

SECURED E-VOTING WITH GRAPHICAL INSIGHTS BY UTILIZING BLOCKCHAIN

A PROJECT REPORT

On EVS

Submitted by

ARSH VISHWAKARMA, DENNIS TANK, VYOMA SHAH

180950131104, 180950131096, 180950131092

In partial fulfillment for the award of the degree of

BACHELOR OF ENGINEERING

in

Department: Computer Science Engineering

Institute of Technology and Management Universe, Halol



Gujarat Technological University, Ahmedabad

[April 2022]



Institute of Technology and Management Universe

Dhanora Tank Road, Paldi Village, Halol Highway, Near Jarod, Vadodara - 391510 (Gujarat),
INDIA.

CERTIFICATE

This is to certify that the project report submitted along with the project entitled **Secured E-voting With Graphical Insights By Utilizing Blockchain** has been carried out by **Arsh Vishwakarma** under my guidance in partial fulfillment for the degree of Bachelor of Engineering in Computer Science and Engineering, 8th Semester of Gujarat Technological University, Ahmedabad during the academic year 2021-22.

Prof. Ninad Bhavsar
Internal Guide

Prof. Madonna Lamin
Head of the Department



Institute of Technology and Management Universe

Dhanora Tank Road, Paldi Village, Halol Highway, Near Jarod, Vadodara - 391510 (Gujarat),
INDIA.

CERTIFICATE

This is to certify that the project report submitted along with the project entitled **Secured E-voting With Graphical Insights By Utilizing Blockchain** has been carried out by **Dennis Tank** under my guidance in partial fulfillment for the degree of Bachelor of Engineering in Computer Science and Engineering, 8th Semester of Gujarat Technological University, Ahmedabad during the academic year 2021-22.

Prof. Ninad Bhavsar

Internal Guide

Prof. Madonna Lamin

Head of the Department



Institute of Technology and Management Universe

Dhanora Tank Road, Paldi Village, Halol Highway, Near Jarod, Vadodara - 391510 (Gujarat),
INDIA.

CERTIFICATE

This is to certify that the project report submitted along with the project entitled **Secured E-voting With Graphical Insights By Utilizing Blockchain** has been carried out by **Vyoma Yogeshkumar Shah** under my guidance in partial fulfillment for the degree of Bachelor of Engineering in Computer Science and Engineering, 8th Semester of Gujarat Technological University, Ahmedabad during the academic year 2021-22.

Prof. Ninad Bhavsar
Internal Guide

Prof. Madonna Lamin
Head of the Department



GUJARAT TECHNOLOGICAL UNIVERSITY

CERTIFICATE FOR COMPLETION OF ALL ACTIVITIES AT ONLINE PROJECT PORTAL

B.E. SEMESTER VIII, ACADEMIC YEAR 2021-2022

Date of certificate generation : 05 May 2022 (11:55:29)

This is to certify that, ***Vishwakarma Arsh Anil*** (Enrolment Number - 180950131104) working on project entitled with ***Secured E-Voting With Graphical Insights By Utilizing Blockchain*** from ***Computer Science & Engineering*** department of ***INSTITUTE OF TECHNOLOGY & MANAGEMENT, UNIVERSE TECHNICAL CAMPUS, VADODARA*** had submitted following details at online project portal.

Internship Project Report	Completed
---------------------------	-----------

Name of Student : Vishwakarma Arsh Anil

Name of Guide : HOD_095_31

Signature of Student : _____

*Signature of Guide : _____

Disclaimer :

This is a computer generated copy and does not indicate that your data has been evaluated. This is the receipt that GTU has received a copy of the data that you have uploaded and submitted as your project work.

*Guide has to sign the certificate, Only if all above activities has been Completed.



GUJARAT TECHNOLOGICAL UNIVERSITY

CERTIFICATE FOR COMPLETION OF ALL ACTIVITIES AT ONLINE PROJECT PORTAL

B.E. SEMESTER VIII, ACADEMIC YEAR 2021-2022

Date of certificate generation : 05 May 2022 (18:13:41)

This is to certify that, ***Tank Dennis Dinesh*** (Enrolment Number - 180950131096) working on project entitled with ***Secured E-Voting With Graphical Insights By Utilizing Blockchain*** from ***Computer Science & Engineering*** department of ***INSTITUTE OF TECHNOLOGY & MANAGEMENT, UNIVERSE TECHNICAL CAMPUS,VADODARA*** had submitted following details at online project portal.

Internship Project Report	Completed
---------------------------	-----------

Name of Student : Tank Dennis Dinesh

Name of Guide : HOD_095_31

Signature of Student : _____

*Signature of Guide : _____

Disclaimer :

This is a computer generated copy and does not indicate that your data has been evaluated. This is the receipt that GTU has received a copy of the data that you have uploaded and submitted as your project work.

*Guide has to sign the certificate, Only if all above activities has been Completed.



GUJARAT TECHNOLOGICAL UNIVERSITY

CERTIFICATE FOR COMPLETION OF ALL ACTIVITIES AT ONLINE PROJECT PORTAL

B.E. SEMESTER VIII, ACADEMIC YEAR 2021-2022

Date of certificate generation : 05 May 2022 (13:50:40)

This is to certify that, **Shah Vyoma Yogeshkumar** (Enrolment Number - 180950131092) working on project entitled with **Secured E-Voting With Graphical Insights By Utilizing Blockchain** from **Computer Science & Engineering** department of **INSTITUTE OF TECHNOLOGY & MANAGEMENT, UNIVERSE TECHNICAL CAMPUS, VADODARA** had submitted following details at online project portal.

Internship Project Report	Completed
---------------------------	-----------

Name of Student : S h a h V y o m a
Yogeshkumar

Name of Guide : HOD_095_31

Signature of Student : _____

*Signature of Guide : _____

Disclaimer :

This is a computer generated copy and does not indicate that your data has been evaluated. This is the receipt that GTU has received a copy of the data that you have uploaded and submitted as your project work.

*Guide has to sign the certificate, Only if all above activities has been Completed.



Institute of Technology and Management Universe

Dhanora Tank Road, Paldi Village, Halol Highway, Near Jarod, Vadodara - 391510 (Gujarat),
INDIA.

DECLARATION

We hereby declare that the Project report submitted along with the Project entitled **Secured E-voting With Graphical Insights By Utilizing Blockchain** submitted in partial fulfillment for the degree of Bachelor of Engineering in Computer Science and Engineering to Gujarat Technological University, Ahmedabad, is a bonafide record of original project work carried out by us at **Institute of Technology and Management Universe** under the supervision of Prof. Ninad Bhavsar and that no part of this report has been directly copied from any students' reports or taken from any other source, without providing due reference.

Name of the Student

Sign of Student

- 1 Arsh Vishwakarma(180950131104)
- 2 Dennis Tank(180950131096)
- 3 Vyoma Yogeshkumar Shah(180950131092)

ACKNOWLEDGEMENT

We would like to express our gratitude to everyone who helped us in completing this report. A special token of appreciation to our project coordinator, who helped us by giving us suggestions and feedback, and also helped in previewing the project with encouragement for our work in the E-voting project “EVS” as a part of Bachelor of Engineering in the department Computer Science and Engineering.

We would like to thank our Internal Guide Prof. Ninad Bhavsar who supported us fully by always solving our doubts and giving us pointers of improvement from his side. We would also like to express our sincere thanks to our Head of department and other professors for their cooperation and contribution in our project.

We would also like to sincerely express our thanks to the college for giving us immense support in all aspects and in all our project works.

Thank You,
Arsh Vishwakarma,
Dennis Tank,
Vyoma Shah

ABSTRACT

Electronic voting, or e-Voting, is the use of modern technologies in the process of marking or casting a vote during elections. E-voting is an election system that allows voters to record a secret ballot and have it tabulated electronically. There are three types of E-voting including Direct recording electronic (DRE) voting machines, which are used to electronically mark and cast votes. Ballot marking devices (BMD), also known as electronic ballot markers (EBM), which electronically mark and print a paper ballot. Online voting or internet voting systems, allow voters to mark and cast their votes online. There are multiple benefits of e-voting like faster counting and delivering results at a faster pace, Increased trust of voters in the voting system which makes democracy better, fewer human errors in voting, reduced cost in the voting system, and reduced ballot waste. The e-voting system provides the guarantee of anonymity with high security, confidentiality, and integrity. This also helps the voters to vote without wasting much effort and the counting of votes becomes easier with records maintained and kept confidential. There are two types of creating e-voting online one is a direct and traditional method and the other is using blockchain. The blockchain method provides more security as well as anonymity which makes it a much better option. The method used in this project is also based on blockchain.

List of Figures

Figure 1 Gantt Chart

Figure 2 Block Diagram of Remote (Internet) Voting Machine System

Figure 3 Blockchain Process in the system

Figure 4 Online Blockchain-based E-voting system

Figure 5 System Methodology Layout

Figure 6 Data Structures & Database Schema

Figure 7 Flow chart of E-voting System

Figure 8 State Transition Diagram

Figure 9 Input-Output Structure

Figure 10 V8's Compiler Pipeline

Figure 11 User Registration Page

Figure 12 User Login Page

Figure 13 User Dashboard

Figure 14 User Creating A Voting Agenda

Figure 15 User Dashboard With Participation Details

Figure 16 User Dashboard With Vote Now Option

Figure 17 Option Selection Page

Figure 18 Seed/Secret Submission Page

Figure 19 Successful Vote Upload Alert

Figure 20 User Dashboard Waiting For Result

Figure 21 User Dashboard With Generate Result Option

Figure 22 User Dashboard With The Results

List of Tables

Table 1 Ideal Features/ Requirements

Table 2 List of features in the proposed system

Table 3 Continuous Evaluations

Abbreviations

HTML - Hypertext markup language
CSS - Cascading style sheets
EVM - electronic voting machines
DPT - voters list database
JSON - JavaScript Object Notation
API - Application Programming Interface
BEV - Blockchain-Enabled Voting
NEC - National Election Commission
SEC - Securities and Exchange Commission
NVLAP - National Voluntary Laboratory Accreditation Program
EMG - Electromyography
QSG - Quick Start Guide
U.S.A - United States of America
EU - Europe
SSL - Secure Sockets Layer
URL - Uniform Resource Locator
PIN -Personal Identification Number
TAN -Transaction Number
HTTPS - Hypertext Transfer Protocol Secure
OTP - One-time password
SMS - Short Message Service
P2P - peer to peer
SHA - Secure Hash Algorithm
js - JavaScript
OS - Operating System
MVC - Model-View-Controller
SEED - a string of anything
DOM - Document Object Model
JIT - just-in-time
ID - Identification
UDP - User Datagram Protocol
UI - user interface
ws - web-socket
SPAM - Unsolicited Bulk Email

Table of Contents

Acknowledgement.....	I
Abstract.....	II
List of Figures.....	III
List of Tables	IV
List of Abbreviations	V
Table of Contents.....	VI
Chapter 1 Introduction to Project.....	1
1.1 Project Summary.....	1
1.2 Project Purpose.....	2
1.3 Project Objective.....	3
1.4 Project Scope.....	4
1.5 Literature Survey and Technology.....	5
1.6 Gantt Chart.....	9
Chapter 2 System Analysis.....	10
2.1 Study of Current System.....	10
2.2 Problem and Weakness of Current System.....	12
2.3 Requirements for New System.....	14
2.4 System Feasibility.....	15
2.5 Process in Proposed System.....	16
2.6 Features of Proposed System.....	18
2.7 Processes and Techniques of Proposed System.....	19
2.8 Selection of Softwares and Algorithms.....	21
Chapter 3 System Design.....	24
3.1 System Design and Methodology.....	24
3.2 Process Design.....	26
3.3 Input / Output and Interface Design.....	28
Chapter 4 Implementation.....	31
4.1 Implementation Environment.....	31
4.2 Module Specifications.....	32
4.3 Results and Outcomes.....	34
4.4 Result Deliberation.....	40
Chapter 5 Testing.....	41
5.1 Testing Strategy.....	41
5.2 Test Results and Analysis.....	42
Chapter 6 Conclusion and Discussion.....	45
6.1 Overall analysis of project viabilities.....	45
6.2 Dates of Continuous Evaluation (CE-I and CE-II).....	46
6.3 Problem Encountered and Possible Solutions.....	47

6.4 Summary of Project work.....	48
6.5 Limitation and Future Enhancement.....	49
References.....	50
Appendix.....	52

1. INTRODUCTION TO PROJECT

1.1 PROJECT SUMMARY

EVS is an electronic voting system that is a highly decentralized application that enables user privacy, integrity, and verification during e-voting at the flexibility of the user's current time and places through systems such as laptops and pc. Depending on the particular implementation, e-voting may use standalone electronic voting machines (also called EVM) or computers connected to the Internet. It may encompass a range of Internet services, from the basic transmission of tabulated results to full-function online voting through common connectable household devices. The degree of automation may be limited to marking a paper ballot or maybe a comprehensive system of vote input, vote recording, data encryption and transmission to servers, and consolidation and tabulation of election results. Here, our system is one that belongs to the section of full-function online voting through common connectable household devices. This system provides users with confidentiality and integrity at the same time it refrains from taking too much personal info of the user.

An e-voting system must be capable to deal successfully with strong requirements associated with security, accuracy, integrity, swiftness, privacy, auditability, accessibility, cost-effectiveness, scalability, and ecological sustainability. Our system provides a maximum of these pointers so that users can vote with high security and without worrying about any other problems faced during the traditional voting system.

1.2 PROJECT PURPOSE

EVS is a project made to make voting so easy that a maximum number of people vote. In this technological era, people feel traditional voting to be cumbersome. So to make voting simple and easy just like any other application this project is created. This makes voting very much effortless and the time consumed is also very little - just a few clicks to vote. You can vote within your comfort of home and also maintain confidentiality as well as anonymity of the vote. Besides this project will also provide with the insights of voting done this way people won't have to wait for the news to relay or to look into the whole news just to know about the results or any other insights regarding the voting done.

1.3 PROJECT OBJECTIVE

EVS is a project which is made by keeping the drawbacks of already existing systems in voting as well as utilizing the best points of current voting systems to their fullest with the addition of technological changes to make it more secure, transparent, convenient, accurate, swift, and cost-effective.

Traditional voting is a tedious job not just for users even for the supervisors and the vote counters as well as the result generators. The ballot supervision, the vote counting, and the result generation take up too much time and effort and if any error occurs or if there is any leak noticed then the work increases. So, if the voting is made online then there would be no need for such supervision, vote counting, and the results, all of these can be recorded and done by the servers and machines making it simple for the users and observers. The votes can be kept anonymous and confidential at the same time recorded as counts for proof of the vote being conducted. Also, the results will be counted on the basis of votes made and votes not done at all. It also maintains records to prevent double voting. The security helps in checking whether the said person is conducting the vote or not. This way the traditional voting best points can be imbibed into the technology to make it better and more reliable.

1.4 PROJECT SCOPE

The scope of the project includes the pointers:

- The project has an email system to get registered. This helps in maintaining security.
- The project then uses the email and password to let the user provide their credentials for logging in to vote.
- According to the process of the project, there is a unique code generated and sent to the mail id provided by the person which maintains confidentiality, integrity, and authenticity of the process.
- The project also provides visual insights to the user about the voting results which makes them get an idea about the voting.
- The project has a blockchain system that makes vote counting and recording easier.
- The records also make sure that no user has voted twice.
- The timer ensures that users can vote at their flexibility of time.

1.5 LITERATURE SURVEY AND TECHNOLOGY

Research Paper:

Technologies on which EVS is made are client/server and blockchain. The important aspects of EVS are data storage, user identification, and knowing your customer techniques including user's credentials, biometrics, and others. The traditional method is username and password login which is less secure than blockchain technology. Requirements of the private blockchain (better option) are anonymity, accuracy, transparency, and integrity.^[1]

Research Paper:

Waterfall development method(2 variations sequential or linear). EVS authenticates the eligibility of individuals casting a vote against the DPT(voters list database) database, the process ensures the claimed resource is the correct person. The authentication process is a verifiable principle to identify whether voting is done with or without revealing identity.

Advanced Encryption Standard for authorization with symmetric key encryption to reduce operation time with a fast-paced system. Blockchain- advantage being authorization and integrity with hash in hex form from the previous block. Decentralized servers make it difficult for attackers to tamper with data as replicas are there. Ethereum is decentralized, has smart contract capability, high success rate. Geth manages consensus write, node network authorization, commanding smart contract data from JSON remote control procedure call protocol API. Unified modeling language datagrams to visualize existing systems as a base to create new ones. A decentralized peer-to-peer network solves issues of centralized one prevents data manipulation, and loss of data, increases security, makes collecting and counting faster and easier in turn encouraging the voters to vote. The waterfall method ensures the robustness and stability of the system.^[2]

Research Paper:

Due to security issues, blockchain was introduced in e-voting.

1. Entirely decentralized i.e. no central authority is needed for verification
2. Vote counting and tracking should be available
3. The anonymity of vote should be provided.^[3]

Conference Paper:

In March 2017, the South Korean province of Gyeonggi-do employed a Blockchain-Enabled Voting(BEV) system to vote on the Ddabok Community Support Project. Nine- thousand residents voted using a blockchain platform developed by the Korean financial-technology startup Block that included smart contracts. The votes, results, and other relevant data were stored in a blockchain. No management or central authority was involved in this process. This was the first time South Korea applied such a technology. BEV is a flexible solution that enables secure, cost-effective voting to facilitate shareholder participation and voting from a distance.

Also, improved identity verification can help increase access and participation. For example, according to a federal court in Texas, 608,470 registered voters lacked verification identification. Approximately 11 percent of US citizens lack government-issued photo identification cards.

BEV can improve this situation. For instance, Voatz accepts 10 different official documents including driver's licenses, state IDs, and passports to verify voter identity.

BEV can increase the speed with which votes are tallied. For example, Agora reported that it published election results on its website five days before the official manual counts ended.^[4]

Research Paper:

Using a Blockchain mechanism all the transactions are clearly visible to the election bodies at every level. Also, the voters are notified regarding the status of their votes which boosts people's faith, further strengthening democratic institutions. Although several approaches have been proposed to ensure transparent and secure e-voting, however, there are several issues that still exist at various levels such as multiple fake registrations of a voter at more than one place and infringement with votes before the day of counting that need to be tackled. With the help of the 5G network, the approach they proposed was

1. Initially, a Blockchain is set up by the National Election Commission(NEC) which is the supreme authority for monitoring the elections for the entire country. The

NECs direct and coordinate the activities of State level Election Commissions which are responsible for the smooth conduct of elections within their boundaries.

2. Next, the several district levels subsidiary election bodies of various states are added to the Blockchain which manages the process of polling in their respective districts and reports to the SECs.

3. The final level consists of the various polling booths located in a district where voters cast their votes. When a voter casts a vote, a secret key is generated for each voter on the basis of his/her biometrics, and the same is displayed in the database of all the entities.^[5]

Research Paper:

There are two methods of realizing anonymity in the blockchain. The first is to generate a wallet address through a public key as a pseudonym of a node and hide its identity by pseudonym. Nevertheless, this method achieves no real anonymity since the real identity of the node can be determined by address clustering and other methods. The other method is to adopt the ring signature scheme for signing transaction data.

They adopted the code-based public-key cryptographic algorithm, which makes the e-voting protocol can resist quantum attacks.^[6]

Research Paper:

Using Blockchain or a Decentralized Database System in e-voting seems to be a solution for all other flaws that come with the traditional centralized systems. However, there is much research yet to be done to be sure about the perfection or proper outcomes of using blockchain over normal systems. There are still countable vulnerabilities which, up to a proportion negate the veracity that, blockchain is an ideal solution. For instance scalability attacks, lack of transparency, and the internet is still not a trustful entity. Overall, it is quite irrefutable that blockchain is still an incipient concept when it comes to e-voting.^[7]

Research Paper:

A model for an e-voting system has been proposed which follows the guideline of NVLAP, EMG, QSG and stand close to U.S.A and EU standards for voting. The has passed many tests accomplishing the completion of the automation tasks that fulfill the standards. However, e-voting is a topic that is rather a concept of philosophical and subjective beliefs which is one of the limitations. In addition to this, the concept is still in an evolutionary stage which explains the impede.^[8]

Research Paper:

When comparing the blockchain e-voting concept with the paper-based voting system- extracts many more problems that are not yet present in paper-based voting. If blockchain is introduced to voting, and even if it solves a fraction of the current problems faced, then there will be new hinders specifically related to blockchain. New technology will bring new methods to penetrate the systems and overall even if the concept works, there is a possibility for a potential monopoly over the processes which might make the system biased.^[9]

1.6 Gantt Chart

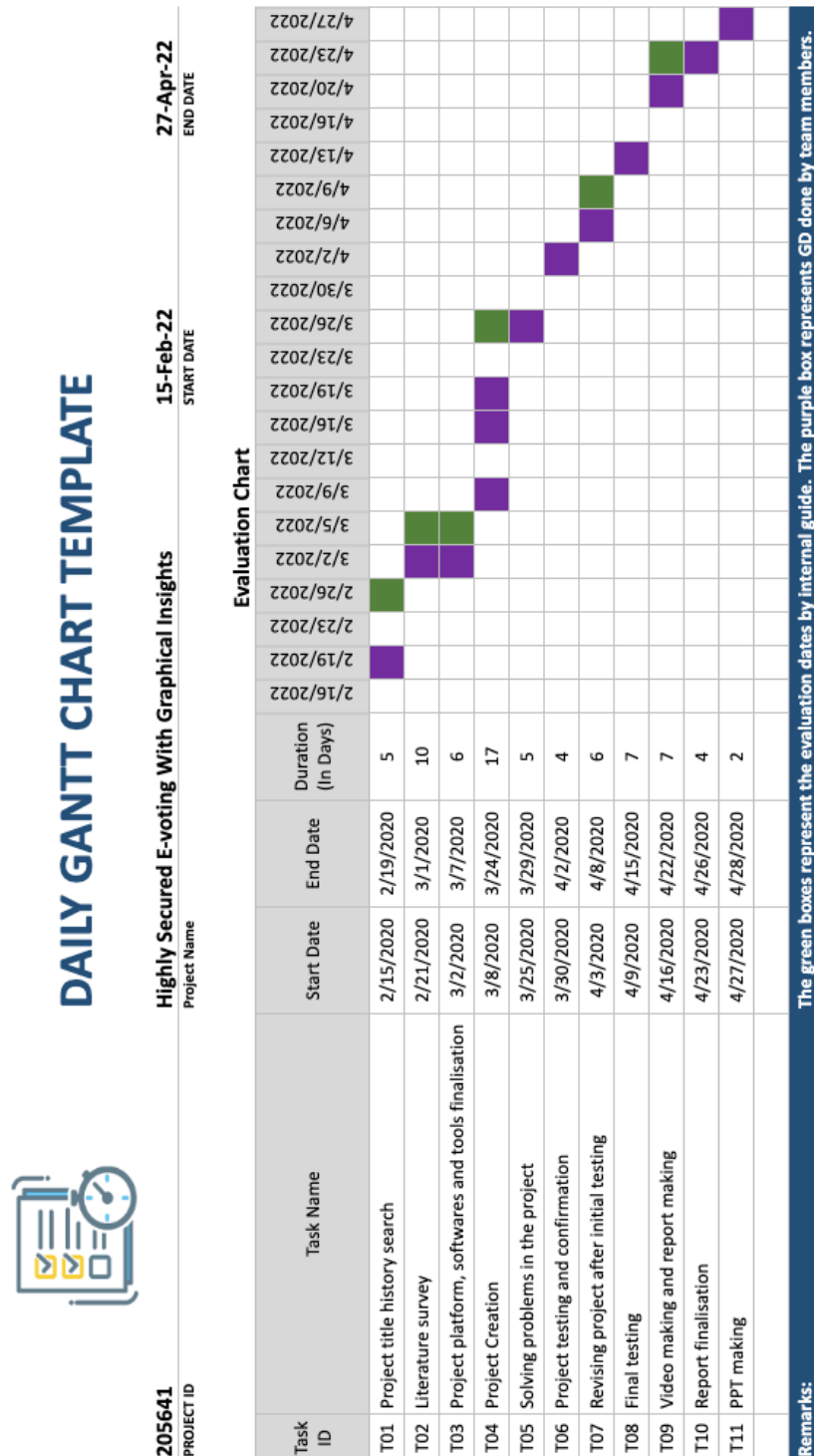


Figure 1 Gantt Chart

2.SYSTEM ANALYSIS

2.1 STUDY OF CURRENT SYSTEM

Internet Voting or Online Voting System helps the users to cast their vote from internet-connected computers or mobile anywhere in the world. In this system, the voters' login to a specific website, and their identity is authenticated. It is followed by the voting process. Once the process is completed, the user logs off from the system. Online voting increases the voter's participation and it is easier than poll site voting. The Internet Voting System contains:

- Database
- Server
- Mixnet (Encryption and Decryption)
- Tallying and Result Consolidation

Database

The database contains voter's information like Name, Age, Telephone Numbers, etc. It is responsible for collecting, storing, and maintaining the data.

Server

The server is responsible for the authentication of the user based on the details entered by the user.

Mixnet

Mixnet is a mixed network that is a set of protocols that aids in Encrypted communication by using a chain of proxy servers called Mixes which take in messages, shuffle and send them randomly to the next destination. Decryption Mixnet involves decrypting messages by using the private key and the message order is shuffled by the node and transmits the result to the next node.

Tallying and Result Consolidation

The completion of the voting process is followed by Result consolidation after the tally process of votes.

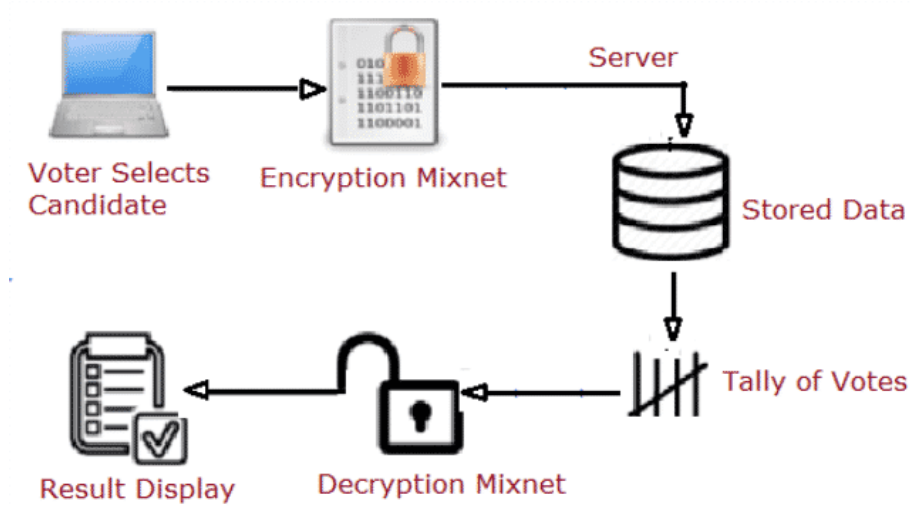


Figure 2 Block Diagram of Remote (Internet) Voting Machine System

SSL is a system used currently for traditional e-voting systems. Secure Sockets Layer (SSL) is a type of protocol that secures confidential data over the internet through a process known as encryption. Hence, the goal of SSL is to provide data privacy. For this purpose, a secure connection between the web browser and the server is created. A Website that has an SSL certificate will contain a small padlock before the website's URL. This means that the site is secured to conduct transactions.

2.2 PROBLEM AND WEAKNESS OF CURRENT SYSTEM

Weakness in the Current System:

- The unauthorized intervention of third parties in the voting process. Given the current state of information technology, there is no guarantee, that a program would not be manipulated to allow the storage and printing of a form or document different from the one appearing on the screen.
- More difficult to detect and identify the source of errors and technical malfunctions than with conventional procedures.
- The possibility that a fully digitized system would fail to produce results and lack physical backup records, makes a public recount difficult or impossible.

Challenges of remote e-voting:

In the context of remote e-voting, special attention should be given to the process of guaranteeing a free and secret vote. Only entitled voters are allowed to cast a vote and this requires that every voter be authenticated (e.g. by using a PIN -Personal Identification Number or TAN -Transaction Number or by the use of a digital signature) and their right to vote verified. In order to prevent multiple votes from being cast or other misuses, a record must be made and checked in order to establish whether he or she has already cast a vote. With a remote electronic voting system, there must be an electronic separation between the vote and the identification of the voter.

Weakness in SSL System:

- Performance - Encryption and decryption of data before the data is used causes the speed of transactions to reduce because of the SSL certificate. But this decrease has noticeable effects only on large websites.
- Cost - Purchasing and setting up an SSL certificate can be quite costly as it varies from website to website. (From the level of identity verification and how many domains and subdomains the certificate is going to cover). There are free certificates available but they don't have much security.

- Expiry - The SSL certificate comes with an expiry time and if not renewed then it will lose its security, in turn, reducing the trust from the user's side.
- Caching - Caching is used for content encryption but if it is too complex to set on the web browser then to handle it one will need an additional server to the system to look after the encryption before it reaches the caching server.
- Protocol Complications - If the SSL certificate isn't implemented properly, the files that should be served through HTTPS will be served via HTTP. Hence, there will be a warning message displayed to the visitors stating that their data is not protected.
- Application Support - In its initial stages, SSL was only meant to support web-based applications. Anything other than that requires purchasing modules from application vendors. Additionally, the setup process isn't easy, it also requires changes in the in-house software.

2.3 REQUIREMENTS FOR NEW SYSTEM

2.3.1 IDEAL FEATURES:

- | |
|--|
| <ol style="list-style-type: none">1) Confidentiality2) Robustness and Integrity3) Authenticity/ Verifiable participation4) Eligibility5) Fairness6) Soundness7) Completeness8) Anonymity9) Auditability and Accuracy10) Democracy/Singularity11) Vote Privacy12) Lack of Evidence13) Transparency and Fairness14) Availability15) Accessibility and Reassurance16) Recoverability and Identification17) Voters Verifiability |
|--|

Table 1 Ideal Features/ Requirements

2.4 SYSTEM FEASIBILITY

2.4.1 Does The System Contribute To The Overall Objectives Of The Organization?

Yes, the system contributes to the overall objectives of the target end-users in organizations such as: -

- Student-centric organizations like Schools, Institutes, and Universities.
- Government elections on a small scale so far.
- Private companies in decision-making through stakeholders as participants.
- Innovation Councils in inferring the Startup Seed Funding Amount, proceeding executions, etc.

2.4.1 Can The System Be Implemented Using The Current Technology And Within The Given Cost And Schedule Constraints?

Yes, the system can be implemented using the current technology, however, may exceed the given cost & schedule(3-4 months) constraints in case of the integration with biometric verification through Aadhaar API which requires the support of licensing with funding.

3rd party OTP integration may also cause costs exceeding 0.16 Rupees per SMS OTP to range from 2-15 thousand Rupees for 5000 - 50000 messages via platforms such as 2factor.in, smsindiahub.in, etc.

2.4.1 Can The System Be Integrated With Other Systems Which Are Already In Place?

The system can be integrated with Aadhaar API, Mobile OTP services, National Voter's Service portal, etc.

2.5 PROCESS IN PROPOSED SYSTEM

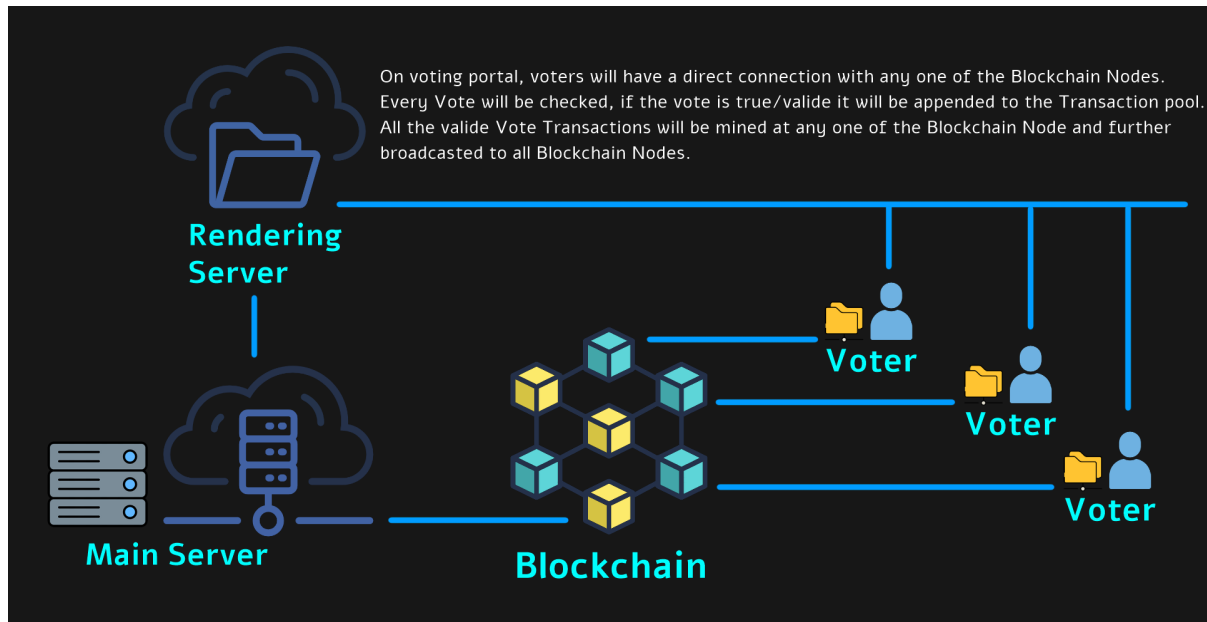


Figure 3 Blockchain Process in the system

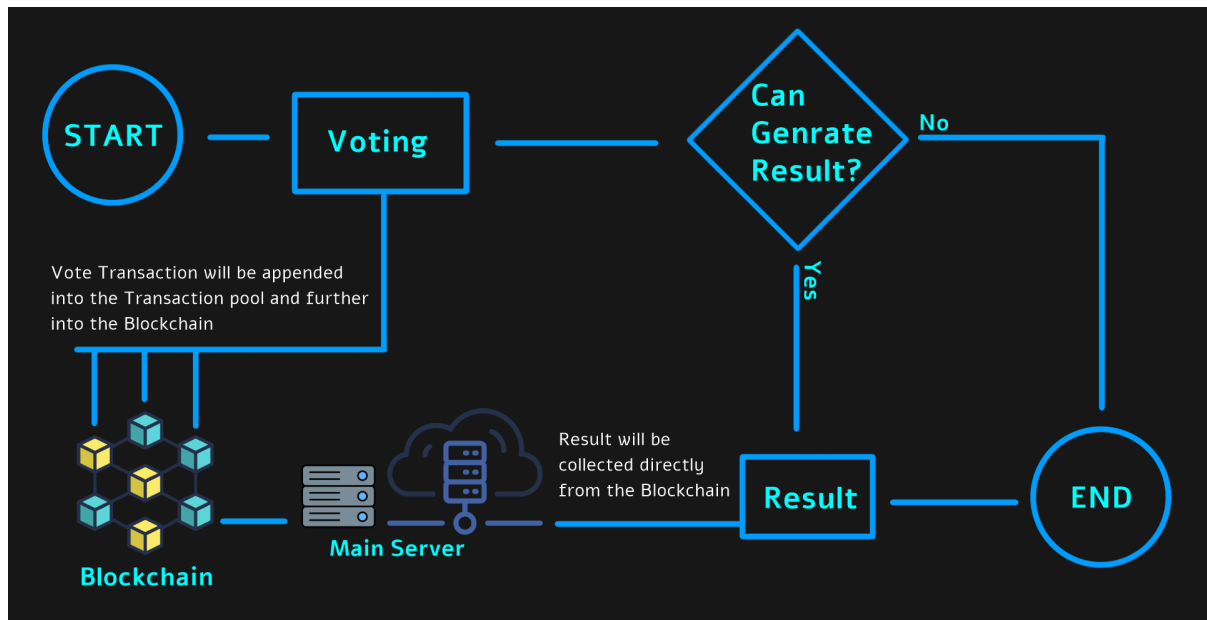


Figure 4 Online Blockchain-based E-voting system

The overall process of EVS:

In the EVS project, the system works with three major sections in consideration that includes the voter registration, voter voting, and the result display for the users. On the developing side, it focuses on the concepts of producing a secret key for the user during registration for voting, the tallying of votes, the storage of casted votes, to ensure no user credential is casting votes more than once, to calculate results of voting and to connect to the user to get the user credentials and to illustrate the results to the user.

2.6 FEATURES OF PROPOSED SYSTEM

Features in the Given System:

- 1) Confidentiality
- 2) Integrity
- 3) Authenticity/Verifiable participation
- 4) Unreusability
- 5) Fairness
- 6) Auditability & accuracy
- 7) Transparency
- 8) Voters verifiability
- 9) Democracy/Singularity

Table 2 List of features in proposed system

Features of a System made from Scratch:

- Meets Specific Requirements needed by the website
- Flexible
- Scalable
- Easy to maintain
- Highly Secure
- Support is provided
- Easy to use
- Reliable
- Easy to handle

2.7 PROCESSES AND TECHNIQUES OF PROPOSED SYSTEM

- API Logic/Algorithm.

An Application Programming Interface (API) is a gateway that allows one App to communicate with other Apps – and defines how that communication occurs. They foster connections between technologies to improve the user experience. API is a collection of software functions and procedures. APIs enable to explain how web applications communicate with each other. They process data transfer between systems and locate between the application and the webserver. APIs enable access to software (or web data) in a controlled and secure way for the program. Then the code sends requests to the receiving software and returns the data.

- Proof-of-work Algorithm.

A solution that is difficult to find but is easy to verify. The purpose of a consensus mechanism is to bring all the nodes in agreement, that is, trust one another, in an environment where the nodes don't trust each other. All the transactions in the new block are then validated and the new block is then added to the blockchain. Note that, the block will get added to the chain which has the longest block height

- P2P Blockchain Server.

P2P is a technology that is based on a very simple principle, and that is the concept of decentralization. The peer-to-peer architecture of blockchain allows all cryptocurrencies to be transferred worldwide, without the need of any middle-man or intermediaries, or central server. With the distributed peer-to-peer network, anyone who wishes to participate in the process of verifying and validating blocks can set up a Bitcoin node. Blockchain is a decentralized ledger tracking one or more digital assets on a peer-to-peer network. When we say a peer-to-peer network, it means a

decentralized peer-to-peer network where all the computers are connected in some way, and where each maintains a complete copy of the ledger and compares it to other devices to ensure the data is accurate.

- Website Design and Pre-renderings.

Web design is the process of planning, conceptualizing, and arranging content online. The web designing process includes stages of choosing a web design tool, then getting the required visual and functional elements, and then finally putting up which type of website illustration it should have adaptive or responsive. Here our website is a responsive website.

Pre-rendering, or prerendering, is a web browser feature that speeds up your web surfing experience. When you view a web page, some content from another page or site might be prerendered in anticipation of you going there next. If you do, the new page loads very quickly because some of its elements were rendered ahead of time.

2.8 SELECTION OF SOFTWARE AND ALGORITHMS

Selected Algorithms:

1. Consensus Algorithm

Principle: A solution that is difficult to find but easy to verify.

Working: As an instance, the Bitcoin network, and by extension, the Proof of Work consensus algorithm has eliminated the need for users to vest their trust in a traditional bank. Instead of transactions being stored in one central location, such as a bank, transactions take place on a public network for everyone to view. Once completed, a transaction can never be reversed or modified. When any amount of Bitcoin passes from one person to another, it is considered a transaction that the network needs to keep a record of. The process of verifying the transactions in the block to be added, organizing these transactions in chronological order in the block, and announcing the newly mined block to the entire network does not take much energy and time. The energy-consuming part is solving the 'hard mathematical problem' to link the new block to the last block in the valid blockchain. When a miner finally finds the right solution, the node broadcasts it to the whole network at the same time, receiving a cryptocurrency prize (the reward) provided by the PoW protocol. With more miners comes the inevitability of the time it takes to mine the new block getting shorter. This means that the new blocks are found faster.

Common cryptographic protocols used in Proof of Work systems: The most widely used proof-of-work consensus is based on SHA-256 and was introduced as a part of Bitcoin. Others include Scrypt, SHA-3, scrypt-jane, scrypt-n, etc.

Features of Proof of Work system:

- It is hard to find a solution to the mathematical problem
- It is easy to verify the correctness of that solution

***We are utilizing currently the Proof Of Work Consensus algorithm based on SHA-256 in Prototype.**

Selected Software:

1. Node.js - Node.js is a platform built on Chrome's JavaScript runtime for easily building fast and scalable network applications. Node.js uses an event-driven, non-blocking I/O model that makes it lightweight and efficient, perfect for data-intensive real-time applications that run across distributed devices. Node.js is an open-source, cross-platform runtime environment for developing server-side and networking applications. Node.js applications are written in JavaScript and can be run within the Node.js runtime on OS X, Microsoft Windows, and Linux. Node.js also provides a rich library of various JavaScript modules which simplifies the development of web applications using Node.js to a great extent.
2. React.js - ReactJS is a JavaScript library used for building reusable UI components. React is a library for building composable user interfaces. It encourages the creation of reusable UI components, which present data that changes over time. Lots of people use React as the V in MVC. React abstracts away the DOM from you, offering a simpler programming model and better performance. React can also render on the server using Node, and it can power native apps using React Native. React implements one-way reactive data flow, which reduces the boilerplate and is easier to reason about than traditional data binding.
3. CSS - Cascading Style Sheets, fondly referred to as CSS, is a simple design language intended to simplify the process of making web pages presentable. CSS handles the look and feel part of a web page. Using CSS, we can control the color of the text, the style of fonts, the spacing between paragraphs, how columns are sized and laid out, what background images or colors are used, layout designs, variations in display for different devices and screen sizes as well as a variety of other effects.

4. HTML - HTML stands for HyperText Markup Language, which is the most widely used language on the Web to develop web pages. It can be assisted by technologies such as Cascading Style Sheets (CSS) and scripting languages such as JavaScript. Web browsers receive HTML documents from a web server or from local storage and render the documents into multimedia web pages. HTML describes the structure of a web page semantically and originally included cues for the appearance of the document. HTML can embed programs written in a scripting language such as JavaScript, which affects the behavior and content of web pages.
5. Adobe Photoshop - Photoshop is a photo editing and raster graphic design software that allows users to create, edit, and manipulate various graphics as well as digital art. It also allows to create and edit raster images with multiple layers and importing the images in various file formats.
6. Tailwind CSS can be used to make websites in the fastest and the easiest way. Tailwind CSS is basically a utility-first CSS framework for rapidly building custom user interfaces. It is a highly customizable, low-level CSS framework that gives you all of the building blocks you need to build bespoke designs without any annoying opinionated styles you have to fight to override. The beauty of this thing called tailwind is it doesn't impose design specifications or how your site should look, you simply bring tiny components together to construct a user interface that is unique. Tailwind simply takes a 'raw' CSS file, processes this CSS file over a configuration file, and produces an output.

3. SYSTEM DESIGN

3.1 SYSTEM DESIGN AND METHODOLOGY

Architecture of the Prototype:

Main Server will manage the connection between the blockchain nodes so that they can communicate with each other. Front-Server is a Server-Side Rendering Server and is responsible for the construction of Web-App. Blockchain nodes will constantly communicate with each other to build and rebuild the blocks as well as the entire chain.

Work Flow:

The Key-Pair is something that is defined as a Wallet in Crypto. More often it can be created by a SEED (a string of anything) or Secret. By using this property we can create an address that can act as a pointer for a single VOTE. On creation of a Voting Session, every registered participant will get an email with a Secret/SEED, however, these Secrets will neither be stored anywhere on the Main Server nor on Blockchain nodes. Every blockchain node will maintain a list of addresses, which can be used to validate if a particular address is allowed to vote or not. These addresses will be created parallelly with the sending of emails. At the time of voting the participant will have to type the SEED at the portal page to vote and only if the Secret is correct the participant vote be uploaded to the Blockchain Transaction.

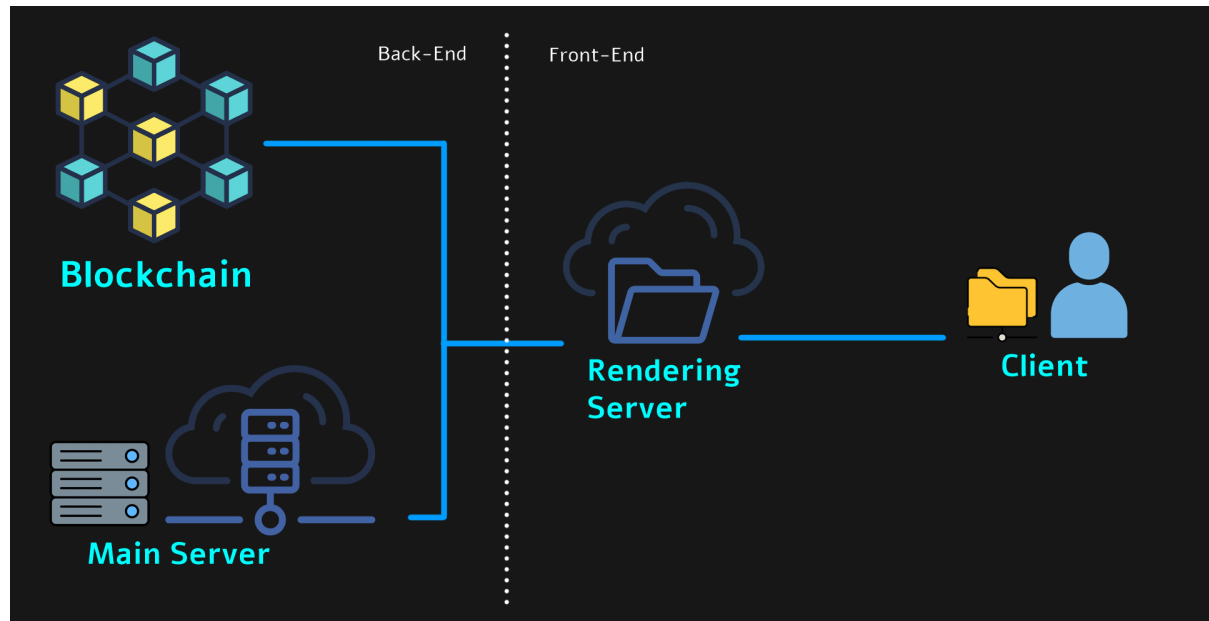


Figure 5 System Methodology Layout

3.2 DATA STRUCTURE & DATABASE DESIGN / PROCESS DESIGN

3.2.1 DATA STRUCTURE & DATABASE DESIGN

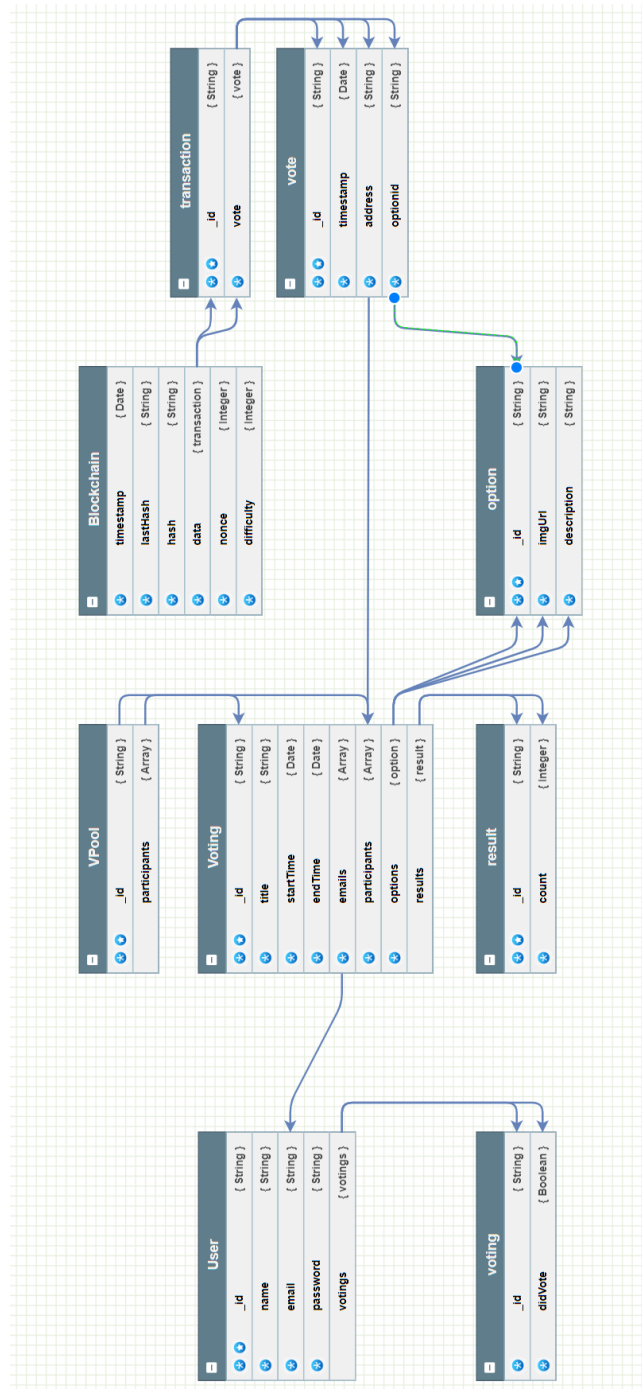


Figure 6 Data Structures & Database Schema

3.2.2 PROCESS DESIGN

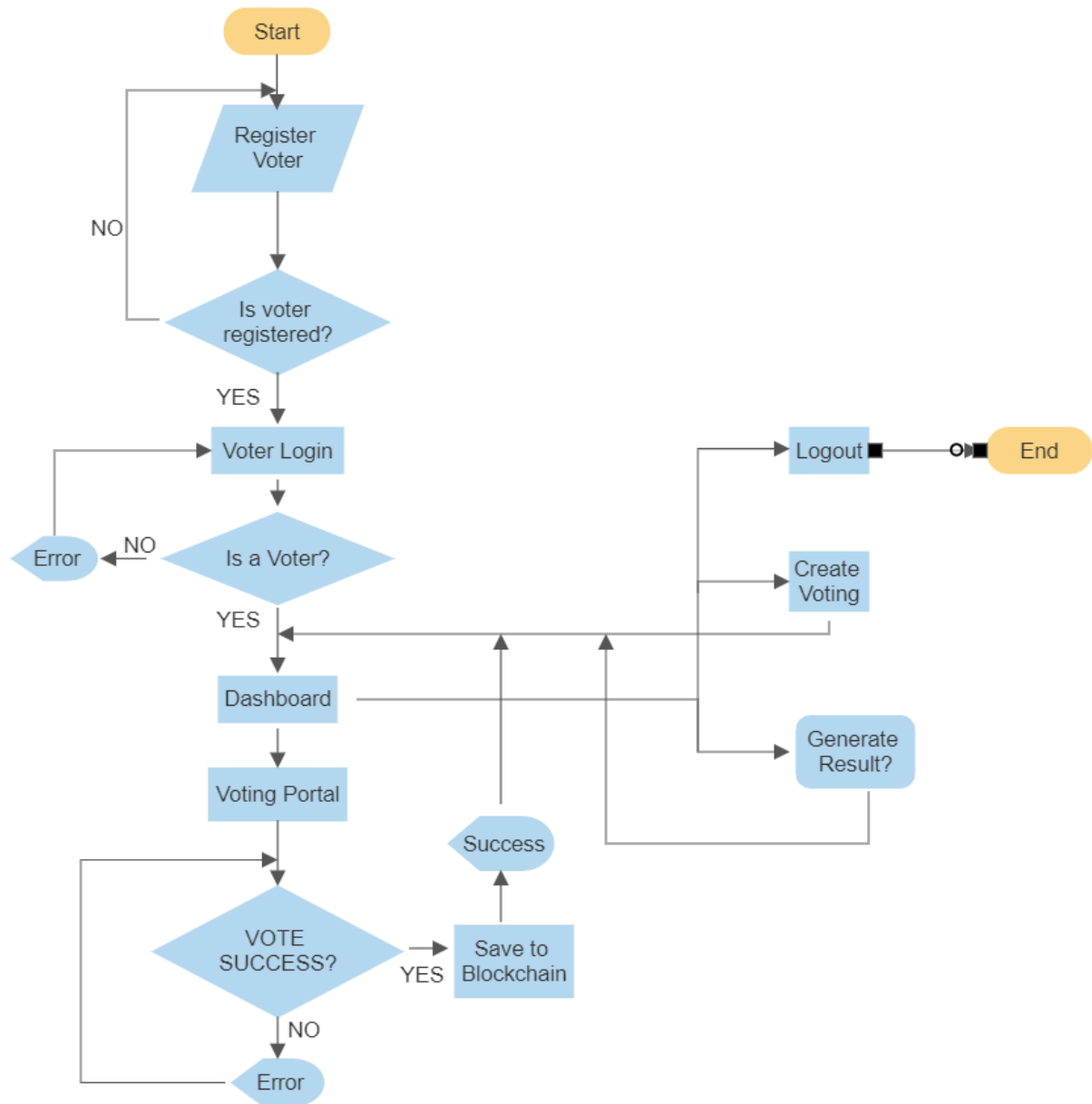


Figure 7 Flow chart of E-voting System

3.3 INPUT / OUTPUT AND INTERFACE DESIGN

3.3.1 State Transition Diagram

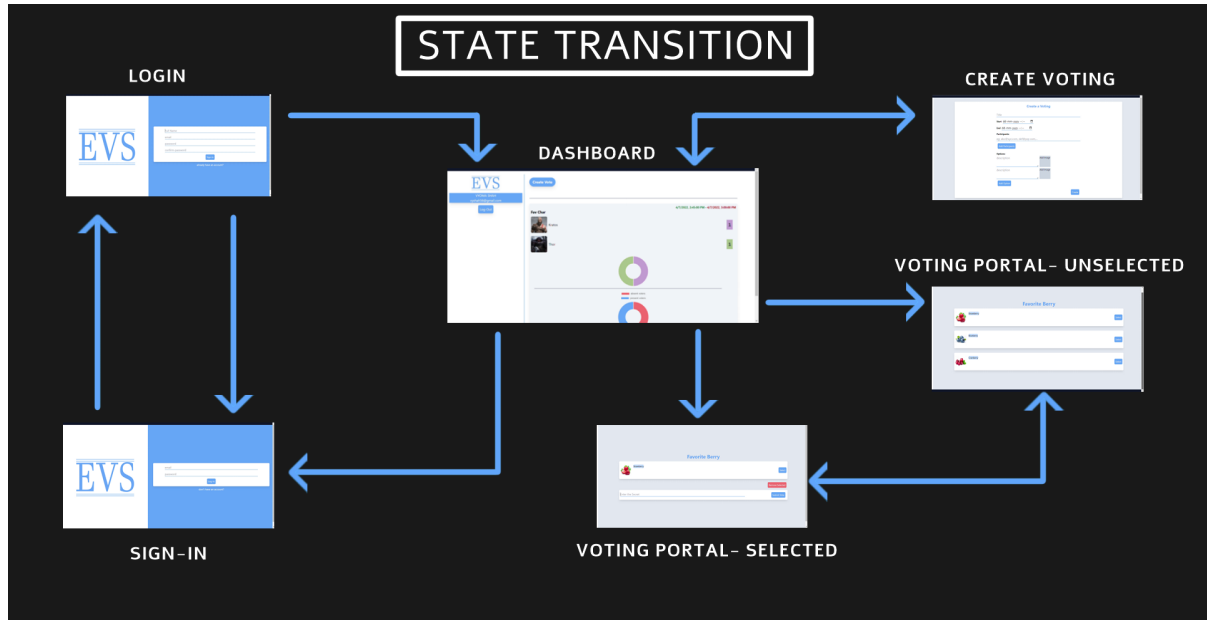


Figure 8 State Transition Diagram

3.3.2 Samples of Forms, Reports, and Interface

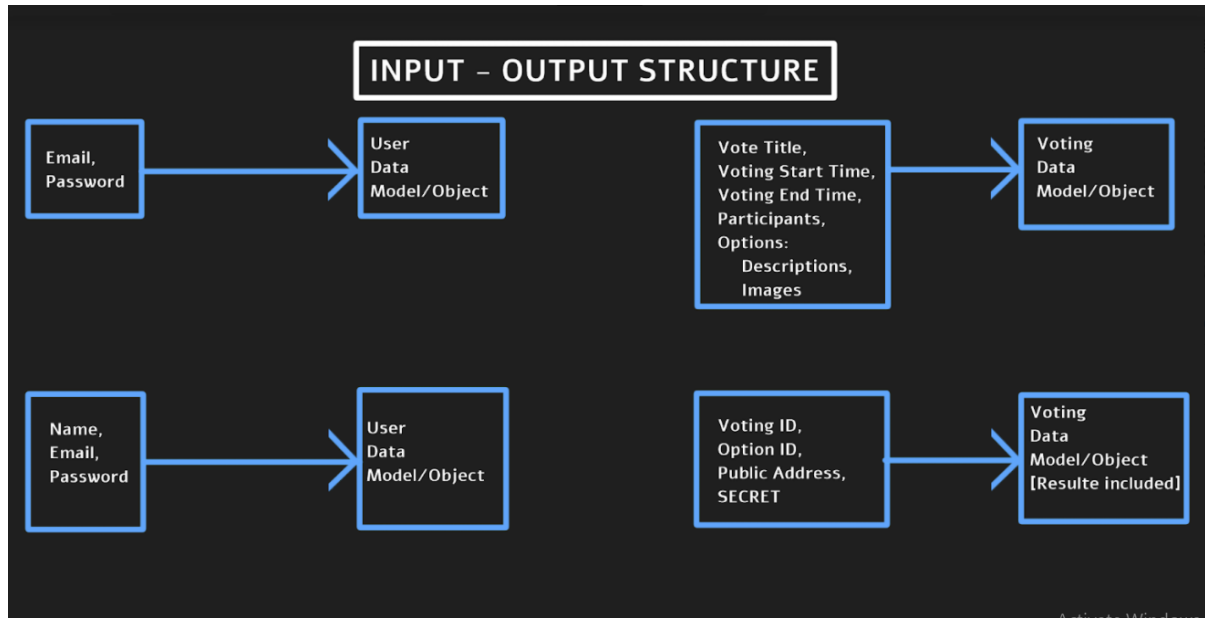


Figure 9 Input-Output Structure

3.3.3 Access Control Mechanism

On the Landing Page, there is a provision for registration with fields such as full name, email id & password. As soon as the user registers himself/herself on the portal, his/her data is stored on the main server in the users.json file with the help of Cake base JSON database.

Otherwise, the user can also log in through his/her valid credentials as saved earlier in the user.json file. After logging in, they have the access to the following: -

- 1) Creating a voting agenda(with description) by setting the date & time for starting & closing the voting period, and adding the participant's email id with the options to choose from which can be any combination of text & image.
- 2) They have the access to vote for any ongoing voting,
 - a) If their email has already participated in that agenda i.e, their role is a participant also.
 - b) As a participant, they must have received an email containing a random Secret/Seed, which they have to enter & submit accurately/ case-sensitively while selecting their choice.
 - c) And the voting period has already started.
- 3) They have the access to generate the result of the voting agendas, where the voting period is over & for the same which they have already voted once(as the system promotes singularity/democracy of votes).
- 4) They have the access to view the graphical insights of the previously participated list of voting agendas.

This Secret which is sent on the participants' email id is a 6-word random uppercase Seed with a “.” appended after each word. This secret acts as a private key for any participant to vote once by typing(not copying) & submitting the exact seed they received on their email id.

Each voter has an individual voting transaction id for his/her votes and a didVote boolean variable which denotes whether he/she voted or not in the backend

4. IMPLEMENTATION

4.1 IMPLEMENTATION ENVIRONMENT

This project's backend is powered by Node.js & the frontend revolves around HTML, CSS & mainly the React.js library. Hence, the key player is the JavaScript engine namely V8 which also powers Google Chrome & was developed by Google.

V8 provides the runtime environment i.e., takes the JavaScript & executes it while browsing. Whereas the DOM & other Web APIs are enabled by the browser.

This JavaScript runtime environment engine is independent of the browser in which it is hosted, thereby providing multi-browser support for the e-voting system at different client-side servers/nodes.

V8 is written in C++ language for faster execution & also promotes mobility as the code executed through it runs on Mac, Windows, Linux, and many more systems. V8 follows a just-in-time(JIT) compilation to increase the execution speed of code. This engine acts as an interface between C++ & JavaScript.

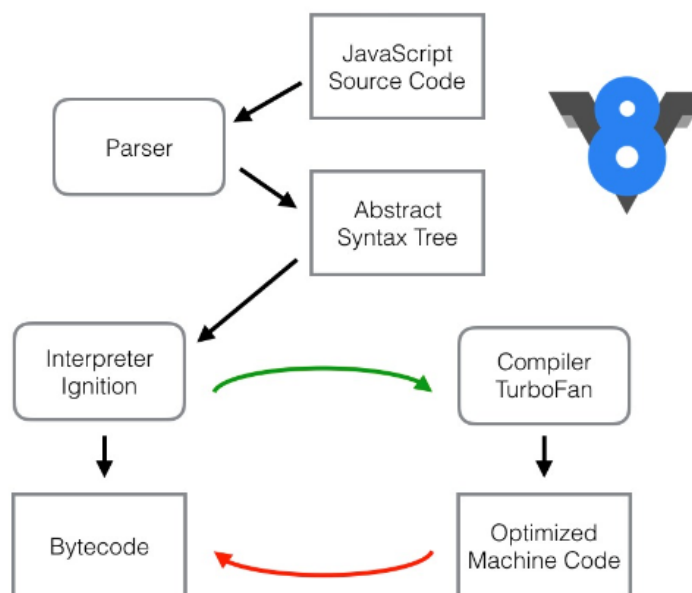


Figure 10 V8's Compiler Pipeline

4.2 MODULE SPECIFICATIONS

Next: -

Next.js is a library in the node for building web-based applications using the React.js framework. It utilizes a mini-react engine which is written in Typescript.js to build a react page. It uses Model View Control Architecture with Server Side rendering. The Static pages are pre-rendered which makes them more optimized and faster.

Express: -

Express.js is a node library in the node for making effective and optimal API. It advances JavaScript's asynchronous nature and makes performance-friendly executables.

Body-parser: -

Body-parser is a library with useful parsing algorithms. With the Express 'Use' facility it parses Socket data asynchronously and converts it to a required data structure, for instance, JSON.

Axios: -

It is a library with a simplified form for HTTP/HTTPS requests. It has a pre-coded boilerplate for performing the requests.

UUID: -

It is a library that provides standards and unique IDs for the data to be stored or processed. It is a very handy library that returns a unique ID when even invoked and the uniqueness of the ID depends on many factors such as time and gea location which makes the ID collision almost null.

Web-Socket 'ws': -

Web-Socket is a socket library for the node which is used for UDP data transfer from Socket to Socket for communication. It can handle multiple sockets at a time to minimize the wholesomeness of managing the sockets. It can be used for real-time communication in chat applications or for P2P connections.

Crypitr: -

It is a node module for encrypting and decrypting any data structure by using any random key. As there is an additional factor that is a requirement for encryption and decryption, it makes this method more powerful.

Multer: -

Multer is a library with a pre-coded boilerplate for image processing i.e. encoding, decoding, reading, and writing the images. It can be used for converting, compressing, saving, or sending Images over the internet. In addition to that, it has its own callback functions for all critical steps which give a bit more control over the algorithm.

Nodemailer: -

Nodemailer is a library used in the node for sending emails asynchronously through the code/server. It can be used for authentication of the email.

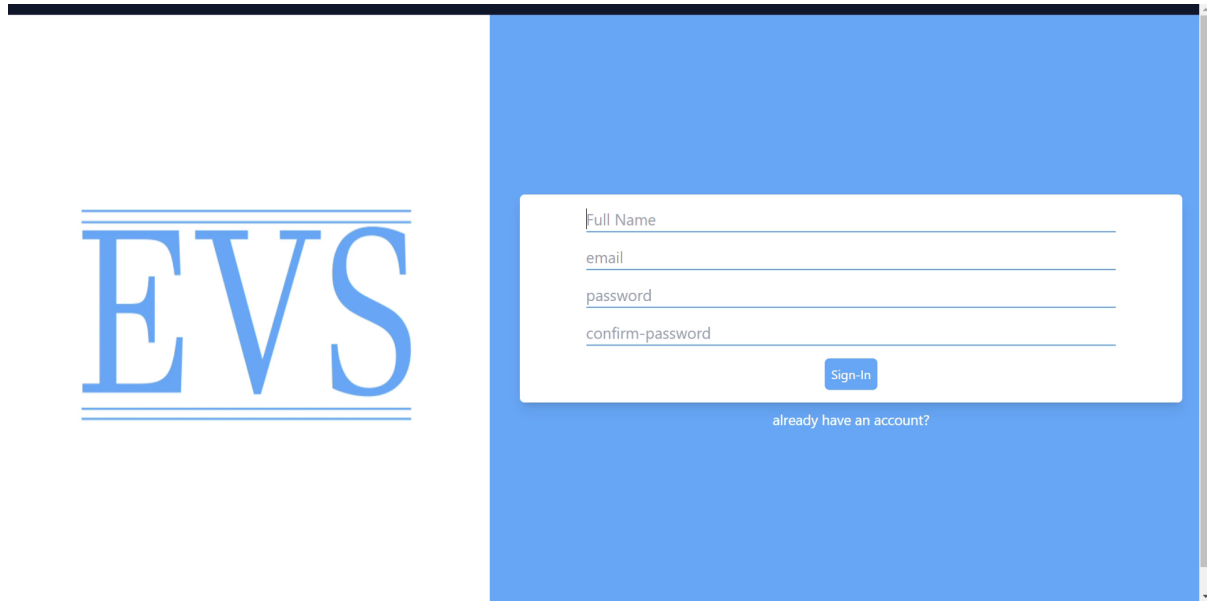
Stellar-Keypair: -

Stellar is a node library for generating Key-pairs (public and private keys) for public cryptography. In addition to that, it can not only generate random key pairs but also specified exclusive key pairs with a SEED.

Tailwind CSS Specifications: -

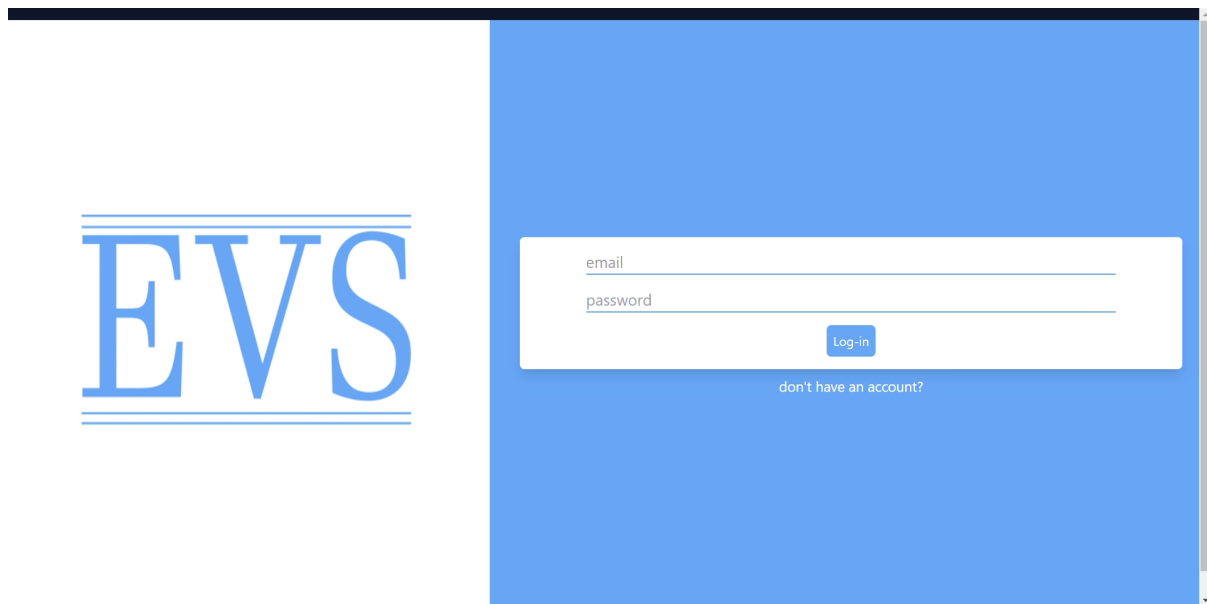
No more silly names for CSS classes and Ids. Minimum lines of Code in the CSS file. We can customize the designs to make the components. Makes the website responsive. Makes the changes in the desired manner. CSS is global in nature and if make changes in the file the property is changed in all the HTML files linked to it. But with the help of Tailwind CSS, we can use utility classes and make local changes.

4.3 RESULTS AND OUTCOMES



The registration page features a blue background. On the left is the 'EVS' logo in blue serif font with horizontal lines above and below. On the right is a white registration form with the following fields: 'Full Name', 'email', 'password', and 'confirm-password'. Below these fields is a blue 'Sign-In' button. At the bottom of the form area is a link that says 'already have an account?'.

Figure 11 User Registration Page



The login page features a blue background. On the left is the 'EVS' logo in blue serif font with horizontal lines above and below. On the right is a white login form with the following fields: 'email' and 'password'. Below these fields is a blue 'Log-in' button. At the bottom of the form area is a link that says 'don't have an account?'.

Figure 12 User Login Page

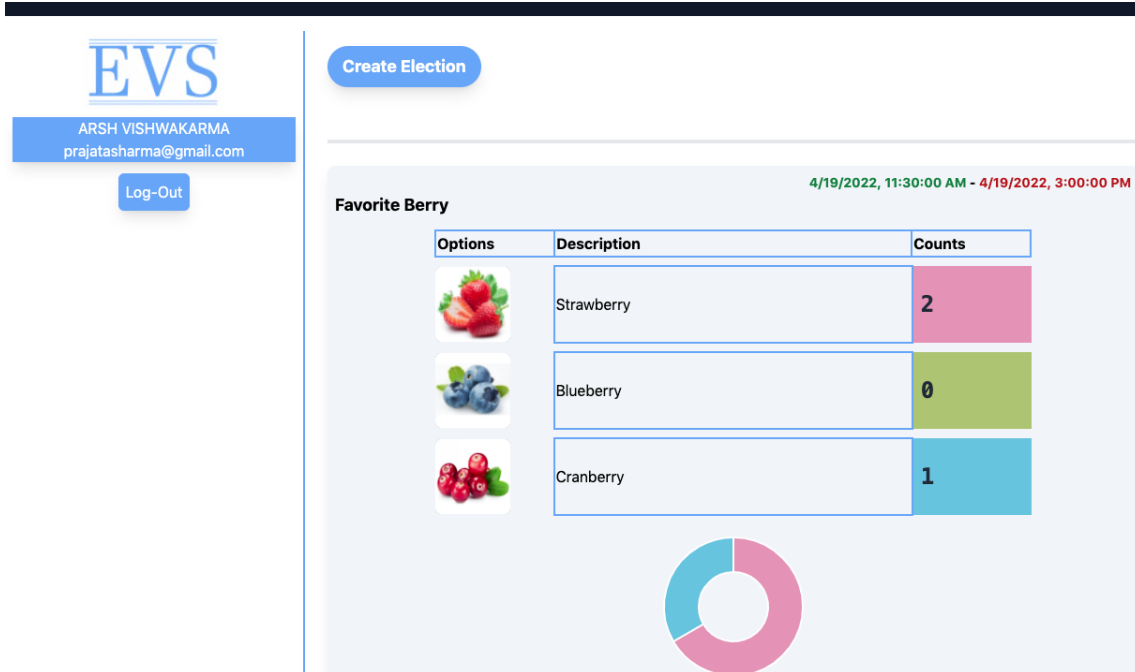


Figure 13 User Dashboard

The screenshot shows the 'Create a Voting' form. It includes the following fields and buttons:

- Title:** A text input field.
- Start:** A date and time input field with a calendar icon.
- End:** A date and time input field with a calendar icon.
- Voters:** A text input field with a placeholder example: 'eg: abc@xyz.com, def@pqr.com,...'.
- Add Voters:** A blue button.
- Options:** A section with two rows, each containing a 'description' text input field and an 'Add Image' button.
- Add Option:** A blue button.
- Create:** A blue button at the bottom right.

Figure 14 User Creating A Voting Agenda

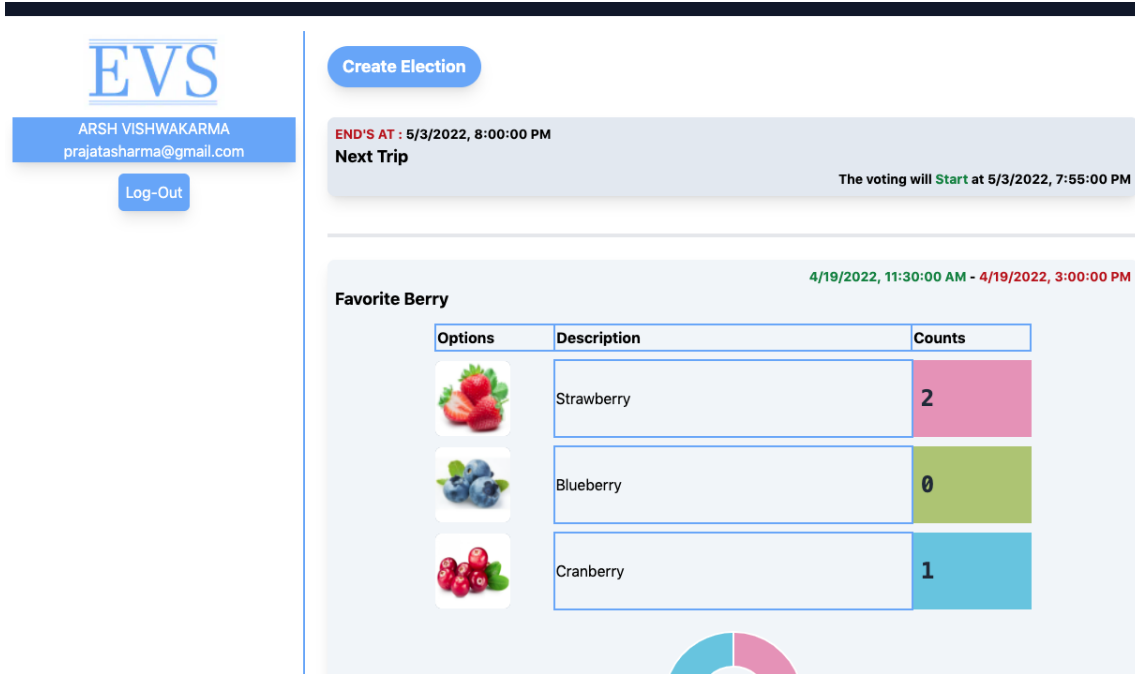


Figure 15 User Dashboard With Participation Details

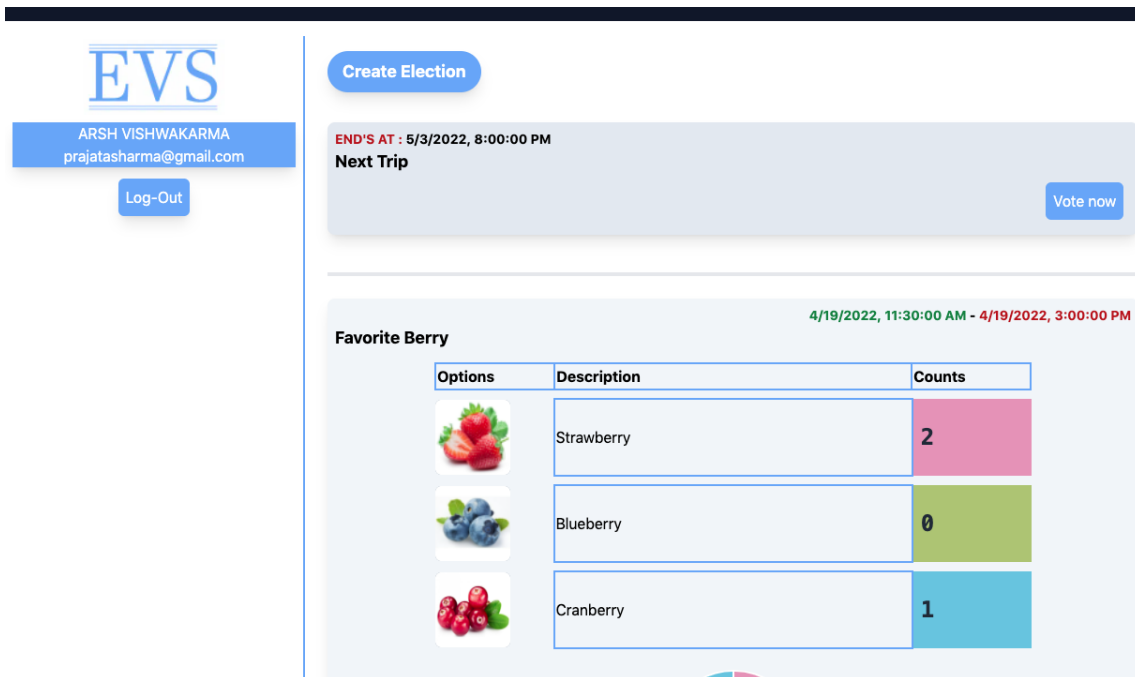



Figure 16 User Dashboard With Vote Now Option

Next Trip

 Hawaii ☐




 Maldives ☐

Figure 17 Option Selection Page

Next Trip

 Hawaii ☒

 Maldives ☐

HIGH.SQUARE.FAILED.MADE.DISCUSS.PRINCIPLE.

[Submit Vote](#)

Figure 18 Seed/Secret Submission Page

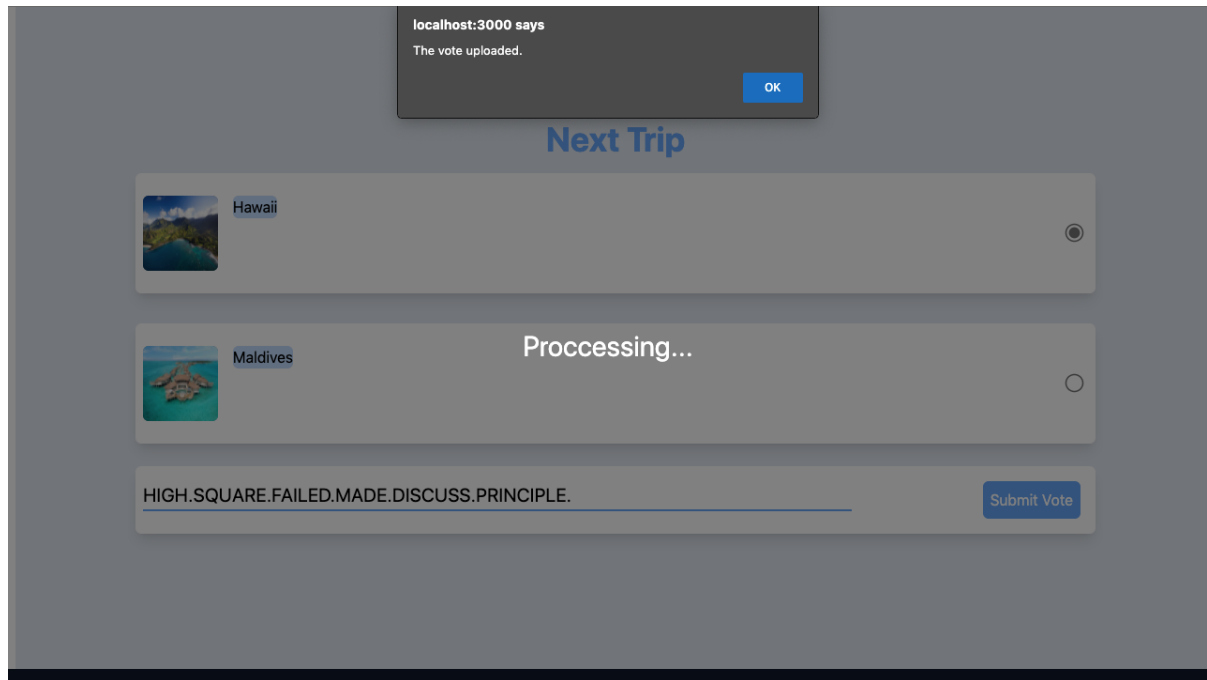


Figure 19 Successful Vote Upload Alert

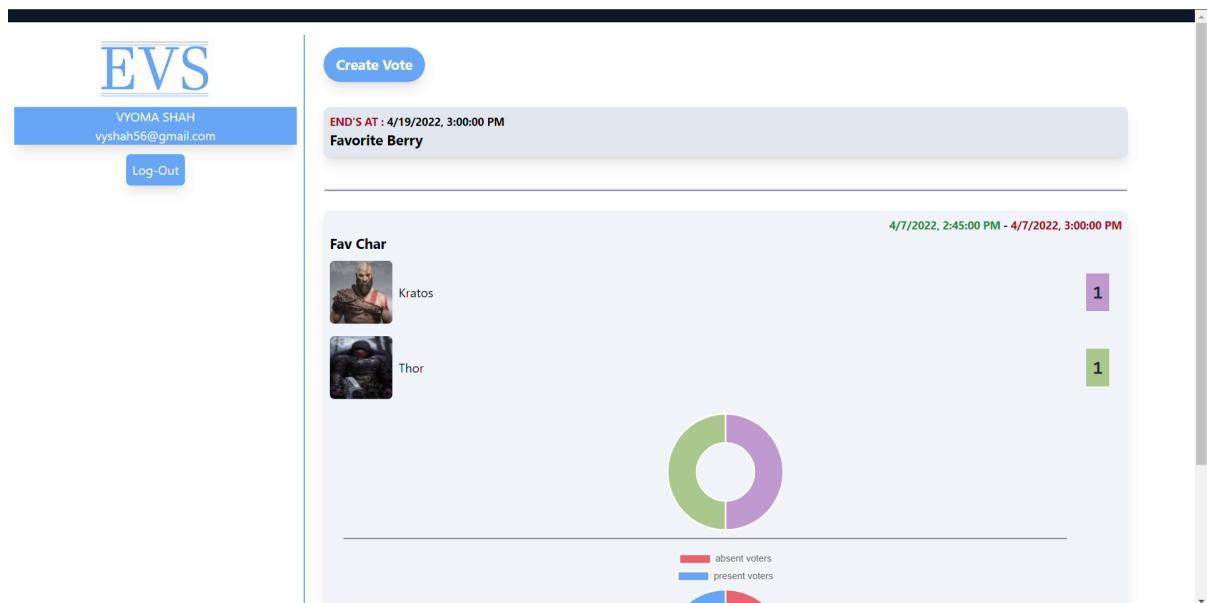


Figure 20 User Dashboard Waiting For Result

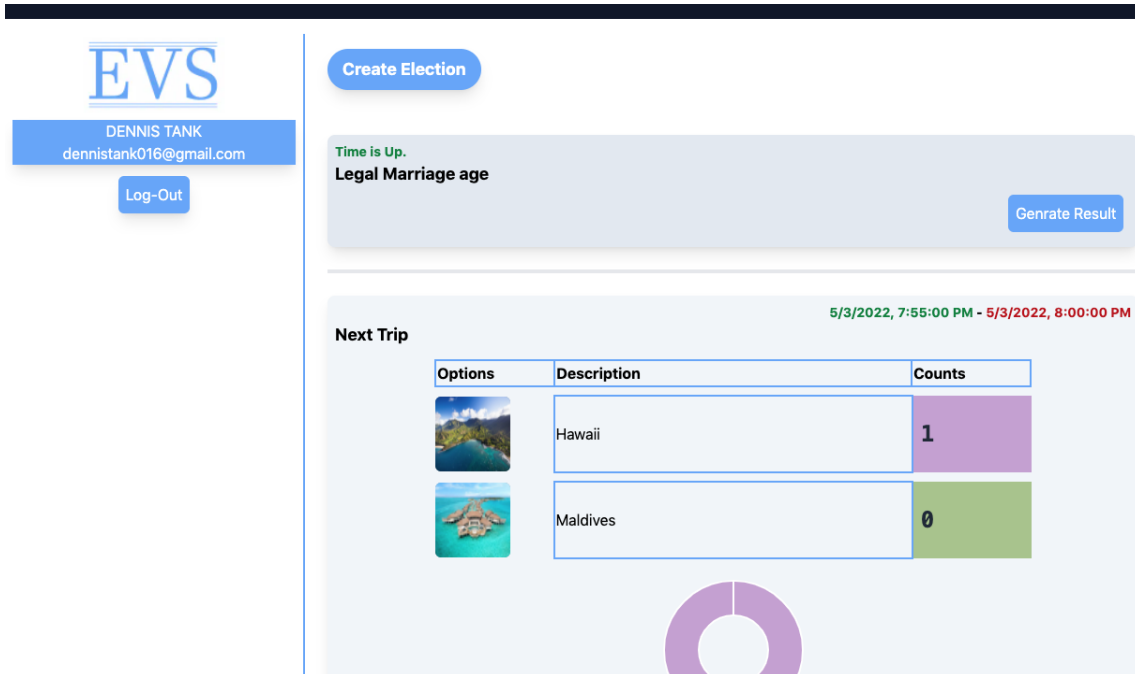


Figure 21 User Dashboard With Generate Result Option

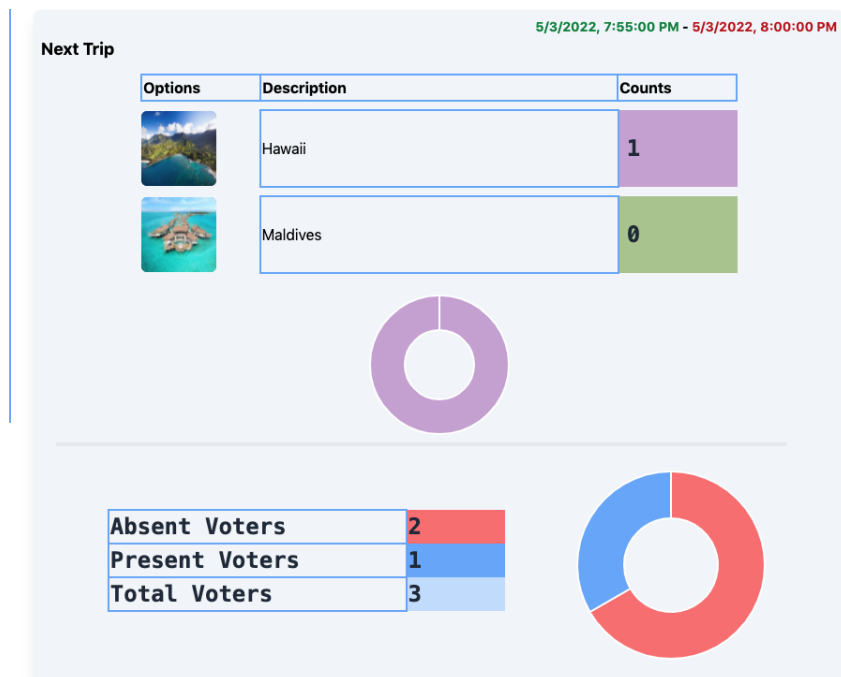


Figure 22 User Dashboard With The Results

4.4 RESULT ANALYSIS

According to the testings done the prototype shows results that were within expectations but on a small scale. That is when we take less number of participants and the way the result is calculated and shown in the form of chart remains the same when the number of participants or candidates increases. The increase in number of candidates will modify the way the chart results are shown but the main result of vote tallying according to the absent voters and present voters remains the same. Though we have not tested on a large scale of participants, it can be tested with more participants as well. Also, if we add the API needed where we can let real participants vote with real values even then the site would work perfectly fine but we'll have to add that API and get its license as well.

The website currently shows the viewers information about the voting that is done and voting that is pending. We can even add the insight where it shows the details about the voting as well as the participants for current voting, past voting and present voting all of them separately and in segregated format.

The website takes only the email information to provide security to the voter and the secret string of the voter. This makes it easier as the user won't have to part with too many of their personal details and thus maintaining their confidentiality and privacy becomes easy. This also helps in maintaining the anonymity in a better way.

5. TESTING

5.1 TESTING STRATEGY

Testing is mostly divided into two parts,

Analog: -

This division will cover the email and acknowledgment received via software. The UI outputs for the confirmations of the processes and the SECRET/SEED string that will be sent from the server to all the participants. For instance, if the user already exists or not for log-in, if the voting was created or not, and if the vote was successfully uploaded or not.

Digital: -

The division will cover the code and the data flow inside and outside the server and the blockchain. It involves all the API requests and algorithm testing.

The strategy is to use the 'Postman' software for the API testing, and to use a code test library in JavaScript 'Jest.js' will be used.

Jest.js: -

Jest is a JavaScript open-source framework mainly used for testing. Jest is majorly used to work with react-native-based web applications and with react, and it mostly focuses on simplicity while doing any unit testing. Unit testing is often not very useful when run on the front end of any software because it is extensive and very time-consuming and raises complexity. But it can easily be removed using the jest framework. Also, the jest framework helps the programmer validate everything developed by using JavaScript, whether it is browser rendering of web applications or any mobile applications. Jest also provides a blended package of a built-in mocking library, an assertion library, and a test runner.

5.2 TEST RESULTS AND ANALYSIS

UI Cases: -

- Processing-Screen: at log-in, sign-in, and vote submission this screen will not allow the user to push any input event.
- Notifications:
 - Home-page: Login user exists or not, invalid email and password.
 - New-voting-create-page: new voting is created or an error occurred.
 - Voting-portal: the vote is uploaded or not.

API Cases: -

- '/login':
 - Expected: to check for the user and send the user object if user exists
- '/sign-in':
 - Expected: to update the database and send the user object
- '/peers':
 - Expected: to send the list of P2P servers in the Blockchain
- '/rand-bc-node':
 - Expected: to send any random Blockchain nodes URL
- '/user'
 - Expected: to send required user's info
- '/voting'
 - Expected: to send required voting info
- '/result':
 - Expected: to calculate the result variables, update the database, and send the info
- '/image':
 - Expected: to upload the image and send a URL of the same
- '/voting/new':

- o Excepted: to update the database with new voting, send the email to all the participants
- ‘/blockchain’:
 - o Excepted: to send the Blockchain
- ‘/votes’:
 - o Excepted: to collect the votes from the blockchain and send an object for the same
- ‘/voting’:
 - o Excepted: to update the database for the voting object
- ‘/transact-vote’:
 - o Excepted: to check the veracity of the vote and update the database if true
- ‘mine’:
 - o Excepted: to mine to transactions to Blockchain

Algorithm Cases :-

- Proof-of-work:
 - o Expected: to calculate the nonce for the valid transaction data, and append it to the blockchain.
- Crypts-encrypt:
 - o Expected: to encrypt the data from a SEED to convert a data object to a cipher.
- Crypts-decrypt:
 - o Expected: to decrypt the cipher from the same SEED to get TRUE encrypted data, if the data is FALSE discard the data object.
- Blockchain-P2P:
 - o Expected: to maintain Blockchain, synchronize the chain at all the nodes
- Transaction-pool:
 - o Expected: to collect all the verified votes and validate them when mining.
- Voting-pool:

- o Expected: to collect and maintain the TRUE Voting data for validation of votes.
- Mailers-mail:
 - o Expected: to create a SECRET string and send it to all participants via email, preserve the SECRET till the email is sent.
- Multer:
 - o Expected: to save the image-doc file with a unique name at the server and return a URL.

Remark: All Tests Results are as expected.

6. CONCLUSION & DISCUSSION

6.1 OVERALL ANALYSIS OF PROJECT VIABILITIES

The project viabilities are considering the expected benefits from the project or proposed system. EVS is an e-voting system that is made to ensure more security than the traditional database as the main purpose of the project. The project provides other benefits as well:

The system provides a very easy system to create a new voting panel.

The system helps to easily add voting contestants and their details.

The system has a flexible time period setter and time counter.

The system provides results in a chart format which is easy to view, read and analyze.

The voters can form new voting without much effort.

The voting system provides a new secret string for each voting done.

The voting system is connected through email of the client for voting in the current scenario which provides confidentiality.

The voting also maintains the anonymous condition for voting and just shows the tally of votes, not the information of the voters.

The voters information, as well as the information of counts of votes, is maintained in the database on servers.

6.3 DATES OF CONTINUOUS EVALUATION (CE-I AND CE-II)

Sr. No.	Evaluation Date	Evaluation Remarks
1	26-2-2022	Research not only on the basis of research papers but go through the other applications made with the same concept of e-voting in mind.
2	5-3-2022	Properly describe the problems or weaknesses of already present methodologies and properly state the ideals focused in this project as well as the benefits that will be present.
3	26-3-2022	Do the testing with more than one topic and make sure that everything that is done is in alignment to the project statement taken
4	9-4-2022	What sort of outcomes are obtained and are they matching with the ideals taken to keep a note of that when testing.
5	23-4-2022	The documentation should be made by keeping in mind the project details, records and its outcomes. All the problems that are encountered and the solutions employed for solving them.
6	30-4-2022	A few changes in the UI of the application and a few minor changes in the report. Also, there was a change mentioned for ppt.

Table 3 Continuous Evaluations

6.4 PROBLEM ENCOUNTERED AND POSSIBLE SOLUTIONS

Initially while building the P2P Server for Blockchain synchronization, there was an issue with port forwarding on the router. As P2P is defined as a peer-to-peer connection, which implies that the connection can be made from one computer to another- both with different Geo-location, it was quite naive to think that it might work directly without any additional configuration in the network. Moreover, P2P connection follows web-socket 'ws' protocol, which needs its own PORT SOCKET as well as system public IP address to communicate with other peers. For this reason being, the only feasible solution for this is to use a single system merely for the sake of presenting the proof of concept as well as running the prototype.

Secondly, the indubitable issue with nodes is the asynchronous nature of the interpreter. As it was a P2P-based prototype, it was quite important for the Blockchain to synchronize, which was not properly delivered by the node. Nonetheless, the synchronization of Blockchain was initially working as it should and the reason for that is, as time passes eventually the blockchain algorithm synchronizes with the best and longest proper chain. However, the writing of the blockchain in the database was hindering the entire flow, as it takes a bit for the system to write the new data to the database. The solution for this was to target a single blockchain server till every server synchronizes, and for the sake of delivering the prototype's proper working concepts, only one/first blockchain is targeted.

The final problem that should be highlighted is the Node-Mailer module for node. It is used to send emails through a coroutine-specific code from a real existing email. Firstly, it required the 'Third Party Application' allowance which was hindering but still doable. Secondly, sometimes randomly the received mail which was sent through the node-mailer is seen as SPAM. A proper solution for this would be to buy a domain with an email service to handle the emails sent. But for the prototype, it would be an over-do.

6.5 SUMMARY OF PROJECT WORK

The Project's main focus is indeed security but it also takes into note other functionalities like the ease of use for the user, easy handling for the clients creating new voting, easy maintenance, confidentiality, anonymity, easy to understand and view, and easy interpretation about the data analysis section of votes result. The vote counting and tallying are also handled by the back-end system which makes it easier to get the results. Also, the connection of the backend system with the frontend system is smooth. The front end displays the insights in a very simple and elegant way which is easier for viewers and analysts to analyze.

The project's process is based on the blockchain p2p network which provides security. The website will provide a domain where voters can register and vote and it also provides a domain where clients can create new voting. The creation of voting is simple where one adds the participant and their details and mentions the time period for voting. The voters can register through their email ids and create a new password. Once the voters are registered they can vote for all the upcoming and ongoing votings that they are eligible for as per the voting criteria. While voting the voters will be asked for the Secret String which is the key to keeping the voter's identity classified and maintaining their privacy. Voters can vote only once they won't be allowed to vote more than once. After voting is done and the voting time period is up the voters can again log in to their dashboards and look at the insights given on voting results. Voters can also view any upcoming voting information on their accounts.

From this project, we were able to learn how to integrate CSS and HTML files to react js in the front end. We were also able to learn how to create an online voting system using blockchain rather than applying the traditional system. We were also able to analyze how we can improve our coding by integrating the codes from different platforms. Also, how to put privacy and benefits of the user as one of the bases for creating a project. The project creates the work easier for the voting people, not just the users but also those who build voting. This makes communication of voting more secure and easy to understand. The project also provides insights for the voting done which makes it easy as everything regarding voting is provided on a single platform.

6.6 LIMITATION AND FUTURE ENHANCEMENT

Though this project is made with high security but there are still other ways where we can enhance the security of the application. The current prototype do not inculcate any type of peer authentication procedure, therefore it can be further enhanced by adding biometric or OTP(or aadhaar) integration for large scale applications in government sector with the support of licensing & funding.

In this prototype, there is no provision for a reminder to users in case he/she forgets to vote within the time period. Different mediums such as email, mobile message or automated call can be utilized to remind the participant before the voting period threshold is reached to improve the voter participation rate to a much higher extent.

The graphical insights can be more curated and detailed by integration of additional database of user's profile such as designation, department, experience, performance etc in private sector & gender, age, assembly constituency etc in government sector.

Also, this prototype lacks the feature of stake weighted voting which is very helpful in many organizations & board meetings for reaching an inference based on contribution of each individual. This can be implemented with the help of parameters such as priority score, percentage stake in the organization, profit generation within a particular time span & many more as defined by rules of the voters

References

- [1] “Blockchain based voting system for Jordan parliament elections” by Mohammad Malkawi, Muneer Bani Yassein, Asmaa Bataineh
https://www.academia.edu/50258025/Blockchain_based_voting_system_for_Jordan_parliament_elections
- [2] “Designing a Blockchain-based Pemilu E-Voting Information System” by Hansrenee Willysandro, Johan Setiawan, Agus Sulaiman
https://www.academia.edu/50156619/Designing_a_Blockchain_based_Pemilu_E_Voting_Information_System
- [3] “Why a decentralized voting system is infeasible without trusting a central authority” by Hugo Lageneste
https://www.academia.edu/50204666/Why_a_decentralized_voting_system_is_infeasible_without_trusting_a_central_authority
- [4] “Blockchain-Enabled E-Voting” by Nir Kshetri and Jeffrey Voas
<https://blockchain.ieee.org/images/files/pdf/blockchain-e-voting2018.pdf>
- [5] “On the Design and Implementation of a Blockchain Enabled E-Voting Application Within IoT-Oriented Smart Cities” by Geetanjali Rathee, Razi Iqbal, (Senior Member, Ieee), Omer Waqar, (Member, Ieee), And Ali Kashif Bashir, (Senior Member, Ieee)
<https://ieeexplore.ieee.org/document/9360732>
- [6] “An Anti-Quantum E-Voting Protocol in Blockchain With Audit Function” by Shiyao Gao , Dong Zheng , Rui Guo , Chunming Jing , And Chencheng Hu
<https://ieeexplore.ieee.org/document/8804187>
- [7] “Blockchain for Electronic Voting System—Review and Open Research Challenges” by Uzma Jafar, Mohd Juzaidin Ab Aziz, and Zarina Shukur

<https://www.mdpi.com/1424-8220/21/17/5874/htm>

[8] A Model for E-voting Systems Evaluation Based on International Standards: Definition and Experimental Validation by Marco Prandini and Marco Ramilli

https://www.jstor.org/stable/10.2979/eservicej.8.3.42#metadata_info_tab_contents

[9] “Going from bad to worse: from Internet voting to blockchain voting” by Sunoo Park, Michael Specter, Neha Narula¹ and Ronald L. Rivest

<https://dc.mit.edu/voting-on-the-blockchain>

[10] “Blockchain Decentralised Voting for verified users with a focus on Anonymity” by Piotr Pospiech, Aleksander Marianski and Michal Kedziora

https://www.academia.edu/49544708/Blockchain_Decentralized_Voting_for_Verified_Users_with_a_Focus_on_Anonymity

Appendix

<https://nextjs.org/docs>

<https://nodejs.org/en/docs/>

<https://reactjs.org/docs/getting-started.html>

<http://expressjs.com/en/5x/api.html>

<https://v2.tailwindcss.com/docs>

<https://www.w3schools.com/react/>

<https://www.npmjs.com/package/cryptr>

<https://www.json.org/json-en.html>

<https://nodemailer.com/usage/>

<https://openbase.com/js/multer/documentation>

<https://openbase.com/js/cakebase>

<https://axios-http.com/docs/intro>

<https://www.npmjs.com/package/body-parser>

<https://openbase.com/js/uuid/documentation>

<https://websockets.readthedocs.io/en/stable/index.html>