Saving Democracy By Modern Technology

Noor Ahmed[1], Prof. Anupama Pattanasetty[2]

[1]PG Student, Department of Artificial Intelligence and Data Science,
Sharnbasava University Kalaburagi,Karnataka, India.
nnoorahmedd@gmail.com
[2]Professor, Department of Computer Science and Engineering
, Sharnbasava University Kalaburagi, Karnataka, India.
anubngp.pama10@gmail.com

ABSTRACT Having a democratic voting system in place is crucial for any nation due to the general distrust of the conventional voting system. Individuals have seen the infringement of their basic rights. Lack of transparency has been a problem with several electronic voting methods. The government has a hard time winning the confidence of its citizens since most voting processes aren't transparent enough. It is easy to abuse, which is why both the old and new digital voting systems have failed. Finding solutions to issues with both the paper and electronic voting systems, such as voting-related injustices and accidents, is the main goal. A fair election with less injustice is possible with the use of blockchain technology integrated into the voting process. Both digital and physical voting methods have their limitations, making them unsuitable for widespread use. This evaluates the importance of finding a way to protect people's democratic rights. To foster confidence between voters and election officials, this article introduces a platform built on blockchain technology, which maximises system stability and transparency. Without the need for traditional polling places, the proposed technology lays the groundwork for digital voting using blockchain. A scalable blockchain may be supported by our suggested architecture via the use of adaptable consensus algorithms. The voting process is made more secure with the use of the Chain Security algorithm. When conducting a chain transaction, smart contracts provide a safe channel of communication between the user and the network. There has also been talk of the voting system's security being based on blockchain technology.

KEYWORDS: Voting system, attributes, Use case diagram, TCP

I. INTRODUCTION

In this context, "voting" means making a selection. Voting or other electoral processes may facilitate this kind of expression. Votes cast via a particular electronic media may be collected, counted, and saved electronically through electronic voting.

The planned project's primary objective is to replace the University of Westminster Student Union's present paper-based election method with an electronic one. At now, the student union's voting method is experiencing low voter participation since it is inconvenient for the majority of students. This problem will be solved by the proposed method, which would allow voters to choose their candidates using any computer with an internet connection.

This project will analyse the student union's present voting procedure and find a way to model it with the Saving Democracy By Modern Technology that will be put into place. Voting procedures will be handled by the system through various election mechanisms.

The system will be designed with a strong emphasis on security. These safeguards will be in place from the moment a voter enters the voting system until they leave, ensuring that every step of the voting process is secure. Voters will be unable to cast multiple ballots for the same candidates thanks to the system's robust security measures.

II. LITERATURE SURVEY

Various approaches and procedures are used in the numerous activities aimed at introducing modifications to electronic and Saving Democracy By Modern Technology. Although some of these measures do a good job of protecting the system's secrecy and security, complex technologies are still required to oversee and manage the voting process and all of the related data.

2.1 BASIC E-VOTINGAPPROACH/ARCHITECTURE

To ensure the safe transmission of data, systems designed to facilitate digital voting via internet portals and smart devices use a variety of encryption and decryption mechanisms.

- ***HOMOMORPHIC ENCRYPTION ECHNIQUE***

A strong and widely-used method, homomorphic encryption is recognised for its various uses. Saving Democracy By Modern Technology design has recently made use of it. This

encryption is based on the El Gamal exponential cryptosystem, which is used in the voting system. We encrypt every vote using the exponential El Gamal algorithm before sending it in. You may immediately tally encrypted votes without decrypting them because to the additive homomorphism characteristic of this crypto scheme.

- ***CENTRALIZED ARCHITECTURE:***

Nevertheless, there are a variety of methods available for encoding data in order to safeguard it from tampering during transmission to the network. Here we may talk about a downside: when the right data is put in the database, there has to be a lot of trust and security. Because of the security risks posed by hacking and other forms of unauthorised access, centralised storage is cumbersome for highly valuable data.

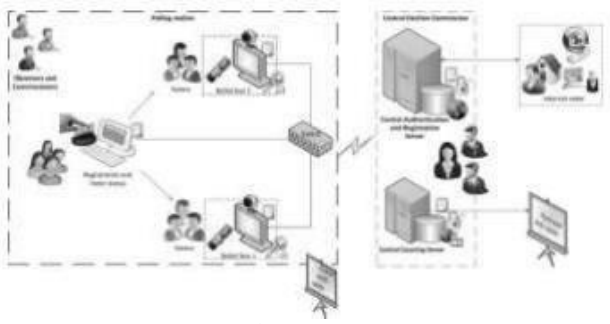

Fig:1 Centralized Architecture of Voting system

The centralised architectural technique makes use of previous models and designs. Potential ethical and security concerns might arise from such. We put the data at danger by collecting it all in one place. It is susceptible to unjust control. Therefore, with the aid of blockchain technology, the fair framework is able to circumvent the issue of data storage in a distributed manner. A distributed ledger, a block chain records all transactions in chronological order. In traditional databases, one entity is responsible for its upkeep and maintenance. This entity has full authority over the database and may do whatever they want with the recorded data, including adding fake data, censoring otherwise legitimate modifications, or manipulating the data itself. A financial network is one example of a use case where the data stored is too sensitive and the temptation to manipulate it is too great to let a single organisation have complete control over the database. In most cases, this is not an issue because the organisation maintaining the database does so for its own benefit and has no reason to falsify the database's contents.

2.2 AIMS AND OBJECTIVES

The following are goals and objectives of the system that is to be developed:

- The creation of an Saving Democracy By Modern Technology would allow citizens to choose their preferred candidates.
- Make sure that only authorised users may access the voting system by establishing a safe authentication mechanism.
- For the purpose of keeping track of votes and user data, construct a database.
- Investigate any security flaws in the system and put a plan into action to prevent unauthorised access to the voting process.
- Turn on the feature that counts votes by candidate.
- In order to facilitate efficient administration of the election system, it is necessary to construct a backend administrative section.
- Build the administrator's tools to add, remove, and edit users', candidates', and sub administrators' information on the system.
- Present the results of the vote graphically so that the administrator may examine them.
- So that people may vote for the candidates of their choice
- Permit voters to peruse candidate biographies throughout the voting process.
- Record the exact time each vote was cast by adding a timestamp to the database. This will allow administrators to easily produce reports based on the results of the vote.
- Stop people from casting multiple ballots for the same candidates.

III. INTERNET TECHNOLOGY

The Internet is a system of publicly accessible, globally distributed computer networks that employ the Transmission Control Protocol/Internet Protocol (TCP/IP) protocol to transfer data in a packet switched format. It was necessary to conduct a thorough investigation of internet technology as it would be used to transmit data between the voting system's client and server.

3.1 INTERNET HISTORY

In its early days, the Internet was a research effort in the late 1960s that aimed to better understand computer-to-computer data transfers using packet switching. The grant money for the study came from ARPA, which is part of the US Department of Defence. Data packets in a packet switching network may travel along any route between their origin and destination [9]. A distinct network address is used to identify the sender and the recipient. The ARPANET network came into being because of the study. The fourth version of the Internet Protocol, which TCP/IP networks would utilise, was developed in 1978. Formerly run by DARPA, the

ARPANET was transferred to the Defence Communications Agency (DCA) in 1983. Internet popularity skyrocketed as a result of this change, which allowed for its broad usage in educational institutions all around the globe.

3.2 TCP/IP PROTOCOL SUITE

One network design that allows for the connection of several networks is the TCP/IP protocol suite. Multiple layers make up the TCP/IP protocol suite reference model, and they all work together to provide data transfer across the internet. The following is a description of the layers and what they do.

Application Layer: Supports the whole suite of high-level protocols included in the TCP/IP package. Here you may find the File Transfer protocol (FTP), which allows you to move files between different hosts. Domain Name System (DNS), Virtual Terminal Protocol (TELNET), Simple Mail Transfer Protocol (SMTP), and other protocols are accommodated at this layer.

Transport Layer: Facilitates data transfer between two hosts on a network. According to the TCP/IP Reference model, two protocols may coexist on the transport layer that sits above the internet layer. The User Datagram Protocol (UDP) and the Transmission Control Protocol (TCP), both of which will be discussed in further detail later in the paper. Because it is a connectionless protocol, UDP does not ensure that datagrams will arrive at their destination on time. When transmitting data, UDP does not regulate the flow or congestion as TCP does.

Internet Layer: It is the foundation of the TCP/IP protocol suite. The main function of this layer is to direct data packets as they go from one network to another. Internet Protocol packets are delivered to their particular destinations via the Internet layer.

Network Access Layer: In the Internet reference model, the lowest layer is the network access layer. At this level, you'll find the protocols that the host machine use to communicate with the other nodes in the network.

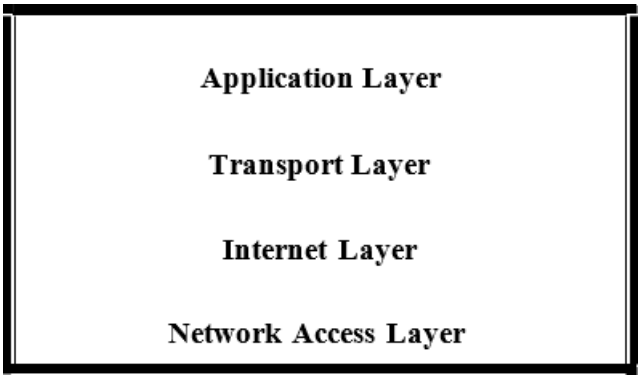

Fig:2 TCP/IP Reference model.

3.3 INTERNET PROTOCOL

Packet transmission is a fundamental function provided by the Internet Protocol. Data packet switching in a packet switched network is made possible by the Internet Protocol, a data-oriented protocol. As a packet service, the Internet Protocol (IP) is not foolproof; it cannot ensure the secure transmission of data packets from their originator to their destination. Internet Protocol data packets are susceptible to duplication, latency, and loss. Datagrams may be sent securely by using the Transmission Control Protocol. The TCP/IP Reference model's Internet Layer defines Internet Protocol.

3.4 TRANSMISSION CONTROL PROTOCOL

Transmission Control Protocol (TCP) is the most used protocol within the Internet Protocol family. Transmit Control Protocol (TCP) is a dependable connection-oriented protocol that ensures error-free transmission of data packets across the Internet from one computer to another. The Transmission Control Protocol (TCP) allows hosts on a network to reliably send and receive datagrams and packets. TCP ensures that data packets travel from their origin to their final destination. Also, TCP separates data for many programmes that are operating on the same host computer at the same time, such as an email server and a web server. Guaranteed packet delivery and data serialisation are two essential features provided by TCP that the Internet Protocol does not. The data service serialisation guarantees that the sequence of data transmission from the source host remains unchanged upon receipt from the destination host.
The destination host will utilize the sequence number that TCP assigns to each data packet that is sent.

IV. SYSTEM DESIGN

4.1 DATABASE DESIGN

A database system must be established to hold all the data collected from the users of the Saving Democracy By Modern Technology before it can be developed. Enforcing and enhancing the security of the voting system will also be greatly aided by the database system that is to be established. The database system will hold user information, which will be used for authentication purposes. Because of its low price tag and availability as open source software, MySQL database server has been chosen as the preferred database. In order to store the massive amounts of data that will be entered, MySQL's enormous storage capacity will be crucial.

4.1.1 Entities & Attributes

Entities and attributes will serve as the building blocks of the database structure that is about to be built. The entities are represented by the database tables that are going to be

constructed. Various fields, represented as characteristics, are stored in the tables. You may configure these properties to hold either text or numeric values, among other data types. A primary key, stored in an attribute of each object, is a value that uniquely identifies a row in a table or entity.

To illustrate the database's logical structure and the links between entities, entity relationship diagrams were constructed. You may find these diagrams in Appendix C. There is a description of all the database entities in the entity table.

DATABASE ENTITY & ATTRIBUTE DIAGRAM

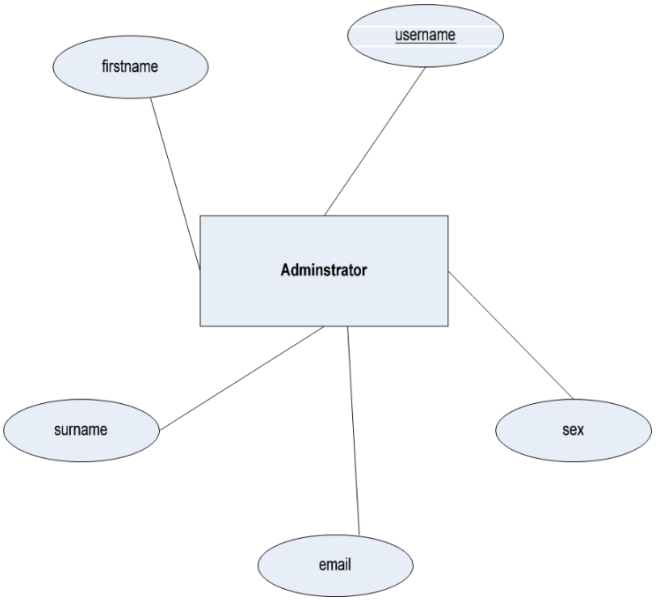

Fig:3 Administrator entity with its attributes

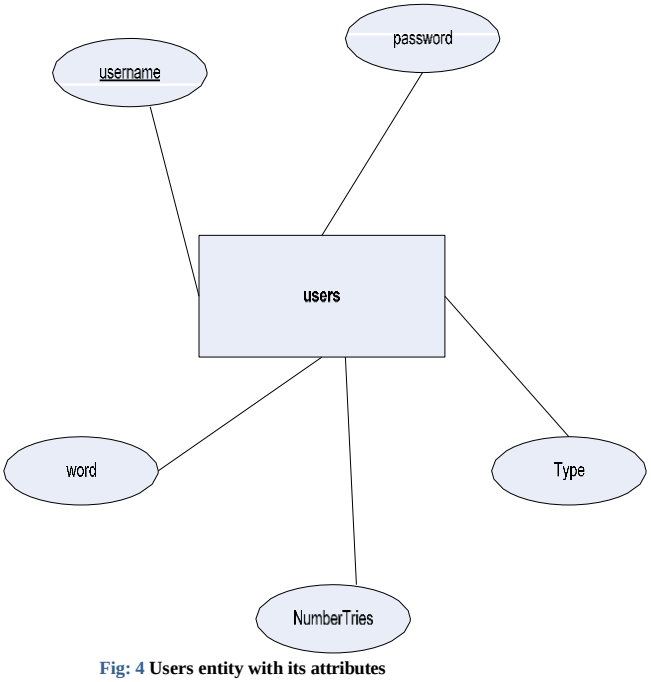

Fig: 4 Users entity with its attributes

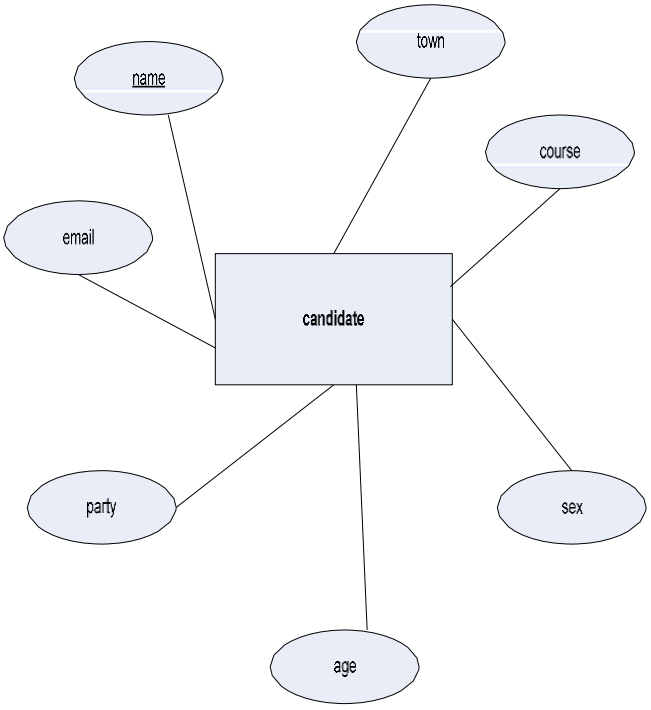

Fig:5 Candidate entity with its attributes

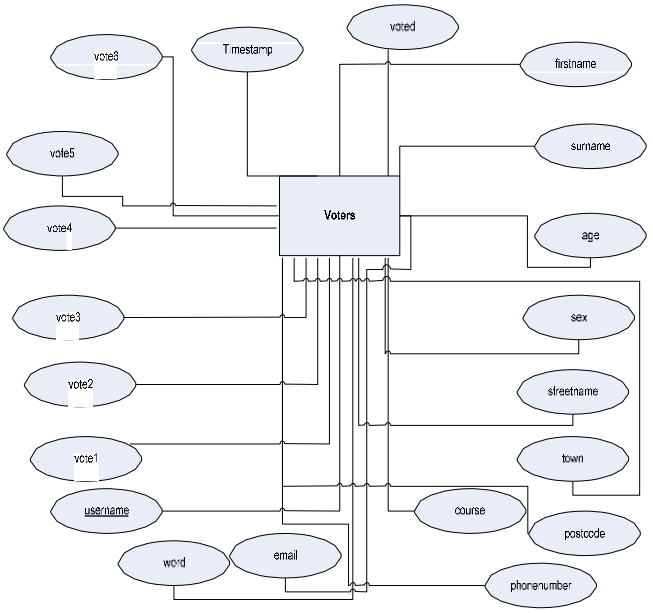

Fig: 6 Voters' entity with its attributes

4.2 SOFTWARE DESIGN

A software design details the algorithms to be used, the user interfaces to interact with the system's components, the data that will be a part of the system, and the structure of the programme that will be implemented. Before building any part of the Saving Democracy By Modern Technology, the system software must be carefully considered and designed. All the steps needed to complete a given task within the

system will be considered during the software design phase. Two design methodologies may be utilised to develop a well-structured design, and the system design would demonstrate the data flow inside the system.
Using a technique called functional decomposition, structured software modelling breaks down the system into sets of interdependent functions, allowing for a more top-down and function-oriented approach to software development. To illustrate the inner workings of a system, the model primarily makes use of data flow diagrams. on page
A design style known as "Object-Oriented Design" (OOD) may help developers simplify their projects by using self-contained objects that can interact with one another. The discipline known as object-oriented design UML modelling diagrams. [4]

4.2.1 Use Case Modeling

It is crucial to utilise a more end-user friendly design approach and avoid using complicated technical jargon when representing the system's architecture to an end user, similar to a system analyst. The needs of the Saving Democracy By Modern Technology may be represented via use case modelling, which shows potential interactions between the system and its users.
People whose jobs it is to interact with the various parts of the system are called "actors." The administrators and voters are the most important parts of the system.
You can see using the use case model which parts of the system each player will be engaging.

ADMINISTRATOR USE CASE DIAGRAM

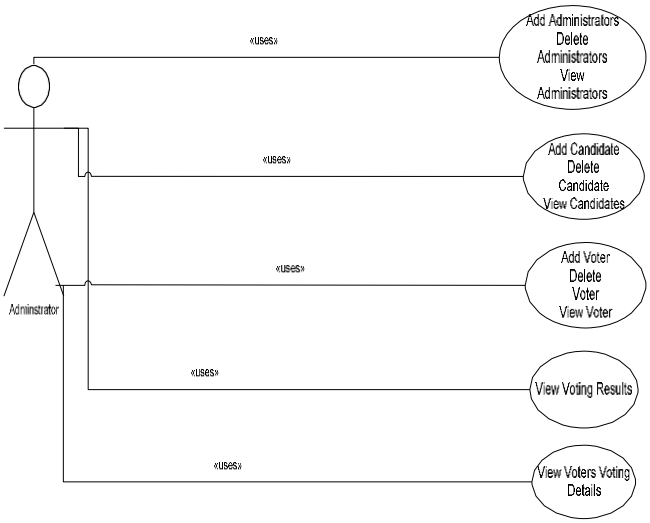

Fig: 7 Administrator use case diagram

VOTER USE CASE DIAGRAM

Fig: 8 Voter use case diagram

4.2.2 System Access Design

Implementation of the system will be contingent upon its possessing robust authentication capabilities. To guarantee that only authorized users may access the system, authentication is a must. The design of the system's login access is crucial to the security of the voting system. Administrators and voters should be able to access the system using different login pages. To prevent voters from gaining access to the administrator's page, the system will provide separate access privileges to each actor utilizing the system. Each user would have their own Python class that checks the system database using SQL statements to verify their login credentials. This would be part of the login page design process. An error message should be sent to the user in the form of a Python bean if the data submitted is incorrect or does not match the information in the database system.

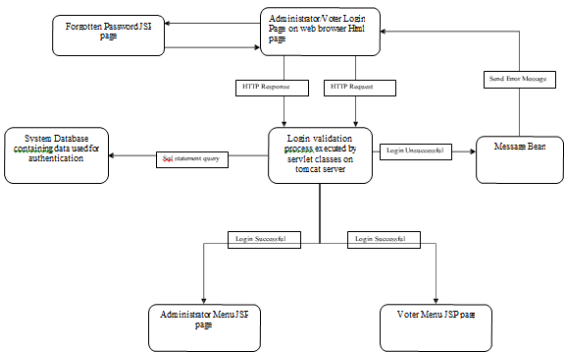

Fig:9 Displays the system's access login design

The basic difficulty that any safe system would have is users forgetting their selected passwords. An adequate facility has to be built to cope with this problem. As part of the voting system's design, the administrators' and voters' login pages will be connected to a page where users can retrieve forgotten passwords. It will be mandatory for every user to have a memorable word that can be used to retrieve their password from the system's database. Python servlets have validation functions built in to them, so users can't get their passwords unless they provide the right username and a secret phrase

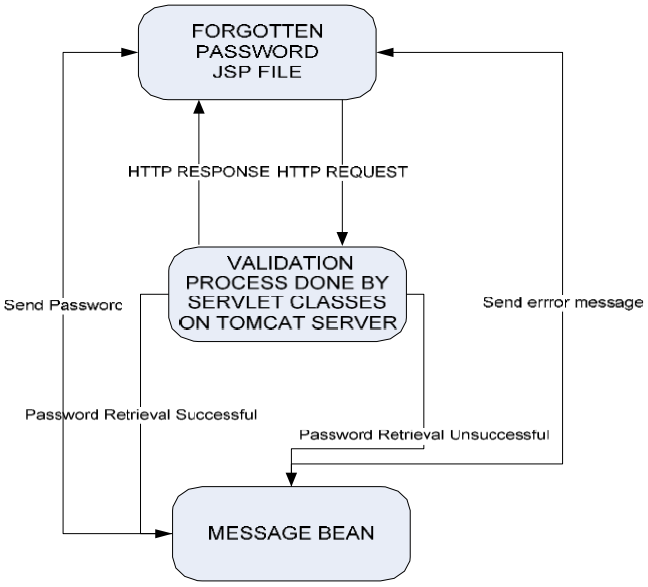

Fig: 10 Design of the forgotten password section

4.2.3 Administrator & Voter Design

The administrator and voter will have access to their designated areas when the authentication procedure is complete and their authority to do so has been granted. After choosing a candidate to vote for and logging out of the system, voters would no longer be able to access the system. The administrator may add, remove, and view administrators, candidates, and voters. When candidates' names are added or removed, the voter's JSP page will likewise dynamically update to reflect the changes.

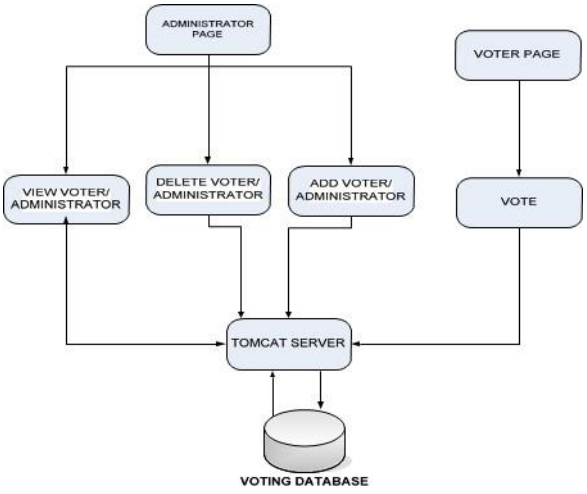

Fig: 11 Design of the administrator and voter system features after login

4.2.4 System Security Design

The suggested system must include robust security measures to protect the honesty of the voting process, which is of the utmost importance. To make the system more secure, three different types of security mechanisms were built into it to protect the database and the data flowing through it. In addition to the login facility, the four measures must be employed.

4.2.5 System Architecture

Several technologies on both the client and server sides would collaborate to form the system's architecture.

FRONT END

The front end of the system is the voting system's user interface, which is accessed via the user's web browser. It is here that users may communicate with the server by sending and receiving HTTP requests. Using HTML, the base of the system may be constructed.

BACKEND

Here, on the server side of the programme, known as the back end, all of the HTTP requests that come in from the client are processed. The servlet and jsps files will be loaded by a Tomcat server engine. The engine may then issue requests, and the client will get the dynamic content in HTML format so that they can browse the website.
Data provided from the system's client will be saved in a database; specifically, the system will make use of the MySQL database.

The JDBC API driver acts as a middleware layer, translating method calls in Python to database API calls, allowing the database to get data from the server.

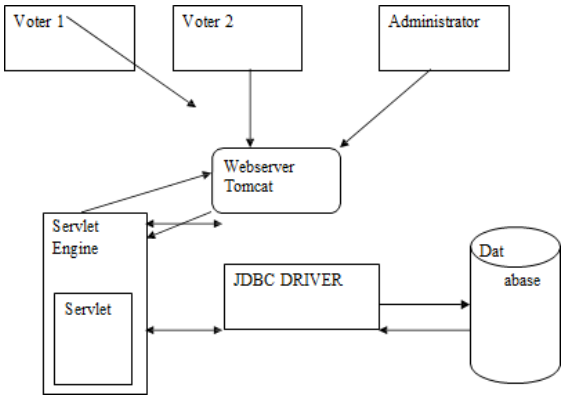

Fig: 12 System Architecture

V. TESTING

The system needs to undergo extensive testing to guarantee its flawless operation. During the testing phase, the Saving

Democracy By Modern Technology's features will be double-checked to ensure they function as intended. Any bugs or flaws will also be found.
An appropriate testing technique must be used to carry out the system testing process efficiently. Considerations about the size and complexity of the system to be tested should be examined while selecting an acceptable testing technique.

5.1 TEST STRATEGIES

The most common approaches of testing software-based systems are white box and black box testing, however there are other ways that may be utilised as well.

5.1.1 Black Box Testing

The tester employs this method, which is also called functional testing, when they are unaware of the system's inner workings. Instead of testing the actual code, the tester runs the tests according to the criteria that have already been defined.
In this kind of test, the end user enters data into the system and verifies that it produces the intended result. Users of the system may do the tests with no previous knowledge of the system's coding, which is a benefit of black box testing. [36]

5.1.2 White Box Testing

The purpose of this testing approach—also called structural testing or glass box testing—is to examine the inner workings of the system's code and logic. In order to find any broken code, the tester must have clear understanding of the code used to build the system. [35]
Both testing methodologies must be used to ensure that the system is tested appropriately.

5.1.3 Test Plan

Making a test plan is necessary for thoroughly testing the Saving Democracy By Modern Technology's functionality. The designed test strategy would disrupt the testing procedures to address any issue with the Saving Democracy By Modern Technology.

Various web browsers, as well as the system and database servers, and online pages, would be the primary targets of the testing procedure. Because the system's functionality depends on the web browsers used by its users, this test must be performed.

Login authentication elements would be the primary emphasis of the testing process. These features are essential to the system as a whole, since they prevent unauthorised access and keep the system secure. The encryption and decryption capabilities of the passwords in use would be verified by conducting a test.

To make sure the user gets the right message if the forms aren't filled out properly, the system's form validation has to be tested. To make sure that the data being obtained from users is really entering the database system, it is necessary to verify the system database engines that link the application to the database system.

5.2 TEST DATA

Table: 2 Test Data Test Ref No	**Test Data**	**Expected Outcome**	**Final result**
1	Connect to server	The Client should be able to Connect to server	Pass
2	Connect to mysql database	The Client should be able connect to data base	Pass
3	Test internet explorer browser compatibility	When user enters the online voting url welcome page should be displayed	Pass
4	Test Netscape browser compatibility	When user enters the online voting url welcome page should be displayed	Pass
5	Test SSL connection from web browser	Using the secure local host port number 8443, the user should be able to enter the website over a secure connection	Pass
6	Web Page Navigation	Webpage navigation links to should open specified web page	Pass
7	Login validation	Error message should be displayed when inappropriate data is entered	Pass
8	Login process to distinguish voter and administrator	Voter should not be allowed to login into admin page, admin should not be allowed to login into voter page	Pass
9	Attempt to guess password more than three time during login	System user should be blocked from accessing the system on third attempt	Pass
10	Voter view and select candidate and submit vote	The voters choice of candidates should be displayed on confirmation page	Pass
11	Voter casts votes	The voters table in voting database should be updated with new votes	Pass
12	Login Block for voter	Voter who has voted once should be flagged and blocked from voting again	Pass
13	Voting results page	The votes counted should be updated when new vote is cast	Pass

14	Add voter, candidate and administrators validation	Error message should be generated if necessary boxes are not filled in and if username chosen is already taken	Pass
15	JDBC connection to database	Data from registration form should be entered into database	pass
16	Password encryption	Password entered into database should be encrypted	pass
17	Administrator should be able to view voters, candidate & admin details from database	Data from database should be printed on screen	pass
18	Administrator should be able to delete voter, candidate and administrator detail	Details of voter, candidate & administrator should be deleted from database	pass
19	Password Decryption	Forgotten password request by user should be decrypted before being sent to user screen	pass
20	Logoff	User should be able to log off successfully from system	pass

VI. CONCLUSION

In this section, we shall go over the overall system's evolution. It will provide a glimpse into the overall steps that were done to complete the project. Goals and goals from the original plan, as well as those that were unattainable, will also be covered. In it, we'll talk about the project's flaws and the things that need fixing so we can make the system better in the future.

The primary goal of this research was to provide a safe method of internet voting. The project's overarching goal was to migrate from paper ballots to electronic ones, so that people could cast their ballots from anywhere in the world with an internet connection.

Researchers looked at the many Saving Democracy By Modern Technology available today, comparing and contrasting their features and learning how to get more people to cast their ballots. In order to choose the most appropriate programming language for building the Saving Democracy By Modern Technology, several server side technologies were researched.

Researchers looked at potential threats to the Saving Democracy By Modern Technology's security and developed strategies to mitigate them. The waterfall methodology was determined to be the best suitable development approach for this specific project after a thorough evaluation of many software development approaches.

The primary goal of the system's design and development was to realize a solution in accordance with the ideas presented in the system proposal. At this stage, the process for building the system was laid out in detail. Developing a user-friendly interface for data retrieval, securing the system, and querying the database using Python classes and scriplets were the primary goals.

In order to find any flaws or weaknesses in the system, it was subjected to extensive testing throughout the project's testing phase. The system was determined to be ready for delivery to end users based on the test findings.

Because of its intended application in the student union election process, the developed system achieved its goals of being both easy to use and secure.

REFERENCES

1. Jayson Falkner, Ben Galbraith, Romin Irani, Casey Kochmer, Sathya Narayana Panduranga, Krishnaraj Perrumal, John Timney, Meeraj Moidoo Kunnumpurath, (2001), Beginning JSP Web Development,Wrox.

2. Peter denHaan, Lance Lavandowska, Sathya Narayana Panduranga, Krishnarag Perrumal, (2004), Beginnign JSP 2 From Novice to Professional, Apress.

3. Aneesha Bakharia, (2001),PythonServerPages,Prima Tech.

4. Bruce W.Perry,(2004), Python Servlet & JSP Cookbook, O'Reilly

5. Simson Garfinkel, Gene Spafford,(1997), Web Security & Commerce, O'Reilly.

6. Time Stamp. URL: http://whatis.techtarget.com/definition/0,,sid9_gci817089,00.html

7. Maydene Fisher, Jon Ellis, Jonathan Bruce (2003), JDBC API Tutorial and Reference. Third Edition, Sun Microsystems.

8. George Reese, (2000), Database Programming with JDBC and Python. O'Reilly.

9. Laura A.Chappell, Ed Tittel (2004), Guide to TCP/IP. Thomson.

10. Transmission Control Protocol URL:http://en.wikipedia.org/wiki/Transmission_Control_Protocol