



TRUSTWORTHY ELECTRONIC VOTING SYSTEM USING BLOCKCHAIN TECHNOLOGY

¹ Afreen Fathima . A, ² Dr. M. Revathi, ³ Dr. S. Uma

¹ PG Scholar, ² Associate Professor, ³ Professor

^{1, 2, 3} Department Computer Science Engineering

^{1, 2, 3} Hindustan college of engineering and technology,

^{1, 2, 3} Coimbatore, TamilNadu, India.

ABSTRACT - Democracy in any country should have a transparent voting system that addresses the people's issues to provide the capacity to the right person. Besides, the current traditional voting systems experience the ill effects of significant disadvantages and missing the absence of security and transparency. I proposed some strategy which recommends a system with the utilization of practicable hashing methods to keep up with information security. Square creation and square fixing helps to make the block chain coordinated. This is prescribed to utilize helpful blockchain, and that implies that an administrating entity possesses the block chain (e.g., political decision commission), so subsequently no unapproved access might be made from outside. The structure proposed examines the viability of the polling process, hashing algorithms' utility, block creation and sealing, data accumulation, and result statement by utilizing the adjustable blockchain method.

Keywords: [Block chain, Vote Identification Token, Cryptographic algorithm, Image comparison and QR-Code.]

1. INTRODUCTION

Electronic Voting is the standard method for directing elections utilizing Electronic Voting Machines, at times called "EVMs" in India. The utilization of EVMs and electronic voting was created and tried by the state- possessed Electronics Corporation of India and Bharat Electronics during the 1990s. They were presented in Indian elections somewhere in the range of 1998 and 2001, in a staged way.

Preceding the presentation of electronic voting, India utilized paper ballots and manual counting. The paper ballots method was generally reprimanded as a result of deceitful voting and stall catching, where party supporters caught corners and stuffed them with pre-filled counterfeit ballots. The printed paper ballots were additionally more costly, requiring significant post-voting assets to count a huge number of individual ballots. Implanted EVM highlights, for example, "electronically restricting the pace of projecting votes to five every moment", security "lock- close" highlight, an electronic database of "voting marks and thumb impressions" to affirm the identity of the citizen,

leading elections in stages north of half a month while sending broad security personnel at every corner have decreased electing extortion and misuse, wipe out stall catching and make more serious and more pleasant elections. The system proposed talks about the viability of the polling process, utilizing hashing algorithms' utility, block creation and sealing, data accumulation, and result announcement by utilizing the adjustable blockchain method.

2. LITERATURE SURVEY

This system gives security between the voter and the agents, which are disseminated all around the hubs that ensure that the data isn't changed. The current system depends on utilizing a non-remote and managed electronic voting system which utilizing the Internet association with transmit votes and store them in a block-chain.

The system comprises three main comments:

1. Super-node.
2. Trusted nodes.
3. Polling stations.

Every one of these components plays out a particular work and connected utilizing a peer-to-peer network. The super-node is considered as the principal node, where all votes are transmitted to it and stored in the chain. The believed nodes are considered as reinforcement chains on account of harm or issues informers in the super- node and liable for gathering the votes and lay out the right chain utilizing the consensus algorithm.

The polling stations are viewed as voting applications addressing the singular voting locale. They permit voters to project their votes.

The current system is parted into three phases along the three components which are:

1. The phase of initiation.
2. The phase of voting.
3. The phase of counting and verification.

The main phase is utilized to set up the equipment and programming apparatuses to be utilized to verify and authorized the authorities, separate electing districts, and utilization of VIT (Vote Identification Token) numbers to recognize and approve the votes. The second phase where every voter validates in his polling station then, at that point,

the voter arbitrarily picks the envelope containing the VIT number.

At long last, the polling station and enters the VIT for authorization. In the event that the authorization is permitted, the voter can cast a ballot and afterward this is added to the block-chain. To affirm the process a printout called VVPAT (Voter-Verified Paper Audit Trail) is created which fills in as an extra protect for voting. The third phase shows when the political race time is finished, here comes the counting and the verifying of the voting process. The votes are counted from the super-node chain and trusted nodes. Then, at that point, the results are contrasted with approve.

3. PROPOSED METHOD

In the proposed system, the arrangement is to carry out web based voting system with three level security, Aadhaar card, photo comparison and QR-Code. Candidate details and voting details are stored in secure format utilizing cryptographic algorithm. Just through website the data's should be visible decrypted format. Client can enlist utilizing aadhaar card number, photo transferring. While client login website client's needs to enter the aadhaar card number, secret phrase to it, when verified then QR-Code is produced with arbitrary key.

Client needs to transfer the photo for comparison and QR-code for confirmation reason. When every one of the stages is successful, then client can login the voter structure, showing the candidate details related information's. In the mean time in the block chain hash code is produced with exchange id. Block chain observing is checked by the administrator as it were. All the voting related exchange is stored in the cryptographic format. Voting should be possible on the specific day as it were. Voter can cast a ballot just a single time. We execute Cryptographic techniques, Block chain and security in this venture. Result and voting percentage can be uncovered in this website.

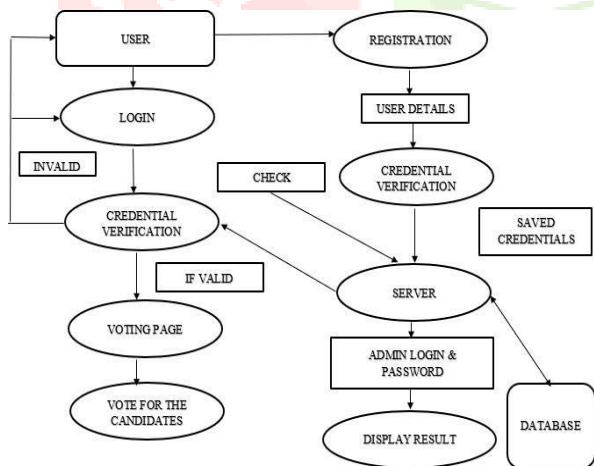


FIGURE 1- BLOCK DIAGRAM

Following are the Algorithm/ technique used in implementing the system:

A. AES ENCRYPTION ALGORITHM:

AES is an iterative rather than Feistel cipher. It depends on two normal techniques to encrypt and decrypt data known's as substitution and permutation network (SPN). SPN is a number of mathematical operations that are completed in block cipher algorithms.

AES can manage 128 bits (16 bytes) as a fixed plaintext block size. These 16 bytes are addressed in 4x4 matrix and AES works on a matrix of bytes. What's more, one more significant component in AES is number of rounds. The number of rounds is depended on the length of key. There are three different key sizes are utilized by AES algorithm to encrypt and decrypt data, for example, (128, 192 or 256 bits). The key sizes choose to the number of rounds, for example, AES involves 10 rounds for 128-bit keys, 12 rounds for 192-bit keys and 14 rounds for 256-bit keys.

Encryption is a famous strategy that assumes a significant part to shield data from gatecrashers. AES algorithm utilizes a specific construction to encrypt data to give the best security. To do that it depends on a number of rounds and inside each round include four sub-processes. Each round comprises of the accompanying four stages to encrypt 128 bit block

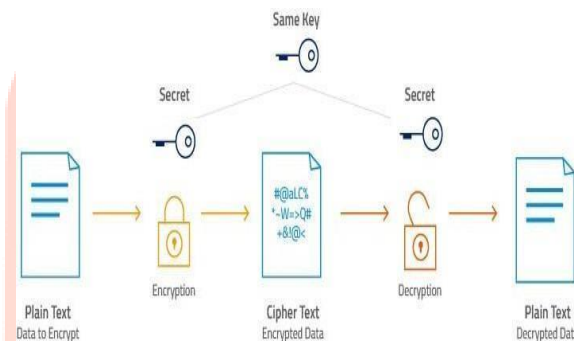


FIGURE 2- ENCRYPTION PROCESS

B. IMAGE COMPARISON:

Here comparison is finished for the two given images (should be of same dimensions) and print the percentage of contrast between them.

1. Check assuming that dimensions of both the image match
2. Get the RGB values of the two images.
3. Calculate the distinction in two comparing pixel of three color parts.
4. Calculate the percentage by partitioning the amount of contrasts with: Number of pixels, to acquire the typical distinction per pixel

C. BLOCKCHAIN TECHNIQUE:

A blockchain is a digitized, decentralized, distributed public ledger that goes about as a common and synchronized database that records crypto currency exchanges. While blockchains are basically decentralized databases, there is no essential responsibility for data. Once conceded consent, verified clients get close enough to block chain systems. This permits them to impart pertinent data to other verified clients, ensuring accountability, scalability, and efficiency. Since blockchains don't need successive investigating, updates, or outsider contribution in funding, it is anticipated that carrying out blockchain advancements in E-Voting might diminish costs. The idea of a public distributed ledger likewise intends that while block chains could be utilized for a type of

confirmation and data access, the E-Voting data wouldn't be reasonable for stockpiling on a public ledger because of privacy suggestions. These contemplations encompass the application and compromises in execution and require further exploration and likely norms for their utilization.

4. RESULTS AND SUMMARY

The results of proposed system are shown as follows: Figure 1. In the Home module, displays all the tabs related to the application, where the user can navigate to particular tabs such as Voter login, Admin Login, User registration, About us etc.

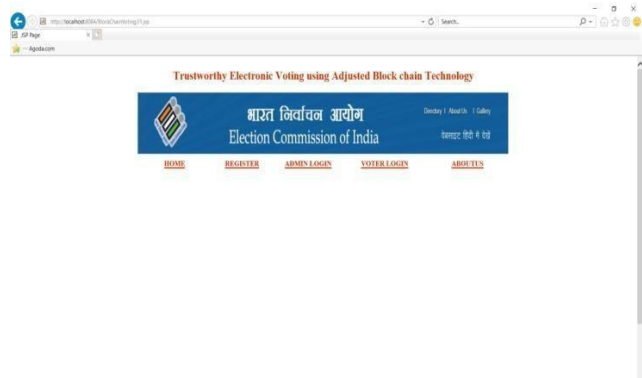


Figure 3. Homepage Module

figure 3. Administrator Module comprises of a login name and one of a kind password utilizing which administrator can login into the internet based E-Voting system. Administrator has the primary control of the system. By signing into the page it can play out the accompanying assignments.

1. ADD CONSTITUENCY
2. VOTERS LIST
3. CANDIDATE LIST

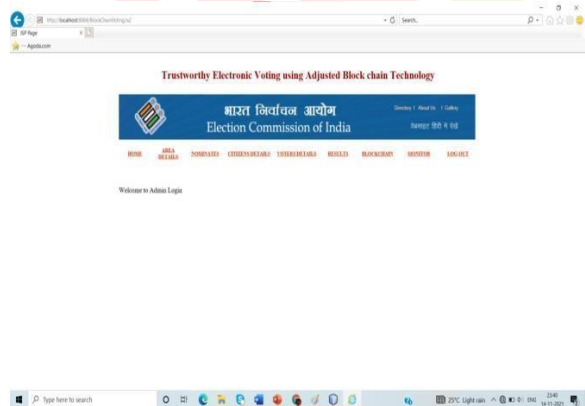
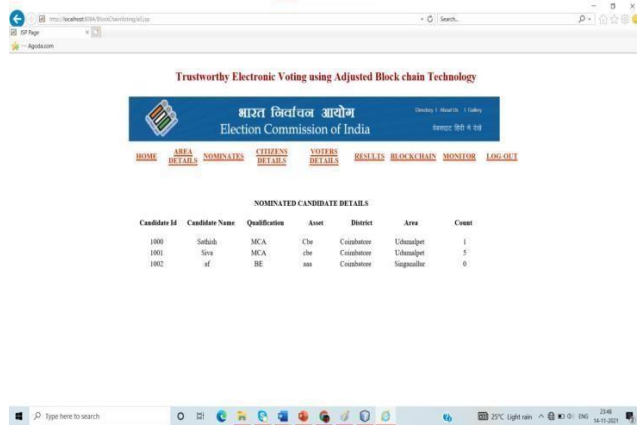


Figure 4. Administrator Module

figure 4. Counting and Categorization of Results Module displays the Result that can be viewed by everyone who visits into the site without any authentication problem. A connection to see the result is kept in the file page and both administrator and voter can see the result in their particular homepages.



Counting and Categorization of Results Module

figure 5. In the Blockchain Module, block chain is implemented for all login form, Vote information, and for Candidate information. The time stamp, hashblock and block chain is implemented for all the histories

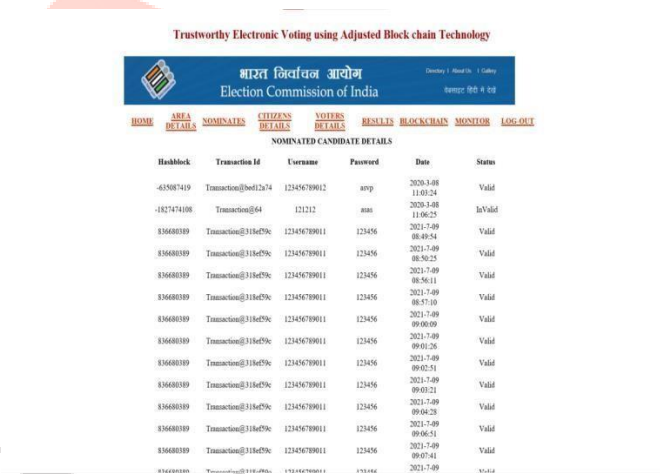


Figure 6. Blockchain Module CONCLUSION

By doing this project there by bringing a new system for online E-Voting for our country and with the advent of technology and Internet in our day to day life, were able to offer advanced E-Voting system to voters both in the country and outside through our online E-Voting system.

Top 4 Reasons to Move to the Online E-Voting Platform

1. Efficient and Cost Effective: The system offers massive cost benefits over paper elections in a vote to cast a ballot comparison. It saves an association the cost of making, printing and postage, since everything can be dealt with electronically. Online elections diminish the utilization of paper and how much work for both the association, as well as voters.
2. Intelligent: The Online E-Voting Platform offers intelligent ballots, savvy agenda highlights, vote tallying, tabulation and reporting. These functions are automatic and needn't bother with to be appointed to personnel in-house. Also, it does not permit administrators to make rules on ballots with the goal that voters can't project invalid votes, nor do they should checked while count.
3. Easy and convenient: The Online E-Voting Platform offers the least demanding and most convenient method for

administrators and voters the same. For administrators, the process of setting up a polling form and it is straightforward and reasonable to direct a political race.

REFERENCES

- [1]. S. M. H. Bamakan, A. Motavali and A. B. Bondarti, "A survey of blockchain consensus algorithms performance evaluation criteria", *Expert Systems with Applications*, vol. 154, pp. 113385, Sep. 2020.
- [2]. RumeysaBulut, AlperenKantarci, Safa Keskin and Serif Bahtiyar, "Blockchain-Based Electronic Voting System for Elections in Turkey", the 4th International Conference on Computer Science and Engineering (UBMK), 2019.
- [3]. Kriti Patidar and Swapnil Jain, "Decentralized E-Voting Portal Using Blockchain", 2019 10th International Conference on Computing Communication and Networking Technologies (ICCCNT), 2019, July.
- [4]. Ashish Singh and Kakali Chatterjee, "SecEVS: Secure Electronic Voting System Using Blockchain Technology", the International Conference on Computing Power and Communication Technologies (GUCON), 2019, September.
- [5]. Mohammad Qataweh, WesamAlmobaideen and OriebAbuAlghanam, "Challenges of Blockchain Technology in Context Internet of Things: A Survey", *International Journal of Computer Applications*, vol. 175, no. 16, 2020.
- [6]. S. Uma, R. Maheshwari, J. K. Mayuri, R. Sowndharya, S. Vano Jenifa, "Design of a Secure Block Chain based E-Voting System", *International Journal of Research in Engineering, Science and Management*, Vol.2, Issue-3, pp. 777-780, March 2019. ISSN (Online): 2581-5792.
- [7]. V. Suruthikeerthana and Dr. S.Uma, "An Extended Visual Cryptography With Dynamically Authenticated Error Avoidance Scheme For Bank Applications", *International Journal of Research in Computer Applications and Robotics*, Volume 4, Issue 4, April 2016, pp.15-23, ISSN: 2320-7345

