Research Article

Secure E-Voting System Using Visual Cryptography & Block Chain Ledger

Ashwini Solankar[1], Santosh Javheri [2]

[1]Savitribai Phule Pune Univresity, PG research Scholar, Maharhatra/India.
[2]Savitribai Phule Pune Univresity, faculty, Maharhatra/India.

Article History: Received: 10 November 2020; Revised: 12 January 2021; Accepted: 27 January 2021; Published online: 05 April 2021

Abstract: Expanding advanced innovation has revolutionized the life of individuals. In this digital world many countries are trying to initiate an E-voting system in regular election process. Researchers are looking forward for the innovative ideas for secure and user friendly system. Block chain is one of the novel concepts that come with number of features to develop E-services. By embracing block chain in the circulation of databases on e-casting ballot frameworks, one can decrease the duping wellsprings of database control. This venture intends to execute casting a ballot result utilizing block chain calculation from each place of decision. In proposed system we have chosen Block chain for its decentralized framework and Here in security and data integrity is mainly achieved by making use of Visual Cryptography (VC) concept. This VC technique comes in when user casts vote on an E-voting portal.

Keywords: Security and Protection, Visual Cryptography, Internet Voting System, Voter Password, Visual secret sharing

1. Introduction

Electronic choice frameworks have started getting utilized in a few nations. Estonia was the essential inside the world to receive relate degree electronic appointive framework for its national races [1]. Before long, electronic determination was embraced by Schweiz for its state-wide races [2], and by Norway for its gathering decision [3]. For partner degree electronic appointive framework to fight with the standard ticket framework, it needs to help similar criteria the conventional framework bolsters, for example, security and secrecy. An E-voting framework ought to have increased security so as confirm it's offered to voters anyway shielded against outside impacts dynamical votes from being produced, or shield a voter's tally from being altered. Numerous electronic choice frameworks have confidence in Tor to cover the personality of voters. In any case, this framework doesn't give absolute lack of clarity or honesty since a few insight organizations round the world administration totally extraordinary parts of the net which may empower them to spot or on the other hand capture cast a ballot.

1.1 Related Work

In an Election system there are number of things which we needs to take care of; but the most challenging task are to provide security and to prevent from suspicious activities during the voting process. The centralized voting system was having many issues related with security. Hence many scholars are looking for decentralized system that is more robust and secure. Block chain is a system that does not need a centralized trusted authority, and provides the process of tracking and recording distributed data that can be shared and is securely handled. To enhance technical features of voting process we are adding one security level by introducing Visual Cryptography with Block chain in it. Visual Cryptography (VC) is a special method of cryptography where we can securely transmit secret data over different transmission mediums.

Online payments can be sent from one person to another person with the use of electronic cash or digital currency. In this transaction interference of any bank portal or financial institution is negligible; this is done with the help of Digital Signature. But as said Digital Signature can be used more than once which allows loss of a trusted third party and problem of double outlay arises. S.Nakamoto[4] proposed a solution to the double-spending problem in which the network is used where node to node transaction are timestamped by hashing and thus chain of transaction is hash based to form a record. This record is proof of work and termed as Block chain. Block chain also included sequence of events as proof of work which comes from largest pool of computing. Thus, to undo theses record becomes difficult to attacker. Peer to peer network with record of transaction and sequence of events in hash form create suitable Block chain which prevents double spending issue for digital currency thus making transaction fast and trustworthy with less interference of financial institute. Even Buterin, Vitalik[12] also mentions about block chain technology ensures the elimination of the double-spend problem, with the help of public-key cryptography, whereby each agent is assigned a private key (kept secret like a password) and a public key shared with all other agents.

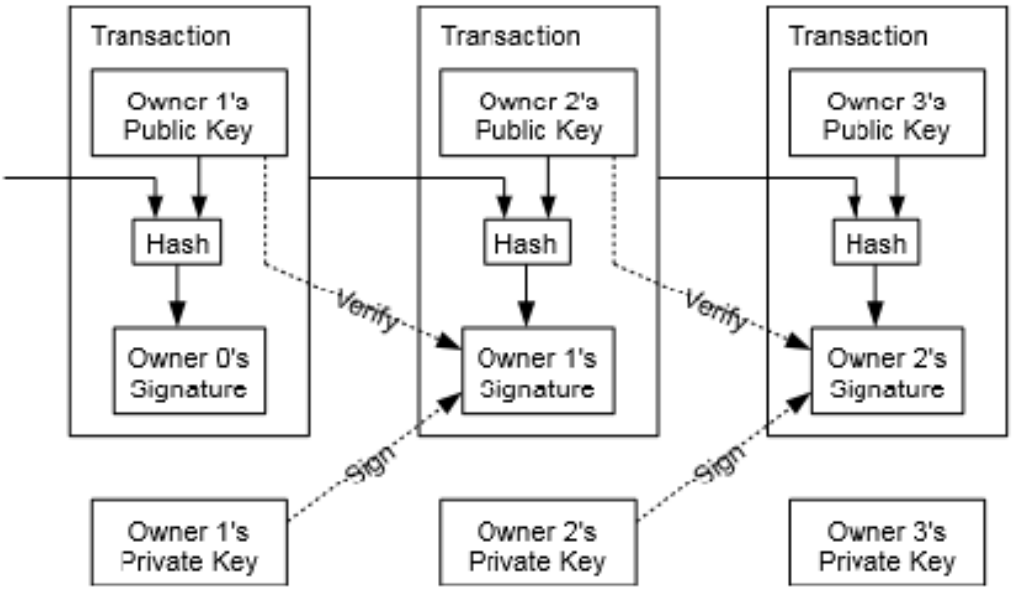

Figure 1. Peer To Peer Network with Transaction Record

Estonia was the first country to use e-voting for general elections through internet in 2005. In this system Maaten E. [5] focuses every citizen of country was provided with ID card with digital signature which holds their authentication as well as public key for security. Card was provided with remote e-voting and advance voting system wherein the citizen was able to re-vote till he finalized his vote. The system gained popularity as well as trust by giving privacy to the voters. Below figure shows the casting of vote for e-voting with pubic key and private key.

The Internet of Things have many devices connected to each other over internet. These devices communicate with each other regarding physical values or some analytics about surrounding. Azad, Muhammad et.al. [6] Mentions how Machine to machine communication happens where two or more machines share values and information to establish a log for analysation and monitoring is represented as M2M. The logs established should identify the machine as well keep the information accurate and maintain security and privacy. This privacy maintaining issue over reputation over decentralized system is termed as M2M-REP (Machine to Machine Reputation) which keeps the log of global reputation and feedback in encrypted form. Supriya Thakur Aras et. al. [7] shares the thought behind Proof of Stake is that it might be increasingly troublesome for mineworkers to procure adequately huge measure of advanced money than to gain adequately amazing processing equipment. S. B. Javheri and U. V. Kulkarni [9] explain about the method when multiusers encryption happens, one needs to perform unlimited addition or multiplication on cipher text homomorphic encryption is required that is a BGN encryption. Kashif Mehboob Khan et.al.[10] proposes methodology has been executed with multi chain and in depth assessment of methodology features its adequacy as for accomplishing principal necessities for an e-casting a ballot scheme. Block chain is a futuristic technology and applies to various businesses. [11] Anusha MN and Srinivas B K[17] aims to provide flexibility to allow casting votes in any remote place even in critical corporate decisions to their users.

1.2 System Preliminary

Block chain

Guy Zyskind et.al.[13] tells about the block chain is a decentralized platform, making legal and regulatory decisions about collecting, storing and sharing sensitive data should be simpler.

The system which can allow decentralize system to come together with entire database which is owned by many users as well maintain data integrity for system can be embraced by Block chain technology as one of the solutions. Data integrity and authentication which can be obtained through block chain. Block chain is a methodology where in data protected and never disclosed without proper authentication. Election process is way to decide authority which will lead the society and this needs total security with votes casted. For evoting

process, each in system generated two keys one as private and other as public. Public key is circulated through all the nodes listed for election process. When one round of selection is completed, node creates a separate block with voter and voted information. When whole process is completed, every block is verified to check validity.

Visual Cryptography

Visual Cryptography is a huge concept mainly used for hiding a data or information which one wants to keep confidential. We have added this concept for user's identification. The OTP process is introduced here in our proposed system. It creates an image which further going to divide into 2 shares. This is done for voter's authentication process that provides more Security to our system. Hussein Khalid Abd-alrazzq1 et.al.[20] focuses on the system that is proposed by them using Visual Cryptography is to provide security for voters to cast their votes.

2. Proposed System

In proposed methodology use of block chain is added with visual cryptography to give more transparency and security to voter and casted vote. Authentication and proof that the system is real with real authorized voter is need of the time. The voter need to timestamp and sign the casted vote to assure that there is no change in authentication. Data needs to be verified for same wherein block chain proves its worth.

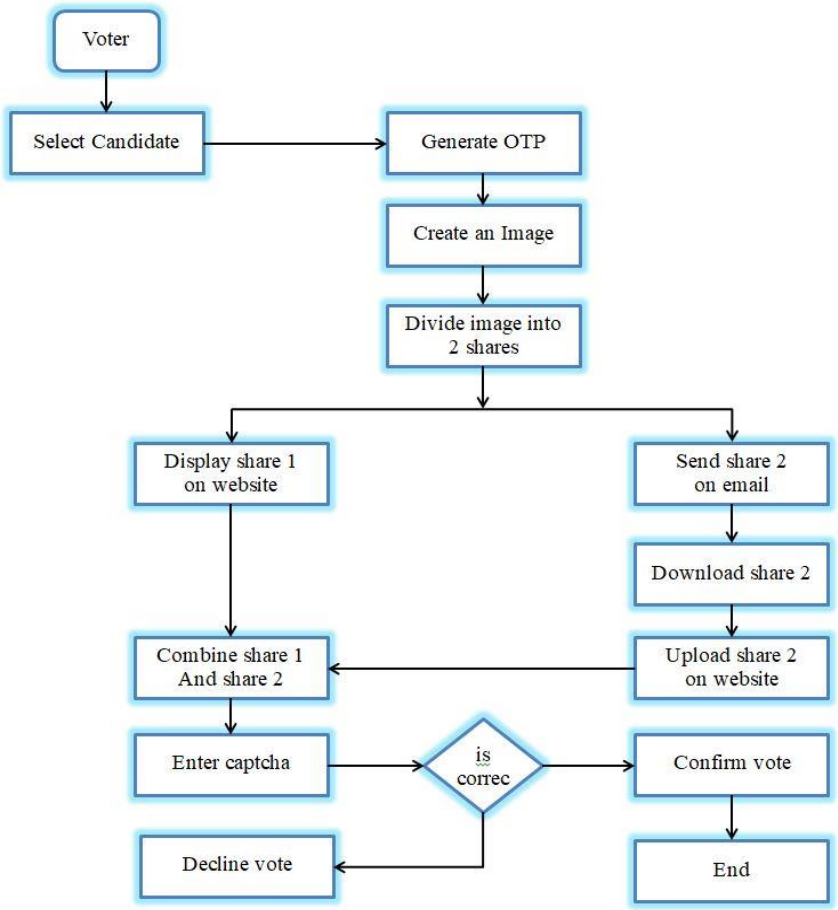

Figure 2. Proposed System Workflow

Algorithm

Proposed algorithm is used to create the block embedded with voting information. AES and Visual Cryptography are applied for security.

input: a block chain called *B*,bn is the last block on the block chain.
input:An image is created as OTP which will be divided into 2 parts
Share1, *s*1 is the first block on the embedded block.
Share2 *s*2 is sent on the voter's mail id.
Input: *T*, the deadline of voting

1. While CurrentTime() < *T*
2. Foreach n ϵ *N*
3. numOfVotes <-DoVotes();
4. foreach numOfVotes ϵVotes
5. votemax <-Compare(numOfVotes);
6. m<-SelectMiner();
7. bm+l<GetTrans(a);
8. *B*'->AddBlock(m,*B*,bb);
9. Foreach n ϵ *N*
10. BroadCast(n)

output:combine *s*1 and *s*2 of shares.
output:Enter captacha for verification process.
Output:if correct then confirm vote.

A method used for defending secrets of images and has a computation-free decryption process is Visual Cryptography Scheme. In (2, 2) VCS each confidential image is divided into two sub-images that is known as shares in such a way that no information can be obtained from any single share. Transparencies are printed in each share. Two shares are stacked and confidential image can be visualized by human eye without any complex cryptographic computations and this is called decryption as shown in figure below each pixel P of the confidential image is encrypted into a pair of sub-pixels in each of the two shares. [19]

Here, In Visual Cryptography there are the steps what we have used in our proposed system in two main methods for mutual authentication.

1. Image Splitting method.

In this process an input image is divided into two black and white images by their pixels homogenously. One image will go on voter's mail and other will go on election website. As we mentioned in system's work flow it is known as shares.

2. Image Merging method.

Voter will download one share what he have received on mail and will upload on election site. Then Admin will combine or merge these two shares to create a captcha.

3. Result

The application of proposed system is represented in figure 3 by comparing with existing system. Existing system maintains only data integrity through block chain. The proposed system maintains data integrity and authentication with the use of Block Chain and Visual Cryptography Scheme.

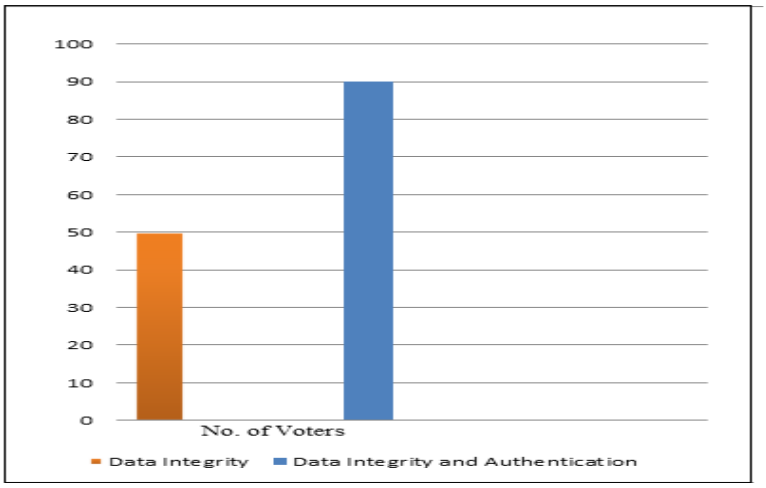

Figure 3. Comparison of existing and proposed system

Analysis is done by considering Block chain based E-voting Recording system [2] by Rifa Hanifatunnisa and Budi Rahardjo and our proposed system. In this we have calculated overall time taken for number of nodes available in the voting system. In proposed system results are recorded by using together Block chain and Visual Cryptography scheme. Hence time taken is little longer than the existing system.

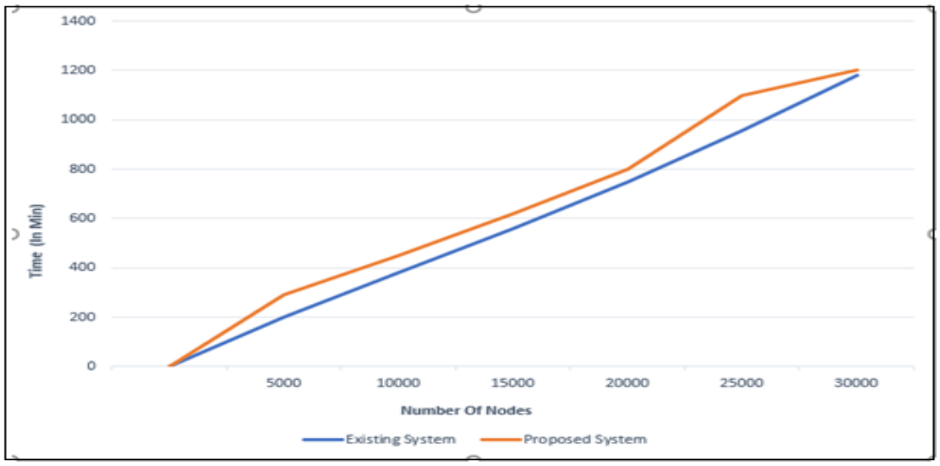

Figure 4. Analysis of Time Taken to execute the Process

4. Conclusion and Future Work

In Proposed system internet-based voting offers many benefits including less cost and more voter participation. E-Voting systems must take into account security as well as human factors, and it should make sure that they give voters with attested and natural indications of the viability of the voting process. This system mainly uses visual cryptography to provide mutual authentication for voters and election servers. In future scope Security can be enhanced by providing double authentication with addition to block chain.

References

1. Ahmed Ben Ayed, “A Conceptual Secure Block Chain-Based Electronic Voting System”, 2017 IEEE International Journal of network &Its Applications(IJNSA),03 May 2017.
2. Rifa Hanifatunnisa, Budi Rahardjo, “Block-chain Based E-Voting Recording System Design”, IEEE 2017.
3. Kejiao Li, HuiLi, HanxuHou, KedanLi, Yongle Chen, “Proof of Vote: A High-Performance Consensus Protocol Based on Vote Mechanism & Consortium Block-chain”, 2017 IEEE 19th International Conference on High Performance Computing and Communications; IEEE 15th International Conference on Smart City; IEEE 3rd International Conference on Data Science and Systems.

4. S. Nakamoto. Bitcoin: A Peer-to-Peer Electronic Cash System. 2009. Accessed: Feb. 13, 2018. [Online].
5. Maaten, E. (2004). Towards Remote E-Voting: Estonian case. Electronic Voting in Europe.
6. Azad, Muhammad & Bag, Samiran & Hao, Feng & Salah, Khaled. (2018). M2M-REP: Reputation System for Machines in the Internet of Things. Computers & Security. 79. 10.1016/j.cose.2018.07.014.
7. Supriya Thakur Aras, Vrushali Kulkarni, "Block-chain and Its Applications – A Detailed Survey", International Journal of Computer Applications (0975 – 8887) Volume 180 – No.3, December 2017.
8. Freya Sheer Hardwick, Apostolos Gioulis, Raja Naeem Akram, Konstantinos Markantonakis, "E-Voting with Block-chain: An E-Voting Protocol with Decentralisation and Voter Privacy", IEEE 2018, 03 July 2018.
9. Javheri S., Kulkarni U. (2021) The Design of Multiuser BGN Encryption with Customized Multiple Pollard's Lambda Search Instances to Solve ECDLP in Finite Time. In: Chiplunkar N., Fukao T. (eds) Advances in Artificial Intelligence and Data Engineering. Advances in Intelligent Systems and Computing, vol 1133. Springer, Singapore.
10. https://doi.org/10.1007/978-981-15-3514-7_35.
11. Kashif Mehboob Khan, Junaid Arshad, Muhammad Mubashir Khan," Secure Digital Voting System based on Block-chain Technology", IEEE 2017.
12. Huaiqing Wang, Kun Chen and Dongming Xu. 2016. A maturity model for block-chain adoption. Financial Innovation, Springer, Open Access, DOI 10.1186/s40854-016-0031-z
13. Buterin, Vitalik. 2015, On Public and Private Block-chains. [Online]https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains/
14. Guy Zyskind et. al. 2015. Decentralizing Privacy: Using Block chain to Protect Personal Data, 2015 IEEE Security and Privacy Workshops (SPW), San Jose, CA, USA, July 2015 [Online]. Available: http://dx.doi.org/10.1109/SPW.2015 Jianliang
15. Meng, Junwei Zhang, Haoquan Zhao, "Overview of the Speech Recognition Technology", 2012 Fourth International Conference on Computational and Information Sciences.
16. Carlo Blundo, University of Salerno, Alfredo De Santis and Douglas R Stinson (1998), "On the contrast in visual cryptography scheme" pp. 1-28.