National Conference on
"Role of Engineers in Nation Building" organized by VIVA Institute of Technology, Mumbai
(6th and 7th March 2020)
International Journal of Engineering Research & Science (IJOER)
ISBN:[978-93-5391-287-1] ISSN: [2395-6992] [Vol-6, Issue-3, March-2020]

A Modern Approach For Secure E-Voting

Snehal Chavan[1], Shweta Dubey[2], Saniket Kudoo[3]
[1]Department of Computer Engineering, Mumbai University, India.
Email: 16302020snehal@viva-technology.org,
[2]Department of Computer Engineering, Mumbai University, India.
Email: 16301034shweta@viva-technology.org,
[3]Department of Computer Engineering, Mumbai University, India.
Email: SaniketKudoo@gmail.com

Abstract— *Voting is a normal process that keeps a nation's governmental system works. Every voting system must follow the basic requirements such as authenticity of user and impartially to achieve unfair voting. Most of the existing electronic system based on system which suffer from universal authenticity and integrity issues of participants and may need improvement. In unified system, the result of voting events has always been questionable by voters. Various voting systems are available for conducting election and providing better security of votes. In this paper, comparative study of various voting systems based on blockchain technology is discussed to get secured and trustworthy results. In order to improve authenticity of voter biometric can be implemented with blockchain technology.*

Keywords —Authenticity, Biometric, Block chain, Security, Voting.

I. INTRODUCTION

Voting is the most important process that has to be undertaken by every individual in a responsible manner. In the democratic Country it gives right to the people of that country to choose the committee members of their choice [2]. This process should be
well-mannered and without any effect to the process.

After each election there is a rumor or doubt in people and opposition parties mind that there are many frauds made by the election members in EVM or while counting the votes[6]. It is difficult for people to accept the elected candidate for that particular post. There are chances that a person cast votes under another person identity which is also a kind of fraud. In other words, each ballot should be counted anonymously, accurately and efficiently [9].In this paper, various techniques were studied and compared which are used for providing better securities in a voting system.

II. LITERATURE SURVEY

Hsin-Te Wu, et.al [1] have proposed voting system that is designed on the basis of blockchains to create a trustworthy voting system. In current blockchain technology, voter-related regulations are provided by smart-contracts to prevent controversies during voting processes. The current electronic voting systems employ centralized servers for data processing; centralized servers are susceptible to malicious attacks and so using the distributed architecture can reduce the risk of post-attack shutdown. Additionally, an anonymous voting system is designed with the goal of providing anonymity. The system did not include mechanisms such as ballot counting and ranking to our scheme and improve the speed of vote counting and complement electronic voting systems.

Ali KaanKoç, et. al. [2] have proposed system that uses block chain with the smart contracts for online voting system. To provide consistency smart contracts logic is widely been used, ethereum along with the network is used. It further makes use of solidity language for Ethereum wallets or android application so that the user can vote. Android application is also been designed so that the people without an Ethereum wallet can also cast their precious vote. After completion of election, the

International Journal of Engineering Research & Science (IJOER)
ISBN:[978-93-5391-287-1] ISSN: [2395-6992] [Vol-6, Issue-3, March-2020]

records of votes will be stored in the Ethereum block chain network. To provide reliability and efficiency this blockchain system for voting was designed.

Budi Rahardjo, et. al. [3] have proposed a decentralized system where the complete database is owned by many users, which is done by using block chain technology. The system makes use of hash values in recording the voting results of each polling station and makes this recording system more secure. It also helps to identify nodes that can control and update data together for achieving the participants trust goals. The block chain algorithm for recording of votes result from every place of election is been researched. In non-functional tested it was found that the system implemented with Python programming language able to handle the whole process of recording the e-voting system.

David Khoury, et. al. [4] have proposed System is designed for writing both registration and voting smart contracts using Solidity language. The system provides voting data immutability along with data integrity and ensured privacy. User mobile phone numbers are used to authenticate them without the need of a third-party server. This system restricts each voter to have a single vote per valid Mobile Station International Subscriber Directory Number. Privacy-aware regarding the confidentiality of the recorded votes. The existing centralized systems facilitate voting process conducted by governments and is based on SMS polling and can be replaced by the designed system. The system offers a step towards ideal environments for such experience, since it is feasible.

Dr. PrasenjitBhavathankar, et. al. [5] have proposed a paper in which the individuals national identity can be integrated with various blockchain applications. The individuals national identification records must contain the fundamental details regarding the individual and also the biometrics details that can be carried anywhere. Aadhar card number is used as a national identification for each individual in this system. Once the QR code is been scanned, the authorized person can see all the details of the vote entered in the system during registration. It allows individuals, machines, algorithms and organizations, to
liberatingly interact and transact with each other with less friction. Also distributed cloud storage is been used to store the data.

Wei-Jr Lai, et. al. [6] have proposed an Evoting system that is effective for voters and maximize government or authority trust. Ethereum blockchain is used to store the votes and all messages which provides the transparency of election that is ensured. It ensures the voting resultscorrectness and the individual participant Ethereum gas cost is kept affordable simultaneously. The system calculates result automatically is maintained in this system through which the voting results can be tallied without the interference of any untrusted third party. The effectiveness of our system can be justified by checking the required Ethereum gases per voter.

Shalini Shukla, et. al. [7] have proposed the application that is designed in such a manner so that the intricacies of the underlying architecture is hidden from the user. Government approved Aadhar number is used to identify each voter uniquely. Each voter gates right to vote only once for each election. To make the votes encrypted and in hash format, a public and private key are allocated to each individual. The scalability of the blockchain application depends on the secondary memory limit of the peer. The proposed framework does not tackle every one of the issues related with electronic voting, but it provides a profitable contrasting option to present, restrictive electronic voting frameworks.

RikardHjort, et. al. [8] have proposed a voting system using concept of blockchain and an early stage implementation of the system is done. System relies heavily on the trust of the election commission side. The electoral commission can relate voters and their choices as voters register their public keys with their IDs to the electoral commission. The electoral commission also holds the election secret key, let it able to see the message created by voters. However, election secret key leakage can cause

International Journal of Engineering Research & Science (IJOER)
ISBN:[978-93-5391-287-1] ISSN: [2395-6992] [Vol-6, Issue-3, March-2020]

huge damage to the election itself as it allows people to see the partial result of the election. Therefore, the voting electoral commission needs to protect the election secret key.

Mohamad H. Hassoun, et. al. [9] have proposed the system using a classification strategy called as weighted voting that observes the performance of face recognition. Instead of evaluating the local distance to merge the results of local classifiers based on rank information, weighted voting strategy is used. Simple pixel feature is an example where such strategies can be used. Specification of how to achieve the final classifier output is given when multiple features are available. Test results are presented for the issues of face recognition on a large human face of database. The sequential classifier, though, performs similar to both combination schemes, but requires much less computation time.

Soojin Park, et. al. [10] have proposed the constituent elements of smart contract that are analyzed and expressed by ontology. And the process of negotiating the components is represented by each transaction. Finally, we construct the component represented by the ontology as XML by including the state information in the transaction. In this way, the smart contract is represented in a formal language that contains state information. It also laid the foundation for a smart contract that can be reused and verified. There are various types of block-chain networks, and the configuration of smart contracts used for each blockchain network differs.

Jon Crowcroft, et. al [11] have proposed the survey paper which include the electronic voting, however, has emerged as an alternative but still not being practiced at a large scale. The flawless method for result accumulation from the blocks is suggested in this paper. It helps to declare the results from the constituencies, polling stations, and the national result. The data accumulation, polling process effectiveness, block sealing and creation, utility of hashing algorithms and result declaration is discussed in framework by using the secured blockchain method. This system also claims to prove the data management and security challenges in blockchain providing an improved version of the electronic voting process.

Yong Yuan, et. al. [12] have proposed a paper that consist the implementation of smart contract in voting system. The characteristics of smart contracts enable contract terms to be followed within untrusted parties without any interference of a trusted authority or any central server. . The open challenges standing faced by smart contracts and the recent research progresses. The smart contracts were enbled by the blockchain operating mechanism and platforms also a research framework for it based on a novel six-layer architecture was proposed. Second, both the technical and legal challenges along with the recent research progresses, are listed. Lastly several application scenarios were presented.

Sanchay Mishra, et. al. [13] have proposed a voting system that uses block chain for data storageand cloud based storage(SAAS) to update the votes which are recorded by the EVM. The systemmake use of block chain which has a feature of Proof-of-Work which does not allow the rapidmanipulation of data. The system stores the votes in a form of hash value and store it in a hashtable so if any tampering with votes takes place it will results to break a link and detects themanipulated votes and discard them by marking as NOTA.The system can identify the point ofmanipulation by tallying the data of EVM with hash table. This system can also be used in suchareas where no broadband internet connection are available.

Ashish Singh, et.al. [14] have proposed a e-voting system that uses a block-chain technologywhich solve the security issues of existing system. This system is de-centralized which storeresults in different locations in a form of bitcoins and the system uses encryption and hashingconcept for ensuring the security.The system ensures that only registered and authenticated usercan vote only one time. One's the voter cast the vote blocks is created and after completion ofblockchain no one can tamper the data.The system uses Voter ID for unique identification ofuser. The security analysis of system shows that the system is more robust and secure againstexisting attacks.

International Journal of Engineering Research & Science (IJOER)
ISBN:[978-93-5391-287-1] ISSN: [2395-6992] [Vol-6, Issue-3, March-2020]

Rong Wang, et. al.[15] have proposed a system is a digital certificate publishing schemean anonymous, it achieves the separation of user registration andauthorization. It has the featuresof anonymity and conditionaltraceability to realize and to protect user's identity privacy.

ChangHyung Le, Lewis Nkenyereye, et. al. [16] proposed an architectural framework whichfocusesonproviding blockchain in IoT platform. One of the existing blockchain system which isLogchainand oneM2M-based IoT platform is used. To ensure blocksintegrity, an algorithm namely blind voting as a general agreement rule is used by Logchain.

III. ANALYSIS

The following table is the summary of various research papers on data security using various encryption techniques.

Table 1. Analysis Table

Sr.No.	Title of paper	Techniques	Advantage	Disadvantage
1.	Towards Secure E-Voting Using Ethereum Blockchain.[1]	Smart Contract	Able to eliminate duplicate votes.	Biometric authentication is not provided
2.	Block chain Based E-Voting Recording System Design.[2]	Block chain and python pycharm	More cost efficient.	All nodes that have not been defaced because of disorder.
3.	Decentralized Voting Platform Based on Ethereum Block chain.[3]	Solidity	Provides data immutability, data integrity and clarity.	Biometric authentication is not implemented.
4.	Online Voting Application using EthereumBloackchain.[4]	Smart contracts, Hyper ledger	Simple, scalable and reliable.	Complexity is high.
5.	DATE: A Decentralized, Anonymous, and Transparent Evoting System.[5]	Smart contract	No deposit required to invest	Time Consuming
6.	A PrivacyPreserving Voting Protocol on Blockchain.[6]	Smart contracts	Low volume of data stored after encryption/decryption.	Complexity is high, therefore use is very less.
7.	A Comprehensive Integration of National Identity with Block chain Technology.[7]	Proof of work	Votes are Stored Securely.	National Identity is must.
8.	A Block chainBased Network Security Mechanism for Voting Systems.[8]	Bilinear pairing	Allows user to conduct data authentication.	Complexity is high
9.	E-Voting Using Face Detection and Recognition (FDR), One Time Password	Template Matching	High speed (Matching Image).	Accuracy is Moderate.

International Journal of Engineering Research & Science (IJOER)
ISBN:[978-93-5391-287-1] ISSN: [2395-6992] [Vol-6, Issue-3, March-2020]

	(OTP).[9]			
10.	Face Time – Deep Learning Based Face Recognition Attendance System.[10]	Deep Convolution Neural Networks(CNN)	Accuracy is high (96%).	Noise and Distance affects accuracy.
11.	A Proposal of Blockchain-based Electronic Voting System.[11]	Distributed database	Transparent System	Anonymity and Coercion less.
12.	Formal Specification Technique in Smart Contract Verification.[12]	Smart-Contract, XML	Allow verification of smart contract.	Lack to exchange data between nodes.
13.	Block Chain Based Cloud Computing Model on EVM Transactions for Secure Voting.[13]	Proof of work, SAAS	Manipulation of data is not possible.	Better networks is required for faster storing of data.
14.	SecEVS : Secure Electronic Voting System Using Blockchain Technology[14]	Blockchain	More robust and secure against existing attacks.	Huge storage of data is required.
15.	A Privacy-Aware PKI SystemBasedon Permissioned Blockchains.[15]	NA	Reduces the cost of CA construction, operation and maintenance in traditional	Single point failure. Poor efficiency of certificate deployed.
16.	Towards a Blockchain-enabled IoT Platform using oneM2M Standards.[16]	Logchain	IoT framework that shows the feasibility of using Blockchain technologies in a standardized IoT service layer platform.	Developing of the described API that can enable blockchain in oneM2M.

NA- Not Applicable.

IV. CONCLUSION

Due to the fast development of technologies, E-votingand its security has become the most important aspect. There are various techniques which are used by many countries to cast votes. In this paper, various techniques used for E-votingbased on blockchain technology but they had not used any biometric techniques for authentication. The Blockchain technology with biometrics are found efficient for E-voting and its security.

ACKNOWLEDGEMENTS

We would like to express a deep sense of gratitude towards our mentor for her constant encouragement and valuable suggestions. The work that we have been able to present is possible because of timely guidance and support.

REFERENCES

[1] E. Yavuz and G. Dalikic, "Towards Secure E-Voting Using Ethereum Blockchain", IEEE, 6th International Symposium on Digital Forensic and Security (ISDFS), Antalya, Turkey, 2018.

[2] RifaHanifatunnisaand Budi Rahardjo, "Block chain Based E-Voting Recording System Design", IEEE, Indonesia, 2017.

International Journal of Engineering Research & Science (IJOER)
ISBN:[978-93-5391-287-1] ISSN: [2395-6992] [Vol-6, Issue-3, March-2020]

[3] D. Khoury and H. Harb, "Decentralized Voting Platform Based on Ethereum Blockchain", IEEE, International Multidisciplinary Conference on Engineering Technology (IMCET), 2018.

[4] Shashank D O, Shalini Shukla , "Online Voting Application using EthereumBloackchain", IEEE Transactions on Computational Social Systems, USA, 2017.

[5] Y.-c. Hsieh and W. Lai, "DATE: A Decentralized, Anonymous, a Transparent E-voting System", IEEE, National Taiwan University, 2018.

[6] W. Zhang and S. Huang, "A Privacy-Preserving Voting Protocol on Blockchain", IEEE, 11th International Conference on Cloud Computing, China, 2018.

[7] K. Mudliar and H. Parekh," A Comprehensive Integration of National Identity with Blockchain Technology", IEEE, Mumbai, India, 2018.

[8] C.Y. Yang and H. T. Wu, "A Blockchain-Based Network Security Mechanism for Voting Systems", IEEE, 1st International Cognitive Cities Conference, Okinawa, Japan, 2018

[9] M. Arsenovic, S. Sladojevic, "FaceTime–Deep Learning Based Face Recognition Attendance System", IEEE, Subotica, Serbia, 2017.

[10] R. Hartanto and M. N. Adji ,"Face Recognition for Attendance System Detection", IEEE, Kuta, Indonesia, 2018.

[11] C. K. Adiputra, R. Hjort, and H. Sato, "A Proposal of Blockchain-based Electronic Voting System", IEEE, London, UK, 2018.

[12] R. Wang, W. T. Tsai and E. Deng, "A Privacy-Aware PKI System Based on Permissioned Blockchains", IEEE Beihang University, Beijing, 2018.

[13] Seung-Min Lee and Soojin Park, "Formal Specification Technique in Smart Contract Verification", IEEE, Jeju, Korea (South), Korea (South), 2017.

[14] Sanchay Mishra,"Block Chain Based Cloud Computing Model on EVM Transactions for Secure Voting",IEEE, China,2019.

[15] Ashish Singh,"SecEVS : Secure Electronic Voting System Using Blockchain Technology",IEEE, Greater Noida, UP,2018.

[16] Rong Wang and Wei-Tek Tsai,"A Privacy-Aware PKI System Based on Permissioned Blockchains", IEEE, China,2018.

[17] ChangHyung Lee1 and Lewis Nkenyereye1,"Towards a Blockchain-enabled IoT Platform using oneM2M Standards", IEEE, Korea, 2018.