Aadhar Based Voting System

Project Report

Submitted in partial fulfilment of the

requirements for the award of the degree

of

Bachelor of Technology

in

Computer Science & Engineering

by

Gaurav Sethi E17CSE146

Ishan Gual E17CSE157

Harsh Arya E17CSE142

Department of Computer Science & Engineering

Bennett University

Greater Boida-201310, UP (India)

Certificate

I hereby certify that the work which is being presented in the B.Tech. Project Report entitled **"Aadhar Based Voting System",** in partial fulfillment of the requirements for the award of the **Bachelor of Technology in Computer Science & Engineering** and submitted to the Department of Computer Science & Engineering of Bennett University Greater Noida UP is an authentic record of my own work carried out during a period from April 2020 to June 2020.

The matter presented in this thesis has not been submitted by me for the award of any other degree elsewhere.

Signature of Candidate

Gaurav Sethi

Ishan Gual

Harsh Arya

Enrl. No. E17CSE146

E17CSE157

E17CSE142

This is to certify that the above statement made by the candidate is correct to the best of my knowledge.

Head

Computer Science Engineering Department

Bennett University Greater Noida UP

Acknowledgement

We would like to thank our **Professor Dr Shashidhar** for providing us not only the opportunity to pursue this intriguing project but also helping us improve upon our thought process and approach through his able guidance and expertise.

We would also like to thank the fellow students of our batch for their valuable critique and suggestions, thus helping us put forward meaningful, relevant and implementable solutions to the problem.

The study has indeed helped us to explore more knowledgeable avenues related to our topic and we are sure it will help us in our future.

Abstract

Our motivation of Aadhar based voting framework in open elections that would permit individuals to vote electronically, from their present city. In this framework, voting depends on Aadhar's biometric database. The voting system is made much easier and effectively secure with the help of blockchain as all the customers need to login by UIDAI (Unique recognizable proof authority of India) . This voting framework would offer higher security and it would expand the voting rate among the citizens of the country.

Table of Contents

1. Introduction

In each nation Election is a fundamental procedure of a vote-based system which permits individuals to show their views and decisions by choosing their leader. Nations invest a huge amount of funds to improve our entire voting framework to give a stable and better government to its residents. A good voting system gives high impact on the preferences of voters. Existing system has various advantages due to this it is considered to be the simplest voting system. In India, the voting framework ought to be straightforward, translucent, and completely secure for a better fulfilling democracy.

To tackle the challenges, we build up our own Aadhar based Voting System. In this we propose a potential new e-voting protocol that utilizes the blockchain as a transparent ballot box. The protocol has been designed to provide the fundamental e- voting properties as well as offer a degree of decentralization and allow the voter to give their vote in a secure manner (within the permissible voting period) using electronic means. The key features of this system will involve reduction in costs of conducting elections and decrease in the number of fake votes.

As it is a centralized voting system, a state can conduct the parliament election and the panchayath elections on the same day. The problems of casting a vote only in one's own constituency can be avoided through this system since a person can cast his vote from any constituency and the person once voted from any part can't cast his vote again.

When smart systems are implemented effectively in our election system that will facilitate the voters to believe in the system that they are using. A transparent and easy way to express their views. This framework will help us to provide more validity and security than the past framework.

1.1 Problem Statement

The present framework may have less transparency and validity because there could be odds of cheating at the voting time. Also, the problem of people being unable to vote because they live or work away from their hometowns, where they are registered. This has been identified as one of the country's biggest voting problems. With the changing times, new technology and ways coming, people have found ways to tamper EVM Machines and try to manipulate the election process. Validation of Voters, Security of the voting procedure, ensuring voted information these are the primary difficulties of the current election voting system.

1.2 Project Specifications

We have proposed an election voting framework that depends on the identity of the voter which is saved as an Aadhar number on a database. In the Aadhar based database, the administration gathers biometric and demographic information of residents and gives a 12-digit unique character number to the individual. Aadhar cards give secure verification in light of the fact that Aadhar number is unique to every person.

First, we install the dependencies such as ganache-cli, NodeJS etc. required for the project to install and run. Then, we set up an environment instead of developing the app against the live Ethereum blockchain, we have used an in-memory blockchain (think of it as a blockchain simulator) called testrpc. After setting up the environment we created our smart contract sol. Then we used Web3js to deploy our app and interact with it. And finally, we used NodeJS console to interact with the contract.

2. Literature Survey

Existing System

Electronic voting is the standard means of conducting elections using Electronic Voting Machines, sometimes called "**EVMs**" in India. The use of EVMs and electronic voting was developed and tested by the state-owned Electronics Corporation of India and Bharat Electronics in the 1990s. They were introduced in Indian elections between 1998 and 2001, in a phased manner. The electronic voting machines have been used in all general and state assembly elections of India since 2004.

Prior to the introduction of electronic Voting, India used paper ballots and manual counting. The paper ballots method was widely criticized because of fraudulent voting and booth capturing, where party loyalists captured booths and stuffed them with pre-filled fake ballots. The printed paper ballots were also more expensive, requiring substantial post-voting resources to count hundreds of millions of individual ballots.

Embedded EVM features such as "electronically limiting the rate of casting votes to five per minute", a security "lock-close" feature, an electronic database of "voting signatures and thumb impressions" to confirm the identity of the voter, conducting elections in phases over several weeks while deploying extensive security personnel at each booth have helped reduce electoral fraud and abuse, eliminate booth capturing and create more competitive and fairer elections. Indian EVMs are stand-alone machines built with once write, read-only memory. The EVMs are produced with secure manufacturing practices, and by design, are self-contained, battery-powered and lack any networking capability. They do not have any wireless or wired internet components and interface. The M3 version of the EVMs includes the VVPAT system.

Proposed System

India is the largest democracy in the world, with its Election becoming the world's second-most-costly after the United States. In our country, more than 900 million people are registered, voters. However, during the elections which were held place last year, close to 300 million didn't cast their ballots. A significant reason for this was the lack of access to polling stations, many being unable to travel to the stations where they registered to vote.

The solution lies in blockchain technology, and This system will allow hundreds of millions of Indian voters to exercise their right to democracy, even if they migrate to other parts of the country. The distributed ledger is immutable with blockchain technology, allowing citizens to be at peace of mind in knowing that the votes cast are genuinely counted. The increased transparency also makes the use of Blockchain a natural fit within the electoral process.

Our democracy is at a crossroads. There is a significant lack of current voting system in technology though there are many ways to make the process easier. Going digital is one of accountability. - Citizens are increasingly losing faith in the democratic system.

Elected candidates must explore the technology to facilitate and make voting more transparent.

Also, the citizens don't know what the process inside the EVM machine is like, how it works, whether it takes into account the vote as we cast it etc.

This is why voting machines are blamed by political parties. Yes, they may be true because the current EVM machines are "BLACK BOX".

After all, we have no idea what exactly is happening inside a machine, too. We believe what the machine gives us at the end of the process.

Everywhere, as we know, Election is a fundamental democratic mechanism that enables people to choose preferred candidates. The voting system in India should be equal, clear and completely safe. For a better democracy. Due to the lack of transparency, there could be a chance of cheating at the time of the voting process. The problems of the new framework are the reliability of voting systems, authentication and data protection.

Our proposed system of voting is based on Aadhar Verification, Aadhar registration being compulsory in India, every citizen of India has one and can his/her phone number can be associated with a particular Aadhar Number. We have used this to our advantage and have enabled two-factor authentication. The person casting a vote would receive a message with a link which would redirect him to a webpage where he can cast his/her vote. Blockchain is incorporated into the voting web page which helps to verify if the vote is registered as it is without any modification, correctly counts every single vote and prevents tampering. The only efficient and precise voting procedure can be accomplished in this way as no one would be left out without having their right to vote for their desired candidate.

2.1 Motivations and Contributions

Our proposed voting machine will contain a few main requirements that can be illustrated, as shown below:

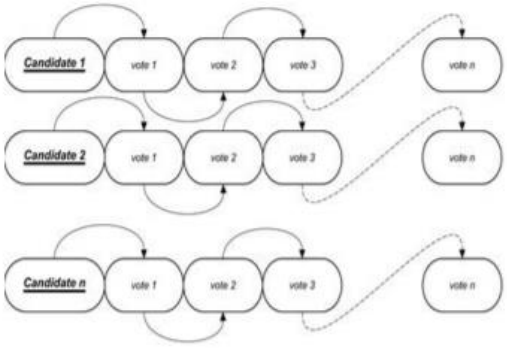
Authentication: our system does not require the registration process. Registration typically requires that all information and records be checked to comply with current laws, which could not be achieved in a safe way. Therefore, the device would verify the identities of the voter based on the biometric, Aadhar card and then let them vote only once.

Anonymity: Voters in the voting process must always be anonymous. The system must aim to achieve political privacy.

Precision: accurate voting is retained, and every vote must be counted and can't be duplicated or deleted.

Verifiability: The program will check that everything is their Votes are counted correctly. Our plan backs up Flexibility, performance, versatility and Main Specifications.

Transparency: The program must stay open and Transparent. Every person needs to learn What's going on inside the unit, how the vote shall be deemed and counted.



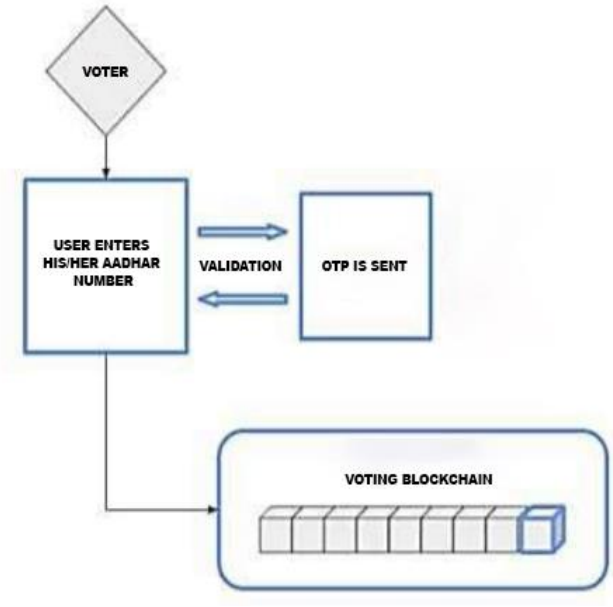
3. System Analysis and Design

Blockchain technology helps to keep away voter fraud by providing a clear record of the votes, and it prevents tampering of any vote. Using this technology, we ensure that the person who is voting is who he/she says they are and they are legally eligible to cast a vote.

To ensure that the system is secure, the block will contain the previous—voter's information. If any of the block's data gets changed, then it would be very easy to find since. All blocks are interconnected to each other. Hence data cannot be altered; no failure exists.

The Blockchain is where the actual voting takes place. The user's vote gets sent to one of the nodes on the system, and the node then adds the vote to the Blockchain.

3.1 Methodology/Approach Used

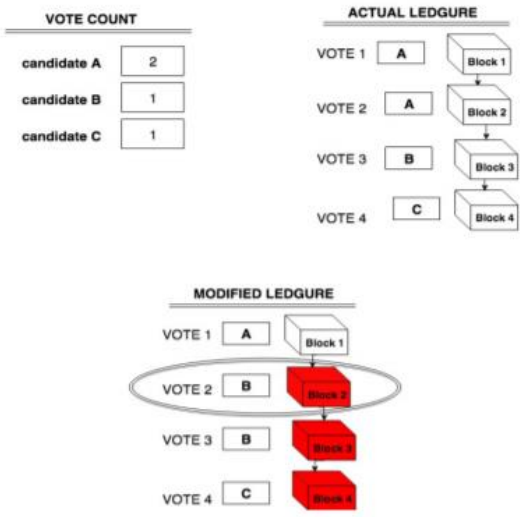


The above diagram shows the design of our approaching system. In this process, the user will go through a sequence of steps that will make a transaction in the Blockchain.

The user or the citizen will open our platform. Then they will be asked to enter their Aadhar card number for the verification, and the verification will be done using Two Factor authentication. The verification process also checks for his/her age and home state for validation. After the successful validation, if the user is allowed to vote, he will be proceeding to vote on the voting page. Once the vote has been received, the block will be created in the blockchain ledger which contains the block number, transaction ID information. This process will be repeated for all the users.

Blockchain concept starts once the voter casts a vote for their candidates. For each vote, a block would be Instantiated, and every vote in a block is stored on the ledger which is distributed and is connected to each other. Once data gets recorded in the ledger, it can never be erased.

Hence to maintain transparency and security of every Vote, Blockchain is integrated with the backend of our platform.



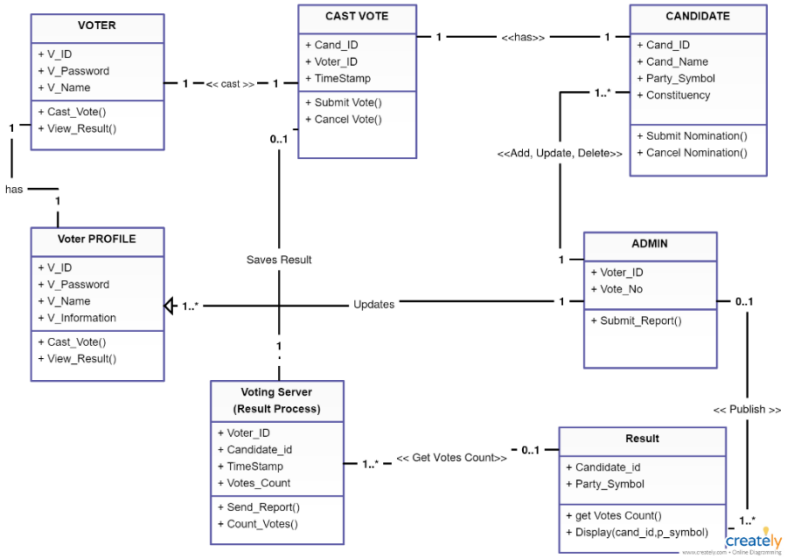
The above example explains to us how the system is secured if we apply Blockchain. The Vote count diagram shows the exact vote count of the candidates; the second diagram shows the sequence in which the votes have registered.

In the third diagram, the vote is modified, the block which shown in red colour is identified as an error vote. But it's very simple to identify where the tamper has occurred; hence it is effortless and more comfortable to find where the error happened, and it is easy to fix it.

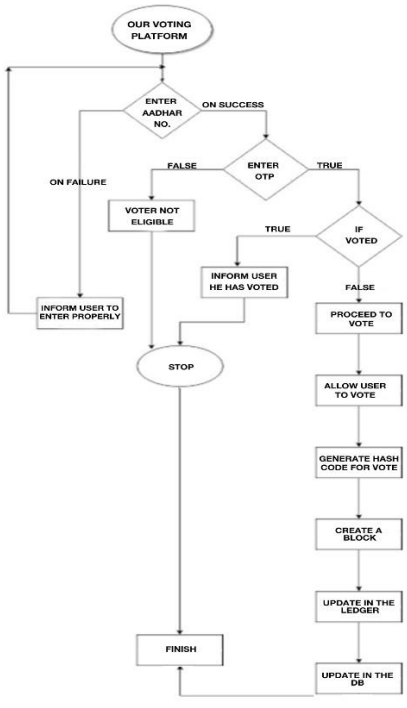
Nodes that experience Interference can perform manual data or system broadcast and can be repeated to update the data. When the process reaches the last turn node, each previous hash that is used by the block in the system is corrected same as the value of hash on the calculation results using the data in the preceding block. Each hash value in the previous block has been added in the calculation of hash values by the block that gets a turn on the system, anyone who tries to change the data in the database of voters will have difficulty because, if one data is changed it makes the following data to change in other blocks.

3.2 Design Diagrams

Entity-Relationship Diagram (ERD)



Working flow of the proposed system



1. Requesting to vote: The user will have to go to our platform online to cast their vote, the system would ask for their Aadhar card number and use their Aadhar Number to generate an OTP for verification. This can, therefore, eliminate the path for fake voting, problems in uncertain credentials, use of. fake identities multiple times by the same person for voting at more than one centres.

2. Casting a vote: Voters will have to choose to either vote for one of the candidates or cast a vote. Vote casting would be done in such a manner that the chances of electoral fraud are minimal and the transparency is achieved. While casting, the system ensures that the person has not voted yet. If the person has already voted, then the message will be displayed, informing the person that he has already exercised his power to vote. Or else the person will be allowed to vote for their desired candidate.

3. Encrypting votes: After the person votes, a block gets instantiated, and immediately hash value is calculated for the corresponding block. Hash of the current vote, as well as the hash of the previous block, will be stored and in this way, each input will be unique and ensure that the encrypted output is unique as well. Block header records all the encrypted information of each vote cast. SHA-256 encrypts all the information related to every vote, and it is not possible to find the encrypted hash function, which is a one-way hash function.

4. Adding the vote to the Blockchain: In this step, once a person votes, his/her vote will be added to Blockchain. Each block gets linked to a previously casted vote. Such that the vote cannot be modified. If a person completes his voting, his/her vote will be added to Blockchain. Each block gets linked to previously vote. If one block gets modified or tampered, then the further blocks from the tampered block will also be changed. Hence tampering is impossible in Blockchain. Information in the Blockchain is put up in an organized way and stored in. blocks. Each block has.:

1. the set of changes to be made to the data
2. a time stamp of the block
3. a reference to the. Block

The third point, every block contains the reference to the preceding block, which is the main feature of Blockchain. This reference helps to connect and create relations between every block. Blockchain can be a solution to solve the problems that occur in the voting system.

4. Algorithms/PSEUDO CODE

index.js

```
var express = require('express');

var morgan = require('morgan');

var path = require('path');

var bodyParser = require('body-parser');

var passwordHash = require('password-hash');

var bodyParser = require('body-parser');

var cookieParser = require('cookie-parser');

var request = require('request');

var fs = require('fs');

Web3 = require('web3')

solc = require('solc')

var app = express();

app.use( bodyParser.json() )

app.use(cookieParser());

app.use(morgan('combined'));




app.use("/", express.static("ui"));
```

```
var username;
var password;

app.post('/login', function(req, res) {

        console.log(req.body);
    username = req.body.username;
    password = req.body.password;
    var hashedPassword = passwordHash.generate(password);
    console.log(hashedPassword);

    if (username == "admin" && password == "password") {

        res.status(200).send({ message: hashedPassword});

    } else {
        res.status(500).send({ message: 'error' });
    }
});

app.post('/auth', function(req, res) {
        var cookie_pass = req.cookies['auth'];
        if (passwordHash.verify('password', cookie_pass)) {
                res.status(200).send({ message: hashedPassword});
```

```
	} else {
		res.status(500).send({ message: 'error' });
	}
});

app.get('/',function(req,res){
	var cookie_pass = req.cookies['auth'];
	if (passwordHash.verify('password', cookie_pass)) {
		res.sendFile(path.join(__dirname, 'ui', 'app.html'));
	} else {
		console.log('ok');
	}
});

app.get('/app', function(req, res){
	var cookie_pass = req.cookies['auth'];
	var cookie_otp = req.cookies['show'];

	if (passwordHash.verify('password', cookie_pass) && cookie_otp != null) {
		//res.sendFile(path.join(__dirname, 'ui', 'clist.html'));
		res.redirect('/info');

	} else if (cookie_otp == null && passwordHash.verify('password', cookie_pass)) {
		res.sendFile(path.join(__dirname, 'ui', 'app.html'));
```

```
	}
	else {
		res.redirect('/');
	}

});

// app.post('/getaddress',function(req,res){

// });

app.get('/info', function(req, res){
	var cookie_pass = req.cookies['auth'];
	var cookie_otp = req.cookies['show'];
	if (cookie_pass == null || cookie_pass == '' || cookie_otp == null || cookie_otp == '') {
		res.redirect('/app');
	} else {
		web3 = new Web3(new
Web3.providers.HttpProvider("http://localhost:8545"));
		 code = fs.readFileSync('Voting.sol').toString()

		 compiledCode = solc.compile(code)
		 abiDefinition = JSON.parse(compiledCode.contracts[':Voting'].interface)
		 VotingContract = web3.eth.contract(abiDefinition)
		 byteCode = compiledCode.contracts[':Voting'].bytecode
```

```
                deployedContract =
VotingContract.new(['Sanat','Aniket','Mandar','Akshay'],{data: byteCode, from:
web3.eth.accounts[0], gas: 4700000})


                contractInstance = VotingContract.at(deployedContract.address)


                res.sendFile(path.join(__dirname, 'ui', 'clist.html'));

        }


});




var port = 8080;

app.listen(8080, function () {

  console.log(`app listening on port ${port}!`);

});
```

Voting.sol

```
pragma solidity ^0.4.11;
// We have to specify what version of compiler this code will compile with

contract Voting {
  /* mapping field below is equivalent to an associative array or hash.
  The key of the mapping is candidate name stored as type bytes32 and value is
  an unsigned integer to store the vote count
  */

  mapping (bytes32 => uint8) public votesReceived;

  /* Solidity doesn't let you pass in an array of strings in the constructor (yet).
  We will use an array of bytes32 instead to store the list of candidates
  */

  bytes32[] public candidateList;

  /* This is the constructor which will be called once when you
  deploy the contract to the blockchain. When we deploy the contract,
  we will pass an array of candidates who will be contesting in the election
  */
  function Voting(bytes32[] candidateNames) {
    candidateList = candidateNames;
  }

  // This function returns the total votes a candidate has received so far
  function totalVotesFor(bytes32 candidate) returns (uint8) {
```

```
    if (validCandidate(candidate) == false) throw;
    return votesReceived[candidate];
  }

  // This function increments the vote count for the specified candidate. This
  // is equivalent to casting a vote
  function voteForCandidate(bytes32 candidate) {
    if (validCandidate(candidate) == false) throw;
    votesReceived[candidate] += 1;
  }

  function validCandidate(bytes32 candidate) returns (bool) {
    for(uint i = 0; i < candidateList.length; i++) {
      if (candidateList[i] == candidate) {
        return true;
      }
    }
    return false;
  }
}
```

5. Implementation

In our study, we have used Blockchain chain technology i.e. a digital ledger technology that can securely maintain continuously growing lists of data records and transactions, has the power to potentially transform health care, according to industry experts. By simplifying and expediting the way the voting industry processes data in such areas as revenue e-voting data interoperability and supply chain validation. blockchain has the power to dramatically reduce back-office data input and maintenance costs and improve data accuracy and security.

Firstly, we create a multiple distributed ledger and e-voting transnational data and store all transaction data into multiple data nodes. Each node will hold the specific block for each transaction. Same block has been replaced for all the nodes, and generates a valid block chain. If any block chain invalid during the validation of data servers, then the system will automatically recover the whole blockchain using the majority of servers. We will address and eliminate the runtime server attacks and recover it using our own blockchain. System will provide each transactional validation, for all servers.

In the admin module, we use the hash generation algorithm and the hash will be generated for the given string. Before executing any transaction, we use peer to peer verification to validate the data. If any chain is invalid then it will recover or update the current server blockchain. Mining algorithm is used for checking the hash generated for the query till the valid hash is generated.

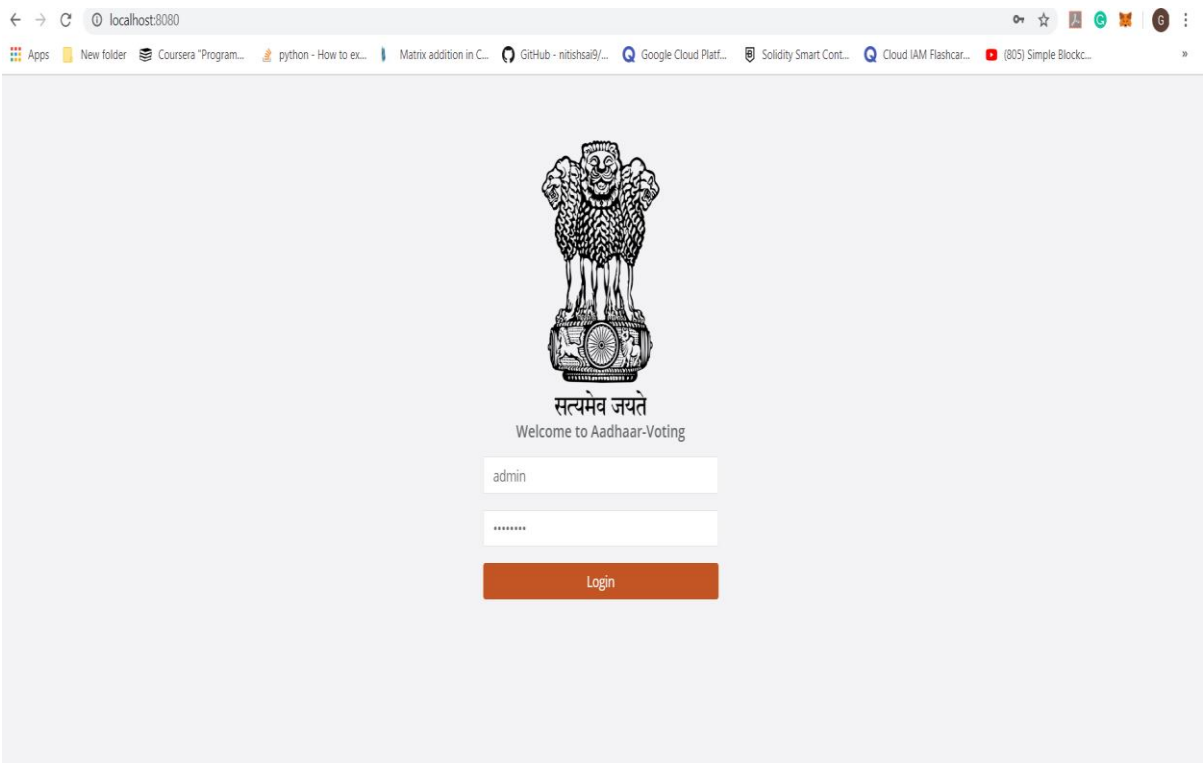
The voting system will only allow the authorized user to vote. Here the voter can see the candidates and vote for their party. After allowing access through admin, users can see all these candidates and can get an option to vote.

6. Result Analysis/Outcomes

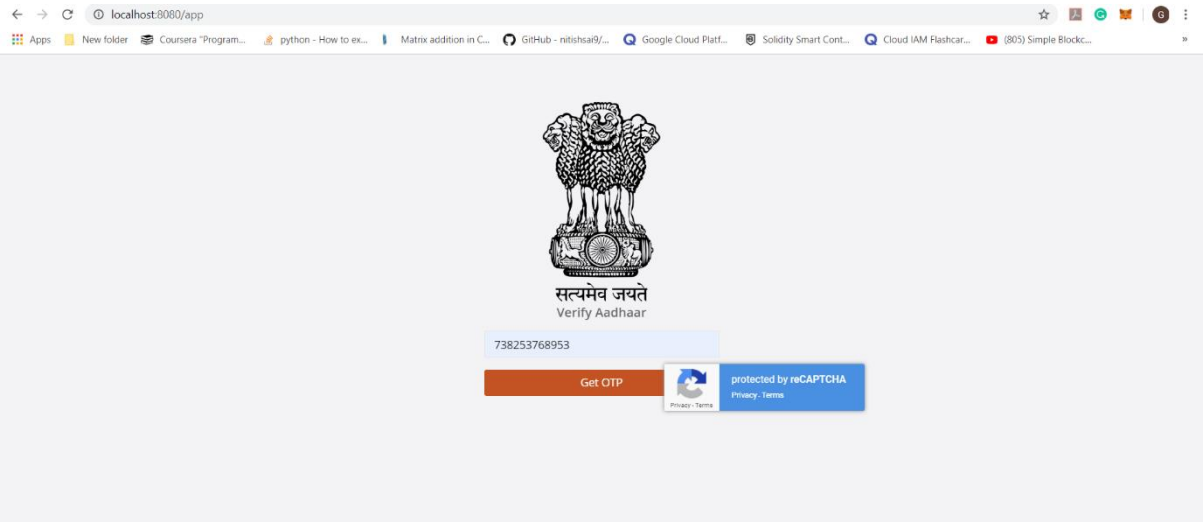
This Aadhar based voting system is very much simple and user friendly. The authority login is to ensure security to prevent piracy, harassment and corruption from candidates standing in election. OTP generation is to authenticate the right Aadhar card owner. Button disabling and automatic logout is to prevent multiple voting by single candidate. Moreover, it is more secure when compared to the existing system and can provide a reliable result. Reliability and trust are the two important factors which will make the citizens of a country satisfied.

The below process is followed to make a vote:

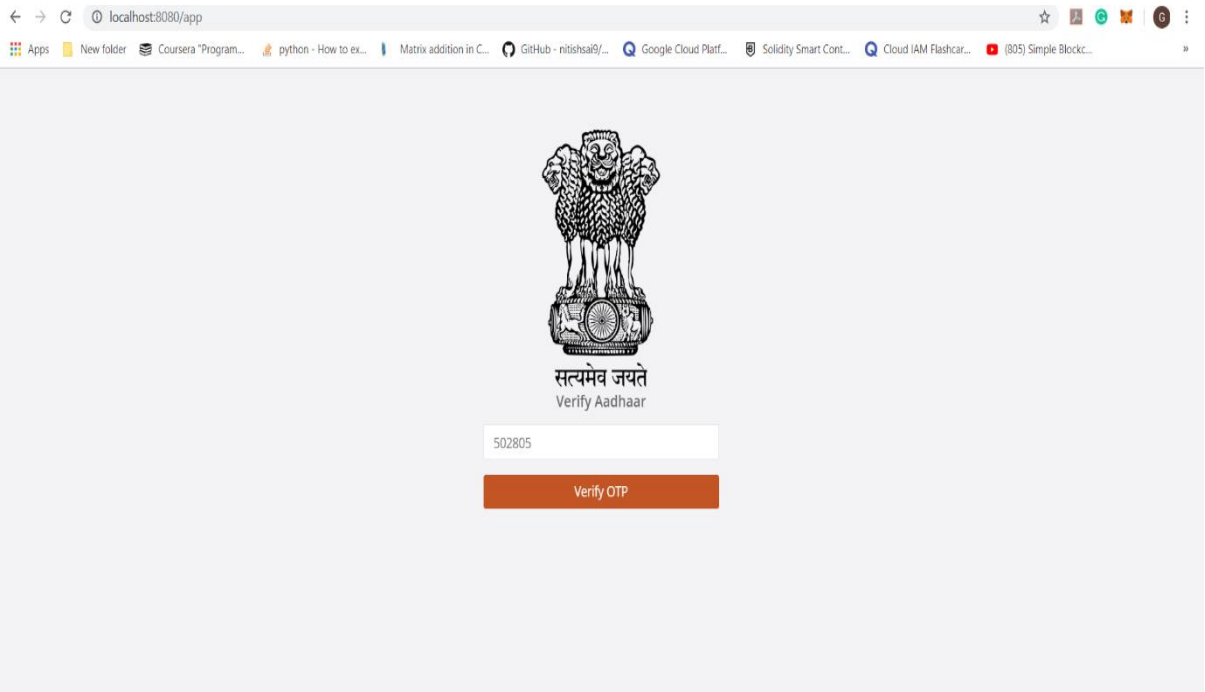
1. Admin login with session id.



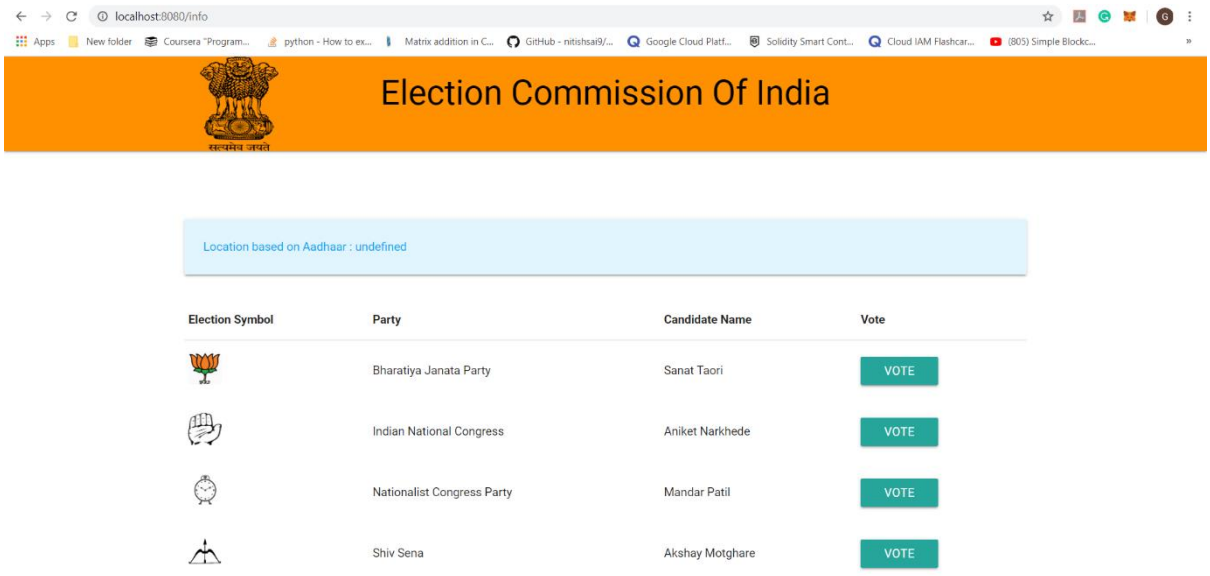
2. User enters its Aadhar number to begin the process of voting with proper authentication through OTP (one-time password) on the respective linked mobile number.



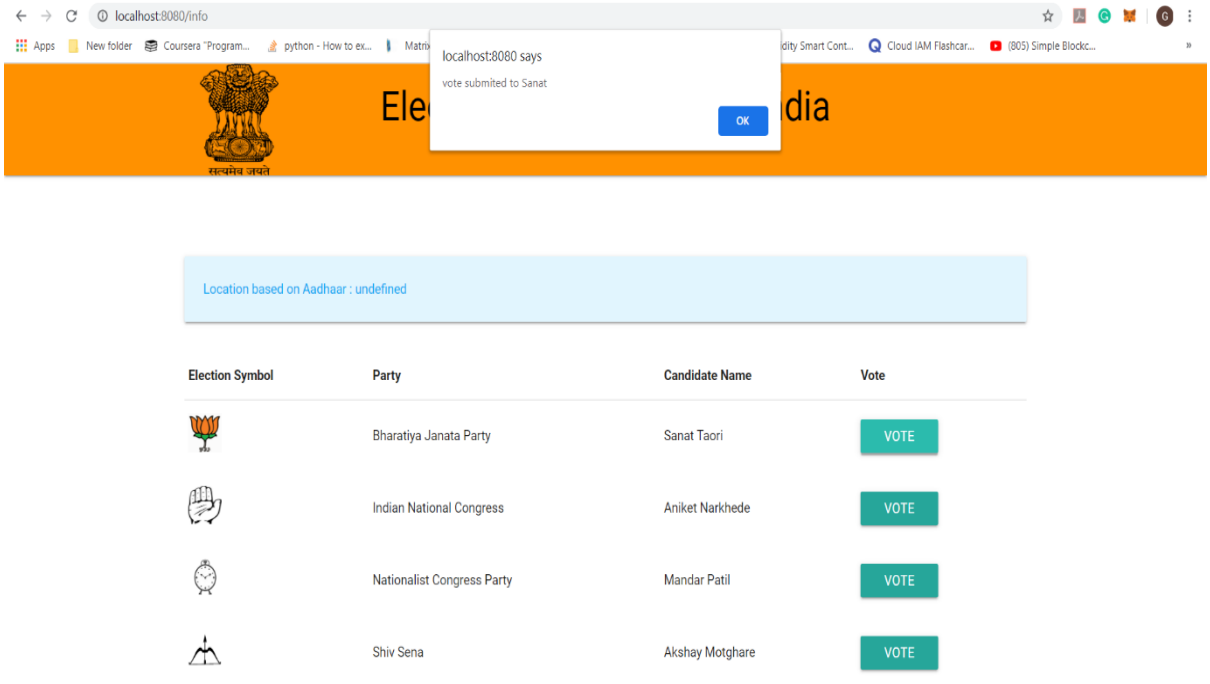
3. OTP received is entered. If the voter is valid then the system will check for the voters age and the address to which he can give vote.



4. The voting palette will be opened with candidate names, their parties and logos and the voter give his vote by clicking the vote button.



5. One voter can give his vote only once, i.e. after one-time voting buttons are disabled and the vote is automatically logged out. Same process continues for many more voters irrespective of their voting wards.



7. Conclusion and Future Enhancement

The idea of adapting Aadhar based voting systems to make the public electoral process cheaper, faster and easier, is a compelling one in modern society. Making the electoral process cheap and quick, normalizes it in the eyes of the voters, removes a certain power barrier between the voter and the elected official and puts a certain amount of pressure on the elected official. It also opens the door for a more direct form of democracy, allowing voters to express their will on individual bills and propositions.

In this project, we introduced a unique, blockchain-based electronic voting system that enables secure and cost-efficient election while guaranteeing voters privacy. We have outlined the systems architecture, the design, and a security analysis of the system. By comparison to previous work, we have shown that the blockchain technology offers a new possibility for democratic countries to advance from the pen and paper election scheme, to a more cost- and time-efficient election scheme, while increasing the security measures of the todays scheme and offer new possibilities of transparency. Using an Ethereum private blockchain, it is possible to send hundreds of transactions per second onto the blockchain, utilizing every aspect of the smart contract to ease the load on the blockchain.

For countries of greater size, some measures must be taken to withhold greater throughput of transactions per second, for example the parent & child architecture which reduces the number of transactions stored on the blockchain at a 1:100 ratio without compromising the networks security. Our election scheme allows individual voters to vote at a voting district of their choosing while guaranteeing that each individual voter vote is counted from the correct district, which could potentially increase voter turnout.

8. References

1. https://en.wikipedia.org/wiki/Electronic_voting_in_India
2. https://www.ijariit.com/manuscripts/v4i2/V4I2-1500.pdf
3. https://www.globalgovernmentforum.com/india-to-develop-blockchain-voting-system/
4. http://ijies.net/finial-docs/finial-pdf/270318333.pdf
5. https://coingeek.com/india-is-working-on-a-blockchain-based-voting-system-report/
6. https://tech.economictimes.indiatimes.com/news/technology/how-can-blockchain-help-aadhaar-ensure-privacy-and-transparency/63028987
7. Hjalmarsson, Friorik & Hreioarsson, Gunnlaugur & Hamdaqa, Mohammad & Hjálmtýsson, Gisli. (2018). Blockchain-Based E-Voting System. 983-986. 10.1109/CLOUD.2018.00151.
8. Agarwal, Himanshu & Pandey, G.. (2013). Online voting system for India based on AADHAAR ID. International Conference on ICT and Knowledge Engineering. 1-4. 10.1109/ICTKE.2013.6756265.
9. Ankit Anand1 , Pallavi Divya2 ,An E_cient Online Voting System, Vol.2,Issue.4, July-Aug. 2012, pp2631-2634.