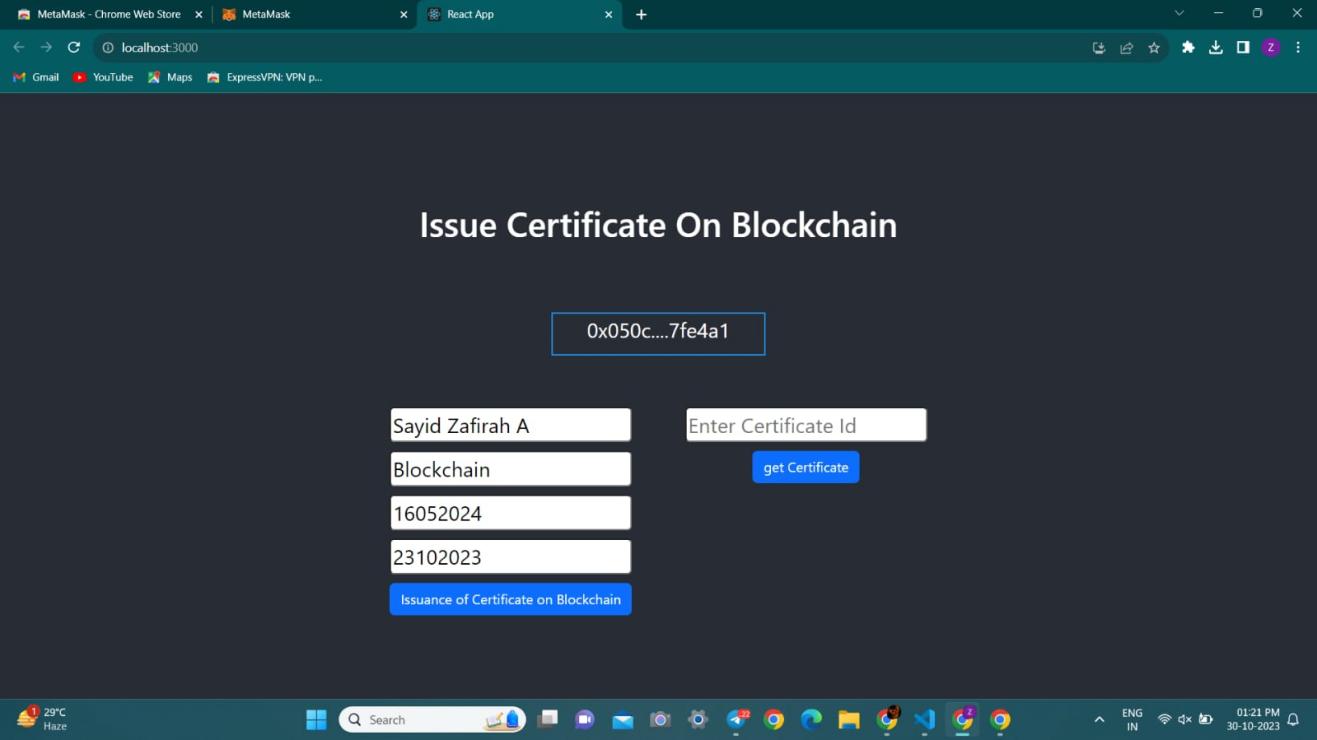
1. **PERFORMANCE TESTING:**

|  |  |  |  |
| --- | --- | --- | --- |
| **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 exploring | 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 command   1. npm install 2. npm bootstrap 3. npm start |  |
| 5 | LOCAL HOST IP ADDRESS | Copy the address and open it to chrome so you can see the front end of your project. | **WhatsApp Image 2023-11-02 at 6.37.48 PM (1)** |

1. **RESULTS **

****

****

****

1. **ADVANTAGES & DISADVANTAGES**

10.1 ADVANTAGES:

1. Voter Authentication:

* Enhanced Identity Verification: Biometrics provide a highly reliable method for verifying a voter's identity, making it difficult for individuals to impersonate others and vote fraudulently.
* Reduction in Voter Fraud: By using unique biometric traits (e.g., fingerprints or iris scans), the system can significantly reduce the risk of voter fraud.

1. Accuracy and Integrity:

* Reduced Errors: Biometric systems can minimize errors associated with manual data entry and identity verification.
* Data Accuracy: Biometric data, once recorded, is difficult to alter or manipulate, which ensures the integrity of the voting process.

1. Prevention of Multiple Voting:

* One Voter, One Vote: Biometrics make it more challenging for an individual to vote multiple times, ensuring that each voter can cast only one vote.

4. Accessibility and Inclusion:

* Inclusivity: Biometric systems can be designed to accommodate voters with disabilities by offering alternative authentication methods, ensuring that the voting process is accessible to a wide range of individuals.

5. Efficiency and Speed:

* Streamlined Process: Biometric authentication can speed up the check-in and verification process at polling stations, reducing wait times and improving the overall voting experience.

10.2 DISADVANTAGES:

1. Privacy Concerns:

* Biometric data is highly personal, and collecting and storing it raises privacy concerns. Voters may be apprehensive about their biometric data being used for purposes other than voting.

2. Data Security Risks:

* Biometric data needs to be stored and transmitted securely to protect against data breaches. Any compromise of this data could have serious consequences for individuals and the election process.

3. Inaccuracies:

* Biometric systems may not always provide 100% accuracy. False positives and false negatives can occur, potentially denying legitimate voters the right to vote or allowing fraudulent votes.

4. Cost and Complexity:

* Implementing and maintaining a biometric system can be costly and complex. It involves the purchase of biometric hardware, software, and ongoing maintenance and support.

5. Accessibility Challenges:

* While biometric systems can be designed to accommodate individuals with disabilities, they may still present accessibility challenges for some voters, particularly those with certain disabilities or medical conditions.

**12. FUTURE SCOPE**

The future scope of biometric security systems for voting platforms holds significant potential for addressing many of the challenges and concerns in electoral processes. While the adoption of such systems is contingent on several factors, including technology advancements and regulatory changes, here are some areas where biometric security systems in voting platforms may evolve in the future:

1. Enhanced Security and Privacy Measures:

* Biometric systems will continue to evolve with even stronger security and privacy measures to protect sensitive voter data and ensure the integrity of elections.

2. Blockchain Integration:

* Integrating blockchain technology with biometric systems can further enhance the transparency and security of voting platforms by creating immutable and auditable records of votes.

3. Accessibility Improvements:

* Future systems will focus on improving accessibility to accommodate voters with various disabilities, ensuring that no one is excluded from the electoral process.

1. Standardization and Interoperability:

* Efforts may be made to standardize biometric authentication methods, making systems more interoperable and universally applicable across different regions and elections.

5. Remote Voting:

* Biometric systems may enable secure remote voting, allowing eligible voters to participate in elections from the comfort of their homes or at remote locations.

1. **CONCLUSION:**

In conclusion, blockchain-powered electronic voting systems offer several compelling advantages, including enhanced transparency, data integrity,reduced administrative overhead, and improved user privacy. With the extraordinary growth in the use of blockchain technologies, a number of initiatives have been made to explore the feasibility of using blockchain to aid an effective solution to e-voting. However, it's essential to consider the associated disadvantages and challenges, such as technical complexity, cost, scalability issues,and privacy concerns.

The work to achieve this is underway in the form of an additional provenance layer to aid the existing blockchain based infrastructure. Furthermore, staying informed about the evolving regulatory landscape and technological advancements in blockchain is crucial for successful implementation. Ultimately, while blockchain has the potential to bring significant benefits such as cryptographic foundations and transparency to achieve an effective solution to biometric security system for voting platform.

**GitHub Link:** <https://github.com/sagari012/Voting-system>

**VideoLink:** <https://drive.google.com/drive/folders/1qGh6SJDZ_yuj4etRMMDhBd2b9fCBv09Z?usp=sharing>