International Journal for Innovative Engineering and Management Research
A Peer Reviewed Open Access International Journal
www.ijiemr.org

ELECTRONIC VOTING SYSTEM

Dr. L. Sridhara Rao
Associate Professor
Department of IT, JBIET
Mail:lsridhararao@gmail.com

P. Sarasawti Devi
Assistant Professor
Department of CSE, KGRCET
Mail:saraswathi_lella@yahoo.co.in

Abstract— In the past years, the voting done in the mode of paper and ballot. The fraud actions were easily taken place when it the voting was done in the mode paper-based voting. During the time of calculation of voting results, there had been lot of tampering with the voting results. The paper-based voting system has faced a lot of issues with the current environment. In today's digital environment, voting has shifted from a paper ballot to a secure digital mechanism. Transparency, decentralisation, irreversibility, and non-repudiation are only a few of the characteristics of a digital electronic voting system. It's been a huge task to create a safe digital-based Automated Election Process. An electronic voting machine is the most promising approach to encourage voters to vote. The Electronic vote cast machine has faced a lot of security threats like DDoS assaults, false votes, vote tampering and manipulation, virus attacks, and other security risks have all been encountered by the system of electronic voting. The recommended system's application of blockchain technology minimises the shortcomings of the existing system and makes the voting process more secure, trustworthy, and transparent. The data in the block chain is stored in blocks and is strongly encrypted, making it hard for a hacker to modify the data chunks. We are able to do so with the help of Blockchain technology, can guarantee the security and protection against any type of fraud and hacking. The issues with the current electronic voting system can also be resolved by using bio-metric and blockchain technology methods.

Keywords—• Decentralization, Electronic Voting

I. INTRODUCTION

In the modern era, organizing the security of an election had been great challenge to the election commission in every democratic country. The election was done in the mode of pen and paper, which was easily rigged. The traditional pen and paper mode was replaced with the electronic voting system. But, the electronic system has been said to be flawed, by the election commission. The e-Voting is considered as inaccurate primarily based on security. People that have physical access to the system and thus vote have a significant probability of influencing it.

To ensure that it is accessible to all voters while simultaneously being protected from outside influences that could alter votes or tamper with a voter's ballot, an E-voting system must have enhanced security. Tor is often used by electronic voting systems to protect the identification of voters. However, considering multiple intelligence services all across world control different regions of the internet, which can allow them to recognize or intercept ballots, this technique does not ensure complete anonymity or integrity. The issues can be easily handled with the use of blockchain - based technology.

A Blockchain is a decentralized electronic record of transactions that is repeated and shared throughout all computers and networks. The main feature of the blockchain that makes it reliable to use in the Electronic Voting system is it containing the Distributed Ledger Technology (DLT) [1]. Properties of DLT are

- A blockchain is programmable.
- All the records are individually encrypted and secure.
- The identity of participants is either anonymous or pseudonymous.
- It is distributed over entire network of systems that all participants have a copy of the ledger for complete transparency
- Immutable – Any validated records are irreversible and cannot be changed
- On a block, a transaction timestamp is recorded.
- The legitimacy of each record is agreed upon by all network participants.

II. LITERATURE REVIEW

Election security has become a matter of national security in every democratic democracy. We can put up a secure voting system by digitizing the election. It can be done using an electronic voting system, which can reduce election costs while simultaneously increasing security [2]. In the beginning of era, the election was done in pen and paper

mode, which has more fraud involved in it. By replacing traditional pen and paper voting with an electronic voting system, fraud can be reduced. It is possible to make the voting process traceable and transparent, as well as to prevent repeated voting [3].

As the voting system is evolved into digitalized mode, there were still a lot of issues faced. The e-voting system has said to been flawed, and there have more attacks toke place with the e-voting system. Any person who has contact with the e-voting machine can tamper the votes. The purpose of evolving from the traditional pen and paper mode to the e-voting system is to bring a new enhancement. The change such as making it eco-friendly, transparent, less error and decentralized. Authentication, accuracy, vulnerability, and consistency are the core characteristics for every electronic voting system [4].

The Electronic voting system proposed has said to be flawed, any person who contact with the can easily tamper the votes casted, and the attacks have been increased from day to day based on increasing technological attacks [5]. Authentication, vulnerability, and accuracy are the basic requirements to any electronic voting system, without authentication a system could can fail from identifying the particular user for whom the access has to be given [6].

Countries began to use online voting; the fundamental criterion for I-voting is the system's privacy, however I-voting has been undermined in recent years [7]. The main attacks on the electronic voting were mostly DDOS attacks, the DDOS attacks were easily attempted on the e-voting system, which has been a main problem to the election commission [8].

To work with a traditional ballot system, an EVM must adhere to all of the same standards as the traditional system, such as security and anonymity. An E-voting system should have enhanced security to ensure that it is available to all voters while also protecting against outside influences that could influence the outcome of votes cast or compromise the security of a voter's ballot. The traditional election using pen and paper and ballot method is still under attack from the functions of security and transparency. Block chain technology is one of the solutions since it improves the decentralized system and allows many people to share a database across all networks in a computer system [9].

The blockchain technology is a crypto currency that is derived from storing data in a distributed database and then storing it in blocks [10]. In 2008, Satoshi Nakamoto debuted the blockchain technology when he invented the first cryptocurrency, Bitcoin, which was based on distributed ledger technology [11].

To design e-voting system based on the block chain technology, first we should understand how the blockchain should work and how it is beneficial to current scenario [12]. The blockchain is a digital asset network that comprises of a constantly growing list of records called blocks that are linked together and secured using encryption. Major usage of Blockchain has been in all cryptocurrency transactions, mainly Bitcoin [13].

The e-voting system still faces a great problem when it comes calculating the election results from various servers where there has been a lot of change by no of voters to the no of votes casted. This raises a higher possibility of manipulation of the election results [14]. Since, there were lot problems faced negative opinions has been raised among the voters and the election commission which need to be solved using new methods and ideologies [15].

Public blockchains allow any user on the network to read and generate transactions, whereas permissioned blockchains contain access restrictions and only allow approved users. In our proposal, we'll use a permissioned blockchain, which is a variant of consortium-based chains and employs the proof-of-authority (POA) consensus process.

We can place limits on a set of selected known entities to validate and certify transactions on the blockchain and filter transactions unilaterally using a permissioned blockchain that uses the POA consensus process, putting their identity and reputation at risk. Otherwise, miners on a public blockchain using the proof-of-work consensus process would have to accomplish it [16].

III. METHODOLOGY

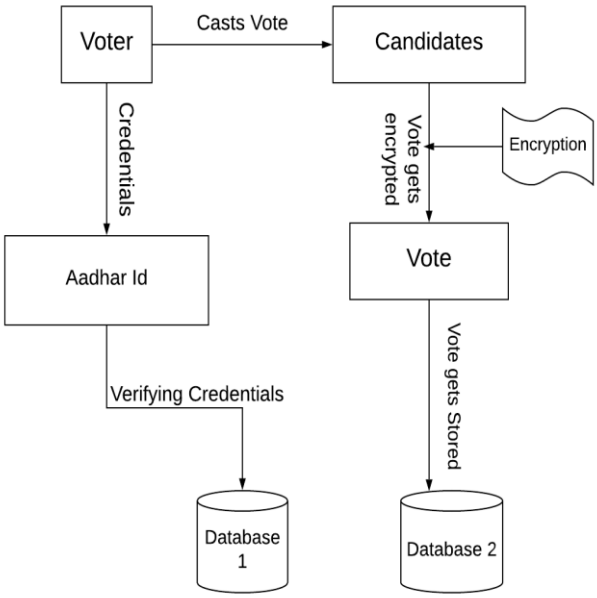

Figure 3.1. Process of voting using Blockchain

As shown in Figure 3.1 the user is authenticated with the bio-metrics (Finger print), the result is stored in the blockchain in blocks of data. A number of encryption techniques are used to encrypt the data of users.

The user must verify whether or not they have a voter id. The user needs to get authenticated with his voter id

International Journal for Innovative Engineering and Management Research
A Peer Reviewed Open Access International Journal
www.ijiemr.org

credentials and fingerprint. The voter id credentials are used to cast a vote under a person's identity and fingerprint is used to make sure whether the user is eligible or not and it can also avoid double voting and other fraud actions. After the user has been validated, he or she can cast a vote by picking a candidate from which to vote. When a user casts a vote, the user's personal information and the vote they cast are encrypted. The encrypted information gets stored in the blockchain. Information is recorded in the blockchain in the form of blocks of data. By this way the user's information can be safe and there cannot be any fraud actions involved.

IV. METHODS

A. *Bio-Metric Analysis*

Biometrics are measurements and calculations of the body that are related to human traits. Biometric authentication (also known as realistic authentication) is a type of identification and access control used in computer science. It's also utilized to track down individuals in groups that are being watched.

Personal identification of voters is a significant consideration when employing e-voting system technology. The challenging goal of biometric recognition is the indisputable identification of voters in real time. Physiological traits such as the face, fingerprints, iris, and retina are used in these procedures.

B. *One-Time Password Authentication*

As the name implies, one-time password (OTP) solutions allow users to log on to a network or service using a unique password that can only be used once. The most frequent and least secure authentication mechanism is the static password.

A one-time password (OTP) is a number or alphanumeric string of characters that is created automatically and used to authenticate a user for a single transaction or login session. A user-created password, especially one that is weak and/or reused across several accounts, is less secure than an OTP.

V. IMPLEMENTATION

To implement a safe and secure application of voting to minimize the threat and attacks that were faced previously. The voter has to register in vote application through mobile number and Aadhar number. After successfully registering, the user has to login to the voting interface page either through bio-metric or Aadhar authentication. Once, the user has logged into the interface he can cast a vote to the candidate that he wish to vote.

A. *PSUEDO CODE*

Admin.java

```
Package com.nvss.votingapp;

import android.content.Intent;
import android.os.Bundle;
import android.view.View;
public class AdminActivity extends AppCompatActivity {
   EditText UserName,Password;
   @Override
   protected void onCreate(Bundle savedInstanceState) {
      super.onCreate(savedInstanceState);
      setContentView(R.layout.activity_admin);
      UserName = findViewById(R.id.username);
Password = findViewById(R.id.password);}
   public void login(View view) {
      if (UserName.getText().toString().trim().equals("admin")
&& Password.getText().toString().trim().equals("admin")){
         Intent intent = new
Intent(AdminActivity.this,AddCandiatesActivity.class);
            startActivity(intent);      } }}
```

V. OUTPUTS

The voter registers to cast a vote to the list of candidates using phone and Aadhar number. After successful registration user login to the interface and cast his vote to his respective candidate as shown in Figure 5.1.

Figure 5.1 Home page

The count of number of votes casted per candidate is visible in the vote cast interface as shown in Figure 5.2. After the completion of voting process, the candidate secured with highest number of votes is declared winning.

Figure 5.2 : Add Candidate page

VI. CONCLUSION

The paper ballot voting system in India has failed to meet the basic needs of the voting system for a clean and trusted voting environment which has caused lot of trouble in the society.

The E-voting system was created to eliminate proximity bottlenecks, unnecessary time delays, and to register votes in a secure and precise manner. To ensure its success, the system has been rigorously evaluated in terms of voting accuracy, ruggedness, responsiveness, battery life expectancy, and security through simulation and small voting sessions.

At all end points, the system can be seen to be fault tolerant (registration, voting platform and the server). The voting device has a battery life of over 6 hours, which is plenty for a fast system like ours. This method will enable unlimited voter participation in remote places at little or no expense to the voter, thereby lowering voter apathy. The mechanism can be improved further to improve the credibility of the votes and to eliminate proximity difficulties.

REFERENCES

[1] Hjálmarsson, Friðrik Þ., Gunnlaugur K. Hreiðarsson, Mohammad Hamdaqa, and Gísli Hjálmtýsson. Blockchain-based e-voting system." In *2018 IEEE 11th International Conference on Cloud Computing (CLOUD)*, pp. 983-986. IEEE, 2018.

[2] Dunn, Michael, and Laurence Merkle. "Overview of Software Security Issues in Direct-Recording Electronic Voting Machines." In *ICCWS 2018 13th International Conference on Cyber Warfare and Security*, p. 182. Academic Conferences and publishing limited, 2018.

[3] Patil, Poonam, and Seema Mane. "Decentralize Electronic Voting System Using Blockchain."

[4] Jones, Douglas W. "Threats to voting systems." In *NIST workshop on threats to voting systems*. 2005.

[5] Jones, Douglas W. "Threats to voting systems." In *NIST workshop on threats to voting systems*. 2005.

[6] Liu, Yi, and Qi Wang. "An E-voting Protocol Based on Blockchain." *IACR Cryptol. ePrint Arch.* 2017 (2017): 1043.

[7] Halderman, J. Alex, Harri Hursti, Jason Kitcat, Margaret MacAlpine, Travis Finkenauer, and Drew Springall. "Security analysis of the Estonian Internet voting system." *Nr. May.* (2014).

[8] Gebhardt Stenerud, Ida Sofie, and Christian Bull. "When reality comes knocking norwegian experiences with verifiable electronic voting." In *5th International Conference on Electronic Voting 2012 (EVOTE2012)*. Gesellschaft für Informatik eV, 2012.

[9] Gupta, Yash G., Amar S. Rajeevan, Govind Mhala, and Bhagyashree Dhakulkar. "Survey On E-Voting using Block Chain Technology." *Software Engineering* 11, no. 1 (2019): 6-11.

[10] Kemmoe, Victor Youdom, William Stone, Jeehyeong Kim, Daeyoung Kim, and Junggab Son. "Recent advances in smart contracts: A technical overview and state of the art." *IEEE Access* 8 (2020): 117782-117801.

[11] Rahman, M. A., KN Abdul Maulud, MA Saiful Bahri, M. S. Hussain, AO Ridzuan Oon, S. Suhatdi, CH Che Hashim, and F. A. Mohd. "Development of GIS Database for Infrastructure Management: Power Distribution Network System." In *IOP Conference Series: Earth and Environmental Science*, vol. 540, no. 1, p. 012067. IOP Publishing, 2020.

[12] Khan, Saad, Aansa Arshad, Gazala Mushtaq, Aqeel Khalique, and Tarek Husein. "Implementation of Decentralized Blockchain E-voting." *EAI Endorsed Transactions on Smart Cities* 4, no. 10 (2020).

[13] Lee, Kibin, Joshua I. James, Tekachew G. Ejeta, and Hyoung J. Kim. "Electronic voting service using block-chain." *Journal of Digital Forensics, Security and Law* 11, no. 2 (2016): 8.

[14] Bisbee, James, and Dan Honig. "Flight to safety: 2020 democratic primary election results and COVID-19." *Covid Economics* 3, no. 10 (2020): 54-84.

[15] Hao, Feng, Shen Wang, Samiran Bag, Rob Procter, Siamak F. Shahandashti, Maryam Mehrnezhad, Ehsan Toreini, Roberto Metere, and Lana YJ Liu. "End-to-End Verifiable E-Voting Trial for Polling Station Voting." *IEEE Security & Privacy* 18, no. 6 (2020): 6-13.

[16] Blog, Ethereum. "On Public and Private Blockchains-Ethereum Blog." (2018).