Secured Voting System Unsing Blockchain

Prof. NandKishor Narkhede[1], Karan Patel[2], Sakshi Dhobale[3], Ganesh Wadhe[4], Sagar Sonawane[5],

[1]Assistant Professor, [2, 3, 4, 5,6]Final Year, Department of Electronic & Computer Science, Shah & Anchor Kutchhi Engineering College, Mumbai, Maharashtra, India.

---***---

***Abstract:** A large mistrust closer to the conventional balloting machine has made democratic vote casting in any country very critical. Humans have seen their essential rights being violated. Different digital vote casting structures have been challenged because of a loose transparency maximum balloting systems aren't transparent enough; this makes it very hard for the authorities to gain voters' trust. The motive is to resolve the ambiguities of traditional and modern digital voting device it that it is able to be without problems exploited. The number one objective is to resolve problems of the conventional and virtual voting device, which consist of any kind of mishap or injustice for the duration of the procedure of voting. Blockchain era may be used inside the vote casting device to have a truthful election and reduce injustice. The bodily vote casting structures have many flaws in it in addition to the virtual vote casting structures aren't ideal sufficient to be implemented on large scale. This appraises the need for a approach to secure the democratic rights of the humans. This text offers a platform based totally on contemporary era blockchain that affords most transparency and reliability of the system to construct a trustful relationship among electorate and election government. The proposed platform offers a framework that may be applied to behavior voting pastime digitally via blockchain without involving any bodily polling stations. Our proposed framework supports a scalable blockchain by way of the use of flexible consensus algorithms. The chain security set of rules applied within the balloting system makes the voting transaction greater at ease. Smart contracts provide a secure connection between the user and the community whilst executing a transaction within the chain. The safety of the blockchain primarily based voting system has additionally been mentioned, additionally encryption of transaction the usage of cryptographic hash and prevention of attack 51% on the blockchain has also been elaborated. The performance assessment of the proposed system indicates that the system may be carried out in a large scale populace*

I. INTRODUCTION

The term voting is understood to be the form of choice. This form of expression can be performed through the ballot, or by any other electoral schemes. The electronic voting is a way in which votes cast by voters of a specific electronic medium can be retrieved, tallied and stored electronically.

The project to be produced will be focusing on converting the current paper-based elections system currently being used by the University of Westminster Student Union into an electronic system. The current voting system being used by the student union is currently suffering from a poor voter turnout due to the fact that the system in place is not convenient for most students. The system to be created will address this issue by providing voters with the capability of casting their votes for their chosen candidates via an internet enabled computer.

The project will focus on the current voting method being used by the student union, and identify a way in which the method can be modelled with the internet voting system to be implemented. The system will implement different election mechanisms used for casting votes.

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 restriction preventing the voter from voting more than once for the election candidates.

II. LITERATURE REVIEW

- 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 stored 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 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 administer 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 them choose candidates.

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 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 prioritised in the building of the voting system, and SSL (Secure Socket Layer) and a mode of password encryption would also be utilised in the construction of the system.

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, to gain more knowledge on the system to be built and to allow analyze different components to be used for constructing the system.

III. METHODOLOGY

A) System Design

This chapter's goal is to describe the way in which the online voting system is to be built. In order to build an efficient and flexible system, the appropriate system development methodology has to be chosen to suit the system to be created. The waterfall design methodology is been utilized to design and develop the online voting system.

In order for any form of computer systems to be built in an efficient and user-friendly manner, a highly structured and well-engineered design has to be created. The design of a software orientated system has to follows certain steps in achieving its end product. The design of a system enables organizations and companies to map out a strategic plan which the system developers would have to follow. The design of a system is very important in the construction of any web-based application, and it prevents the occurrence of mistakes and errors during the implementation phase which can be highly costly to the organization funding the specify project.

B) System Requirements

The online voting system to be built will be used by two sides, the students who would be voting and the administrators who are in charge of creating and maintaining information on the system.

The system has to be very secure due to the fact that it is a voting system, the main objective of the voting system is to ensure that votes being cast by voter cannot be rigged or unduly compromised in any shape or form. A high level of user authentication has to be established to maintain security.

The information and usability of the voting system has to be very constructive, efficient and easy to understand by the user. Good systems are easy to utilize, the user should be saved from any form of complexity.

C) Design Techniques

In order to design and build a well-structured system, it is highly vital to plan and understand how the data being inputted and outputted would be conveyed around the system.

There are a number of tools that can be used to plot the construction of the voting system from start to finish. The use of system models would be highly essential in describing and visualizing the way in which the system would be operated.

In the case of the design for the secure online voting system, User Case diagrams would be used to how a graphical representation of how the users will be able to interact and operate the system. Data flow diagrams would be used to showcase the entire architecture of the whole system. This form of design would be very helpful to the system developers and would help in engineering the system in a consistent and efficient manner.

D) System Architecture

The architecture of the system would comprise of a number client and server-side technologies working together.

FRONTEND

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 jsps, 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 stored 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.

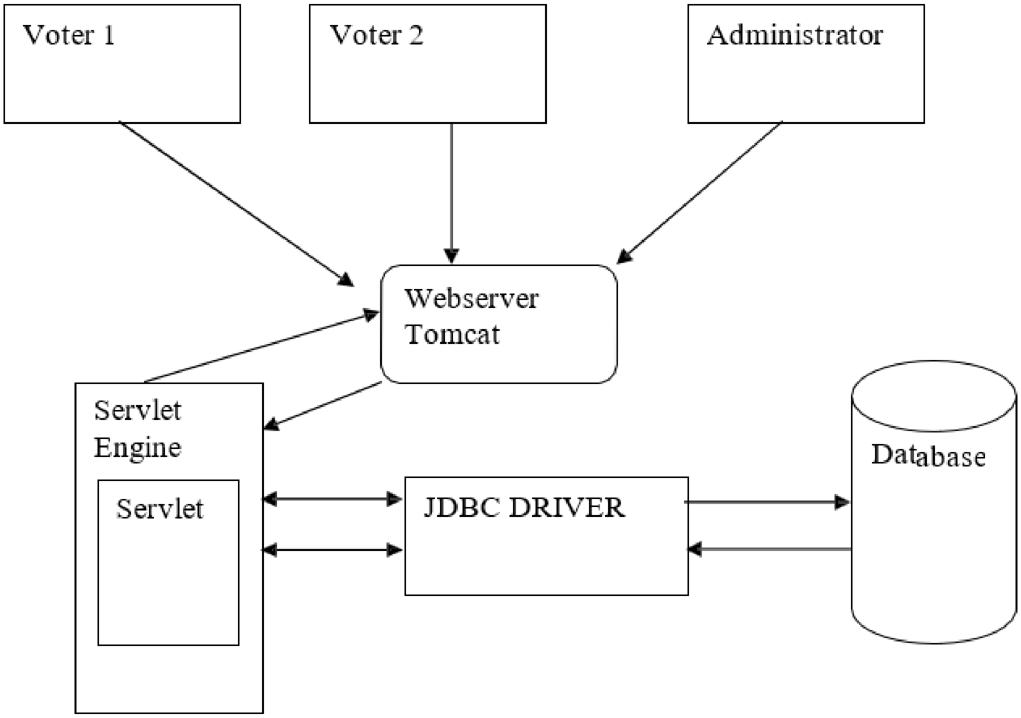

Fig 3.1 System Architecture

E) System Security Design

A top priority requirement for the proposed system is to have highly efficient and secure features, to safe guard the integrity of the voting system. In order to strengthen the system's security, three forms of security measures where engineered into the system to safeguard the data flow within the system and the information being stored in the database. The four measures to be used in addition to the system's login access facility are shown in table

System access attempts log	This security measure would enable the database to record the number of attempts a user tries to log into system with a wrong password. The system should lock the user out, if the attempted tries exceed a certain number. This measure will be used to prevent password guessing
Password Encryption	This security measure would be used to encrypt password entered into the system through the use of an encryption algorithm, thus in the case of the database being compromised, the password stored would be useless. In order for a user to obtain their password from the forgotten password page, a decryption method would be use to decrypt the encrypted password back to its original form to be displayed to the user
Secure Socket Layer (SSL) Transmission	The form of security would ensure that any data inputted from the users web browser would be encrypted and useful to a hacker who would want to acquire information

F) Administer & 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 7-9. 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.

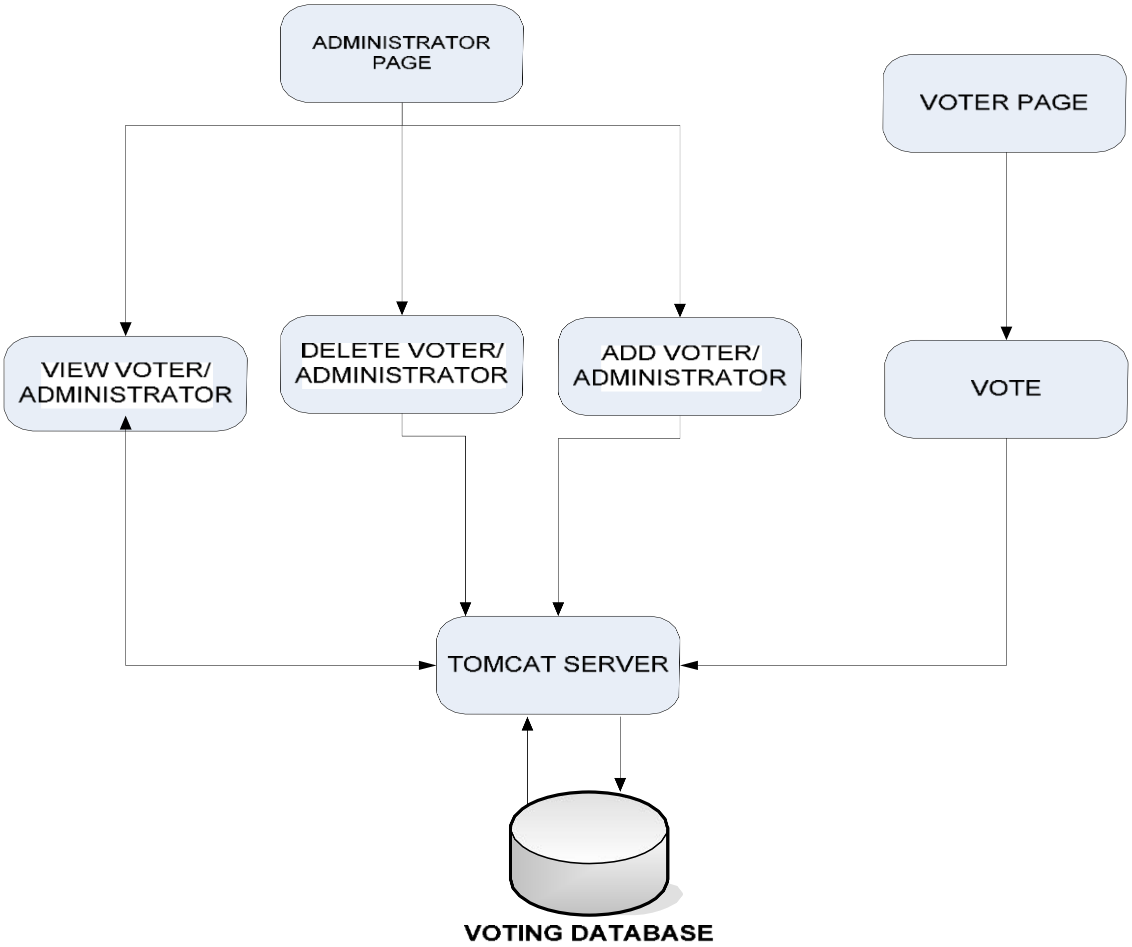

Fig 3.2 Design of the administrator and voter system features

G) Justification

There are a number of other server-side technologies that can be used to implement a web-based voting system. ASP (Active Server Pages) is pure examples of a server scripting language that can be used build a dynamic web-based system, developed by Microsoft, it can be used to generate dynamic content for web pages, but ASP is restricted to operating on only windows-based platform, while JSP is platform independent, which means that it can be run from an operating system platform making it a more reliable server-side scripting like.

PHP is another server-side scripting language that can be an equivalent technology to use for building dynamic web sites. It is an open-source scripting language and it widely accepted by most operating system platforms and many kinds of web servers. JSP would still be a preferred choice for building the web-based system due to the fact that Python is proven to be a lot more secure technology in comparison to the other mentioned scripting languages.

IV. Database Entity and Attribute

Database

In order to develop the online voting system, a database system has to be in place to be used to store all the data retrieved from the users of the system. The database system to be created will also play a major part for enforcing and strengthening the security of the voting system. Authentication of the system's users will rely on the details of the users which would be stored in the database system. MySQL database server has been selected as the database of choice, due to the sheer fact that it is open source which cuts the cost of having to buy database software. MySQL has a very large storage capacity which will be essential for storing the large amount of data to be inputted.

Entities and Attribute

The database to be constructed will make use of entities and attributes as a form of structure for the database information. The entities take the form of each table to be created in the database. The tables house different fields which take the form of attributes. These attributes can be set to store certain types of data, be it text or integer values. Each entity will have an attribute which will hold a primary key, a primary key is a value that can be used to identify a unique row in a table or entity.

Entity relationship diagrams were created to show the logical structure of the database and the relationships between entities. The entity table gives a description of the entities used in the database. The entities used in the database system have been described in table.

Entity Table

Entity Name	Description
Administrator	The administrator table will be used to store all the details of the administrators utilizing the system. Each administrator will have a unique username. The attributes utilized in this entity are shown in figure.
Candidates	The candidates table will be used to store all the details of the elections candidates. Each candidate will have a unique username. The attributes utilized in this entity are shown in figure
Users	The user's tables will be used to store the encrypted passwords of the voters and administrators. A field within the table called "type" will also be used to differentiate voters from administrators within the table. The tries field will be used to store the number of login attempts by each user. The attributes utilized in this entity are shown in figure
Voters	The voters table will be used to store the details of each voter in the system. Due to the high security measures to be taken when developing the system, the voters table will also contain fields with the records of each candidate voted for by the voter, this design has to be done to prevent the possibility of a voter voting more than one. Through this means if there is any need for suspicion of vote rigging by the elections organizer the database table can prove that each voter voted only once. A field called "voted will also be used to record when each voter has cast their vote by incrementing to 1. A timestamp field will also be added to record the exact time each voter cast their vote. The attributes utilized in this entity are shown in figure

V. Testing

Testing

In order to ensure that the system works perfectly, it has to be rigorously tested. The testing procedure would be used to check all the features developed for the online voting system work efficiently, the test procedure would also be used to identify any hidden errors or deficiencies the system may possess.

In order to conduct an efficient testing process on the system, a suitable testing procedure has to be utilized. In choosing an appropriate testing strategy to use, some considerations have to be reviewed in terms of the size and complexity of the system to be tested.

Testing Strategies

There is a number of testing strategies that can be utilized to conduct adequate testing processes, the black box and white box testing methods are the most popular methods used to test software developed systems.

A) Black Box Testing

This testing strategy which is also known as functional testing is used by a tester who has no knowledge of the internal structure of the system. The tester does not test the programming code itself but instead performs the test based on previously understood requirements.

This form of testing is usually conducted by the end user, who would enter an input into the system and check for an expected output. The advantage of using black box testing is that the test can be done by the users of the system, without them needing to have prior knowledge of the system's code.

B) White Box Testing

This testing strategy which is also known as functional testing is used by a tester who has no knowledge of the internal structure of the system. The tester does not test the programming code itself but instead performs the test based on previously understood requirements.

This form of testing is usually conducted by the end user, who would enter an input into the system and check for an expected output. The advantage of using black box testing is that the test can be done by the users of the system, without them needing to have prior knowledge of the system's code.

Test Plan

In order to efficiently test the full functional capability of the online voting system, a test plan has to be created. The test plan created would break the testing processes in order to tackle any malfunctioning feature of the online voting system.

The testing process would focus on testing the system's server, database server and web pages on different web browsers. This test has to be carried out to ensure that the system would be able to function on any web browser utilised by the system's users.

The testing process would focus on the system login authentication features; this is an integral part of the system, because it ensures security of the system is upheld again unauthorized access. A test would be carried out to check if the password being utilized are encrypted and decrypted.

The system's form validation would also have to be tested to ensure the error message to be presented to the user if the forms are not filled correctly is functioning appropriately. The system database engines which connect the application to the database system have to be tested to ensure that information being retrieved from the users are populating the database system.

VI. 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 that where 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 where 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 where addressed and counter measures on how to project the system's security where researched. A number of software development methodologies where reviewed, upon careful consideration, the waterfall 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

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.

[7] URL: http://whatis.techtarget.com/definition/0,,sid9_gci817089,00.html

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

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

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

[11] Transmission Control Protocol

[12] URL: http://en.wikipedia.org/wiki/Transmission_Control_Protocol

[13] Andrew S.Tanenbaum, (1996), Computer Networks. Third Edition. Prentice Hall

[14] Mark Andrews: Story of a Servlet

[15] URL: http://Python.sun.com/products/servlet/articles/tutorial/

[16] Cisco Systems Inc.(2002): Introduction to TCP/IP URL:http://www.cisco.com/univercd/cc/td/doc/product/iaabu/centri4/user/scf4ap1

[17] .htm#xtocid6

[18] URL:http://www.jguru.se/jguru/Channel_Html/generic/images/developers/servlet

[19] _lifecycle.gif

[20] Introduction What is JDBC

[21] URL: http://Python.sun.com/docs/books/jdbc/intro.html

[22] Bruce Schneier: Analysis of SSL 3.0 Protocol URL: http://www.schneier.com/paper-ssl.pdf

[23] URL: http://www.Homomorphicsecurity.com/Homomorphiclabs/node.asp?id=2293