

DECENTRALIZED VOTING SYSTEM USING BLOCKCHAIN

Submitted in partial fulfillment of the
requirements for the award of
Bachelor of Engineering degree in Computer Science and Engineering

By
G. Manikanta (Reg.No - 39110341)
&
K. Dileep Kumar (Reg.No - 39110450)



**DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING
SCHOOL OF COMPUTING**

SATHYABAMA

**INSTITUTE OF SCIENCE AND TECHNOLOGY
(DEEMED TO BE UNIVERSITY)
Accredited with Grade “A” by NAAC
JEPPIAAR NAGAR, RAJIV GANDHISALAI,
CHENNAI - 600119**

April - 2023



SATHYABAMA

INSTITUTE OF SCIENCE AND TECHNOLOGY

(DEEMED TO BE UNIVERSITY)

Accredited with **A** grade by NAAC

Jeppiaar Nagar, Rajiv Gandhi Salai, Chennai - 600 119

www.sathyabama.ac.in



DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

BONAFIDE CERTIFICATE

This is to certify that this Project Report is the bonafide work of **G. Manikanta (39110341)** who carried out the Project Phase-1 entitled **“DECENTRALIZED VOTING SYSTEM USING BLOCKCHAIN”** under my supervision from June 2022 to April 2023.

Internal Guide
Dr. M. Selvi, M.Tech., Ph.D

Head of the Department
Dr. L. LAKSHMANAN, M.E., Ph.D.



Submitted for Viva voce Examination held on 20.04.2023

Internal Examiner

External Examiner

DECLARATION

I, **G. Manikanta (Reg.No - 39110341)**, hereby declare that the Project Phase-2 Report entitled “**DECENTRALIZED VOTING SYSTEM USING BLOCKCHAIN**” done by me under the guidance of **Dr. M. Selvi., M.Tech.,Ph.D** is submitted in partial fulfillment of the requirements for the award of Bachelor of Engineering degree in **Computer Science and Engineering**.

DATE: 01-11-2022



PLACE:Chennai

SIGNATURE OF THECANDIDATE

ACKNOWLEDGEMENT

I am pleased to acknowledge my sincere thanks to **Board of Management of SATHYABAMA** for their kind encouragement in doing this project and for completing it successfully. I am grateful to them.

I convey my thanks to **Dr. T.Sasikala M.E., Ph. D, Dean**, School of Computing, **Dr. L. Lakshmanan M.E., Ph.D.**, Head of the Department of Computer Science and Engineering for providing me necessary support and details at the right time during the progressive reviews.

I would like to express my sincere and deep sense of gratitude to my Project Guide **Dr. M. Selvi, M.Tech., Ph.D.**, for her valuable guidance, suggestions and constant encouragement paved way for the successful completion of my phase-1 project work.

I wish to express my thanks to all Teaching and Non-teaching staff members of the **Department of Computer Science and Engineering** who were helpful in many ways for the completion of the project.

ABSTRACT

Electronic voting or e-voting has been used in varying forms since the 1970s with fundamental benefits over paper based systems such as increased efficiency and reduced errors. However, there remain challenges to achieve widespread adoption of such systems especially with respect to improving their resilience against potential faults. Blockchain is a disruptive technology of the current era and promises to improve the overall resilience of e-voting systems. This paper presents an effort to leverage benefits of blockchain such as cryptographic foundations and transparency to achieve an effective scheme for e-voting. The proposed scheme conforms to the fundamental requirements for e-voting schemes and achieves end-to-end verifiability. The paper presents details of the proposed e-voting scheme along with its implementation using the Multichain platform. The paper presents an in-depth evaluation of the scheme which successfully demonstrates its effectiveness to achieve an end-to-end verifiable e-voting scheme.

Keywords: electronic voting, e-voting, blockchain, e-government, verifiable voting

Chapter No	TITLE	Page No.
	ABSTRACT	v
	LIST OF FIGURES	vii
1	INTRODUCTION	9-13
2	LITERATURE SURVEY	14-15
	2.1 Inferences from Literature Survey	16
3	REQUIREMENTS ANALYSIS	
	3.1 Decentralized Voting System And Requirements	17
	3.2 Software Requirement Specification Document	17
	3.3 System Deliverables	18
	3.4 Research To be Carried Out	18
	3.5 System Design	18
	3.6 Unified Modeling Language	19
4	DESIGN AND IMPLEMENTATION	
	4.1 System Access Design	20
	4.2 Administrator and Voter Design	21
	4.3 System Architecture	22
	4.4 Implementation and Design	24
	4.5 Man-In-The-Middle Attack (MITM)	25-26
	4.6 Authentication	26
	4.7 ENCRYPTED COMMUNICATION	26-27
	4.8 Symmetric Key Cryptography	27-28
	4.9 Asymmetric Key Cryptography	28
	4.10 Digital Certificates	29
	4.11 Encryption Algorithm	29-30
	4.12 Secure Socket Layer (SSL)	30
5	APPLICATIONS & SCREENSHOTS	31-36
6	RESULT & CONCLUSION	37
7	FUTURE WORK	38
	REFERENCES	39-41

LIST OF FIGURES

FIGURE NO	FIGURE NAME	Page No.
3.6	Use Case Diagram for Blockchain Base Decentralized Voting System	19
4.1	Displays the system's access login design	20
4.2	Design of the forgotten password section	21
4.3	Design of the administrator and voter system features after login	22
4.4	System Architecture	23
4.5	System Overview	25
4.6	Man-In-The Middle Attack	26
4.7	Secure Socket Layer	30

LIST OF TABLES

TABLE NO	TABLE NAME	PAGE NO
2	COMPARISON OF CURRENT SYSTEM WITH COMPARED	13

CHAPTER 1

INTRODUCTION

Elections are a fundamental pillar of the democratic system enabling the general public to express their views in the form of a vote. Due to their significance to our society, the election process should be transparent and reliable so as to ensure participants of its credibility. Within this context, the approach to voting has been an ever evolving domain. This evolution is primarily driven by the efforts to make the system

secure, verifiable and transparent. In view of its significance, continuous efforts have been made to improve overall efficiency and resilience of the voting system. Electronic voting or e-voting has a profound role in this. Since its first use as punched-card ballots in the 1960's, e-voting systems have achieved remarkable progress with its adoption using the internet technologies (Gobel et al, 2015). However, e-voting systems must adhere to specific benchmark parameters so as to facilitate its widespread adoption. These parameters include anonymity of the voter, integrity of the vote and non-repudiation among others.

Blockchain is one of the emerging technologies with strong cryptographic foundations enabling applications to leverage these abilities to achieve resilient security solutions. A Blockchain resembles a data structure which maintains and shares all the transactions being executed through its genesis. It is primarily a distributed decentralized database that maintains a complete list of constantly germinating and growing data records secured from unauthorized manipulating, tampering and revision.

The system will be built to have strict security features. These security features will commence from the point of voter login into the voting system, to casting their vote for their chosen candidate to the point of their exit from the system. The system will have secure restrictions preventing the voter from voting more than once for the election candidates.

The system to be implemented needs to address the issues covering security needs of a vote being cast over the internet. Authentication and validation of the users, access rights, information encryption and vote security need to be looked into in an in-depth fashion in order to produce a secure means of voting online.

1.1 Aim and Objectives

The aims and objectives of the system to be produced have been stated below

- To build an online system this would enable voters to cast their votes on chosen candidates.
- Create a secure authentication facility to check validate users logging into the voting system.
- Create a database to be used to store votes, and user information on the system.
- Study and implement a security method to be used to ensure that votes being cast in the system will not be compromised and any outside attack
- Enable the system to tally votes cast according to the candidate voted for.
- Create a backend administration section which will be used to enable the administration manage the election system effectively
- Create tools for the administrator to add, delete and update details of voters, candidates and sub administrators on the system.
- Display voting results in a graphical fashion for the administrator to analyze.
- To enable voters to cast their votes for their chosen candidates.
- Enable voters to view biographies of the candidates being voted for in the election.
- Timestamp votes cast to the database to know when each vote was cast.
- Enable administrators to generate reports on the vote results.
- Prevent voters from voting more than once for their choose candidates

1.2 Existing System

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

1.3 Problems With Existing System

The current system in use today has a number of problems my proposed system would aim to correct. The system is highly insecure and prone to election malpractice. Due to the fact that any student can come and fill out a ballot sheet without prior authentication to determine who he/she says they are, is a major concern. The administration of the voting system as a whole is highly inefficient, slow and time consuming, and is highly prone to human error.

1.4 Software Design Methodologies

The most important aspect of software development is; the meticulous planning that takes place before the project can begin. Developing a software system is usually a complex and time-consuming process. In order to control the software system process we try to adhere to some kind of framework that introduces certain degrees of structure to the overall development process. Software engineering methodologies are the backbone for developing software; the methodologies simply assist one in how one should go on about building a software system which meets its purpose. Various methodologies are used for different types of software development depending on the scale of the software to be built. Hence one follows the various stages of development methods, such as the planning stage, followed by the requirement stage, design stage, testing, and lastly maintenance stage. These are the type of framework that can minimize time consumption, allow for good control in the process stage and reduce the complexity and uncertainties of the software development.

This project involves building a dynamic web-based voting system. In order to achieve this, an appropriate software design methodology which would suit the project has to be chosen.

- Rapid Application Development
- Prototyping

1.4.1 Rapid Application Development

Rapid Application Development (RAD) is one of the major players in information systems development. RAD is a methodology for compressing the analysis, design, build, and test phases into a series of short, iterative development cycles in order to develop systems at a quicker pace. The two key features of RAD are timeboxing and Joint Application Development (JAD). Timeboxing is an approach for fixing the resource allocation for a project. It limits the time available for the refinement of requirements, design, construction and implementation as appropriate. JAD involves both the developers and the customer to identify what the customer wants from the system that is about to be built. Hence, both parties participate in the building of the system.

1.4.2 Prototyping Methodology

A prototype is a form of a system or a partial complete system which is quickly constructed to examine some parts of systems requirements that are not to be used as the final completed working system. A user interface prototype is very useful, because it forms a means of visualizing what the proposed system is going to look like, and how the system is going to work to the potential users. Prototyping is a methodology that is very vital for producing fast, reliable and efficient systems.

Advantages of Prototyping

- Early presentation of the system to users can help point out any discrepancies in the system to the developers
- Any requirements specified by the client that have been missed out can be identified
- The usability of the system can be tested out by the users, at an early stage.

Disadvantages of Prototyping

- Prototyping method involves a considerable amount of user involvement, which may not be available to the developers.
- Prototyping may cause the developers to sway from the functional aspects of the system and focus more on the graphical user interface due to pressure from the users.

CHAPTER 2

LITERATURE SURVEY

G. Rathee *et al.* [14] introduced a digital voting system based on blockchain that could be implemented in a technologically advanced environment. The system assumes that all the connected external entities are trustworthy. However, the security in the system could be a huge risk, as intruders can enter the system to rig the votes. Whereas in our proposed voting system, the use of encryption and secure networks minimize the risk of intruders barging into the votes.

M. Pawlak *et al.* [15], proposed a system that does not require any operating entities. However, it could not secure a voter's identity, and also required complex computing. The system was able to collect votes from users but due to complex computation, upon higher user rate the latency became an issue. The identities of the voters became vulnerable. The system could not compute a large amount of data hence it has failed to be implemented at a large scale. Whereas in our proposed voting system the latency is managed by the use of consensus algorithms. The use of cryptographic hash in blockchain omits the risk of the vulnerability of a voter's identity.

A proposed system by D. Chaum *et al.* [16] improved the robustness and fair tallying of votes. End-to-end verification was made possible for voters to assure their count of the vote is integrated. Each voter was able to view if his vote was considered and recorded correctly. The voters were given a unique code that they could enter into the system to verify their vote. Whereas in our proposed voting system the verification of votes has been further simplified. Voters can verify their votes through registered phone numbers and email addresses. Verification of votes after the voting activity builds up the trust of voters

The voting system without polling stations was discussed by P. Mccorry *et al.* [17]. He suggested that voting through the internet using blockchain can give good results if implemented correctly. They discussed some technical flaws in digital voting systems. The robustness of the system could not be controlled. The error of doubling

users gets minimal by using end-to-end verification. These voting systems had low latency and did not secure the privacy of voters. This latency in the system is controlled by using an exible consensus algorithm and smart contracts the blockchain voting system being proposed.

	VMS	[14]	[15]	[16]	[17]
	✓	X	X	X	X
	✓	X	X	X	X
Algorithm	✓	X	X	X	X
	✓	X	X	X	X
	✓	X	X	X	✓

Table 2 : Comparison of current systems with proposed

Table 2 shows a detailed comparison of our proposed VMS with other voting systems based on blockchain technology. The state-of-the-art blockchain voting system was based on a single xed consensus algorithm however our proposed system supports a exible consensus algorithm at run time that helps to control the performance of the voting activity. We have also proposed a solution for the prevention of the 51% attack to prevent malicious activities during the voting process. Our system has further proposed the Chain Security Algorithm which automatically varies the validity of the chain each time a new block is added to it or some unauthorized change occurs in block data. We have also proposed a mechanism of Unspent Transaction Output(UTXO) and Smart Contracts that allow the system to prevent any incomplete and malicious transaction in the blockchain.

The above discussion shows that there has been a lot of debate about making a secure, efficient, and transparent voting system in the past but any comprehensive solution or system has not been proposed that could fulfill all requirements and key purposes of the voting system. The novelty of the proposed system besides implementing blockchain is to assure security, transparency, and integrity of results in

a voting system that empowers the trust of voters. This article proposes a more efficient and better implementation of blockchain in digital as well as a traditional voting system that is already being used. It gives higher authorities more detailed insight into the system while keeping it decentralized and transparent for every voter

2.1 INFERENCES FROM LITERATURE SURVEY

The simple rationalization could be a 'chain' of blocks. A block is an associate degree mass set of information. knowledge square measure collected and methods to suit in an exceedingly block through a process known as mining. every block may be known employing a science hash (also referred to as a digital fingerprint). The block shaped can contain a hash of the previous block, so blocks will kind a sequence from the primary block (known because the Genesis Block) to the shaped block. during this method, all the information may be connected via a connected list structure.

It eliminates the need to print ballot papers or open polling stations-voters can vote from wherever there is an Internet connection. Despite these benefits, online voting solutions are viewed with a great deal of caution because they introduce new threats.

Voters save time and cost by being able to vote independently from their location. This may increase overall voter turnout. The citizen groups benefiting most from electronic elections are the ones living abroad, citizens living in rural areas far away from polling stations and the disabled with mobility impairments.

CHAPTER 3

REQUIREMENT ANALYSIS

3.1 DECENTRALIZED VOTING BACKGROUND AND REQUIREMENTS

Electronic voting has been an area of research focus for many years by using computing machines and equipment for casting votes and producing high quality and precise results in accordance with the sentiments of the participating voters. Various attempts have been adopted in practice to support the election process. Initially the computer counting system allowed the voter to cast a vote on papers. Later on, those cards went through the process of scanning and tallying at every polling cell on a central server (Kadam et al, 2015; Rockwell, 2017; Hao et al, 2010). Direct Recording Electronic (DRE) voting systems were put in place later on which were admired and acknowledged greatly by the voters in-spite of the resistance from computer scientists. If the voting system is well understood by the voters, the system's usability can be increased remarkably.

3.2 SOFTWARE REQUIREMENTS SPECIFICATION DOCUMENT

H/W CONFIGURATION:

- | | | |
|-------------|---|---------------------------|
| • Processor | - | I3/Intel Processor |
| • Hard Disk | - | 160GB |
| • Key Board | - | Standard Windows Keyboard |
| • Mouse | - | Two or Three Button Mouse |
| • Monitor | - | SVGA |
| • RAM | - | 4G |

S/W CONFIGURATION:

- | | | |
|----------------------|---|-----------------------------|
| • Operating System | : | Windows 7/8/10 |
| • Server side Script | : | Python, HTML, Java Script |
| • IDE | : | Anaconda Navigator |
| • Libraries Used | : | PANDAS, Flask, Scikit-learn |

- **Technology** : **Python 3.6+**
- **Platform** : **Blockchain.**
- **Database** : **sqlite**

3.3 System Deliverables

The system to be delivered at the end of the implementation and testing phase would consist of an amiable website, which would act as the front-end of the system and also as the main entry point to the system. A Python application in the form of Servlets would be produced to facilitate the numerous requests, which would be sent to the web server to be used.

A database would also have to be constructed to store the data to be retrieved of the system's users; it will also be a highly essential tool for authenticating the system's users. Security would be highly prioritized in the building of the voting system, and SSL (Secure Socket Layer) and a mode of password encryption would also be utilized in the construction of the system.

3.4 Research To Be Carried Out

In order to progress in the design and paramount construction of the online voting, an extensive form of research has to be carried out, to gain more knowledge on the system to be built and to allow analysis of different components to be used for constructing the system. The topics of the research to be carried out are listed below.

- Existing electronic voting systems in use
- Website development software
- Server side programming languages
- Internet Security

3.5 System Design

The voting system's design is an important factor to the usability and durability of the whole system. The system will be engineered in a simple and straight-forward pattern, minimizing complexity and maximizing simplicity, usability and efficient structuring.

3.6 Unified Modeling Language (UML)

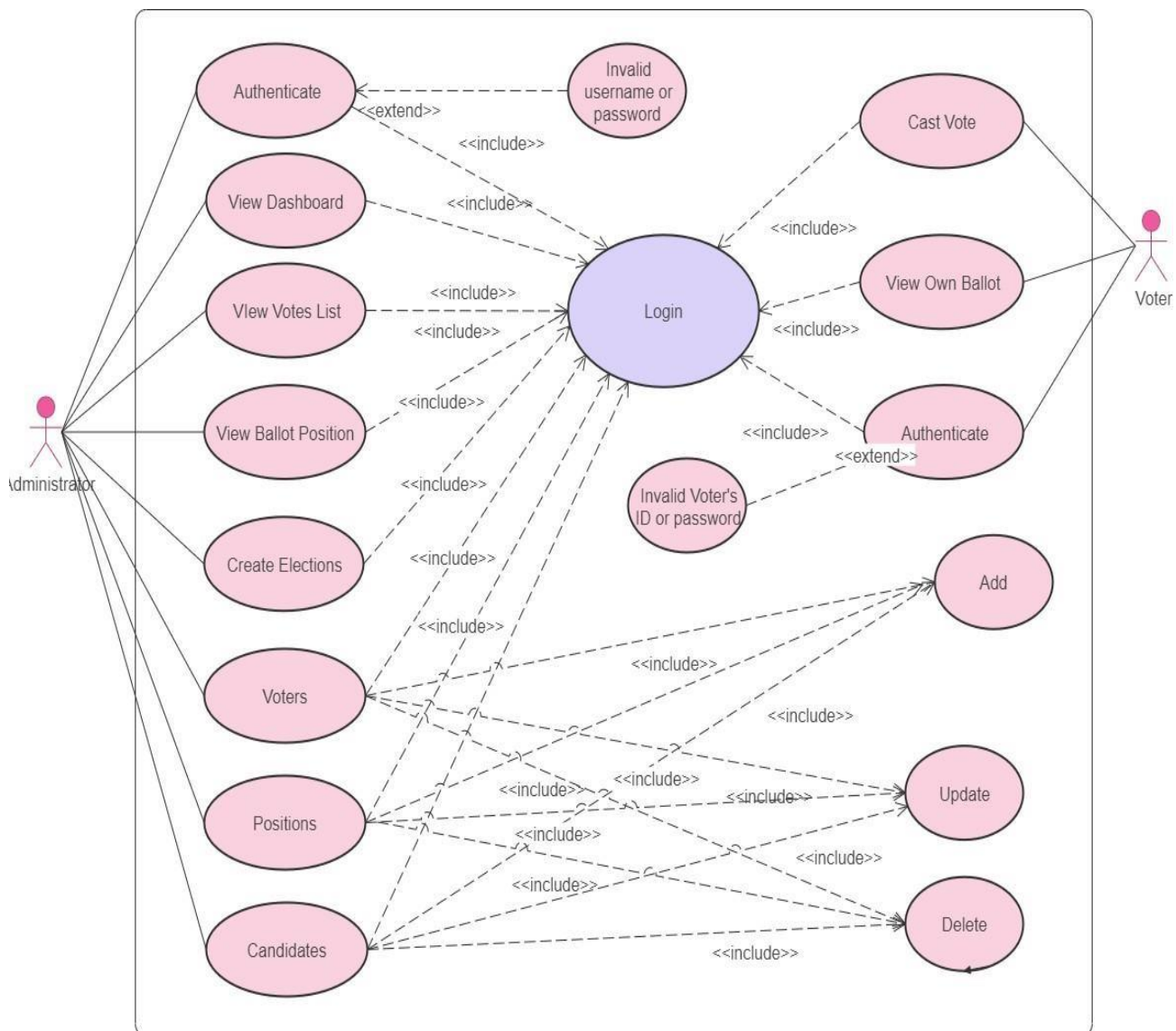


Figure 3.6 Use Case Diagram for Blockchain Base Decentralized Voting System

CHAPTER 4

DESIGN AND IMPLEMENTATION

4.1 System Access Design

The system to be implemented will need to have strong authentication features. The users of the system need to be authenticated to ensure that they have the right to use the system. For a voting system to be deemed secure, the system's login access must be well designed. The login page for the system must facilitate separate logins for administrators and voters. Each actor using the system will have their own access rights, to ensure that the voters would not be able to gain access to the administrator's page. In designing the login page, a Python class would be implemented for each actor to validate their login criteria with the data stored in the system database through the use of sql statements. If the data entered is of the wrong format or does not match the information in the database system, an error message in the form of a Python bean should be sent back to the user as shown in figure 4.1.

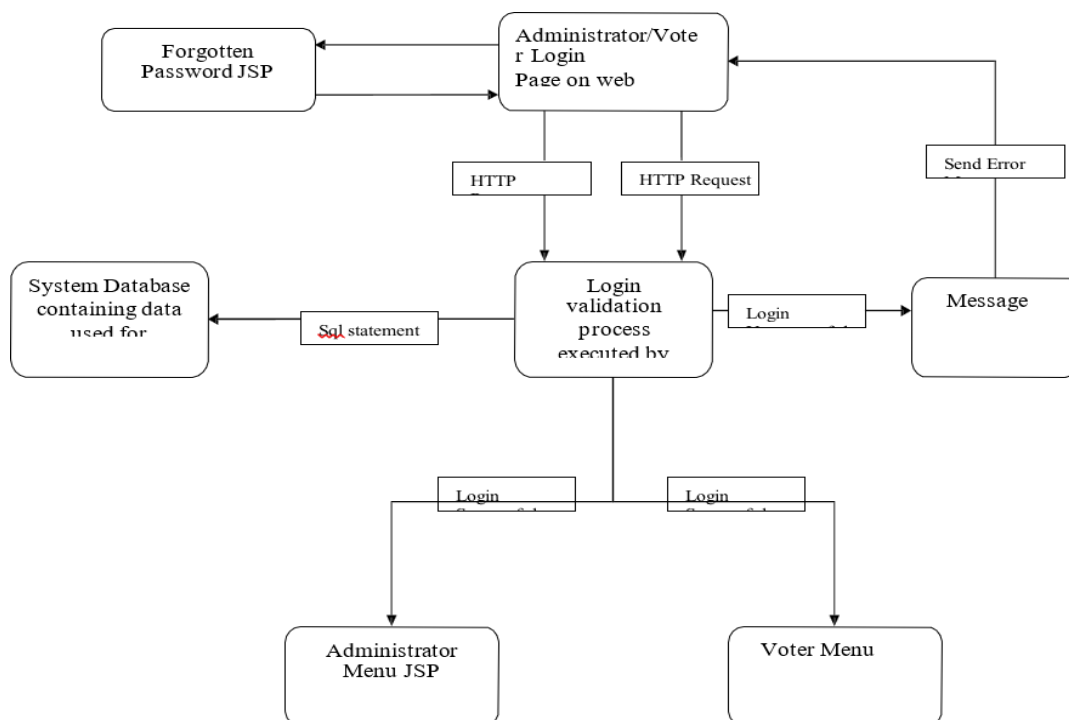


Figure 4.1 Displays the system's access login design

System users will always have a problem with forgetting their chosen passwords, it is a fundamental problem which every secure system would have, and an appropriate facility has to be made to deal with this problem. In the design of the voting system, the login page for both the administrators and the voters will be linked to a page for accessing passwords that have been forgotten by the user as shown in figure 7-8, it will be a requirement for every user to have a memorable word which will be used to query the system's database and retrieve the user's password. There would be a validation function embedded in a Python servlet which would prevent users from retrieving their password without entering their correct username and memorable word.

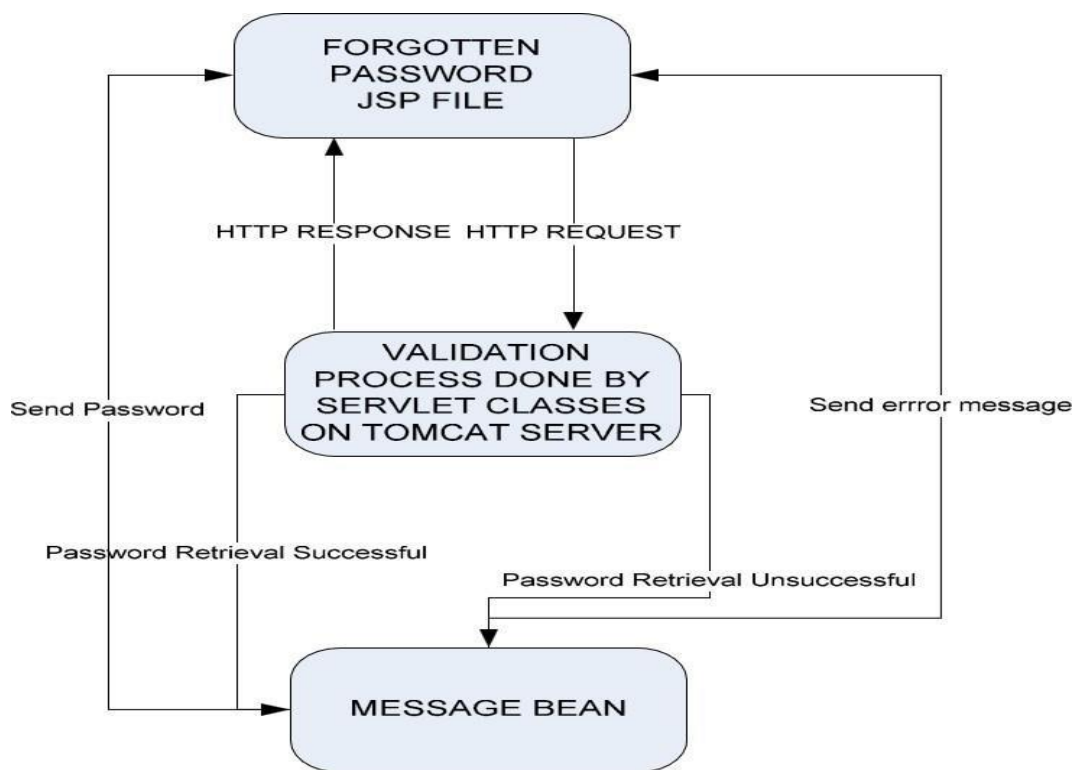


Figure 4.2: Design of the forgotten password section

4.2 Administrator & Voter Design

Once the authentication process has been carried out, the access permission given, the voter and administrator would be able to gain access to their specified facilities

as shown in figure 4-3. The voter would be able to select a candidate to vote for and logout of the system, the voter would be blocked from gaining entry to the system after casting their vote. The administrator would have access rights to adding, deleting and viewing candidates, voters and administrators. Addition and deletion of candidate names will also dynamically change the candidate's names on the voter's JSP page.

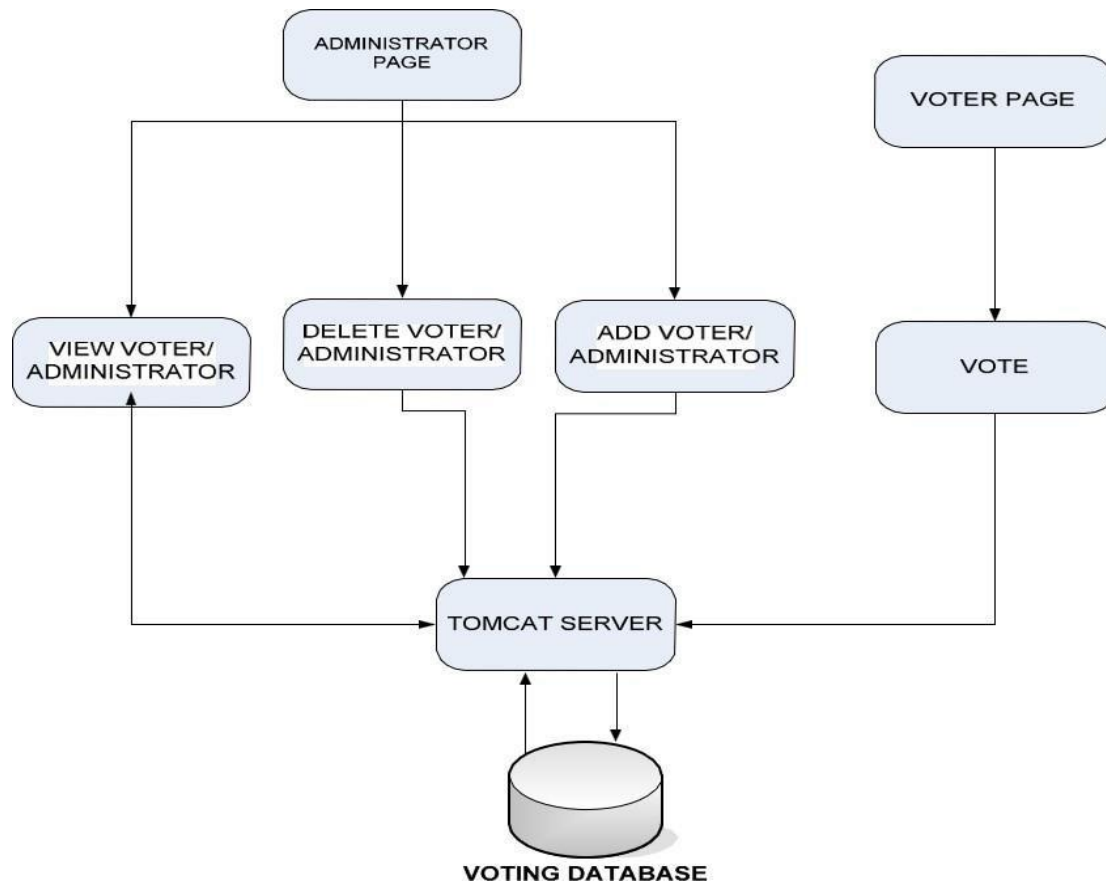


Figure 4.3: Design of the administrator and voter system features after login

4.3 System Architecture

The architecture of the system would consist of a number of client and server side technologies working together as shown in figure 4.4.

FRONT END

The front end of the system will represent the user's web browser interface of the voting system; this is where the users will be able to send HTTP requests and receive HTTP responses from the server. In order to build the front end of the system, HTML would be utilized.

BACKEND

The back end of the system will represent the server side of the application; this is where the processing of HTTP requests sent from the client will take place. A Tomcat server engine will be used to load the servlet and jsp, which can then send requests from the tomcat server engine, the dynamic content will then be sent back to the client in HTML format to enable the client to view the information on the web page.

A database will be utilized to store data sent from the client of the system, MySQL database will be used to store data being used by the system. In order for the database to be able to retrieve information from the server, a middleware layer has to be established in form of the JDBC API driver which will be used to translate Python methods calls to database API calls.

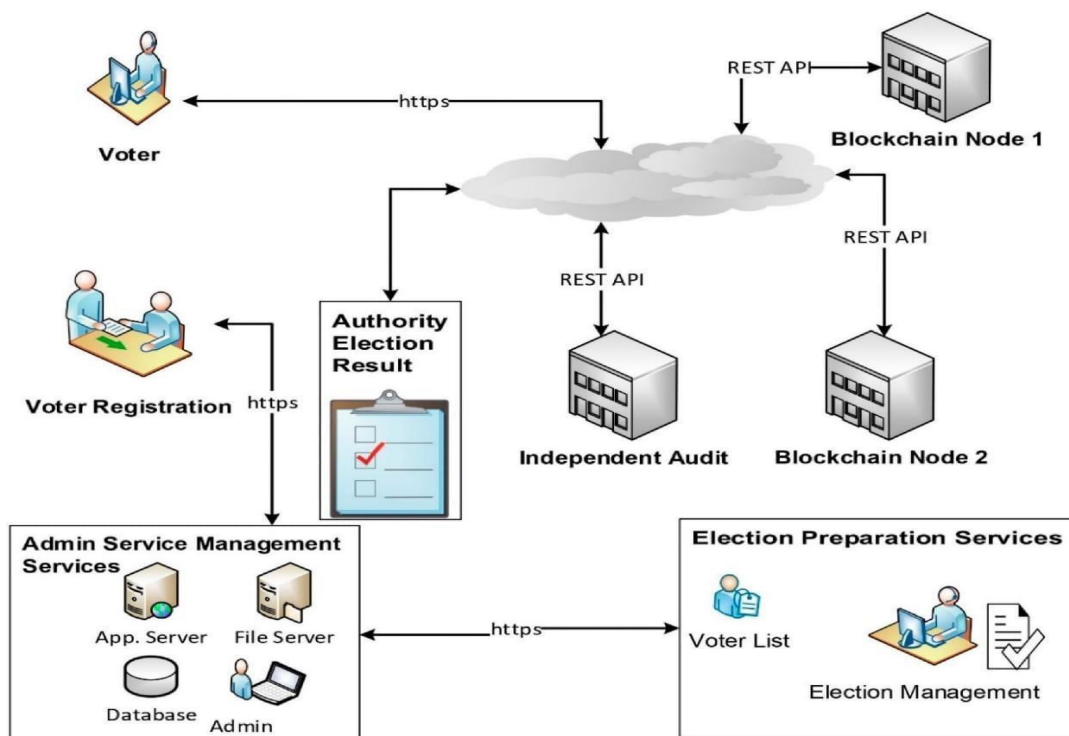


Figure 4.4 System Architecture

4.4 IMPLEMENTATION AND DISCUSSION

In this section we will illustrate the design and functional phase of our application, The User accesses the web application where the platform is hosted and register's itself as well as casts its vote in an secured and transparent manner.

1. Registration Phase: The Voter has to Register itself first with its unique id and attributes such as name roll no and mobile number. All this data is stored in the database.

2. Login: The voter after registration tries to login themselves to cast a vote. In this phase the voter first logs in using a password. After successful login, to cast their vote voter has to authenticate themselves. For real-time authentication OTP verification is used for enhanced security.

3. Blockchain Technology: This technology is mainly used for its security features. Blockchain provides a secure and transparent environment. Blockchain encrypts the voter message (Casted vote) using Asymmetric encryption algorithm. A public key is provided by Blockchain and the private key is with the host. Public key is used for verification purposes by the ledger..

4. Database: User database is stored in database. Details like name, gender, Unique Id are stored in the database. MySQL is the proposed database to be used.

5. Ethereum Network: Ethereum network provides a framework for blockchain creation and storage. Every block is created and its details are stored in an encrypted ledger. These created blocks are distributed among nodes which provides high fault tolerance to the system.

6. Result phase: The processing and tallying of votes is done in the results phase. Results are generated and displayed on the website. Users can verify their votes using their own public key. This provides transparency to the voting system

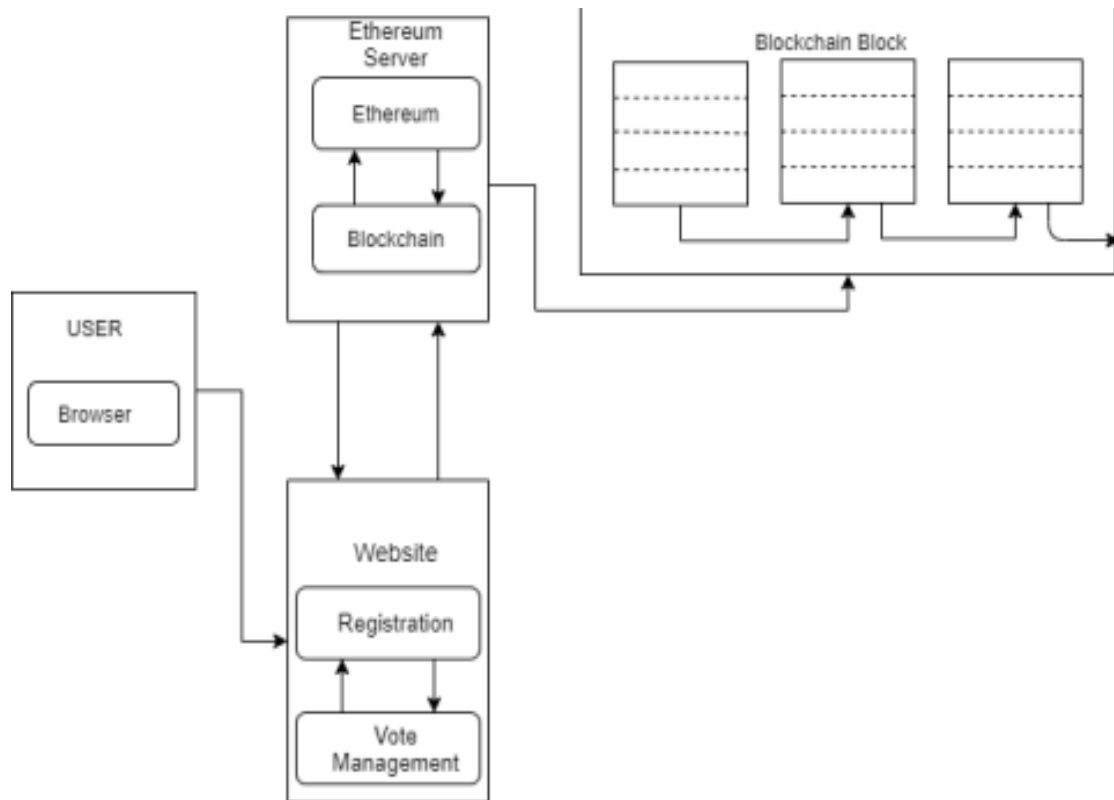


Figure 4.5 System Overview

4.5 Man-In-The-Middle Attack (MITM)

MITM attack is an attack in which data being transmitted between two parties on a network is intercepted, read and modified by a system attacker without the communicating parties knowing that their data has been compromised.

To describe the MITM attack process, this form of attack can be explained as Stephanie being the client would like to establish a connection directly with Michael the server. Stan the attacker would lie in wait for Stephanie to send a request to Michael, upon Stephanie sending the request; Stan would intercept the request, manipulate it and send it to Michael for processing. Michael thinking he is responding to Stephanie directly sends a response which Stan intercepts as shown in figure.

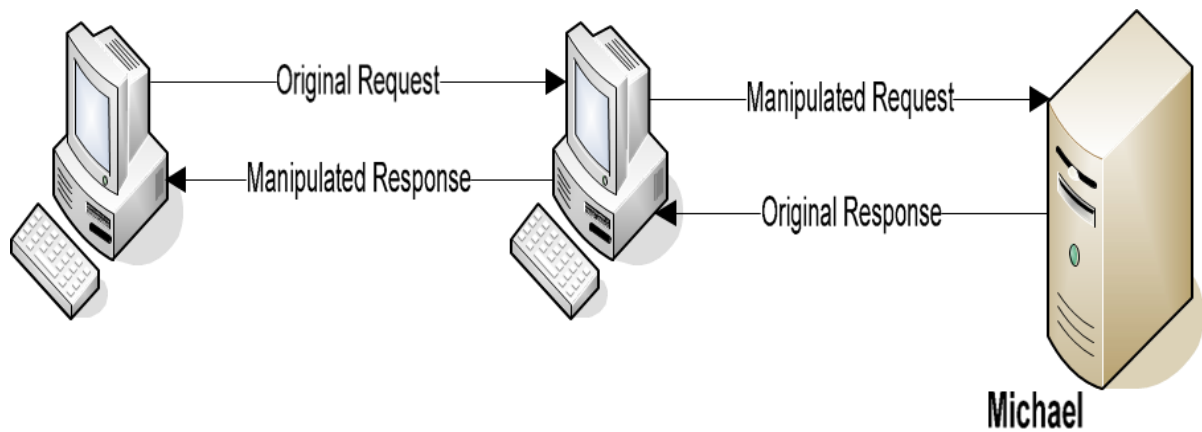


Figure 4.6 MITM Attack Method

4.6 AUTHENTICATION

Authentication is the process of establishing whether someone or something is who or what it is declared to be. In most internet network systems authentication is generally done through the use of login usernames and passwords.

The user of the system is assumed to know the password in order to get authenticated. Every user is initially registered on the system by a system administrator using an assigned or self-declared password. On each subsequent use, the user must know and use the previously declared password. The main weakness of these kinds of systems that is considerable is that passwords can be guessed, stolen, accidentally revealed, or forgotten by the user. System hackers use password guessing as a simple method of attacking a computer system, be it on a network or offline.

Password guessing requires the hacker to have known usernames and suitable password guesses, by persistently trying the guessed passwords into the system, the attacker could finally break in, and this is mainly due to poor passwords being chosen by users. The best way to protect a system from this form of unwanted intrusion is to prevent users from having an infinite number of login attempts with wrong passwords; the user should be locked out of the system after a specific number of failed login attempts.

Another form of password theft can be achieved by a hacker illicitly tapping into a

system terminal on a network and logging the passwords entered. A way of countering this form of attack is by encrypting the data traffic on the network.

For this reason, Internet business and many other transactions require a more stringent authentication process. The use of digital certificates issued and verified by a Certificate Authority (CA) as part of a public key infrastructure is considered likely to become the standard way to perform authentication on the Internet.

4.7 ENCRYPTED COMMUNICATION

The communication process over the internet is intrinsically insecure, due to the fact that data being transferred over the internet medium can be susceptible to attacks and eavesdropping from different points of the transmission route. There is an essential need that online systems which deal with confidential and sensitive data, such as an online voting system, have to provide a means in which data communication between the client to the server is encrypted, thereby making the data being transmitted unusable to a would-be system attacker. There are a number of cryptographic algorithms which can be used to encrypt data; algorithms like HOMOMORPHIC, DES, and Blowfish can all be used at some point of an online system to make it secure. These algorithms are going to be discussed, but the main encryption processing techniques which are behind these algorithms are the Symmetric key cryptography and the Asymmetric key cryptography.

4.8 SYMMETRIC KEY CRYPTOGRAPHY

This form of encryption is also known as the secret key cryptography. Symmetric key cryptography makes use of the same private key while performing an encrypted communication between two users. The same secret key is used for the encryption and decryption of data being transmitted between the two or more users.

This form of cryptography makes use of stream ciphers and block ciphers for encrypting plain text. A stream cipher is an encryption method that is used to encrypt plain text or digits one character at a time while block ciphers encrypt blocks of data.

Symmetric Key cryptography example is the Data Encryption Standard (DES) algorithm.

4.8.1 Block Chipers

A block cipher is an encryption method which encrypts large blocks of text; the block cipher regards the input stream for encryption as blocks of fixed sized bytes which can be up to 128 bits long.

The block cipher can encrypt a 128 bit plaintext and generate a 128 bit cipher text as the output result. The block cipher also has a reverse mechanism, which is in the form of a decryption function that converts the 128 bit ciphertext and decrypts it back to the 128 bit plaintext. In order for a block cipher to encrypt data, the function would need a secret key which comes as a string of bits normally 128 to 256 bits long.

4.9 ASYMMETRIC KEY CRYPTOGRAPHY

This form of encryption makes use of one public key which is available to all users and a private key which is known only by the message recipient. The public key can be exchanged between users who can use it to encrypt data being transmitted to another user, the private key which should be kept secret, is used to decrypt the encrypted data to produce the original unencrypted data. This form of key cryptography is used by the Rivest, Shamir, and Adleman (HOMOMORPHIC) encryption algorithm.

4.10 DIGITAL CERTIFICATES

A digital certificate is security identification medium used in juxtaposition with Asymmetric cryptography. Digital certificates can be provided by the certification authority (CA). The true owner of the public key is determined and the owner is verified to determine if the owner of the public key is who he/she claims to be. The certificate can hold the digital signature of the CA which the CA signs using their private key. The CA's public key is also included to verify that the certificate is valid.

Through the use of a digital certificate the user of an online system can be sure of whom they may be dealing with on the internet. The process of verifying the certificate is done by the user's browser software.

4.11 ENCRYPTION ALGORITHM

Encryption algorithms are used to turn plain text to cipher text. Different forms of encryption algorithms exist and each form has a unique method of generating keys and encrypting input streams.

4.11.1 (HOMOMORPHIC) Encryption Algorithm

The HOMOMORPHIC encryption algorithm is mainly an internet based encryption algorithm, which can be used for authentication. The HOMOMORPHIC encryption algorithm uses the public/private key cryptography technique to encrypt and decrypt data being transported between users. In order to generate the public key and private key to be used to encrypt and decrypt the data to be sent to the user, two prime numbers have to be utilised.

A complex process of mathematical calculations have to take place to acquire a set of two prime numbers that would represent the public key used to encrypt the data and the private key used to decrypt the data once received by the receiver.

The HOMOMORPHIC algorithm works as follows: take two large primes, p and q , and compute their product $n = pq$; n is called the modulus. Choose a number, e , less than n and relatively prime to $(p-1)(q-1)$, which means e and $(p-1)(q-1)$ have no common factors except 1. Find another number d such that $(ed - 1)$ is divisible by $(p-1)(q-1)$. The values e and d are called the public and private exponents, respectively. The public key is the pair (n, e) ; the private key is (n, d) . The factors p and q may be destroyed or kept with the private key.

The HOMOMORPHIC encryption algorithm is used by the Secure Socket Layer (SSL) for encrypting data being transmitted over a secure connection.

4.11.2 Data Encryption Standard Algorithm (DES)

The DES encryption algorithm uses the symmetric key cryptographic technique, whereby the same secret key is used for encrypting and decrypting data. The encryption algorithm is a block cipher which applies a 56 bit key to each 64 bit block of data to be encrypted.

4.11.3 Blow Fish Algorithm

Blowfish is an encryption algorithm which was created by Bruce Schneier. It is a symmetric block cipher with a block size of 64 bits and a variable length key from 32bits to 448 bits.

4.12 Secure Socket Layer (SSL)

In the world of electronic commerce, security is a highly essential feature to have in any web system. A socket is a term for a communications port between computers over any interconnection medium using any computer-to-computer protocol.

SSL is a protocol that is used for sending secure encrypted data over the internet. SSL layer is present between TCP/IP protocol and the application layer as shown in figure. SSL protocol can protect users from “man in the middle attacks”.

The SSL protocol is based on the public key cryptography which has a public and private key pair, the public key can be revealed to everyone but the private key is only known to the recipient of the message being sent. The message is encrypted with the public key and decrypted with the private key.

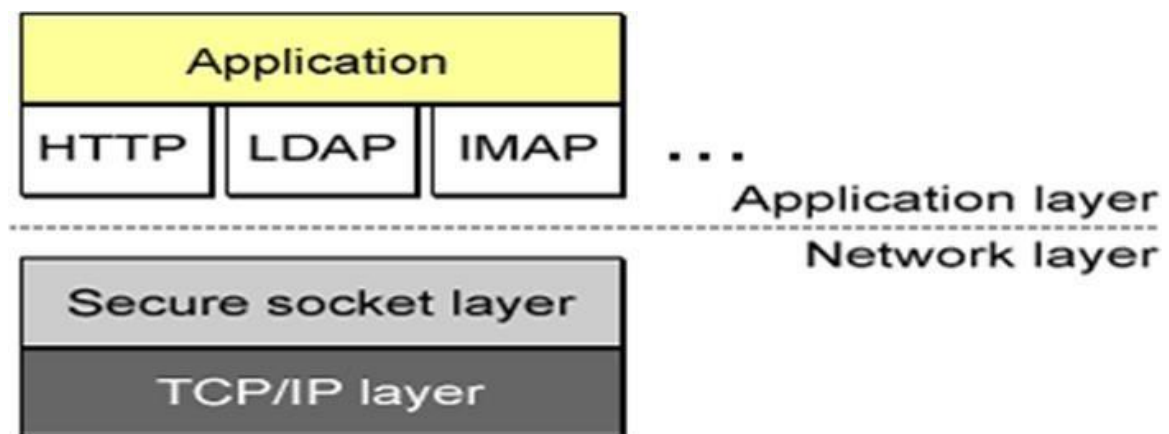
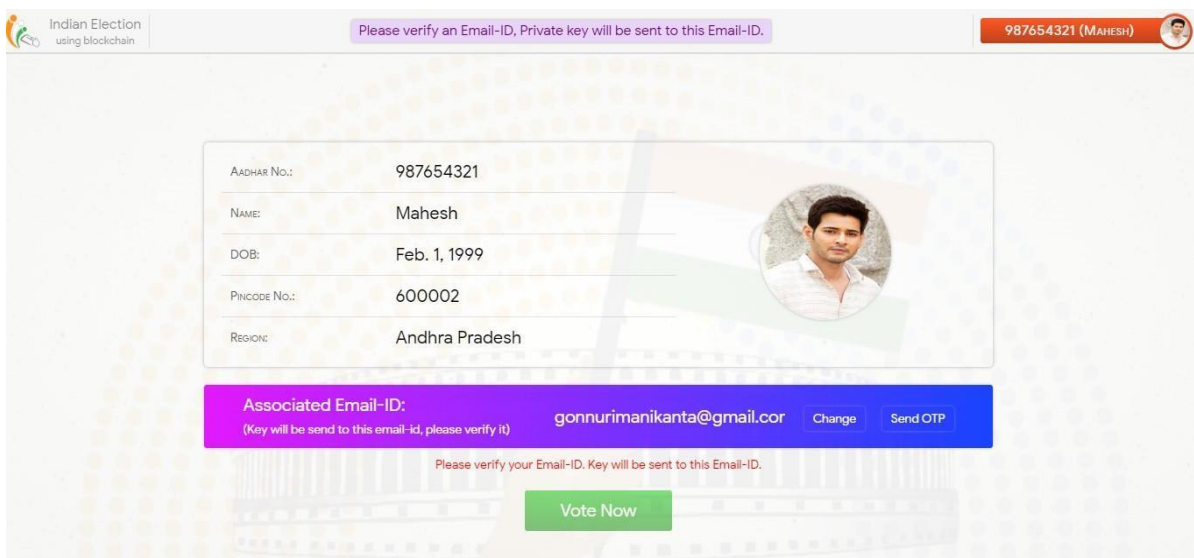
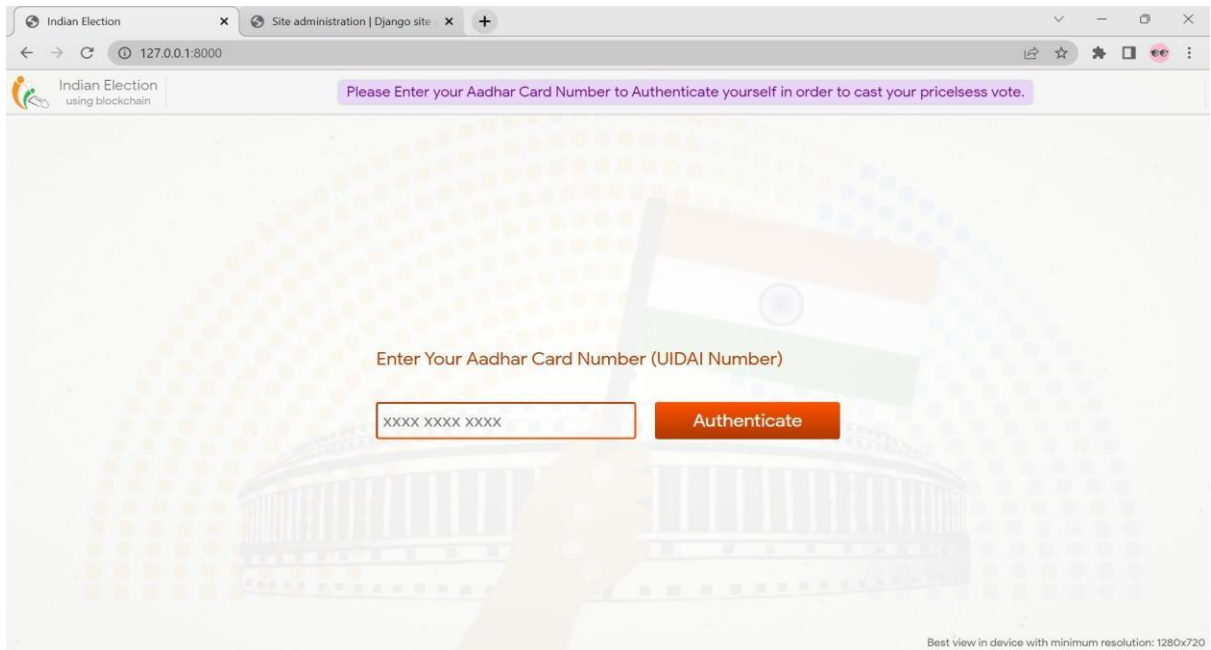


Figure 4.7 Secure Socket Layer

CHAPTER 5

APPLICATIONS & SCREENSHOTS



Don't reply, OTP for email verification Inbox x



way2track01@gmail.com


to me ▾

1


Verify your email id to get the private key to cast your priceless vote. **hdFVfc95** is your OTP for email verification.
Thank you.

↩ Reply

➦ Forward


 Indian Election
using blockchain

Email Verified.

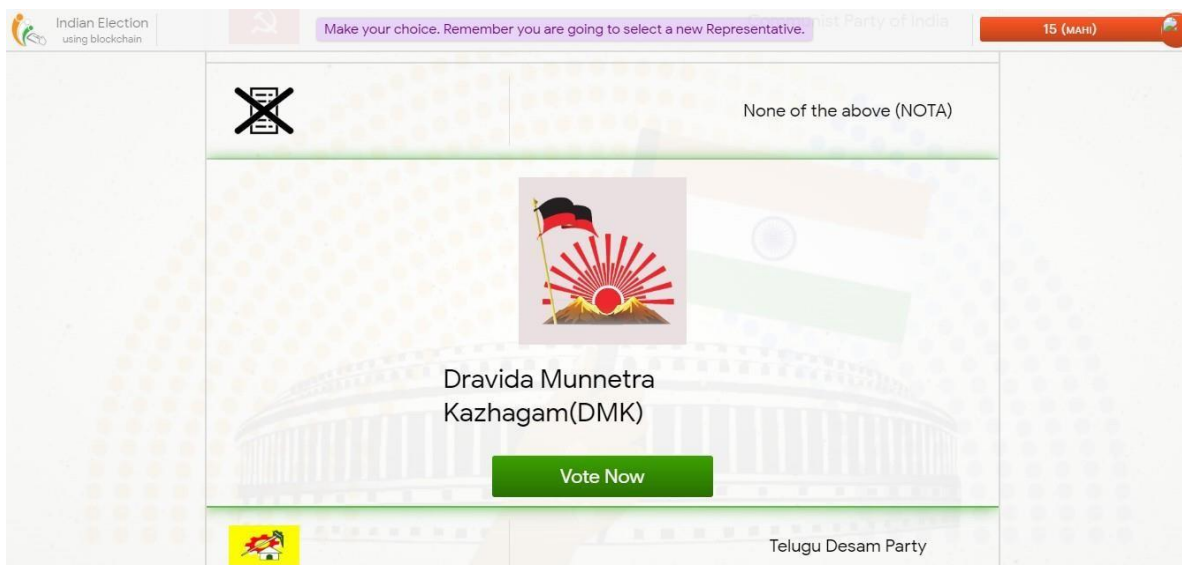
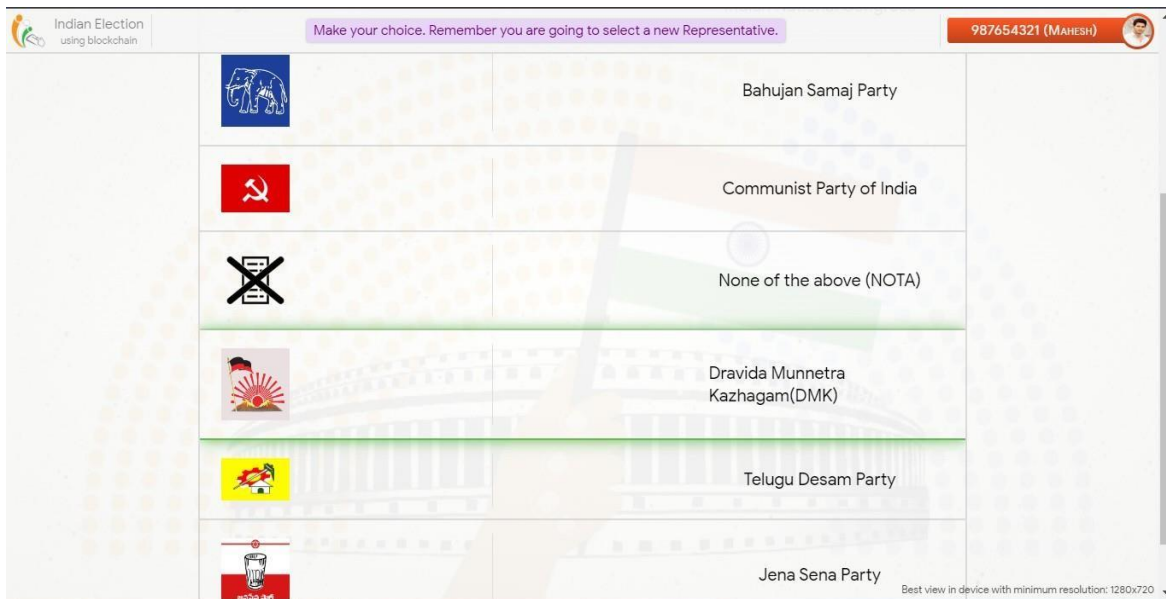
987654321 (MAHESH) 

AADHAR No.:	987654321
NAME:	Mahesh
DOB:	Feb. 1, 1999
PINCODE No.:	600002
REGION:	Andhra Pradesh

Associated Email-ID:
(Key will be send to this email-id, please verify it)

gonnurimanikanta@gmail.cor  [Change](#)

Vote Now



way2track01@gmail.com

to me ▾

Paste the Following Private as it is in order to cast your vote.

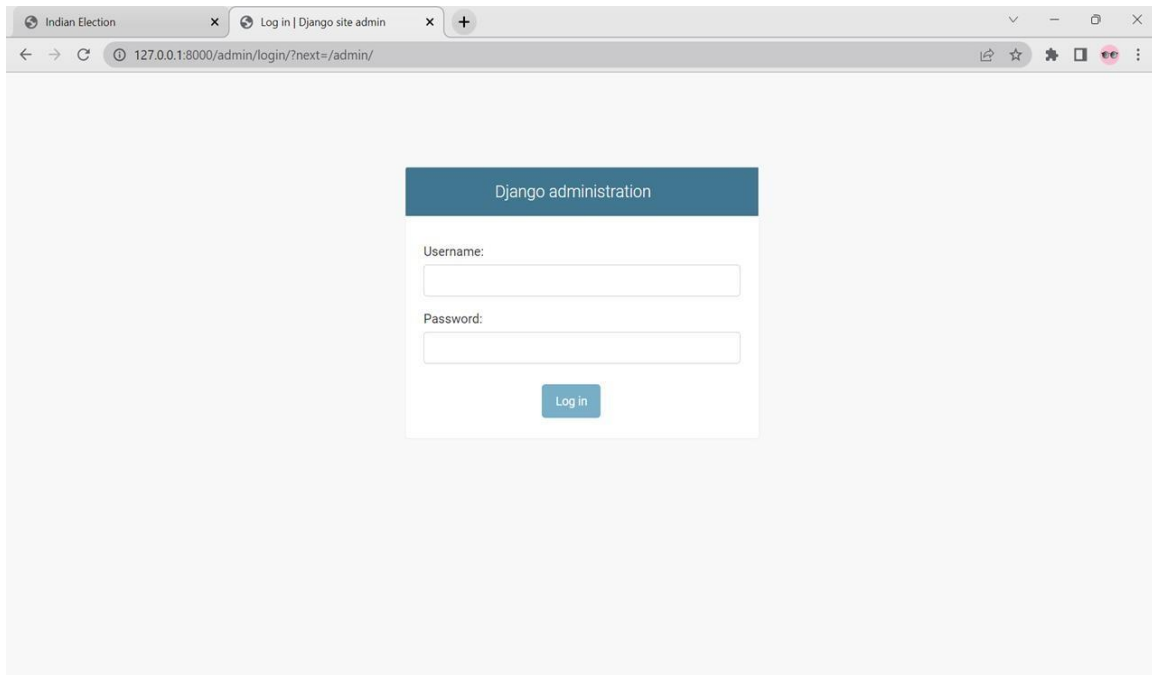
-----BEGIN PRIVATE KEY-----

MIGHAgEAMBMGBYqGSM49AgEGCCqGSM49AwEHBG0wawIBAQQgUnrMm49TBudGgy1O
inncz58UD6wCFc9kV2zxf5liM6hRANCAATMJ+CTAlcZvEWyL9NAmqvIEgFctLbe
6XftQz89A1dBWaBjf3tT1k0F67+DhszNapskWN8GQ45bynlFKI23rJao

-----END PRIVATE KEY-----

NOTE: DON'T REMOVE -----BEGIN PRIVATE KEY----- AND -----BEGIN PRIVATE KEY-----

Thank you.



Home » Home » Blocks » Add block

AUTHENTICATION AND AUTHORIZATION	
Groups	+ Add
Users	+ Add

HOME	
Blocks	+ Add
Mining infos	+ Add
Political partys	+ Add
Vote backups	+ Add
Voterss	+ Add
Votes	+ Add



Add block

Prev hash:

Merkle hash:

This hash:

Nonce:

Timestamp: Date: Today  Time: Now 

Note: You are 5.5 hours ahead of server time.

[Save and add another](#) [Save and continue editing](#) [SAVE](#)

Home » Home » Political partys » Add political party

AUTHENTICATION AND AUTHORIZATION	
Groups	+ Add
Users	+ Add

HOME	
Blocks	+ Add
Mining infos	+ Add
Political partys	+ Add
Vote backups	+ Add
Voterss	+ Add
Votes	+ Add

Add political party

Party id:

Party name:

Party logo:

Candidate name:

Candidate profile pic:

[Save and add another](#) [Save and continue editing](#) [SAVE](#)

Home · Home · Voters · Add voters

AUTHENTICATION AND AUTHORIZATION

Groups + Add

Users + Add

HOME

Blocks + Add

Mining infos + Add

Political partys + Add

Vote backups + Add

Voterss + Add

Votes + Add

Add voters

Uuid:

Name:

Dob: Today

Note: You are 5.5 hours ahead of server time.

Pincode:

Region:

Profile pic:

Email:

☐ Vote done

Indian Election using blockchain		Vote count.	
2		None of the above (NOTA)	3
3		Communist Party of India	3
4		Bhartiya Janta Party (BJP)	2
5		Telugu Desam Party	2
6		Indian National Congress	1
7		Jena Sena Party	1
8		Dravida Munnetra Kazhagam(DMK)	1

CHAPTER 6

RESULT & CONCLUSION

This chapter will discuss the development of the entire system as a whole. It will give an insight into the general procedures that were taken to accomplish the project. It will also discuss the aims and objectives of the initial proposal and the objectives that could not be accomplished. It will cover the drawbacks the project possesses and the necessary work that can be used to enhance the system in the future.

The main project objective was to build a secure online voting system, which would be used. The aim of the project was to convert the current use of paper based voting to an electronic form of voting, which would enable voters to vote remotely from any location through the use of the internet.

Research was carried out on the different forms of online voting systems that currently exist, noting their features, and how to influence the participation of voters to an election. Various forms of server side technologies were investigated in order to choose the right programming language to use for the development of the online voting system.

Security issues that may affect the integrity of the online voting system were addressed and counter measures on how to protect the system's security were researched. A number of software development methodologies were reviewed, upon careful consideration, the methodology was chosen as the most appropriate development method to use for this particular project.

During the design and development of the system, the main effort was focused on designing and developing the system to achieve a solution based on the concepts of the system proposal. This phase provided a clear description of how the system was to be created. The main emphasis was on creating an intuitive user interface for retrieving information, querying the database by the use of Python classes and scriptlets and ensuring security was of top priority.

CHAPTER 7

FUTURE SCOPE

Blockchain technology allows people to verify that their votes are recorded and counted correctly. Any voter may be able to check the counting without the security being hampered. Also there are security concerns in blockchain-based e-voting too, but it is more secure than the traditional voting systems which use EVMs. In future the EVMs will be placed in museums for the next generation.

In continuation of this work, we are focused on improving the resistance of blockchain technology to the 'double spending' problem which will translate as 'double voting' for e-voting systems. Although blockchain technology achieves significant success in detection of malleable change in a transaction, successful demonstration of such events have been achieved which motivates us to investigate it further. To this end, we believe an effective model to establish trustworthy provenance for e-voting systems will be crucial to achieve an end-to-end verifiable e-voting scheme. The work to achieve this is underway in the form of an additional provenance layer to aid the existing blockchain based infrastructure.

REFERENCES:

- [1] Quoc Khanh Nguyen, Quang Vang Dang. Blockchain Technology for the Advancement of the Future, 4th International Conference on Green Technology and Sustainable Development (GTSD), January 2018. <https://doi.org/10.1109/GTSD.2018.8595577>
- [2] Hussein Hellani, Abed Ellatif Samhat, Maroun Chamoun, Hussein El Ghor, Ahmed Serhrouchni. On Blockchain Technology: Overview of Bitcoin and Future Insights, IEEE International Multidisciplinary Conference on Engineering Technology (IMCET), 2018. <https://doi.org/10.1109/IMCET.2018.8603029>
- [3] Rifa Hanifa Tunisia, Budi Rahardjo. A review paper on Blockchain Based E-Voting Recording System Design, 11th International Conference on Telecommunication Systems Services and Applications (TSSA), 2017. <https://doi.org/10.1109/TSSA.2017.8272896>
- [4] Kanika Garg, Pavi Saraswat, Sachin Bisht, Sahil Kr. Aggarwal, Sai Krishna Kothuri, Sahil Gupta. A Comparative Analysis on E-Voting System Using Blockchain, 4th International Conference on Internet of Things: Smart Innovation and Usages, 2019. <https://doi.org/10.1109/IoT-SIU.2019.8777471>
- [5] Ahmed Ben Ayed. A CONCEPTUAL SECURE BLOCKCHAIN- BASED ELECTRONIC VOTING SYSTEM, International Journal of Network Security & Its Applications (IJNSA) Vol.9, No.3, May 2017. <https://doi.org/10.5121/ijnsa.2017.9301>
- [6] S. Nakamoto. Bitcoin: A Peer-to-Peer Electronic Cash System, www.Bitcoin.Org, p. 9, 2008.
- [7] A. G. Malvik and B. Witsoe. Elliptic Curve Digital Signature Algorithm and its Applications in Bitcoin, pp. 1-5, 2016.
- [8] Zibin Zheng¹, Shaoan Xie¹, Hongning Dai², Xiangping Chen⁴, and Huaimin Wang³. An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends, IEEE 6th International Congress on Big Data, 2018.
- [9] Fridrik P. Hjalmarsson, Gunnlaugur K. Hreidarsson. Blockchain-Based E-Voting System, 2018. <https://doi.org/10.1109/CLOUD.2018.00151>

- [10] David Khoury, Elie F. Kfoury, Ali Kassem, Hamza Harb. Decentralized Voting Platform Based on Ethereum Blockchain, IEEE International Multidisciplinary Conference on Engineering Technology (IMCET), 2018. <https://doi.org/10.1109/IMCET.2018.8603050>
- [11] Julia kolosova, Andrejs Romanovs. The Advantages and Disadvantages of Blockchain Technology, 2018 DOI 978-1-7281-1999-1/18.
- [12] A. Barnes, C. Brake, and T. Perry. Digital Voting with the use of Blockchain Technology, Team Plymouth Pioneers - Plymouth University, 2016.
- [13] The ethos blog. <https://www.ethos.io/cryptocurrency-news-ethos-blog>. Accessed: 2020-01-27.
- [14] Private, public, and consortium blockchains - what's the difference? <https://www.binance.vision/blockchain/private-public-and-consortium-blockchains-whats-the-difference>. Accessed: 2020-01-24.
- [15] Hashing algorithm <https://www.movable-type.co.uk/scripts/sha256.html>. Accessed: 2020-01-27.
- [16] What is blockchain? <https://www.investopedia.com/terms/b/blockchain.asp>. Accessed: 2020-01-24.
- [17] Himanshu Agarwal and GN Pandey. Online voting system for India based on aadhaar id. In 2013 Eleventh International Conference on ICT and Knowledge Engineering, pages 1- 4. IEEE, 2013.
- [18] Soumyajit Chakraborty, Siddhartha Mukherjee, Bhaswati Sadhukhan, and Kazi Tanvi Yasmin. Biometric voting system using aadhar card in india. International journal of Innovative research in Computer and Communication Engineering, 4(4), 2016.
- [19] Basit Shahzad and Jon Crowcroft. Trustworthy electronic voting using adjusted blockchain technology. IEEE Access, 7:24477-24488, 2019.
- [20] Scott Wolchok, Eric Wustrow, J Alex Halderman, Hari K Prasad, Arun Kankipati, Sai Krishna Sakhamuri, Vasavya Yagati, and Rop Gonggrijp Security analysis of india's

electronic voting machines. In Proceedings of the 17th ACM conference on Computer and communications security, pages 1-14, 2010.

[21] Marwa Chaieb and Souheib Yousfi. Loki vote: A blockchain-based coercion resistant e-voting protocol. European, Mediterranean, and Middle Eastern Conference on Information Systems, Springer, pages 151-168, 2020.

[22] David Khoury, Elie F Kfoury, Ali Kassem, and Hamza Harb. Decentralized voting platform based on ethereum blockchain. 2018 IEEE International Multidisciplinary Conference on Engineering Technology(IMCET), IEEE, pages 1-6, 2018.

[23] Rifa Hanifatunnisa and Budi Rahardjo. Blockchain based e-voting recording system design. 2017 11th International Conference on Telecommunication Systems Services and Applications (TSSA), IEEE, pages 1-6, 2017.

[24] Haibo Yi. Securing e-voting based on blockchain in p2p network. EURASIP Journal on Wireless Communications and Networking, SpringerOpen, 2019(1):1-9, 2019.