Blockchain And Finger Print Enabled E-Voting

Aravind P[1], Gokul Raj S[2],Mohanraj S[3]and Dr.W.Gracy Theresa[4]
Adhiyaman College Of Engineering, Hosur,

Abstract

Election Polling is a complex system as well as costly system. Here we are presenting a novel Secure, Privacy Preserving and cost effective election polling concept which uses Internet Connectivity, BlockchainStorage and Homomorphic encryption. E-Voting is a web based application which uses Blockchain storage and Fingerprint for secured voting. The Votes are converted into encrypted data and stored in Blockchain Technology. A Blockchain is animproving list of transcription which are converted to blocks using cryptography. Each block contains cryptographic of the preceding block a timestamp of voting and data transaction. Fingerprint is used for validation to identify fake voters with their id by comparing with the Fingerprint and Fingerprint in database. This system is used by Election Officer and Booth Manager for checking the voters those who are process of polling. This system promote many votes and the votes are transferred correctly, securely, permanently and transparently.

Keywords: *E-voting, Voters, Blockchain, Fingerprint, Homomorphic Encryption.*

I. INTRODUCTION

Voting Election are a main fundamental pillar of an Indian democratic system enabling the Indian public to express their party member in the form of vote. Due to their interest to our society, the election polling process should be frank and transparent. This system is primarily driven by the hard efforts to make the system caring, Verifiable securing and transparent. In view of its significance, continuous efforts have been made to improve overall efficiency and resilience of the voting system. Electronic voting or e-voting has a profound role in this. Since it's first Use as punched-card ballots in the 1960's, e-voting systems have achieved remarkable progress with its adaption using the Internet technologies. These parameters include Anonymity of the voter, integrity of the vote and non-repudiation among others.

Blockchain is one of the emerging technologies with strong cryptographic foundations enabling applications to leverage these abilities to achieve resilient security solutions. A Blockchain resembles a data structure which maintains and shares all the transactions being executed through its genesis. It is primarily a distributed decentralized database that maintains a complete list of constantly growing data records secured from unauthorized manipulating, tampering and revision. Blockchain allows every user to connect to the network, send new transactions to it, verify transactions and create new blocks. Each block is assigned a cryptographic hash (which may also be treated as a Fingerprint of the block) that remains valid as long as the data in the block is not altered. If any changes are made in the block, the cryptographic hash would change immediately indicating the change in the data which may be due to a malicious activity. Therefore, due to its strong foundations in cryptography, Blockchain has been increasingly used to mitigate against unauthorized transactions across various domains.

Bitcoin remains the most distinguished application of Blockchain however researchers are keen to explore the use of Blockchain technology to facilitate applications across different domains leveraging benefits such as non-repudiation, integrity and anonymity.

In this paper, we explore the use of Blockchain to facilitate e-voting applications with the ability to assure voter anonymity, vote integrity and end-to verification. We believe e-voting can leverage from fundamental Blockchain features such as self-cryptographic validation structure among transactions (through hashes) and public availability of distributed ledger of records. The Blockchain technology can play key role in the domain of electronic voting due to inherent nature of preserving anonymity, maintaining decentralized and publicly distributed ledger of transactions across all the nodes. This makes Blockchain technology very efficient to deal with the threat of utilizing a voting token more than once and the attempt to influence the transparency of the result.

For verification the person's Fingerprint will be scanned at the client-side and matched one-to-one at the servers with the data extracted from the local database. We use Fingerprints for authentication because processing Fingerprints is faster and better than other biometric data. Moreover by using Fingerprints it is ensured such fake entries are blocked right at the very beginning.

Our basic concept was to encrypt the data before sending them to the Cloud provider. But, this one will have to decrypt them each time he has to work on them. The client will need to provide the private key to the server to decrypt the data before execute the calculations required, which might affect the confidentiality of data stored in the Cloud. The Homomorphic Encryption method is able to perform operations of encrypted data without decrypting them. In this work we focus on the application of Homomorphic Encryption method on the Cloud Computing security, particularly the possibility to execute the calculations of confidential data encrypted without decrypting them. This paper discuss on Literature Survey, problem statement, existing system, proposed system, system architecture, modules, and conclusion.

II. OBJECTIVE

Our main objective is to build a Blockchainand Fingerprint authentication based tamper-proof E-voting systemwhere Eligible voters cast a ballot using computer.

III. LITERATURE SURVEY

Gaby G. Dagger, Mateo Milinkovic and Jordan Mahler (2018) this paper deals with the Voting is a fundamental part of democratic systems, it gives individuals in a community the faculty to voice their opinion. In recent years, voter turnout has diminished while concerns regarding integrity, security, and accessibility of current voting systems have escalated. E- Voting was introduced to address those concerns; however, it is not cost-effective and still requires full supervision by a central authority. The Blockchain is an emerging, decentralized, and distributed technology that promises to enhance different aspects of many industries.

Pashine, naive and kelapure [4] proposed an android platform for online voting system. This application provide diversion of long process also provide security to the voter and its voter comfort system voter no need to go polling booth easily vote for candidate in hometown itself. And also provide the option of gesture recognition but authentication is the problem of android platform. In this application which is partitioned into three panels Admin Panel, Candidate Panel and Voter Panel.

Khasawneh [2] Proposed An E-Voting System For Biometric Security Is Providing A Two Sided Solution Such As Server And User Side. After Casting The Vote System Will Generate Hardcopy For Voter And Also Generate Unique Number. This Unique Number and Voter Name and Identification Number Is Secured. All Content Are Stored In Special Box This Box Is Secured Box, This Information Is Used For Verifying The Vote Before Stored In Final Database. This Side Copy Is Printed With Unique Barcode That Can Be Easily Readable Automatically And Scanned Then Randomly Choose One Copy, Then This Copy Is Tested This two sided process providing verification and correctness for the system.

Fires I. Hazzan, Seifedine Kadar [6] this paper deals with the design and development of a web-based voting Fingerprint in order to provide a high performance with high security to the voting system also we use web technology to make the voting system more practical. The new design is proposed an election for a university for selecting the president of the university. The proposed EVS allows the voters to scan their Fingerprint, which is then matched with an already saved image within a database. Developed Web-based Voting System using Fingerprint Recognition. This system has provided an efficient way to cast votes, free of fraud, and make the system more trustable, economic and fast. We have used Minutiae-based Fingerprint identification and matching with high accuracy

Haidari Imam Mohammed University Putra Malaysia (2013) proposed the design and development of a Fingerprint Electronic Voting System. The suggested Fingerprint voting system allows the user to scan his Fingerprint, in order to check his eligibility by comparing his current Fingerprint with the one already stored in the system's database, by the use of MATLAB using Gabor algorithm. Gabor algorithm shows better result if it compared with other algorithms that depend on Minutiae technique because it combines both local and global features. Once the users complete the identification process, they will be allowed to cast their vote using friendly geographical user interface. The counting of the votes will be immediately and that makes the voting process efficient, fast, and secure.

IV. PROBLEM STATEMENT

The present technique requires an aggressor connect specifically with the casting a ballot procedure to disturb it. On the other end, Internet is harder to control and deal with the security as Network and web related assaults are harder to follow.

Internet voting is vulnerable to cyber-attack and fraud vulnerabilities inherent in current software, as well as the basic manner in which the Internet is organized.

V. EXISTING SYSTEM

Electronic voting (also known as e-voting) refers to voting using electronic means to either aid or take care of the chores of casting and counting votes. Depending on the particular implementation, e-voting may use stand-alone electronic voting machines (also called EVM) or computers connected to the Internet. It may encompass a range of Internet services, from basic transmission of tabulated results to full-function

online voting through common connectable household devices. A worthy e-voting system must perform most of these tasks while complying with a set of standards established by regulatory bodies, cost-effectiveness, scalability and ecological sustainability. The vast majority of the ongoing work discusses security, exactness, respectability, quickness, protection, and review capacity however existing frameworks are powerless for assaults at some degree.

A. Some of the disadvantages of existing system:

- Centralized architecture.
- Attack prone.
- Not trustable.
- Non-transparent vote casting process.

VI. PROPOSED SYSTEM

Election Polling is a complex system as well as costly system. Here we are presenting a novel Secure, Privacy Preserving and cost effective election polling concept which uses Web Technology Blockchain Data Storage and Homomorphic encryption. This system has two types of users one is Election Officer & another is Booth Manager, Booth Manager System developed with voter's functionality where voters are going to poll. Voters have to go the Booth where the Booth manager verify the voter and allow him to poll on the Booth's Laptop where the voting system is running. Voters are identified by Fingerprint Authentication to identify fake voters with an id, and the persons Fingerprint matching or not. This proposed system has a method to execute operations on encrypted data without decrypting them which will provide us with the same results after calculations as if we have worked directly on the raw data.

VII.SYSTEM ARCHITECTURE

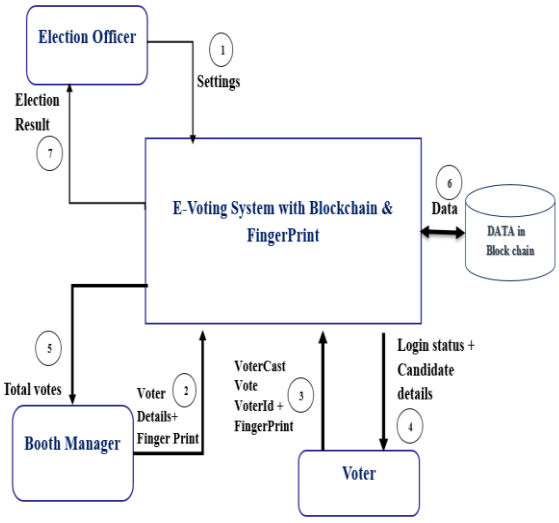


Figure 1.1 Blockchain and Fingerprint E- Voting System Architecture

The followsteps takes Place in figure 1.1:

Step 1: The election officer set the booth manager and candidate details.

Step 2: Then the Booth manager set the Voter details and Fingerprint.

Step 3: Verification of voters in Booth.

Step 4: After verification voters login page will open.

Step 5: Booth manager identifies how many votes are polled in Booth.

Step 6: After a vote is polled the data is stored in Blockchain database.

Step 7: Then the election is completed. The election result is displayed in graph by election officer.

VIII. BLOCK CHAIN TECHNOLOGY

A. Blockchain

A block chain, originally block chain, is a growing list of records, called *blocks*, which are linked using cryptography. Each block contains a cryptographic hash of the previous block, a timestamp, and transaction data (generally represented as a Merkle tree root hash).

B. Blockchain Structure

A Blockchain is a decentralized, distributed and public digital ledger that is used to record transactions across many computers so that the record cannot be altered retroactively without the alteration of all subsequent blocks and the consensus of the network. This allows the participants to verify and audit transactions in expensively. A Blockchain database is managed autonomously using a peer-to-peer network and a distributed time stamping server. They are authenticated by mass collaboration powered by collective self-interests

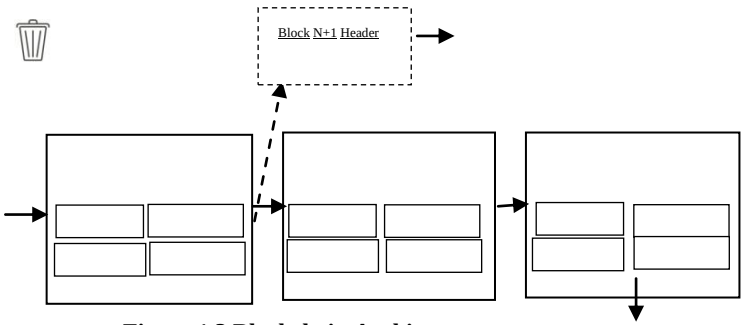
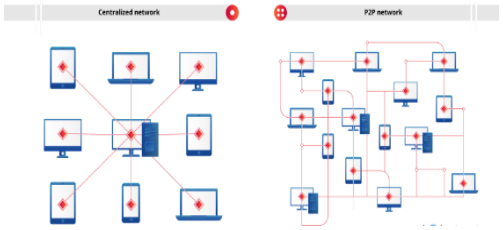


Figure 1.2 Blockchain Architecture

The result is a robust workflow where participant's uncertainty regarding data security is marginal. The use of a Blockchain removes the characteristic of infinite reproducibility from a digital

asset. It confirms that each unit of value was transferred only once, solving the long-standing problem of doubled spending. Blockchain have been described as a value-exchange protocol. This Blockchain-based exchange of value can be completed quicker, safer and cheaper than with traditional systems A Blockchain can assign title rights because, when properly set up to detail the exchange agreement, it provides a record that compels offer and acceptance.



Centralized Network vs P2P Network

In a P2P network, the "peers" are computer systems which are connected to each other via the Internet. Files can be shared directly between systems on the network without the need of a central server. In other words, each computer on a P2P network becomes a file server as well as a client.

C. Types of Blockchains

Currently, there are three types of Blockchain networks - public Blockchains, private Blockchains and consortium Blockchains.

1) Public Blockchains

A public Blockchain has absolutely no access restrictions. Anyone with an internet connection can send transactions to it as well as become a validator (i.e., participate in the execution of a consensus protocol). Usually, such networks offer economic incentives for those who secure them and utilize some type of Proof of Stake or Proof of Work algorithm. Some of the largest, most known public Blockchains are Bitcoin and Ethereum.

2) Private Blockchains

A private Blockchain is permissioned. One cannot join it unless invited by the network administrators. Participant and validator access is restricted. This type of Blockchains can be considered a middle-ground for companies that are interested in the Blockchain technology in general but are not comfortable with a level of control offered by public networks. Typically, they seek to incorporateBlockchain into their accounting and record-keeping procedures without sacrificing autonomy and running the risk of exposing sensitive data to the public internet.

3) Consortium Blockchains

A consortium Blockchain is often said to be semi-decentralized. It, too, is permissioned but instead of a single organization controlling it, a number of companies might each operate a node on such a network. The administrators of a consortium chain restrict users' reading rights as they see fit and only allow a limited set of trusted nodes to execute a consensus protocol.

D. Fingerprint Authentication

In order to authenticate a person we require them to have a valid UID number. The number will be checked in the local database records first. If it is not found then it will search the central repository. It involves one-to-many match. If the person's number is not found in the central database then of course s/he will be devoid of taking part in the voting process. This record is extracted from the local database and sent to authenticating servers for further processing. For verification the person's Fingerprint will be scanned at the client-side and matched one-to-one at the servers with the data extracted from the local database. This process puts less stress on the local database and improves data traffic. We use Fingerprints for authentication because processing Fingerprints is faster and better than other biometric data. Moreover aadhar details would be insufficient to establish the true identity of a person since they can be easily faked but by using Fingerprints it is ensured that such fake entries are blocked right at the very beginning.

IX. RESULT AND DISCUSSIONS

- Election officer has to login by using username and password.
- Election officer is responsible for declaring the winner and can check the total number of votes of a particular candidate.
- Booth manager is responsible for checking the total number of votes of a particular booth but restricted from checking the votes of a particular candidate and fingerprint identification.
- Every vote polled is encrypted and added homomorphically to the encrypted votes of the respective candidate.

A. Electoral dist. Maintenance

Election officer has the authority to add, delete or edit the election district list. Candidate details like name, age, party, district can checked, edited, added or deleted. Likewise even the booth details like the reference number, district, and the booth manager in-charge can be seen or edited. Mainly the election officer has the authority and the secret key to decrypt the individual votes of each candidate from different booth and announce the winner of election district wise.

B. Booth Maintenance

Booth manager will have information about his booth regarding booth reference number, booth location, number of candidates contesting for election and total number of voters destined to vote in his booth. He has the authority to see the voter details who belong to his booth. He can add or delete any voter from the list. Voter is allowed to vote provided his voter-id is valid and cast his vote. This happens under the booth manager assistance. After voting, Booth manager can view the total number of votes, indirectly representing the total number of voters polled but individual votes per candidate can be viewed in the encrypted format.

C. Voter Details

Voter Details have to display as per the booth.The Indian voter ID card is an identity document issued by the Election officer of India who have reached the age of 18, which primarily serves as an identity proof for Indian citizens while casting their vote. It also serves as general identity, address, and age proof for other purposes such as applying for a passport.

D. Voting Process

In this module the process of voting is carried out. The voter's identity is to be validated, whether he belongs to his assigned booth and whether it has polled or not. Provided he hasn't already voted, he can cast his vote. This vote will be encrypted and added to the particular candidate to whom he/she has voted and this data is stored.

E. Homomorphic Encryption

Homomorphic Encryption on data, a small module is developed which shows addition, subtraction, and multiplication operations on encrypted data which uses the RNS (Residue Number System) algorithm. It is easier when compared to palmer and also it is robust and more efficient.

F. Election Result in graph

As per the election, result has to display in the graph.

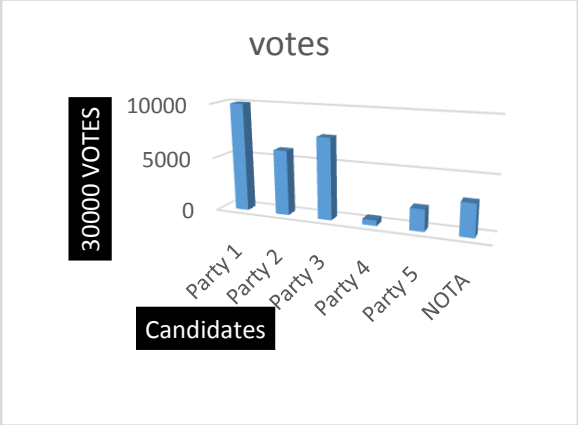


Figure 1.2 Voting results are displayed in a graph.

X. CONCLUSION

Blockchain technology is currently in a nascent state. There haven't been enough distributed-ledger-technology and Blockchain-based applications to sufficiently evaluate whether this technology is superior to current voting systems. No full implementation of Blockchain based E-Voting (BEV) for a national election has occurred. However, we argue that BEV has a future in elections and might transform voting. Political violence related to elections has been common in Africa and other developing countries. BEV can ensure security and transparency and reduce electoral violence. We using Fingerprint for fake voter'sidentification. This has faster authentication. It can also produce more mathematically accurate election results. Because BEV doesn't require management from a central authority, voting related costs will decrease. Finally, BEV should reduce the cost of paper based elections and increase voter participation. By this system achiveing more votes and the votes are recorded accurately, permanently, securely and transparently.

REFERENCES

[1] Yavneh, M. O., &Gbolagade, K. A. (2013). Overview of Biometric Electronic Voting System in Ghana. International Journal of Advanced Research in Computer Science and Software Engineering

[2] Feng Hai and Peter Y A Ryan (Ends).Real-world Electronic Voting: Design, Analysis and Deployment, Series in Security, Privacy and Trust.CRC Press, 2016.

[3] C. Culnane, P. Y. A. Ryan, S. Schneider, and V. Teague.Y Vote: Averifiable voting system.ACM Trans. Inf. Syst. Secur., 18(1):3:1-3:30, June 2015.

[4] F. Hai, M. N. Kreeger, B. Randell, D. Clarke, S. F. Shahandashti, and P.H.-J. Lee. Every vote counts: Ensuring integrity in large-scale electronic voting.USENIX Journal of Election Technology & Systems, 2(3):1-25, 2014.

[5] Siamak F. Shahandashti and Feng Hai. DRE-ip: A Verifiable E-Voting Scheme without Tallying Authorities. The 21st European Symposium on Research in Computer Security (ESORICS), 2016.

[6] Divya G Nair, Binu. V.P, G. Santhosh Kumar," An Improved E-voting scheme using Secret Sharing based Secure Multi-party Computation", arXiv: 1502.07469v1 [cs.CR] 26 Feb 2015.

[7] Prof. S.M. Jambhulkar, Prof. Jagdish B. Chakole, Prof. Praful. R. Pardhi "A Secure Approach for Web Based Internet Voting System using Multiple Encryption", 2014 International Conference on Electronic Systems, Signal Processing and Computing Technologies,2014.

[8] Pranay R. Pashine, Dhiraj P. Ninave, Mahendra R. Kelapure, Sushil L. Raut, Rahul S. Rangari, Kamal O.Hajari," A Remotely Secure E-Voting and Social Governance System Using Android Platform",International Journal of Engineering Trends and Technology (IJETT) – Volume 9 Number 13 - Mar 2014

[9] Himanshu Agarwal, G.N.Pandey, "Online Voting System for India Based on AADHAAR ID", Eleventh International Conference on ICT and Knowledge Engineering 2013.

[10] K. P. Kaliyamurthie, R. Udayakumar, D. Parameswari and S. N. Mugunthan, "highly secured online voting system over network", 4833 Indian Journal Science and Technology Print ISSN: 0974-6846 Online ISSN: 0974-5645 Vol 6 (6S) May 2013.

[11] Hao, F., Kreeger, M. N., Randell, B., Clarke, D., Shahandashti, S. F. and Lee, P. H.-J. (2014). Every vote counts: Ensuring integrity in large-scale electronic voting, in 2014 Electronic Voting Technology Workshop/Workshop on Trustworthy Elections (EVT/WOTE 14). San Diego, CA: USENIX Association, 2014.

[12] Rockwell, M. (2017) Bitcongress – Process for block voting and law, http://bitcongress.org/ last accessed: December 2017.

[13] Narayanan, A., Bonneau, J., Felten, E., Miller, A. and Gold, S. (2015) Bitcoin and Cryptocurrency Technologies, Chapter 2 and 3, Draft October 2015.

[14] Nakamoto. S. (2009) Bitcoin: A peer-to-peer electronic cash system, 2009 [Online]. Available: http://bitcoins.info/bitcoin-a-peer-to-peer-electroniccash-system-satoshi-nakamoto. Last accessed: December 2017.

[15] Multichain (2017) Open platform for Blockchain applications. Available at: www.multichain.com last accessed: December 2017.

[16] McCorry, P., Shahandashti, S. F. and Hao. F. (2017) A smart contract for boardroom voting with maximum voter privacy in the proceedings of FC 2017.

[17] Kraft, D. (2015) Difficulty Control for Blockchain-Based Consensus System, Peer-to-Peer Networking and Applications by Springer, March 2015

[18] Kadam, M., Jha, P. Jaiswal, S. (2015) Double Spending Prevention in Bitcoins Network, International Journal of Computer Engineering and Applications, August 2015

[19] Rosenfeld. M. (2017). Analysis of hashrate-based double-spending. [Online]. Available:http://arxiv.org/abs/1402.2009 last accessed: December 2017.

[20] Rura L., Issac B., and Haldar M. K. (2016) Implementation and evaluation of steganography based online voting, International Journal of Electronic Government Research.

[21] Shahandashti, F. S. and Hao, F. (2016) DRE- imp: A Verifiable E-Voting Scheme without Tallying Authorities, the 21st European Symposium on Research in Computer Security (ESORICS), 2016.