TEST Engineering & Management

May-June 2020
ISSN: 0193-4120 Page No. 4294-4298

Electronic Voting System Based on Blockchain Technology

[1]A Aravind, [2]Aditya Agarwal, [3]Ayush Jaiswal, [4]Ayush Panjiyara, [5]Nikhil S Tengli

[1,2,3,4,5]School of Computing and Information Technology, REVA University

Article Info
Volume 83
Page Number: 4294-4298
Publication Issue:
May - June 2020

Article History
Article Received:*19 November 2019*
Revised: *27 January 2020*
Accepted: *24 February 2020*
Publication: *12 May 2020*

Abstract

Conducting a successful election is a great challenge for any country. Initially people preferred traditional voting system where the voter has to cast his or her vote on a ballot paper that is later counted by some government representatives, but this method is not economical as it requires a lot of manpower as well as resources. Then came electronic voting like remote Internet voting and onsite machine voting which are the best way of casting vote in any election till date but as these can be tampered or their hardware or software can be manipulated so there is no 100% guarantee of fair elections. But now the time has changed, and, in this project, we have designed an Electronic voting machine that works on most reliable and secure technology i.e. Blockchain.

Keywords**:** *Blockchain, Ballot Paper, Election, Electronic Voting, Internet Voting, Reliable, Secure*

1. Introduction

Every county in this world has their own government but only in majority of countries people have the right to select their leaders. Voting is the process which provide people a way to select their leader based on majority of votes.

In any nation, leading a secure and safe election is an extraordinary test. Experts in computer security around the globe has considered the potential outcomes of online voting, with an intention to reduce the cost of hosting any election across the nation, while maintaining and enhancing the security for election hosting. As we investigate the past of any democratic country, we will find that election in those days were conducted using pen and paper, which is found to be insecure and vulnerable to frauds. So, to minimize the fraud and to make voting process traceable it become very crucial to replace the traditional pen-paper based voting system to new electronic systems.

Then came Electronic Voting Machine (EVM) which works on IC chips and buttons. In this people have to visit pooling booths verify their identity and cast their vote by pressing respective button. These machines are used to reduce the security issues as well as to decrease the time for getting the accurate and error free results [7].But time has demonstrated that EVMs can be altered and can be controlled i.e. any person who has the physical access to these machines can easily manipulate or even can delete all the votes that are present in the EVMs. Security Community also states that EVMs are most vulnerable to physical access.

Figure 1: Electronic Voting Machine (EVM)

As the technology is advancing things are getting more and more secure and reliable. In this advancing world comes a replacement and prominent technology i.e. Blockchain.

A blockchain, is the continuous chain of records called blocks. Each new block added to the chain contains the cryptographic hash of pervious block, a timestamp and transaction data. [13].

May-June 2020
ISSN: 0193-4120 Page No. 4294-4298

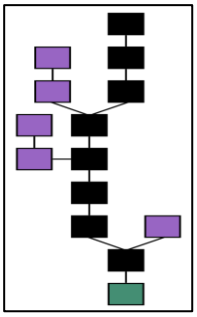

Figure 2: A simple Blockchain

A blockchain is a dispersed, permanent, indisputable, open record. This new innovation works through four fundamental highlights [1]:

1. The records present in any blockchain network exists at multiple location.
2. Control of appending any new transaction to the blockchain network is distributed.
3. Any new block that is added to the network must reference to previous block making it immutable.
4. A transaction must be approved by majority of nodes to be a part of blockchain network.

The above technical features works on advanced cryptography, making it more secure then previous databases [3]. This is the reason why many are considering Blockchain as tool to create new modern democratic process.

2. Problem Statement

From past many years in most of the democratic countries majority of the people are not satisfied with the results of the elections which is the most important process in any democratic country. There is no transparency in the results and there are no such records also which can be verified.

As we look in our own country in past few years a lot of political parties and people are question the machines that are being used for conducting the election as these are not tamper proof and can be easily manipulated. So there is a need for such a system that can have transparency and also is highly secure.

Other problems with current election system is that it is completely static that is a person from some location can not vote for his region if he is outside of region and also the cost of conducting even a simple election is too high.

3. Literature Survey

With the advent of blockchain technology, there have been many studies done on the electoral system for different democratic nations and have been determining more efficient and secure way of hosting any type of election.

"ANALYSIS OF ELECTRONIC VOTING SYSTEM IN VARIOUS COUNTRIES" by **S. Kumar, E. Walia** and **"Electronic voting machine — A review"** by **D, Ashok Kumar & T, UMMAL SARIBA BEGUM** have done rigorous study on the available voting system around the globe and found that none of the government assure secure and safe election as there is no scope of finding whether the voter is authentic or not [7][6][10][11].

According to **"A Study on Decentralized E-Voting System Using Blockchain Technology"** by **H Patil, K Rathi, M Tribhuwan [2]** people in major democratic countries like India, Japan, US do not trust their voting system. Their research also prove that block-chain technology is the best solution which creates transparency in voting and counting process and also make records more and more secure from hackers.

"A Secure Verifiable Ranked Choice Online Voting System Based on Homomorphic Encryption" by **X. Yang, X. Yi, S. Nepal, A. Kelarev and F. Han** have made an attempt to make a system that can collect votes from remote voters using public and private key pair method utilizing ElGamal cryptosystem where the voters will be having a private and public key pair which is used to encrypt the votes casted in ballot. But there is drawback of storage and maintenance of the databases which will be holding the all the public keys as well as the records also there is a possibility of attacks by the hackers who can easily corrupt the records [3].

"A secure e-Government's e-voting system" by **M. H. Sedky and E. M. R. Hamed** have also proposed a system that utilizes the existing electronic voting procedure just using an authentication method to reduce the identity fraud but still utilizing central database to store voter information as well as votes. Anybody having access to the central server can easily manipulate votes as well as the identity of voter even before the start of election [4].

A case study presented in **"Security Analysis of the Estonian Internet Voting System"** by **D. Springall** shows that in the year 2005 Estonian presented a web based electoral system where the voters have to download an application and verify their identity using some election ID or some mobile ID and cast the vote. Various companies performed tests on the system and found that there are various and very serious issues in the code which created a loop hole for the attackers and most prominent attack was Distributed Denial of Service (DDoS) [5].

Various risks that are associated with conducting any sort of transaction on online platform are given by **"Internet-based security incidents and the potential for false alarms"** by **M. P. Evans and S. M. Furnell** according to them integrity and security are two major concerns for conduction on online elections among these two threats most dangerous are identity fraud and DDoS. In identity threat attacker uses a legitimate identity to

May-June 2020
ISSN: 0193-4120 Page No. 4294-4298

gain access to the central server either to create false request or to manipulate the data stored. While in DDoS the server queue is flooded with anonymous packets that are created by the attacker making the server port busy to address these fake packets which lead to not able to serve authentic request.

To resolve the issue of message theft and message legitimacy then came into picture is cryptography. According to **"An Introduction to Cryptography"** by **J. Hoffstein, J. Pipher, and J. H. Silverman [8]**cryptography is the process in which the secret of any message is encoded into some special character known as cipher text by the means of a secret key and this process is known as Encryption. While to get back the secret of that message from the cipher text we have to again utilize the secret key to decode the message and this process is known as Decryption. In cryptography complete encryption and decryption method are known to the user except for the secret key, which means security of the cryptosystem is dependent on the secret key, this is most popularly known as Kerckhoff's principle [9].

Blockchain technology utilizes cryptography to protect the identity of a sender, and also ensure that records are sealed/tamper-proof. Therefore, implementing cryptography into e-voting may ease the privacy for the electronic electoral system.

4. Methodology

E Voting can be done in various ways like using EVMs at polling stations, using remote devices to caste and store vote at a centralized server and many more. The approach presented in this project can be saliently encapsulated as follows:

1. Loading of Smart Contract

- Initially the Election Commission will prepare a candidate list and feed it to the smart contract.
- Then they will deploy this smart contract on a blockchain server and start the voting process on the day of election.

2. Voting Phase

- User will use their credentials to login to the portal.
- Then user will be prompted to enter his or her Aadhar number. An authentication message will be sent to the registered mobile number of the Aadhar card holder.
- On the successful validation of Aadhar details and user, he/she will be taken to the actual voting page where he/she can see the candidate list.
- Then the voter will press the Vote button and cast his/her vote. One voter can cast his or her vote only once i.e. after one-time voting buttons are disabled and the vote is automatically logged out.
- Result Phase
- Once the election is over now voter can login to the portal again to check the results of voting.

Figure 3: Admin Side Architecture

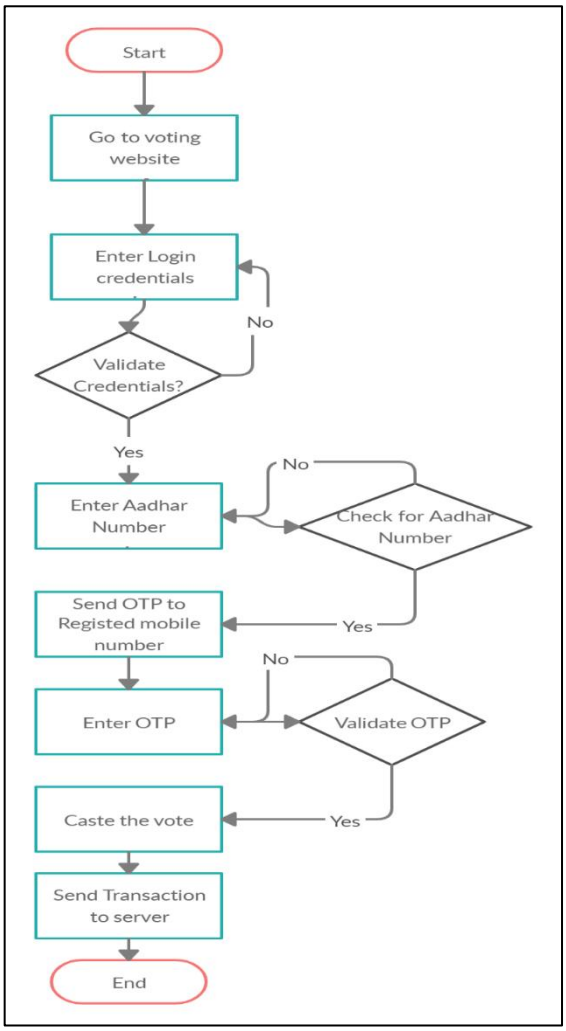

Figure 4: Client/ Voter Side Workflow

5. Results and Discussion

The system incorporates a technique where it helps to conduct a secure and verifiable election from any remote location using the block-chain technology. Block-chain technology is much more secure providing 70-80% security for the data whether it can be the votes that are casted or user data.

As we compare our system with the present system around the globe it can be said that our system is much more secure as the block chain framework will store the

May-June 2020
ISSN: 0193-4120 Page No. 4294-4298

votes collected from the voters in a form of chain in which all the blocks are interlinked to each other so making any change to any of the block will result in the destruction of the chain assuring that it is not easy to manipulate records in this.

Also, it utilizes the Aadhar based OTP verification system thus allowing only the authentic users can only cate their vote that too only one time as it will automatically take the user out of the voter as soon as he/she submit its vote.

As the system is hosted on a server allowing it to be accessed from anywhere but still there is a drawback of booth capturing where the voter chooses his/her leader at the gun point by the attackers.

Here are the screenshots of the project that shows how it works:

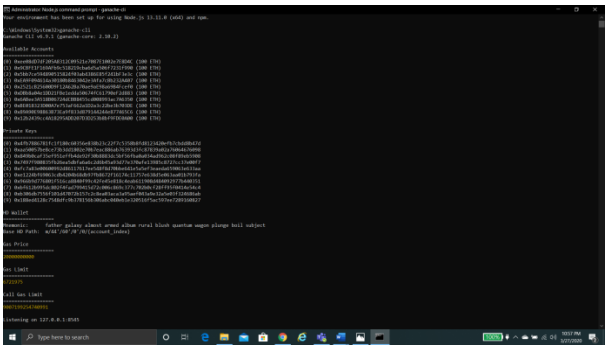

Figure 5: Starting of the server

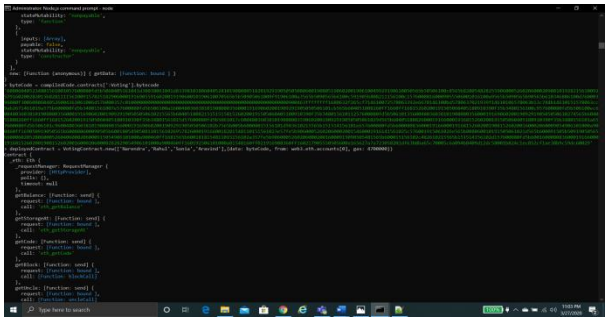

Figure 6: Deploying Smart Contract

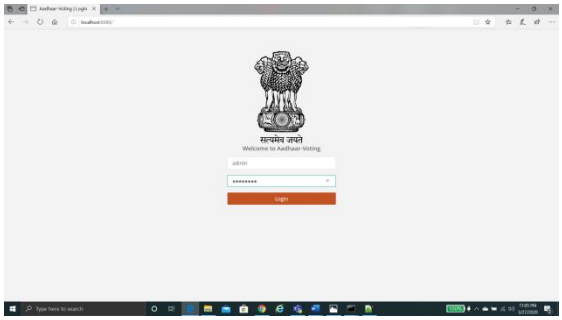

Figure 7: Login Page

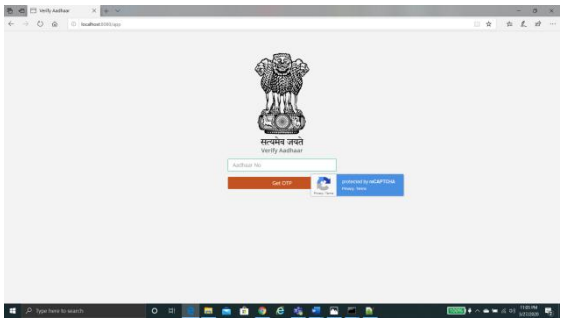

Figure 8: Aadhar Number entering

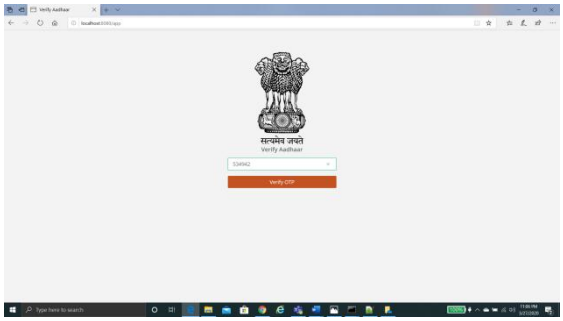

Figure 9: OTP entering

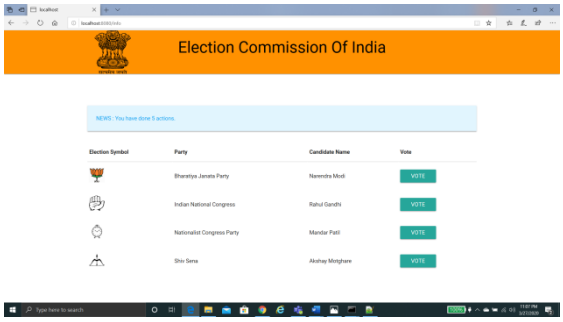

Figure 10: Actual Voting Page

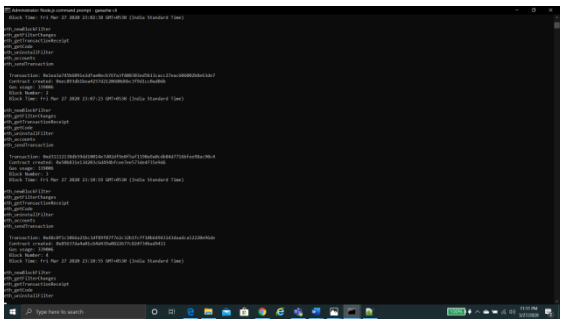

Figure 11: Block Created

6. Conclusion

This project leads us to great shortfall of our election conduction system i.e. tampering of EVMs and no data integrity for the casted votes. So, this project helped us to fix the issue of data security with respect to the votes as we are using Blockchain technology as our base structure

May-June 2020
ISSN: 0193-4120 Page No. 4294-4298

which gives profitable properties to electronic electoral system, for example authenticity, integrity, verifiability and many more. The system doesn't believe on human trust however on computational cryptographic trust. This blockchain-based electronic voting is secure such that nobody can corrupt it.

Also this project helped us to make our voting system remotely available as the current system is limited to particular constituency only but using this voter can easily access its own region candidate list from any polling station.

7. Future Works

- Adding more security feature like capturing live photograph of the voter while voting to avoid booth capturing.
- Use database to store login credentials and constituency details
- Use actual Aadhar database

References

[1] L Pandey, "Blockchain Technology in Voting System", 2020 International Journal of Creative Research Thought (IJCRT), pp 1274-1277.

[2] Mrs. Harsha V. Patil, Mrs. Kanchan G. Rathi, Mrs. MalatiV.Tribhuwan, "A Study on Decentralized E-Voting System Using Blockchain Technology ", International Research Journal of Engineering and Technology (IRJET), vol. 5, pp 48-53, 2018.

[3] X. Yang, X. Yi, S. Nepal, A. Kelarev and F. Han, "A Secure Verifiable Ranked Choice Online Voting System Based on Homomorphic Encryption," in *IEEE Access*, vol. 6, pp. 20506-20519, 2018.

[4] M. H. Sedky and E. M. R. Hamed, "A secure e-Government's e-voting system," *2015 Science and Information Conference (SAI)*, London, 2015, pp. 1365-1373.

[5] D. Springall et al., "Security Analysis of the Estonian Internet Voting System," in Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security - CCS '14, 2014, pp. 703– 715.

[6] D, Ashok Kumar & T, UMMAL SARIBA BEGUM. (2012). "Electronic voting machine — A review". International Conference on Pattern Recognition, Informatics and Medical Engineering, PRIME 2012.41-48.

[7] S. Kumar, E. Walia, "Analysis Of Electronic Voting System In Various Countries" , 2011 3rd International Journal on Computer Science and Engineering (IJCSE), pp. 1825-1830.

[8] Hoffstein, J. Pipher, and J. H. Silverman, "An Introduction to Cryptography", vol. XVI. 2008.

[9] G. Z. Qadah and R. Taha, "Electronic voting systems: Requirements, design, and implementation", Comput. Stand. Interfaces, vol. 29, no. 3, pp. 376–386, 2007.

[10] T. Kohno, A. Stubblefield, A. D. Rubin and D. S. Wallach, "Analysis of an Electronic Voting System", IEEE Symposium on Security and Privacy 2004. IEEE Computer Society Press, May 2004.

[11] Thomos M. Buchsbaum, "E-Voting: International developments and lesson learnt", Technical Report by Australian Federal Ministry for Foreign Affairs, 2004.

[12] M. P. Evans and S. M. Furnell, "Internet-based security incidents and the potential for false alarms," Internet Res., vol. 10, no. 3, pp. 238–245, 2000.

[13] "Blockchain", *Wikipedia*, https://en.wikipedia.org/wiki/Blockchain.