SAFEGUARDING ONLINE VOTING WITH BLOCKCHAIN TECHNOLOGY

D. Naga Swetha
Assistant Professor Department of Computer Science and Engineering G.Narayanamma Institute of Technology and Science (for Women)
Telangana, India.
swetha@gnits.ac.in

Abstract:

India is the biggest democracy in the world with some million voters and five hundred and above constituencies in the House. India has over one billion people and India. Vote is a conduit of parliament and government. The technology used in the voting process has been reinvigorated in recent years. The new voting system has several safety gaps, and it is hard even to prove simple safety features. A vote system contains multiple questions which can be shown to be right. There are grounds for an electronic machine government to maximize voting participation and reduce election expenditure. Electronic voting devices are still running in any respect and it is impossible to authentically recognize the voter or to protect an electronic voting machine from wrongdoers by using an electronic voting unit. The proposed architecture could build a compliant high-security voting system using blockchain technologies to improve privacy and transparency for users.

Keywords: Electronic Voting System, Voter ID, Security, Block Chain, Vote.

I. INTRODUCTION

Modern societies are based on elections, whether in ballet or electronic voting (e-voting). The apathy of voters, particularly among the younger computer and technology generations, has increased in recent years. E-voting is being promoted to draw young people as a future alternative. A range of practical and security demands, including transparency, precision, auditability, systems, and data integrity, confidentiality, availability, and authority delivery, are defined for a robust electronic voting system. A distributed network composed of several interconnected nodes is supported by block chain technology. Each node has its own copy of the distributed directory containing the whole history of all transactions processed by the network. The network is not regulated by a single authority. They approve the contract if the majority of nodes consent. Users will stay anonymous with this network. A fundamental study of the block-chain technologies shows that e-voting should be done on an appropriate basis and, in addition, e-voting can be acceptable and more efficient.

II. RELATED WORK

A steady voting method with quick votes was proposed in this paper[1] via an RFID-based system of biometric vote. This manual contains two authentication measures. First of all the verification data in LPC 2148 is contained by an RFID tag. The second is to check, with a fingerprint scanner, whether or not RFID belongs to the user. The drawback of this paper is maximised on the basis of the RFID protocol.

This document uses the Aadhaar card issued with UIDAI QR code[2]. Instead of an offline mode online and store voting data on a stable server. The findings will be seen by the admin after you have entered your user id and password. This method [3] is an intelligent voting technology, enabling all INDIA voters, from their nearest voting stations, to cast a vote from anywhere on INDIA. The procedure is a technology for identifying fingerprints. Building a secure, intelligent voting infrastructure focused on biometrics. Provisions a secure voting process for voters from all areas of India from the nearest polling station without neglecting to vote for the suburban constituencies.

This paper[4] proposes a protected voting system that prohibits fraudulent voting. Biometrics are used to authenticate an individual and to validate the skill of the elector. The details found in the adhaar card are the main

criteria for authentication and conformation. Protection is provided by biometrics, such as fingerprint. As a guide, the data stored in the Aadhaar fingerprint is authenticated in vote time. The standard machine[5] now used is automatically checked with delays, such as multiple ballot castings by a single member and voting invalidity. The intelligent and fingerprints are automatically analysed to eliminate these disadvantages by casting a mere number of votes.

The feasibilities of a publicly available crypto-system E-Voting Protocol were seen in this paper [6]. The security of the proposed e-voting is based on the public encryption RSA protocol. It allows the voter to vote on a mobile computer without any extra costs and commitments (PC). This is implemented to replace the previously inefficient electoral system, since voters are guaranteed to count their ballots.

This system[7] provides some form of defence from threats, because polling from voting customers to voting servers takes place. The attacks include passive as well as active safety risks for intruders. When we use the logo or image of the elector's face to match photos stored in our files, it's better to authenticate electors rather than USERNAME. This paper uses a block-chain voting system[8]. It takes time to popularise block chains in a voting system because it is a new idea, and voting for yourself is a critical question in a democratic environment. The proposed model [9] is secure than other models and can be used in major elections on a wide scale. Once the NCVVS system has been voted on, a confirmatory feder print email will be sent to voters that is established by the standard SHA feature (including referendum fingerprint) (256). The suggested work [10] is based on an architecture for block chains which eliminates all risks from communication. It is a decentralised architecture that includes a hacking and encryption security concept

III. Existing Approach

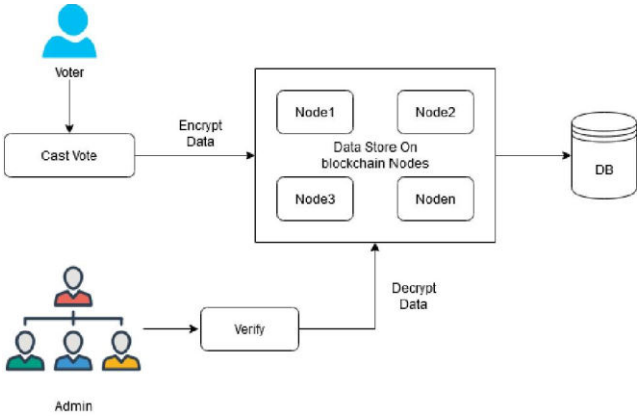
A lot of work has been done in this field thanks to its extensive use and applications. This section mentions some of the approaches that have been implemented to achieve the same purpose. These works are mainly differentiated from the algorithm for E-voting systems.

The existing machine had security risks that can potentially undermine the election process. In addition to human error; internet e-voting is susceptible to a range of threats such as hacking by domestic and foreign saboteurs, technical glitches, voter impersonation and even system failure.

IV. Proposed Approach

Our online voting system is supported by Block Chain Principles in the creation of a smart e-voting system by using web interface block chain concepts. Blockchain. Like a global ledger or simple database of all transactions, the entire history of all transactions on the network. Ethereum Virtual Machine. So you can write more powerful programs than on top of Bitcoin. It refers to the blockchain, what executes smart contracts, everything. Node. Using this to mean you can run a node and through it read and write to the Ethereum blockchain, i.e., use the Ethereum Virtual Machine. A full node has to download the entire blockchain. Light nodes are possible but in the works.

V. System Architecture



VI. ALGORITHM

6.1 AES Algorithm for Encryption

AES (advanced encryption standard).It is symmetric algorithm. It used to convert plain text into cipher text .The need for coming with this algo is weakness in DES. The 56 bit key of des is no longer safe against attacks based on exhaustive key searches and 64-bit block also consider asweak.AES was to be used128-bit block with128-bit keys. Rijendeal was founder. In this drop we are using it to encrypt the data owner file.

Input:

128_bit /192 bit/256 bit input (0, 1)
Secret key (128_bit) +plain text (128_bit).

Process:

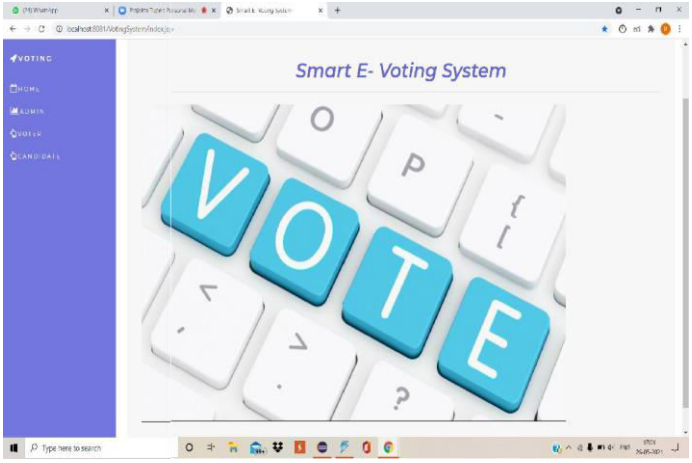
10/12/14-rounds for-128_bit /192 bit/256 bit input
Xor state block (i/p)
Final round:10,12,14
Each round consists: sub byte, shift byte, mix columns, add round key.

Output:

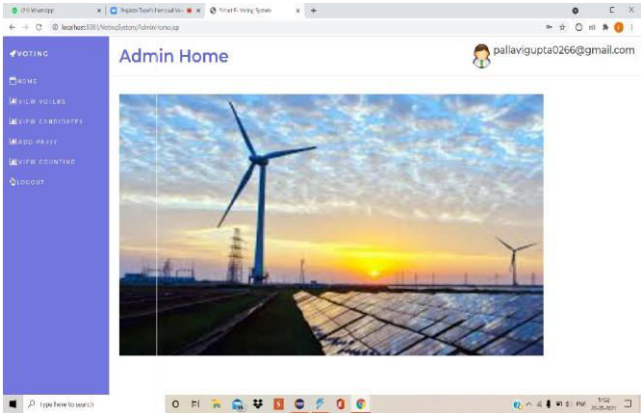
cipher text(128 bit)

VII. RESULTS

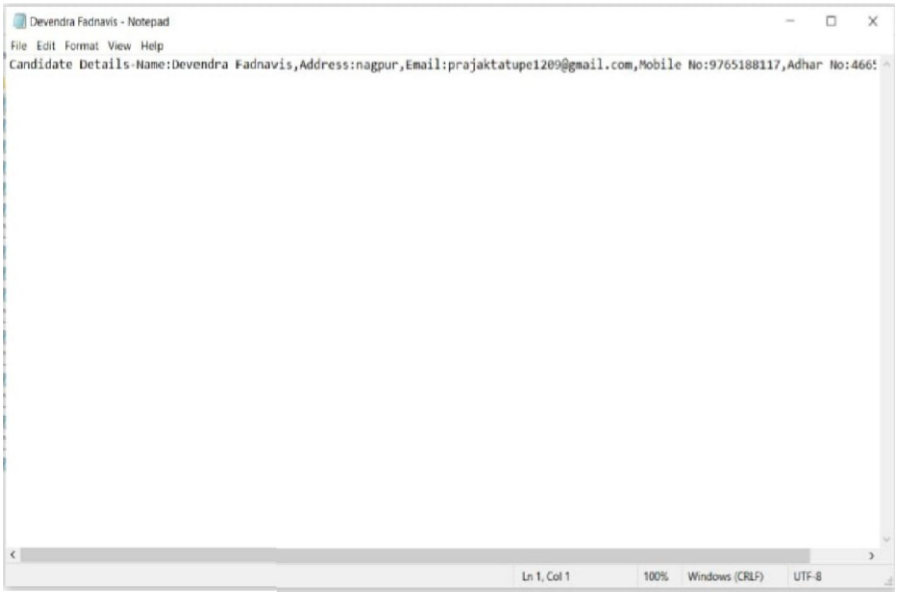
7.1 Home Page



7.2 Admin Page



7.3 Voters Details Stored at Blockchain Node



7.4 Data Stored in Encrypted Form

VIII. CONCLUSION

This paper describes an electronic voting system which offers secrecy, authentication, auditability, security, double vote prevention and a system of justice through authenticated vote options for voters and public opinion systems on the Internet.

REFERENCES

[1] J. Deepika, S. Kalaiselvi, S. Mahalakshmi, S. Agnes Shifani, "Smart Electronic Voting System Based On Biometric Identification-Survey", International Conference on Science Technology Engineering Management (ICONSTEM).

[2] Ravindra Mishra, Shildarshi Bagde, Tushar Sukhdeve, J. Shelke, "Review on Aadhaar Based Voting System using Biometric Scanner", International Research Journal of Engineering and Technology(IRJET).

[3] Girish H S, Gowtham R, Harsha K N, Manjunatha B, "Smart Voting System", International Research Journal of Engineering and Technology (IRJET).

[4] K. Lakshmi, R. Karthikamani, N. Divya "Aadhar Card based smart e-voting system", International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 8958, Volume-8, Issue-2S, December 2018.

[5] G.Saranya, R.Mahalakshmi, J.Ramprabu, "Smart Electronic Voting Machine surveillance", International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 8958, Volume-8, Issue- 2S, December 2018.

[6] Ashish Singh, Kakali Chatterjee, SecEVS: Secure Electronic Voting System Using Blockchain Technology, International Conference on Computing, Power and Communication Technologies (GUCON) Galgotias University, Greater Noida, UP, India. Sep 28-29, 2018.

[7] Cosmas Krisna Adiputra, Rikard Hjort, and Hiroyuki Sato, A Proposal of Blockchain-based Electronic Voting System, Second World Conference on Smart Trends in Systems, Security and Sustainability.

[8] Jena Catherine Bel.D, Savithra.K, Divya.M, A Secure Approach for E-Voting Using Encryption and Digital Signature, International Journal of Engineering Development and Research.

[9] Abhijit J. Patankar, Kotrappa Sirbi, Kshama V. Kulhalli, "Preservation of Privacy using Multidimensional K-Anonymity Method for Non-Relational Data", International Journal of Recent Technology and Engineering (IJRTE) ISSN: 2277-3878, Volume-8 Issue-2S10, September 2019.

[10] Ashraf Darwish and Maged M El-Gendy, A New Cryptographic Voting Verifiable Scheme for E-Voting System Based on Bit Commitment and Blind Signature, International Journal of Swarm Intelligence