Voting System for Handicapped People using Blockchain System

Aishwarya Gade[1], Vaishnavi Pawar[2], Safiya Shaikh[3], Samiksha Mali[4], Prof. Mrs. S. P. Kakade[5]

Students, Department of Computer Science & Engineering[1,2,3,4]

Assistant Professor, Department of Computer Science & Engineering[5]

Dr. Daulatrao Aher College of Engineering, Karad, Maharashtra, India

Abstract: *Blockchain technology enable a never-ending supply of distributed economy- related applications. The proposed model is an Android app with additional security features such as authentication and encryption. The system uses a unique identity key for authentication, and iris is used for authorization. The security of this project is ensured by the use of a 128-bit AES encryption technique, SHA-256, and blockchain. A blockchain is created to keep track of the overall number of votes cast, and the vote is cast as a transaction. Atomically and structural integrity is maintained as a result of this. Using iris recognition, a new and secure voting method is being developed. Iris is one of the most secure biometrics for determining a person'sidentity. This article's main objective is to.*

Keywords: SHA (Secure Hash Algorithm), AES (Advanced Encryption Standard).

I. INTRODUCTION

It is time for physically disabled people to participate in elections independently. Voting on the blockchain will be an encrypted piece of data that is fully open and publicly stored on a distributed blockchain network rather than a single server. The blockchain voting system is decentralized and wide open, yet it ensures that voters are protected. Using a blockchain system voting process can be made more secure, transparent, immutable, andreliable.

Blockchain is a shared, trusted, public ledger of transactions that everyone can inspect but that no single user controls. It is a distributed database transaction data records, cryptographically secured from tampering and revision. The ledger is created using a linked list, or chain of blocks, where each block contains a certain number of transactions that have been verified by the network in agiven timespan.

Blockchain is an emerging technology platform for developing decentralized applications and data storage, over and beyond its role as the technology underlying the cryptocurrencies. Blockchain is the underlying technology that many cryptocurrencies like Bitcoin and Ethereum operate on, its way is unique but securely recording and transferring information has broader applications outside of cryptocurrency transactions cannot be deleted or edited, thereby creating animmutable audit trail. Only adjustments are possible to a transaction by adding another transaction to the chain. They are not fully secure since it is easy to attack votes. It also threatens privacy and transparency. Additionally, it takes too much time to countthe votes. Today, there is a viable solution to overcome the risks and electronic voting, which is blockchain technology. If the technology is likely correctly, the blockchain is a digital, decentralized, encrypted, transparent ledger that can withstand manipulation and fraud. Because of the distributed structure of the blockchain, an electronic voting system reduces the risks involved with electronic voting and allows for a tamper-proof for voting system. A blockchain-based electronic voting system requires a wholly distributed voting infrastructure.

II. LITERATURE SURVEY

2021 IEEE International Conference on Information Technology E-Voting System Based on Blockchain Technology: A Survey (ICIT) Mohammad Qatawneh, Abdullah Quzmar University of Jordan, Amman, Jordan. Sarah Al-Maaitah, Mohammad Qatawneh, Abdullah Quzmar University of Jordan, Amman, Jordan. This survey paper discusses the possible opportunity forapplying BC technology in e-voting systems to improve the process of voting by tackling the issuesof trust lessness, privacy, and security. This paper aims to evaluate different applications of blockchain as a service to implement distributed electronic voting systems. Some of them have been only a draft paper; others are implemented in

DOI 10.48175/IJARSCT-5736

the real world. A blockchain- based e-voting application improves security, and privacy and decreases the cost, evenmore, which can be consummate.

Blockchain for Electronic Voting System—Review and Open Research Challenges Uzma Jafar*, Mohd Juzaiddin Ab Aziz and Zarina Shukur Faculty of Information Science and Technology, The National University of Malaysia, Bangi 43600, Malaysia; MDPI Journal July 2021. The purpose of this investigation is to analyze and evaluate current research on blockchain-based electronic voting systems. The article discusses recent electronic voting research using blockchain technology. The blockchainconcept and its uses are presented first, followed by existing electronic voting systems. Then a set of deficiencies in existing electronic voting systems are identified and addressed. The blockchain's potential is fundamental to enhancing electronic voting, current solutions for blockchain-basedelectronic voting, and possible research paths on blockchain-based electronic voting systems.

Accessible Voting Systems for Visually Impairments Ruba Ghazi Alzamel and Randa Ali Obeidallah - Computer Information System Department, The Hashemite University, International Journal of u- and e-Service, Science and Technology 2016

III. EXISTING SYSTEM

The Existing System of Election is running manually. The elector has to Visit Booths to Vote for a Candidate so there is a waste of time. The elector has to manually register into the Voter List. Also, Vote counting has to be done manually. All the information about the elector or candidate must be filled in manually. The elector must be present in his/her Constituency to give his/her Vote. There are Electronic Voting Machines used which Takes More Cost. The government's prior voting system was a paper-based one in which voters could readily pick up ballot sheets from electoral authorities, tick off who they would like to vote for, and then cast their votes by merely handing over the ballot sheet back to the electoral official. Some of the existing systems are:

1. Paper-based voting
2. Direct record
3. Punch card

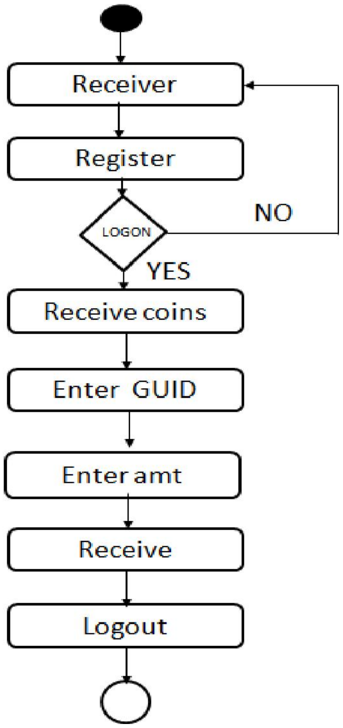
IV. PROBLEM STATEMENT

The traditional voting system does not take into account the physically disabled people's participation in elections and does not focus on issues and obstacles that face them during casting their vote. However, electronic voting carries significant risks such as if an electronic voting system is compromised, all castvotes can probably be manipulated and misused. They are not fully secure since it is easy to attack voters. Today, there is a viable solution to overcome the risks and electronic voting, which is blockchain technology with Iris Based Authentication.

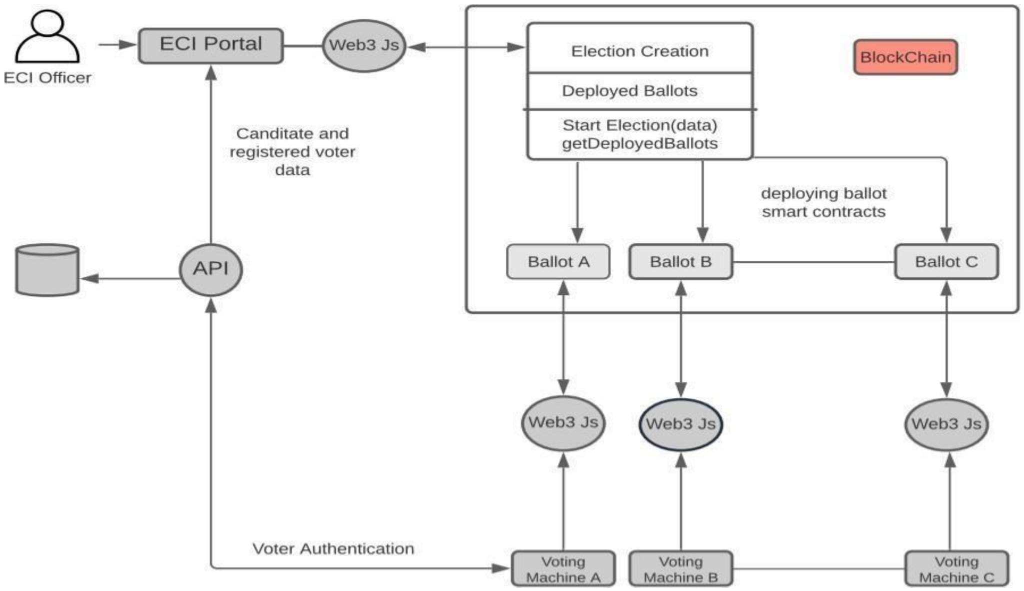
V. PROPOSED SYSTEM

This Online Voting System will manage the voter's information by which the voter can log in and use his voting rights. There is a database that is preserved by the election commission of India in which complete data of voters with the real data is stored. At the time of registration, the voter will be asked for full name, age, iris recognition, and verified details by the administrator. During this period, requesting a vote, the more elect will be asked to recognize his/her iris. Then elector will be authenticated, and he can give a vote for one of the candidates from the list.

VI. FLOW CHART



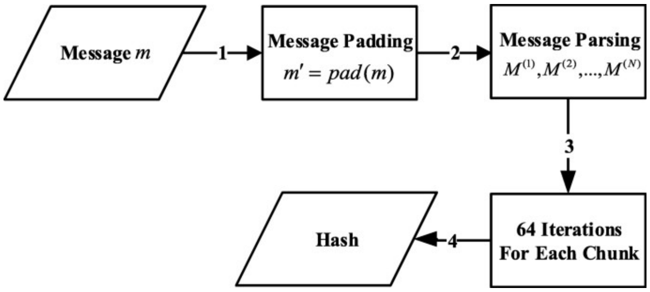
VII. ACTIVITY



VIII. MODULES AND WORKING

1. Election module
2. Iris Authentication Module
3. Cast Vote Module
4. Blockchain in platform Module

DOI 10.48175/IJARSCT-5736



Election Module

This module is available for Election Admin which performs the following activities.

- Maintains various masters required for voting such as Election details, Region Details, Parties details, candidate details, voter details, etc.
- See Election Results in different forms
- Set Current Election for Voting

IRIS Authentication Module

The iris recognition process is complete in the following way:

- Hough Transformation
- Dorman's Rubber Sheet Model
- Data Conversion (Raw data obtained from above b steps converted to binary)
- Hamming Distance (If the bit shifting is 0, i.e., Hamming distance is 0, it is a perfect match. Ifit is 0.5 or more then the two strings are different.)

Cast Vote Module

It provides UI to cast votes to voters where the elector will vote based on iris authentication, the elector can choose their preferred candidate to cast their elector. Once voted, cannot revote again.

Blockchain in Platform Module

The ballot is signed with the private key once it has been voted on, and if it is found to be valid, it is sealed (mined). The preceding ballot is contained in one block in this section. Then transactions (ballots) will be generated based on the valid data. Following that, they're enclosed in blocks. Any attempt to tamper with the records will render them void. Blocks will store the voter's votes in the form of transactions on a ledge.

IX. ALGORITHM

Compute the hash value based on SHA-256

We compute the hash value based on SHA-256 by comparing the hash value to an expected hash value, it is possible to determine the data's integrity. SHA-256 is a popular hashing algorithm e-voting scheme for computing the hash value, which can be discovered in.

1. Compute the hash value based on SHA-256
2. The message is denoted by m with binary expression.
3. Pad m with 100...000 sequence and the length of m with 64-bit expression, i.e., m'=pad(m).
4. m' is broken into 512-bit chunks, i.e., $M^{(1)}$, $M^{(2)}$,..., $M^{(N)}$.
5. There is a total of 64 constants, denoted by *the letters* W0, W1,..., and W63
6. Eight working variables labeled A=0*x*6*A*09*E*667, B=0*xBB*67*AE*85, C=0*x*3*C*6*E* *F*372, D=0*xA*54*FF*53*A*, E=0*x*510*E*527*F*, F=0*x*9*B*056 88*C*, G=0*x*1*F*83*D*9*AB*, and H=0*x*5*BE*0*CD*19 are used as the initial hash value.

7. Compute the 64-cycle cryptographic iterative computation for the first chunk, i.e., $M^{(1)}$. Based on the outcome of the previous piece, for the next section, repeat the iterative computation.
8. The result of the last iterative computation is the hash.

Mining and Generation of Voting Blocks

All votes in the blockchain are cryptographically linked block by block. Many safe hash algorithms, like SHA-256, can be used to address the challenge of condensing the message in the current block into a message digest.

A fresh block is created by users on the peer-to-peer network. The new blocks are created using the POW approach. When a new vote is submitted and authenticated, the miner creates a new block containing the vote's information and broadcasts it to the network. If two blocks with the same timestamp have the same signature, the block with the higher signature wins. The value is given precedence over the others.

X. APPLICATION

Currently, we are going to implement a handicap voting system using blockchain for a safe and anyone voting-based policy. But it is equally applicable for the following domains with few changes-

- Public and private sectors for elections
- Schools and Colleges for elections

XI. CONCLUSION

Implementation of the secure voting process using blockchain platform and Iris-based authentication

REFERENCES

[1]. Accessible Voting Systems for People with Visual Impairments Science and Technology 2016, International Journal of u- and e-Service. Hashemite University's Computer Information

[2]. System Department is led by Ruba Ghazi Alzamel and Randa Ali Obeidallah.

[3]. R. Youmaran, Algorithms to process and measure biometric information content in the low-quality face and iris images. University of Ottawa 2011.

[4]. "A Novel Approach for Iris Recognition," by M. M. Khaladkar and S. R. Ganorkar, vol. 1, no. 4, 2012.