ONLINE VOTING SYSTEM

Antaro shyla S M
Department of Electronics and communication Engineering
Hindusthan college of Engineering and technology
Coimbatore-641032,India

Akash S
Department of Electronics and communication Engineering
Hindusthan college of Engineering and Technology
Coimbatore-641032,India

Dhileep K
Department of Electronics and communication Engineering
Hindusthan college of Engineering and Technology
Coimbatore-641032,India

Dinesh kumar S
Department of Electronics and communication Engineering
Hindusthan college of Engineering and Technology
Coimbatore-641032,India

MS Vanitha R(Assistant professor)
Department of Electronics and communication Engineering
Hindusthan college of Engineering and Technology
Coimbatore-641032,India

Abstract— **Voting is one of the fundamental rights of every citizen of a democratic country. By utilizing the right of the voting, people elect their most suitable leader who will lead them. In this modern era where technology is being used in every aspect of life, election is a place to apply the best technology. This project, describes the design, operation of smart EVM using microcontroller, RFID to improve the election process by avoiding the electoral fraud and to ensure safety, security, reliability, guarantee and transparency and smooth conduct of elections in the country as the voting is of crucial importance in the society where people determine its government. The usual system for voting in india is ballot paper-based voting system, where voting is sometimes unfair. In this proposed system we have used Arduino and RFID Scanner that can identify each voter, count votes and can prevent fake votes. The proposed system is more digital, technology-based and secured system. The microcontroller processes the information and send the details to the required mobile phone with the help of Internet of things(IOT) Technology.**

Keywords— E-polling, voting system, block chain application, block chain voting, E-voting, electoral system.

I. INTRODUCTION

India has democratic government. As now all Indian citizen become a part of the growing digital India .They have a digital ID that is Aadhar card. Voting schemes have evolved from counting hands in early days to systems that include paper, punch card, electronic voting machine. An electronic voting system which is used nowadays provide some characteristic different from the traditional voting technique, and also it provides improved features of voting system over traditional voting system such as accuracy, convenience, flexibility, privacy, verifiability and mobility. But Electronic voting systems suffers from various drawbacks such as time consuming, consumes large volume of paper work, no direct role for the higher officials, damage of machines due to lack of attention, mass update doesn't allows users to update and edit many item simultaneously etc. These drawbacks can overcome by Online Voting System. This is a voting system by which any voter can use his/her voting rights from anywhere in the country. Voter can cast their votes from anywhere in the country without visiting to voting booths, in highly secured way. That makes voting a fearless of

violence and that increases the percentage. India is the largest democratic and Republic country in the world. In any democratic and republican country elections are necessary and also a heart to the democracy. In a democracy people have the privilege of being ruled by a government of their own choice. People choose their representatives through elections which are the normal features of democracies all over the world. But these elections should be held freely, fairly, transparently and impartially. For this purpose, the constitution of India provides an Election Commission with autonomous (Art 324-329), consisting a Chief Election Commissioner and other Election Commissioners (at present two other election commissioners).

II. SOFTWARE DEVELOPMENT

The online voting system is for the citizens from all over India that consists of the data and information. In this project, user should vote for their candidate by using only the aadhar card. For that user needs to register first and then he/she will receive the OTP through mobile number. Then only user can login to the application. Then he/she can vote for their decided candidate.

A. ***Java***

A platform is the hardware or software environment in which a program runs on Linux, Solaris, and MacOS. Most platforms can be described as a combination of the operating system and hardware. The Java platform differs from most other platforms in that it's a software-only platform that runs on top of other hardware-based platforms. The Java API is a large collection of ready-made software components that provide many useful capabilities, such as graphical user interface (GUI) widgets. The Java API is grouped into libraries of related classes and interfaces; these libraries are known as *packages.* An application is a standalone program that runs directly on the Java platform. A special kind of application known as a *server* serves and supports clients on a network. Examples of servers are Web servers, proxy servers, mail servers, and print servers. Another specialized program is a *servlet.* A servlet can almost be thought of as an applet that runs on the server side. Java Servlets are a popular choice for building interactive web applications, replacing the use of CGI scripts. Servlets are similar to applets in that they are runtime extensions of applications. Instead of working in browsers, though, servlets run within Java Web servers, configuring or tailoring the server.

B. ***JDBC***

In an effort to set an independent database standard API for Java; Sun Microsystems developed Java Database Connectivity, or JDBC. JDBC offers a generic SQL database access mechanism that provides a consistent interface to a variety of RDBMSs. This consistent interface is achieved through the use of "plug-in" database connectivity modules, or drivers. If a database vendor wishes to have JDBC support, he or she must provide the driver for each platform that the database and Java run on.

To gain a wider acceptance of JDBC, Sun based JDBC's framework on ODBC. As you discovered earlier in this chapter, ODBC has widespread support on a variety of platforms. Basing JDBC on ODBC will allow vendors to bring JDBC drivers to market much faster than developing a completely new connectivity solution.

C. ***SQL***

The designers felt that their main goal was to define a SQL interface for Java. Although not the lowest database interface level possible, it is at a low enough level for higher-level tools and APIs to be created. Conversely, it is at a high enough level for application programmers to use it confidently. The highest level of MySQL structure is a database, within which you can have one or more tables that your data. For example, let's suppose you are working on a table called users, within which you have created columns for surname, firstname, and email, and you now wish to add another user. One command that you might use to do this is: INSERT INTO users VALUES.

D.NETWORKING

- **UDP**
  UDP is also connectionless and unreliable. What it adds to IP is a checksum for the contents of the datagram and port numbers. These are used to give a client/server model - see later.
- **TFC**

TCP supplies logic to give a reliable connection-oriented protocol above IP. It provides a virtual circuit that two processes can use to communicate.

- **Internet addresses**
  In order to use a service, you must be able to find it. The Internet uses an address scheme for machines so that they can be located. The address is a 32 bit integer which gives the IP address. This encodes a network ID and more addressing. The network ID falls into various classes according to the size of the network address.
- **Network address**
  Class A uses 8 bits for the network address with 24 bits left over for other addressing. Class B uses 16 bit network addressing. Class C uses 24 bit network addressing and class D uses all 32.
- **Subnet address**
  Internally, the UNIX network is divided into sub networks. Building 11 is currently on one sub network and uses 10-bit addressing, allowing 1024 different hosts.
- **Host address**
  8 bits are finally used for host addresses within our subnet. This places a limit of 256 machines that can be on the subnet.

III.WORKING PRINCIPLE

1.BALLOT CHAIN WEB DASHBOARD

Initially, the election commission board set under registration process in server. In Under registration process, the Electoral Server is integrated with Aadhar and Blockchain to conduct election securely.

2. END-USER MODULE

2.1.Election commission admin

Election officer has the authority to add, delete or edit the election district list. Likewise, even the booth details like the reference number, district, and the booth manager in-charge can be seen or edited. In voting process, when election commission checks the voting progress in server.

2.2.ECI authority

Once the election commission deselects, the voting progress gets closed in server. The e-voting machine assigned as voting closed at this time voter cannot able to poll their vote. Mainly the ECI authority has the secret key to decrypt Ballot chain votes of each candidate from different booth and announce the winner of election district wise. Finally, the election commission selects the Result announcement option in the server, at this time election commission will start to count the vote automatically and announce the result.

2.3.Returning officer

Returning Officer In every constituency, one Officer is designated as Returning Officer by the Commission in consultation with the concerned State government. However, an Officer can be nominated as Returning Officer for more than one constituency. All the nomination papers are submitted to the Returning Officer. Papers are scrutinised by him/her and if they are in order, accepted by him/her. Candidate details like name, age, party, district can check, edited, added or deleted by RO. Election symbols are allotted by him/her in accordance with the directions issued by the Election Commission. He/she also accepts withdrawal of the candidates and announces the final list. He/she supervises all the polling booths, votes are counted under his/her supervision and finally result is announced by him/her. In fact, the Returning Officer is the overall in charge of the efficient and fair conduct of elections in the concerned constituency.

2.4.Presiding officers

Every constituency has a large number of polling booths. Each polling booth on an average caters to about a thousand votes. Every such booth is under the charge of an officer who is called the Presiding

Officer. He/she supervises the entire process polling in the polling booth and ensures that every voter gets an opportunity to cast vote freely. After the polling is over, he/she seals all the ballot boxes and deliver them to the Returning Officer.

2.5.Pooling officer

Every Presiding Officer is assisted by three to four polling officers. Pooling Officer login to the ballotchain dashboard with given username and password. The Pooling officer receiving the vote may demand that the voter Aadhar identify himself/herself before he or she inserts the ballot in the ballot box.

2.6.Citizen

The Citizen can verify ballots on the blockchain to make sure the validity of the voting process.

3.POLL-SITE INTERNET VOTING

The model of an Aadhaar-linked electronic voting system that would enable electors to cast their votes from any part of the country — irrespective of where they are registered to vote to develop a blockchain system that will allow voters registered in any part of the country to exercise their franchise even after they move cities.

3.1Blockchain integration

Smart contract: The role of smart contract includes 1.) stores the encrypted ballots. 2.) verify the validity of the ballots. 3.) count the encrypted ballot. 4.) verify the correctness of the voting result. 5.) publish the voting result and provide the platform for the voters to verify the voting process.

3.2Voter verification module

This module uses the QR code and fingerprint biometric authentication provided by the Aadhaar card in India.

•DCNN based biometric verification

The individual’s biometric features are captured and compared to previously captured and confirmed biometric features of that individual. All biometric data is first captured by a sensor as an image. This image is then further processed into a biometric template. DCNN Algorithm used for verification and de-duplication are based on comparing these biometric templates.

End core counting

In this module Artificial Intelligence applied to the electoral count using Counting Sort Decision Algorithm. It is the most vital and robust module that has been developed to run on the Election Day for counting of votes, monitoring of end-to-end process and declaration of Results by the System. The Application is designed in a way that the series of work to be done by the Returning Officer in the System will automatically be popped up one after another.

4. RESULT ANNOUNCEMENT

The counting result is announced by the ECI Authority after ending the election. When an election is over, the final result for each smart contract is published.

5. Notification system

The voter receives confirmation from the system that the ballot has been received. Confirmation is preferably sent over a different channel (SMS, for example). The voter checks the receipt/confirmation SMS and VIVL Link and exits the system.

IV.SYSTEM ARCHITECTURE

Smart Contract:

Defining a smart contract includes identifying the roles that are involved in the agreement (the election agreement in our case) and the different components and transactions in the agreement process. The

Blockchain application layer includes smart contracts, chain code, and Ballot Chain. This layer comprises two sub-layers: 1) presentation layer and 2) execution layer. The presentation layer includes scripts, APIs, and user interface. These tools are used to connect the application layer with the blockchain network. The execution layer includes smart contracts, chain code and underlying rules. The presentation layer sends instructions to the execution layer, which runs transactions. For example, instructions are sent to chain code in HF and smart contract in EVM.

Casting a vote:

Voters can need to opt to either vote for one among the candidates or solid a vote. It ensures that the electoral fraud won't happen and therefore the transparency is going to be achieved. While casting, the system ensures that the person is not voted however. If the person has already voted, then the message is going to be displayed because the person is already voted. As an alternative, the person is going to be allowed to vote for his or her desired candidate. Adding the encrypted votes to the Block chain: During this step, once an individual completed his vote, a block is instantiated and in real time hash code is calculated for the corresponding block, hash of the current vote in addition because the hash of the previous block is going to be hold on. This fashion every input is going to be unique and make sure that the encrypted outputs are going to be unique in addition. Block header records all the encrypted data of every vote solid. SHA-256 encrypts all the knowledge associated with each vote, and it's inconceivable to search out the encrypted hash function.After the text edit has been completed, the paper is ready for the template. Duplicate the template file by using the Save As command, and use the naming convention prescribed by your conference for the name of your paper. In this newly created file, highlight all of the contents and import your prepared text file. You are now ready to style your paper; use the scroll down window on the left of the MS Word Formatting toolbar.

Digital Signature

A digital signature (DS) refers to a cryptographic approach to authenticate digital content and guarantee its integrity. DS utilizes a public key cryptography (PKC) system. PKC consists of a public and private key that are paired together but asymmetric (not identical). The public key in the pair is usually shared with the authorized entities and the owner of this key pairs does not disclose the private key. Either of the keys can be applied to encrypt a message; the opposite key that is not employed to encrypt the message from the pairs is utilized to decrypt the message.

Hash

Signing a message with a sender’s private key: To generate a digital signature of a message, the sender’s signing algorithm produces a one-way hash of the message. A cryptographic hash function depicted. The hash algorithm is a one-way function which is practically infeasible to invert. The hash also known as the digest of the message is encrypted with the sender’s private key. The digest along with other information such as the hashing algorithm is appended with the original message as a DS of the transmitted data. Verifying the message with the sender’s public key: The receiver’s signature algorithm verifies the electronic signature associated with the original content in two steps: 1) generating the hash or digest of the message, 2) decrypting the appended digital signature using the sender’s public key. If both digests are identical, the data has not been changed. Otherwise, either the message or signature has been altered or the digest has not been decrypted with the private key of the corresponding public key.

The consensus layers

No centralized body is commissioned to monitor the transaction or prevent attackers from manipulating or altering data when a node exchanges data on the blockchain network. To avoid fraud-related activities such as double-spending attacks, the trustworthiness of the block must be checked, and the data flow should be controlled to ensure the smooth exchange of information. These requirements are met using validation protocols known as consensus algorithms. In the blockchain context, a consensus algorithm is a method of reaching an agreement between multiple insecure nodes on a single data block. Several consensus mechanisms from the literature are described below and presented In Figure 6.7 which shows five categorizations of consensus mechanism: PoW, Proof of Stake (PoS), Byzantine Fault Tolerance (BFT), Proof of Authority (PoA) and Proof of Elapsed Time (PoET).

Attacker module

In this module the attacker performs the Man-in-the-Middle Attacks: Our voting system has strong resistance to this attack. First, as the voters and the smart contract both sign their messages and the voting data is encrypted, it is impossible for an adversary to forge the signature or alter the data on any parties involved in the transactions. Second, the public keys used for signature verification are all published on the blockchain, preventing the adversary from cheating any parties by replacing the original public key with the adversary’s public key. The encryption of the ballot also eliminates the possibility of the ballot leakage.

Denial-of-Service (DoS) Attacks: DoS attack is feasible to launch since the network service is provided in a relatively centralised way. In addition, the servers have relatively limited processing ability for a large number of requests. Distributing the service on different nodes is one of the solutions to DoS attack as it is almost impossible for the adversary to compromise all the servers.

Vote integrity verifier link (VIVL)

The voter can therefore see his vote on the blockchain, verifying that it was counted and counted correctly. Verifiability means that processes exist for election auditing to ensure that it is done correctly. Three separate segments are possible for this purpose: (a) uniform verification or public verification that implies that anybody such as voters, governments, and external auditors can test the election after the declaration of the tally; (b) transparent verifiability against a poll, which is a weaker prerequisite for each voter to verify whether their vote has been taken into account properly.

SELF-TALLYING SYSTEM

The tallying of the election is done on the fly in the smart contracts. Each ballot smart contract does their own tally for their corresponding location in its own storage. The final tally, the sum of all votes, which occurs when the deadline is reached, can then be obtained and verified, by any observer, against the product of all submitted ballots. Which would ensure universal verifiability, due to the homomorphic properties of the encryption method used.

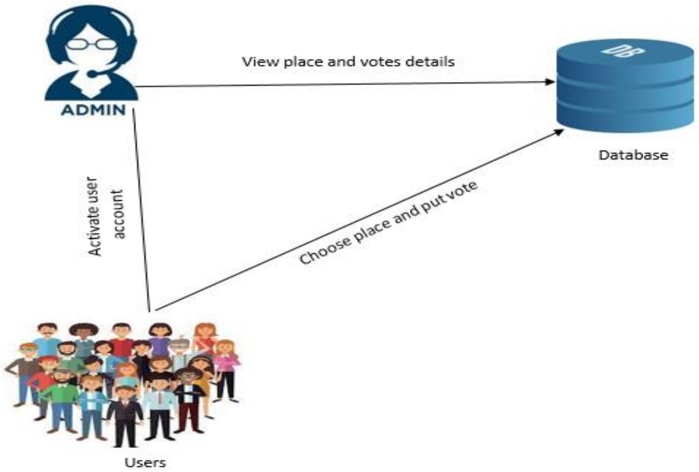

FIGURE1.ARCHITECTURE OF VOTING SYSTEM

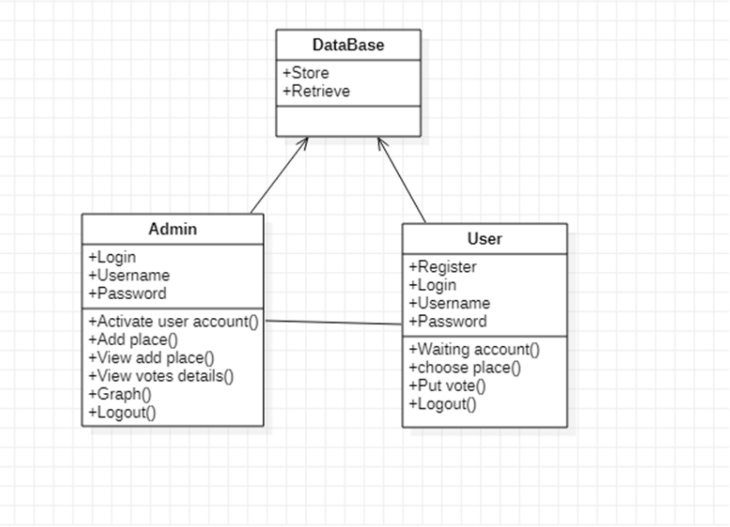

FIGURE2. METHODS OF VOTING SYSTEM.

IV.CONCLUSION

The idea of adapting digital voting systems to make the public electoral process cheaper, faster and easier, is a compelling one in modern society. Making the electoral process cheap and quick, normalizes it in the eyes of the voters, removes a certain power barrier between the voter and the elected official and puts a certain amount of pressure on the elected official. It also opens the door for a more direct form of democracy, allowing voters to express their will on individual bills and propositions. In this project, we introduced a unique, blockchain-based electronic voting system that utilizes smart contracts to enable secure and cost-efficient election while guaranteeing voters privacy. We have outlined the systems architecture, the design, and a security analysis of the system. By comparison to previous work, we have shown that the blockchain technology offers a new possibility for democratic countries to advance from the pen and paper election scheme, to a more cost- and time-efficient election scheme, while increasing the security measures of the today’s scheme and offer new possibilities of transparency. Using a Ballot chain private blockchain, it is possible to send hundreds of transactions per second onto the blockchain, utilizing every aspect of the smart contract to ease the load on the blockchain. For countries of greater size, some measures must be taken to withhold greater throughput of transactions per second, for example the parent & child architecture which reduces the number of transactions stored on the blockchain at a 1:100 ratio without compromising the networks security. Our election scheme allows individual voters to vote at a voting district of their choosing while guaranteeing that each individual voter’s vote is counted from the correct district, which could potentially increase voter turnout.

REFERENCES

[1] S. Shukla, A. N. *asmiya, D. O. Shashank, and H. R. Mamatha, “Online voting application using ethereum blockchain,” in 2018 International Conference on Advances in Computing, Communications and Informatics (ICACCI), pp. 873–880, Bangalore, India, September 2018.

[2] S. Komatineni and G. Lingala, “Secured E-voting system using two-factor biometric authentication,” in Proceedings of the 2020 Fourth International Conference on Computing Methodologies and Communication (ICCMC), pp. 245–248, Iccmc, Erode, India, March 2020.

[3] M. G. Gurubasavanna, S. Ulla Shariff, R. Mamatha, and N. Sathisha, “Multimode authentication basedelectronic voting kiosk using raspberry pi,” in Proceedings of the International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud), I-SMAC, pp. 528–535, Palladam, India., September 2018.

[4] K. Curran, “E-voting on the blockchain,” =e Journal of British Blockchain Association, vol. 1, no. 22–7, 2018.

[5] M. Audi Ghaffari, An E-Voting System Based on Blockchain and Ring Signature, School of Computer Science University of Birmingham, Birmingham, UK, 2017.

[6] Y. Abuidris, A. Hassan, A. Hadabi, and I. Elfadul, “Risks and opportunities of blockchain based on e- voting systems,” in Proceedings of the 2019 16th International Computer Conference on Wavelet Active Media Technology and Information Processing, pp. 365–368, Chengdu, China, December 2019.

[7] K. Curran, ``E-voting on the blockchain," J. Brit. Blockchain Assoc., vol. 1, no. 2, pp. 1-6, Dec. 2018.

[8] M. Shafiq, Z. Tian, A. K. Bashir, X. Du, and M. Guizani, ``IoT malicious traffic identification using wrapper-based feature selection mechanisms," Comput. Secur., vol. 94, Jul. 2020, Art. no. 101863.

[9] X. Yang, X. Yi, S. Nepal, A. Kelarev, and F. Han, ``A secure verifiable ranked choice online voting system based on homomorphic encryption," IEEE Access, vol. 6, pp. 20506-20519, 2018.