**PROJECTREPORT**

**BIOMETRIC SECURITY FOR VOTING PLATFORM**

|  |  |
| --- | --- |
| **Date** | **28October2023** |
| **TeamID** | **NM2023TMID11861** |
| **ProjectName** | **BIOMETRICSECURITYFOR VOTING PLATFORM** |

**TEAMMEMBERS**

|  |  |
| --- | --- |
| 814620114306 | Gunal S S |
| 814620114311 | Manivasagan M |
| 814620114312 | ManojKumar M |
| 814620114321 | Saran V |

* **ABSTRACT**
* **INTRODUCTION**
  + ProjectOverview
  + Purpose

# IDEATION&PROPOSEDSOLUTION

* + FunctionalRequirement
  + Non-FunctionalRequirement

# PROJECTDESIGN

* + DataFlowDiagrams
  + SolutionArchitecture

# PROJECTPLANNING&SCHEDULING

* + TechnicalArchitecture
  + SprintPlanning&Estimation
  + SprintDeliverySchedule

# CODING&SOLUTIONING

* + Feature1
  + Feature2
  + DatabaseSchema

# PERFORMANCETESTING

* + PerformanceMetrics

# RESULTS

* + OutputScreenshots
* **ADVANTAGES&DISADVANTAGES**
* **CONCLUSION**
* **FUTURESCOPE**
* **APPENDIX**
* SourceCode
* Git Hub & Project Demo Link

# ABSTRACT

Presentlyvotingisperformedusingballotpaperandthecountingisdonemanually,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 alsomade hugeloss of human lives. In our proposed system voting and counting is done with thehelpofcomputerinOnline.Itsavestime,avoiderrorincountingandtherewillbeno

invalid

votes.Itmakestheelectionprocesseasy.Italsoavoidstheprocessofphysicaltouchingor visiting

anyplacesandso inthetimeofpandemictooitwillbemorehelpfultoconductelections.

The systemdeals withthe online votingand 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 andcountingthe numberofvotes, ittakes the lotoftimeto for theexistingprocess, toovercome thedrawbacksintheexistingsystemthisparticularsystemwasproposedtomarkourwork much

easierandtoreducewastageof time.Andmoreoverusdoesn’tgettheaccurateresultsin the present existingsystem. So, there is a need for Online Voting Systems.

# 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 inthis. Since its first use as punched-card ballots in1960’s, e-votingsystems have achievedremarkable progress withits adaptionusingthe internettechnologies (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 ofconstantly germinatingand growing data records secured from unauthorized manipulating, tampering and revision. Blockchain CORE Metadata, citation andsimilarpapers atcore.ac.uk Provided byUWLRepositoryallows everyusertoconnect 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 madein 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 transactionsacrossvariousdomains(Nakamoto,2009; Kraft,2015;Narayananetal,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 tofacilitate 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. Thismakes blockchain technology very efficient to deal with the threat of utilizinga 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.

## ProjectOverview

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.

## Purpose

Thepurposeofimplementingabiometricsecuritysystemfora

voting platform project is to enhance the security, integrity, and accessibility of thevoting process in elections. Biometric security systems utilize unique physical or behavioral characteristics of individuals to verify their identity.

# LITERATURESURVEY

RaspberryPiandimageprocessingbasedonElectronicVotingMachine(EVM)

[1], provides a smallcomputer capable ofimage processingand controls the entire votingsystem. 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 hasnot voted, the person will be allowed to cast his or her ballot. Each voting [www.ijcrt.org](http://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](http://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 guidelineswere 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 systemwhere 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 ofvotingsystembasedonAadhar is that, the electoralelections willallow people to vote in their current city electronically. The Smart Voting System using RFID [9], provides a RFID (Radio Frequency Identification) approach by which fromanywhere 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 usingRFID tags instead ofvoterid. This programallows the voters to see results at any time which mayprevent consequences which opens the way for disruptive voting.

## Existingproblem

Thevotingsystemcurrentlybeingusedbytheassociationisapaper-basedsystem,in

which the voter simply picks up ballot’s sheets from electoral officials, tick off who they would like to vote for, and thencast theirvotes by merely handingover the ballot sheet backto 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.

## References

* + 1. Md. Maminul Islam, Md. Sharif Uddin Azad, Md.AsfaqulAlam, 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. AngelinBlessy,“Smart Voting System Support through Face Recognition”, 2018 InternationalJournalofEngineeringResearch 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 ,NithyaKumari 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. LaasyaPriya, 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.

## ProblemStatementDefinition

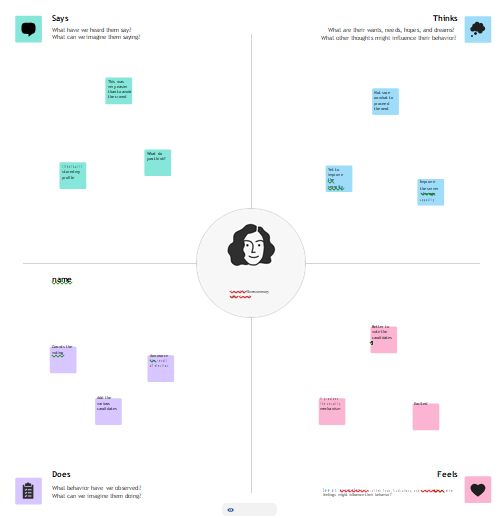
The existing voting systems often rely on paper-based or electronic methods that are susceptible to various issues, such as identity fraud, ballot tampering, and data breaches. To overcome these challenges, the project's primary objective is to develop a biometric security system that can enhance the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

**ChallengestoAddress:**

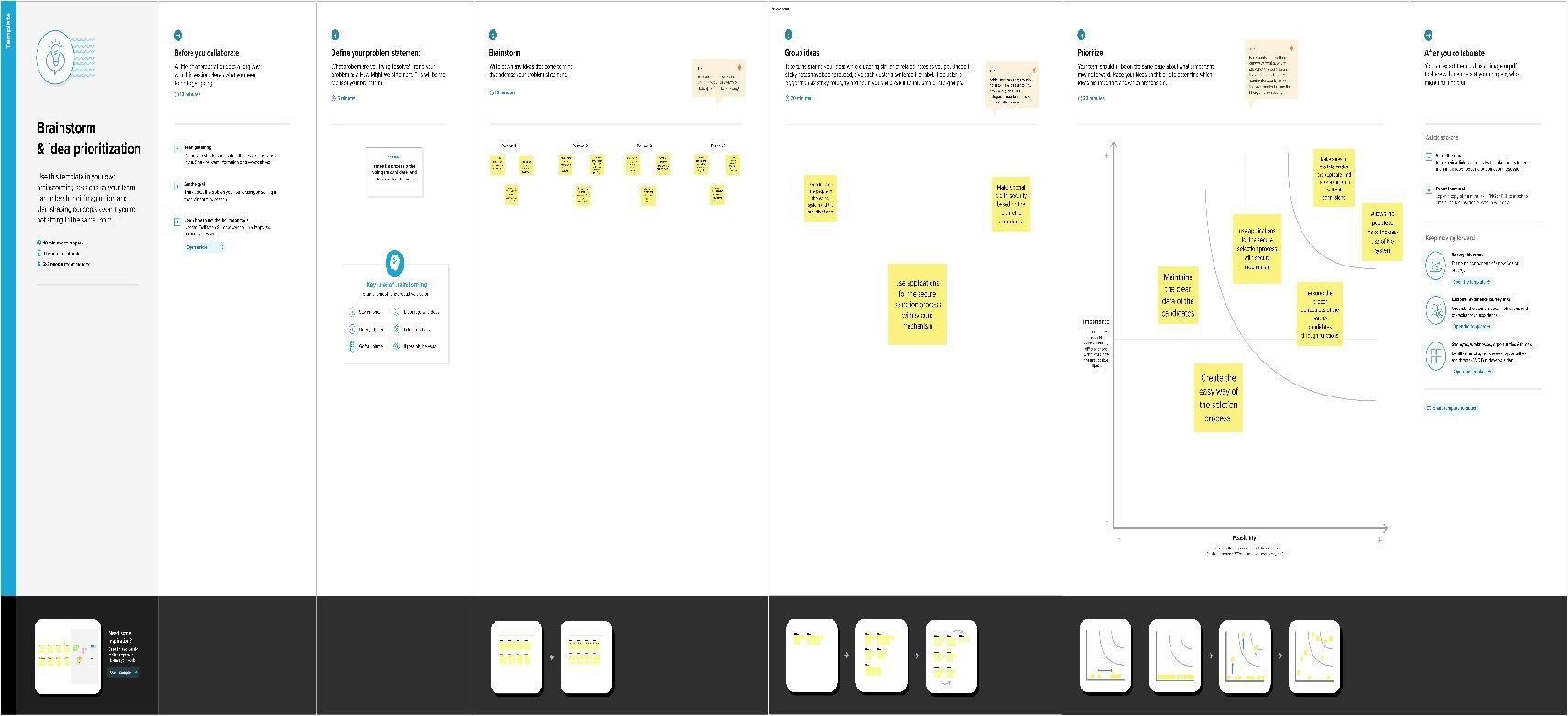
* + 1. Voter Authentication: Developing a reliable method to authenticate voters using biometric data, ensuring that onlyeligible voters can participate inthe election.
    2. Data Privacy and Security: Ensuring the protection of biometric data, as well as the election data, against unauthorized access, 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. RobustnessAgainstAttacks:Developingmechanismstodefendagainst various formsof attacks, such as spoofing, replay attacks, and denial-of-service attacks.
    5. BackupandContingencyPlans:Preparingforcontingencies, suchasnetwork failures, equipment malfunctions, or other unexpected issues, to ensure the continuity of the voting process.

# IDEATION&PROPOSEDSOLUTION

* 1. **EmpathyMapCanvas**



* 1. **Ideation&Brainstorming**



# REQUIREMENTANALYSIS

## Functionalrequirement

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:

### VoterRegistration:

* + - Registrationprocessforeligiblevoters,includingbiometricdatacapture(fingerprint,facial recognition, etc.).
    - Verificationandvalidationofvoteridentityduringregistration.
    - Asecuredatabasetostorevoterinformationandbiometricdata.

### VoterAuthentication:

* + - Biometricauthenticationofvotersatpollingstations.
    - VoterIDverificationusingbiometricdata.
    - Real-timevalidationofvotereligibility.

### BallotCasting:

* + - Secureanduser-friendlyinterfaceforcastingvotes.
    - Confirmationmechanismstoensurevoterscasttheirvotescorrectly.
    - Theabilitytopreventmultiplevotesbythesameindividual.

## Non-Functionalrequirements

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:

* + - **AuthenticationSecurity:** Thesystemshouldprovideahighlevelofsecuritytoensure that only eligible voters are allowed to cast their votes.
    - **DataEncryption:** Alldatatransmittedand storedshouldbeencryptedtoprotectagainst unauthorized access.
    - **BiometricDataProtection:**Biometricdatashouldbesecurelystoredandtransmitted to prevent identity theft and fraud.
    - **Redundancy:**Thesystemshouldhaveredundancyandfailovermechanismstoprevent service disruptions due to security breaches or technical failures.

### Scalability:

* + - Thesystemshouldbecapableofhandlinga large numberofconcurrentusers, especially during peak voting periods.
    - Itshouldscaleeasilytoaccommodateanincreasingnumberofvotersandpolling locations.

### Availability:

* + - Thesystemshould have highavailability, ensuringthat voterscanaccess anduseitat any time during the voting period.
    - Itshouldincludebackupanddisasterrecoverymeasurestoensurecontinuedoperationin case of system failures.

# PROJECT DESIGN

## DATAFLOWDIAGRAM

A two-dimensional diagram explains how data is processed and transferred in a system. The graphicaldepictionidentifies eachsource ofdataandhow it interactswithother 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.

## LEVEL0

TheLevel0DFDshowshowthesystemisdividedinto'sub-systems'(processes),eachof 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 datastoresthatmustbepresentinorderforthesystemtodoitsjob,andshowstheflowofdata between the various parts of the system.

ADMIN

Data Store

Voter

Information

## FigureNo.5.1.1:DataFlowDiagram(level 0)

### LEVEL1

The nextstage is tocreatethe Level1Data Flow Diagram. This highlights the mainfunctions carriedoutbythesystem. Asarule,todescribethesystemwas usingbetweentwoandsevenfunctions twobeingasimplesystemandsevenbeingacomplicatedsystem.Thisenablesustokeepthemodel manageable on screen or paper.

Database

Delete Voter

Database

VOTERINFORMATION

Add Voter

Database

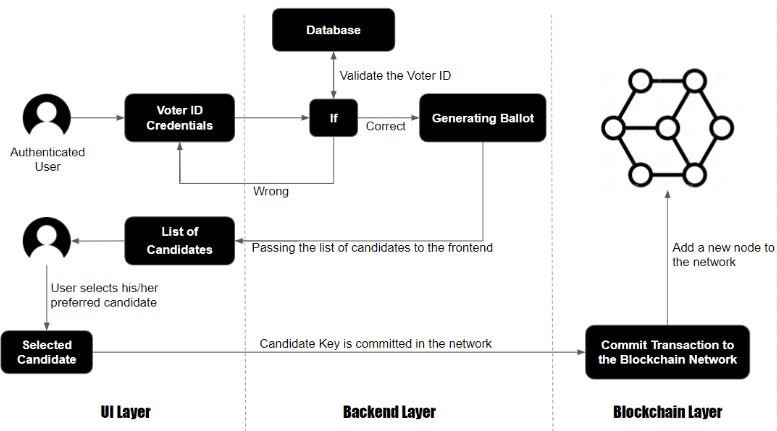
Update voter

Login

Admin

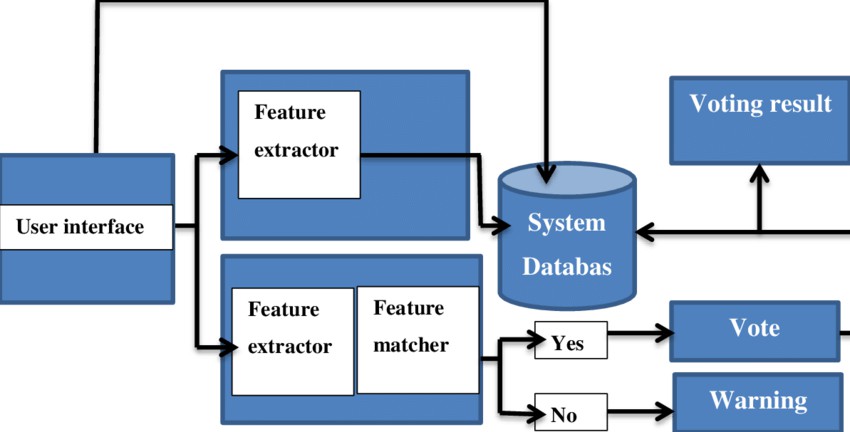
**FigureNo.5.1.2:DataFlowDiagram(Level1)**

* 1. **SolutionArchitecture**

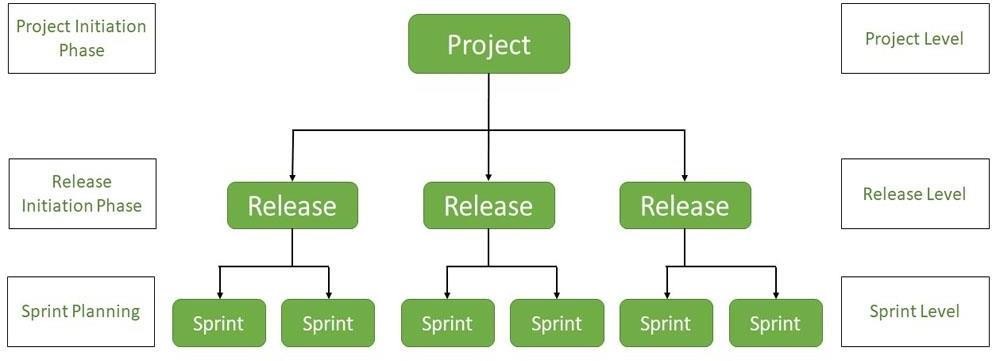


# PROJECTPLANNING&SCHEDULING

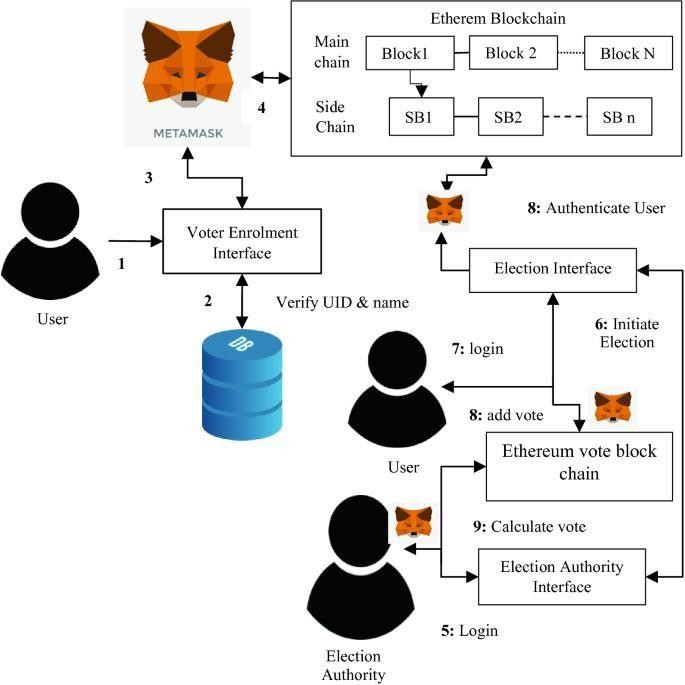
* 1. **TechnicalArchitecture**



* 1. **SprintPlanning&Estimation**



* 1. **SprintDeliverySchedule**



# CODING&SOLUTIONING

## Feature1

A biometricsecurity systemforavotingplatform projectisdesignedtoenhancethe securityandintegrityof thevoting processbyverifyingtheidentity ofvotersusingunique physiological or behavioral characteristics. Here are some key features of such a system: **Biometric Enrollment:**

Voter registration process involves capturingand storing biometric data (e.g., fingerprints, iris scans, facial recognition) ofeligible voters.

Ensuresecurestorageandencryptionofbiometrictemplatestoprotectagainstdatabreaches.

### BiometricVerification:

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

Real-timeverification compares the presented biometric data with the enrolled templates toconfirm the voter's identity.

### Multi-ModalBiometrics:

Supportmultiplebiometricmodalitiestoincreaseaccuracy andaccommodatevoters with disabilities or conditions that may affect certain biometrics.

## Feature2

### DataPrivacyandProtection:

Strictdataprivacymeasurestoensurethatbiometricdataisnotmisusedoraccessedby unauthorized personnel.

Compliancewithdataprotectionregulationsandencryptionprotocols.

### VoterDatabaseManagement:

Centralizeddatabasemanagementtoupdateandmaintainvoterrecords,ensuring accuracy and eliminating duplicate entries.

### Anti-SpoofingMeasures:

Implementanti-spoofingmechanismstodetectfraudulentattemptstousefake biometric data, such as liveness detection.

### AuditTrail:

Maintainanaudittrailofallbiometricverificationsfortransparencyandaccountability.

### RedundancyandFail-SafeMechanisms:

Implementbackupsystemstoensurethecontinuityofthe votingprocess incaseof system failures or biometric authentication issues.

### SecureTransmission:

Ensurethatbiometricdata issecurelytransmittedbetweenpollingstationsandthe central database to prevent interception or tampering.

### Accessibility:

Provideaccommodationsforindividualswithdisabilities,ensuringthatthebiometric system is accessible to all eligible voters.

## DatabaseSchema

1. UsersTable

**user\_id(PrimaryKey):**Unique identifierforeachuser.

**username:** User's username for login. **password:**User'spassword(hashedandsalted). **email:** User's email address.

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

1. VotersTable

**voter\_id(PrimaryKey):**Uniqueidentifierforeachregisteredvoter.

**user\_id(ForeignKey):**ReferencestheUserstable.

**full\_name:**Fullnameofthevoter.

**date\_of\_birth:**Voter'sdateofbirth.

**national\_id:**Voter'snationalIDorpassportnumber.

**biometric\_data:**Storageforbiometricdata

1. ElectionsTable

**election\_id(PrimaryKey):**Uniqueidentifierforeachelection.

**start\_date:**Dateandtimewhentheelectionstarts. **end\_date:** Date and time when the election ends. **description:** A brief description of the election.

1. CandidatesTable

**candidate\_id(PrimaryKey):**Uniqueidentifierforeachcandidate. **election\_id (Foreign Key):** References the Elections table. **full\_name:** Full name of the candidate.

**party\_affiliation:**Thepoliticalpartythecandidaterepresents.

**position:**Thecandidate'spositionintheelection(e.g.,presidential,senatorial).

1. VotesTable

**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(ForeignKey):**ReferencestheCandidatestable. **vote\_time:** Timestamp when the vote was cast.

1. BiometricLogsTable

**log\_id(PrimaryKey):**Unique identifierforeachbiometric logentry.

**voter\_id (Foreign Key):** References the Voters table. timestamp:Timestampwhenthebiometricdatawascaptured.

**biometric\_type:**Typeofbiometricdata(e.g.,fingerprint,facialrecognition).

**device\_id:**Identifierforthebiometriccapturedevice.

1. AuditLogsTable

**log\_id(PrimaryKey):**Uniqueidentifierforeachauditlogentry.

**user\_id(ForeignKey):**ReferencestheUserstable.

action:Descriptionoftheactionperformed (e.g.,login, logout,data modification). timestamp: Timestamp when the action occurred.

# PERFORMANCE TESTING

## PerformanceMetrics

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:

### FalseAcceptanceRate(FAR):

FAR measures thepercentageofunauthorizedusers whoareincorrectlygrantedaccess. Inthe context of voting, this would indicate the percentage of fraudulent votes that go undetected.

### FalseRejectionRate(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.

### EqualErrorRate(EER):

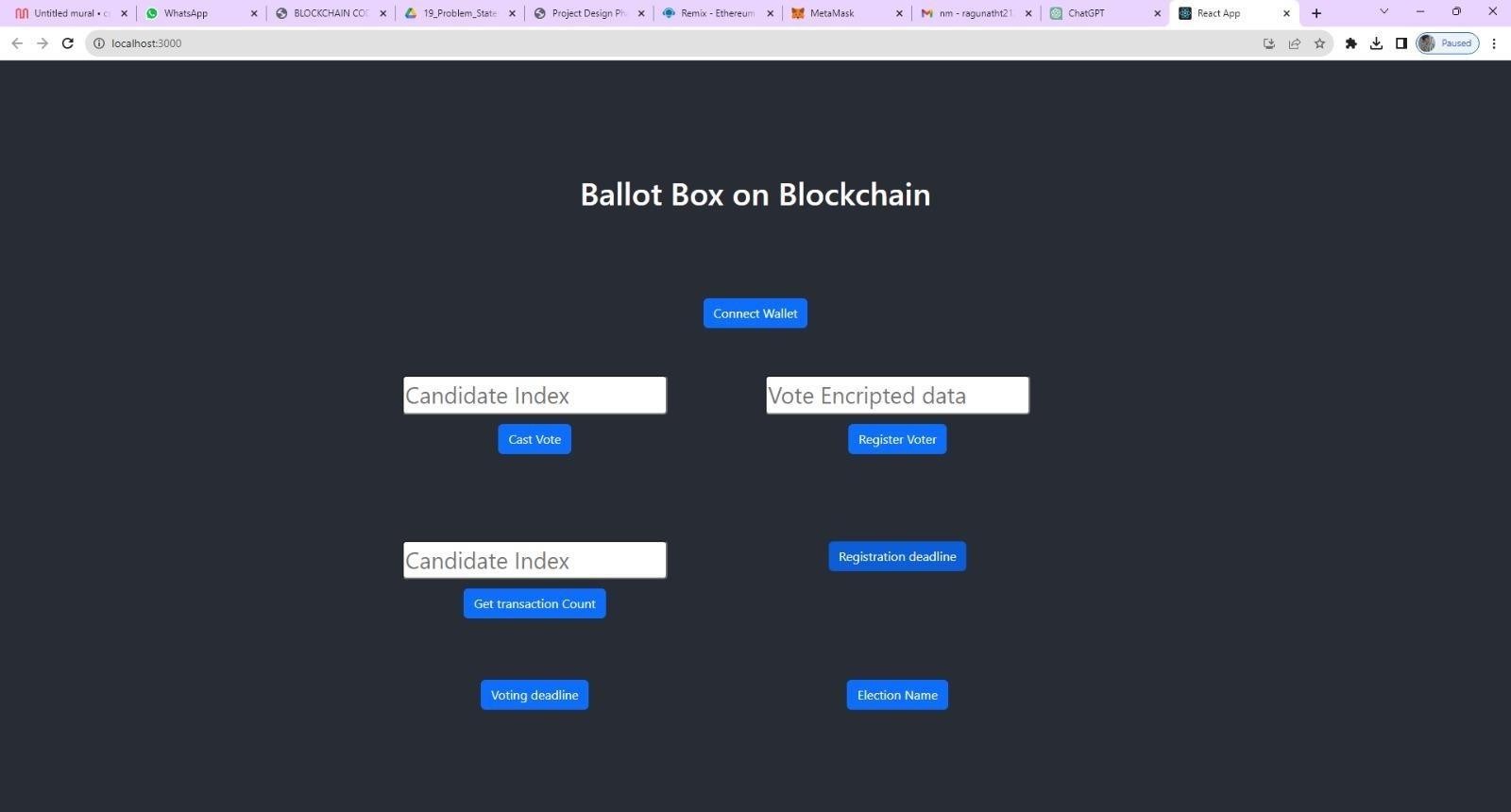
EER is the point at which the FAR and FRR are equal. This is a critical metric for balancing security and usability.

### Accuracy:

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

# RESULTS

* 1. **OutputScreenshot**



# ADVANTAGES&DISADVANTAGES

## Advantages:

Implementing a biometric security system in a voting platform project can offer several advantages. Biometricauthenticationreliesonuniquephysicalorbehavioralcharacteristicsof an individualto verify their identity. Here are some advantages of using biometric security in a voting platform:

### EnhancedSecurity:

Biometricdata ishighly uniqueanddifficulttofake, makingitarobustsecuritymeasure against impersonation and voter fraud.

### ReducedVoterFraud:

Biometricauthenticationhelpspreventmultiplevotingbythesamepersonorindividuals assuming false identities.

### AccuracyandReliability:

Biometricsystems arehighlyaccurate, reducingtheriskoferrorsandensuringthatonly eligible voters can cast their ballots.

### IncreasedTrust:

Theuseofbiometrics canenhancepublictrust inthe votingprocess,asitprovidesa transparent and secure way to verify voter identities.

### PreventionofVoterSuppression:

Biometricsystemscanhelppreventvotersuppressiontactics,aseligiblevotersarelesslikely to be turned away or denied the right to vote.

### Convenience:

Biometricauthenticationcanstreamlinethe votingprocessbyeliminatingthe needfor physical ID cards or paper-based verification methods.

### FasterVotingProcess:

Biometricsystemscanspeedupthe votingprocess,reducingwaittimesatpollingstationsand improving overall efficiency.

### Accessibility:

Biometricsystemscanbedesignedtoaccommodateindividualswithdisabilities,ensuring inclusivity in the voting process.

### TamperResistance:

Biometricdata isdifficulttotamperwith,reducingtheriskofdata manipulationor interference with the voting system.

### AuditTrail:

Biometricsystemscanprovideanaudittrailofwho votedandwhen, improvingtransparency and accountability in the electoral process.

## Disadvantages:

While a biometric securitysystemfor a votingplatform mayseemappealing, it also comes withseveraldisadvantagesandchallengesthat needtobecarefullyconsidered. Someofthe key disadvantages include:

### PrivacyConcerns:

Biometric data is highly sensitive, and its collection and storage raise significant privacy concerns.Citizens maybeuncomfortablewiththeirbiometric informationbeingstoredina government database, as it can be vulnerable to misuse or data breaches.

### VulnerabilitytoHacking:

Biometric data can be stolen or hacked, just like any other form of data. If biometric data is compromised, itcanhavelong-lastingconsequences forindividuals,asitisnoteasytochange or replace biometric characteristics like fingerprints or irises.

### FalsePositivesandNegatives:

Biometric systems are not infallible and can produce false positives (granting access to an unauthorizedindividual)orfalsenegatives(denyingaccesstoanauthorized individual).This canresult fromfactorssuchaspoorimagequality,variations inbiometrictraits,orhardware limitations.

### TechnicalChallenges:

Implementing a biometric system for voting requires robust technology infrastructure, includinghigh-qualityscanners,databases,andspecializedsoftware.Thesesystemsarecostly to set up and maintain.

### InclusivityandAccessibility:

Biometric systems may not work well for all individuals, including those with disabilities or certain medicalconditions. It'sessentialtoensurethatthe votingsystemremainsinclusiveand accessible to all citizens.

### EnrollmentChallenges:

Enrollingcitizens intothebiometricsystemcanbeatime-consumingandresource-intensive process. Not all citizens may have access to enrollment centers, especially in remote areas, which can lead to unequal access to voting.

### LongLinesandDelays:

Biometric verificationcanslowdownthe votingprocess, asitrequiresadditionalsteps for authentication. This can lead to long lines at polling stations and discourage voter participation.

### LegalandEthicalIssues:

Theuseofbiometricdata invotingsystems canraiselegalandethicalquestionsregarding consent, data ownership, and the right to anonymity. Developing a legal framework for biometric voting can be complex and contentious.

### MaintenanceandUpkeep:

Biometricsystemsrequireregularmaintenanceandupdatestoremainsecureandaccurate. This adds ongoing costs and logistical challenges to the voting platform.

### Cost:

Implementingbiometricsecuritysystemscanbeexpensive,requiringsignificantfinancial resources for both initial setup and ongoing maintenance.

# 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 biometricvotingsystems.Privacyconcerns mustbeaddressed,asthecollectionandstorageof biometric data raise important ethicaland legalquestions. Safeguards, includingstringent data protection measures and secure storage protocols, must be inplace to mitigate these concerns.

# FUTURESCOPE

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 incorporateaccessibility features to make it inclusive for people with disabilities. This could involve voice recognition or other accessible biometric modalities.

# APPENDIX

## SourceCode

importReact,{useState}from"react";

import{Button,Container,Row,Col}from'react-bootstrap'; import 'bootstrap/dist/css/bootstrap.min.css';

import{contract}from"./connector";

functionHome(){

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("");

consthandleCandidateIndex=(e)=>{ setCandidateIndex(e.target.value)

}

consthandleCastVote=async()=>{ try {

lettx=awaitcontract.castVote(CandidateIndex.toString())

let wait = await tx.wait() console.log(wait); alert(wait.transactionHash)

}catch(error){

alert(error)

}

}

consthandleVoterBiometricData=(e)=>{ setVoterData(e.target.value)

}

consthandleRegisterVoter=async()=>{ try {

lettx=awaitcontract.registerVoter(VoterData) let wait = await tx.wait()

console.log(wait) alert(wait.transactionHash)

}catch(error){ alert(error)

}

}

consthandleCandidateIndexs=(e)=>{ setCandidateIndexed(e.target.value)

}

consthandleCandidate=async()=>{ try {

lettx=awaitcontract.candidates(CandidateIndexed.toString()) setCandidatesData(tx)

console.log(tx);

//alert(wait.transactionHash)

}catch(error){ alert(error)

}

}

consthandleRegdeadline=async()=>{ try {

lettx=awaitcontract.registrationDeadline() setRegDeadlne(tx)

console.log(tx);

//alert(wait.transactionHash)

}catch(error){ alert(error)

}

}

consthandleVoteDeadline=async()=>{ try {

lettx=awaitcontract.votingDeadline() setVoteDeadlne(tx)

console.log(tx);

//alert(wait.transactionHash)

}catch(error){ alert(error)

}

}

consthandleElecName=async()=>{ try {

lettx=awaitcontract.electionName() setElection(tx)

console.log(tx);

//alert(wait.transactionHash)

}catch(error){ alert(error)

}

}

consthandleWallet=async()=>{ if (!window.ethereum) {

returnalert('pleaseinstallmetamask');

}

constaddr=awaitwindow.ethereum.request({ method: 'eth\_requestAccounts',

});

setWallet(addr[0])

}

return(

<div>

<h1style={{ marginTop:"30px", marginBottom:"80px"}}>BallotBoxon Blockchain</h1>

{!Wallet?

<ButtononClick={handleWallet}style={{marginTop:"30px",marginBottom:"50px"

}}>ConnectWallet</Button>

:

<pstyle={{width:"250px",height:"50px",margin:"auto",marginBottom:"50px", border: '2px solid #2096f3' }}>{Wallet.slice(0, 6)}. ..{Wallet.slice(-6)}</p>

}

<Container>

<Row>

<Colstyle={{marginRight:"100px"}}>

<div>

<input style={{ marginTop: "10px", borderRadius: "5px" }} onChange={handleCandidateIndex}type="number"placeholder="CandidateIndex" value={CandidateIndex} /><br />

<ButtononClick={handleCastVote}style={{marginTop:"10px"}} variant="primary">Cast Vote</Button>

</div>

</Col>

<Colstyle={{marginRight:"100px"}}>

<div>

<input style={{ marginTop: "10px", borderRadius: "5px" }} onChange={handleVoterBiometricData}type="string"placeholder="VoteEncripteddata" value={VoterData} /><br />

<ButtononClick={handleRegisterVoter}style={{marginTop:"10px"}} variant="primary">Register Voter</Button>

</div>

</Col>

</Row>

<Rowstyle={{marginTop:"100px"}}>

<Colstyle={{marginRight:"100px"}}>

<div>

<input style={{ marginTop: "10px", borderRadius: "5px" }} onChange={handleCandidateIndexs}type="number"placeholder="CandidateIndex" value={CandidateIndexed} /><br />

<ButtononClick={handleCandidate}style={{marginTop:"10px"}} variant="primary"> Get transaction Count</Button>

{CandidatesData?CandidatesData?.map(e=><p>{e.toString()}</p>):<p></p>

}

</div>

</Col>

<Colstyle={{marginRight:"100px"}}>

<div>

<ButtononClick={handleRegdeadline}style={{marginTop:"10px"}} variant="primary">Registration deadline</Button>

{RegDeadline?<p>{RegDeadline.toString()}</p>:<p></p>}

</div>

</Col>

</Row>

<Rowstyle={{marginTop:"50px"}}>

<Colstyle={{marginRight:"100px"}}>

<div>

<ButtononClick={handleVoteDeadline}style={{marginTop:"10px"}} variant="primary">Voting deadline</Button>

{VoteDeadlne?<p>{VoteDeadlne.toString()}</p>:<p></p>}

</div>

</Col>

<Colstyle={{marginRight:"100px"}}>

<div>

<ButtononClick={handleElecName}style={{marginTop:"10px"}} variant="primary">Election Name</Button>

{Election?<p>{Election.toString()}</p>:<p></p>}

</div>

</Col>

</Row>

</Container>

</div>

)

}

exportdefaultHome;

## GitHubLink:

[**https://github.com/814620114306/Biometric-security-system-for-voting-platform.git**](https://github.com/814620114306/Biometric-security-system-for-voting-platform.git)

## ProjectDemoLink:

<https://youtu.be/E-u1YAst2QI?si=Oh5SCnGVBjw3A_wR>