ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 5, May 2019

E-Voting System Using Visual Cryptography

Akshay Hiwrale[1], Ashutosh Sharma[2], Suhasni Pandita[3],Komal Kour[4], Prof. Kanchan Wankhade[5]

Student, Department of Information Technology, Dhole Patil College of Engineering, Pune, India[1,2,3,4]

Assistant Professor, Department of Information Technology, Dhole Patil College of Engineering, Pune, India[5]

ABSTRACT: This method aims to maintain data integrity, which is protected from manipulations that should not happen in the election process. This process begins when the voting process at each node has been completed. Before the election process begins, each node generates a private key and a public key. Public key of each node sent to all nodes listed in the election process, so each node has a public key list of all nodes. When the election occurs, each node gathers the election results from each voter. When the selection process is completed, the nodes will wait their turn to create the block. Upon arrival of the block on each node, then done verification to determine whether the block is valid. Once valid, then the database added with the data in the block. After the database update, the node will check whether the node ID that was brought as a token is his or not. In the proposed system we solve existing following problems solve.

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

I.INTRODUCTION

Lately, electronic voting systems have begun being used in many countries. Estonia was the first in the world to adopt an electronic voting system for its national elections [1]. Soon after, electronic voting was adopted by Switzerland for its state-wide elections [2] and by Norway for its council election [3]. For an electronic voting system to compete with the traditional ballot system, it has to support the same criteria the traditional system supports, such as security and anonymity. An e-Voting system has to have heightened security in order make sure it is available to voters but protected against outside influences changing votes from being cast, or keep a voter's ballot from being tampered with. Many electronic voting systems rely on Tor to hide the identity of voters [4]. However, this technique does not provide total anonymity or integrity since many intelligence agencies around the world control different parts of the Internet which can allow them to identify or intercept votes.

II.LITERATURE SURVEY

Increasingly digital technology in the present helped many people lives. Unlike the electoral system, there are many conventional uses of paper in its implementation. The aspect of security and transparency is a threat from still widespread election with the conventional system (offline).Block chain technology is one of solutions, because it embraces decentralized system and the entire database are owned by many users.[1]

E-voting is a potential solution to the lack of interest in voting amongst the young tech savvy population. For e-voting to become more open, transparent, and independently auditable, a potential solution would be base it on block chain technology. Block chain technology has a lot of promise; however, in its current state it might not reach its full potential.[2]

Electronic voting has been used in varying forms since 1970s with fundamental benefits over paper based systems such as increased efficiency and reduced errors. With the extraordinary growth in the use of block chain technologies, a number of initiatives have been made to explore the feasibility of using block chain to aid an effective solution to e-voting. It presented one such effort which leverages benefits of block chain such as cryptographic foundations and transparency to achieve an effective solution to e-voting. The proposed approach has been implemented with Multi-

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 5, May 2019

chain and indepth evaluation of approach highlights its effectiveness with respect to achieving fundamental requirements for an e-voting scheme. [3]

Public block chains are open for all. Anyone can join them to post transactions and to participate in the mining and consensus process of adding new block of transaction to the block chain .These block chains usually use Proof of Work (PoW) or Proof of Stake (PoS) for consensus mechanism. Having more number of participants' works well for this model, as it further reduces the possibility of a 51% attack.[4]

III.RELATED WORK

Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System"
A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

Christopher D. Clack, "Smart Contract Templates: foundations, design landscape and research directions."
In this position paper, we consider some foundational topics regarding smart contracts (such as terminology, automation, enforceability, and semantics) and define a smart contract as an agreement whose execution is both automatable and enforceable. We explore a simple semantic framework for smart contracts, covering both operational and non-operational aspects. We describe templates and agreements for legally-enforceable smart contracts, based on legal documents. Building upon the Ricardian Contract triple, we identify operational parameters in the legal documents and use these to connect legal agreements to standardized code. We also explore the design landscape, including increasing sophistication of parameters, increasing use of common standardized code, and long-term academic research. We conclude by identifying further work and sketching an initial set of requirements for a common language to support Smart Contract Templates.

EppMaaten, "Towards remote e-voting: Estonian case"
This paper gives an overview about the Estonian e-voting system. Paper discusses how the concept of e-voting system is designed to resist some of the main challenges of remote e-voting: secure voters authentication, assurance of privacy of voters, giving the possibility of re-vote, and how an e-voting system can be made comprehensible to build the public trust.

J Paul Gibson, "A review of E-voting: the past, present and future"
Electronic voting systems are those which depend on some electronic technology for their correct functionality. Many of them depend on such technology for the communication of election data. Depending on one or more communication channels in order to run elections poses many technical challenges with respect to verifiability, dependability, security, anonymity and trust. Changing the way in which people vote has many social and political implications. The role of election administrators and (independent) observers is fundamentally different when complex communications technology is involved in the process. Electronic voting has been deployed in many different types of election throughout the world for several decades.

Muhammad Ajmal Azad, "M2M-REP: Reputation of Machines in the Internet of Things" 2017.
The Internet of Things (IoT) is the integration of a large number of autonomous heterogeneous devices that report information from the physical environment to the monitoring system for analytics and meaningful decisions. The compromised machines in the IoT network may not only be used for spreading unwanted content such as spam,

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 5, May 2019

malware, viruses etc, but can also report incorrect information about the physical world that might have a disastrous consequence. The challenge is to design a collaborative reputation system that calculates trustworthiness of machines in the IoT-based machine-to-machine network without consuming high system resources and breaching the privacy of participants. To address the challenge of privacy preserving reputation system for the decentralized IoT environment, this paper presents a novel M2M-REP (Machine to Machine Reputation) system that computes global reputation of the machine by aggregating the encrypted local feedback provided by machines in a fully decentralized and secure way.

IV.PROPOSED SYSTEM

We need transparency, authentication and provability in the voting platform. We need to assure that the people who attend the elections are real people and use correct credentials that we know in electronic environments, and we should be able to prove that any time, also we need our elections are 100% transparent as desired. So, we need to gather and check signed and time stamped data of the elections. Because, nobody should be able to change the votes after they are casted. Also, we need individuality in elections, so that nobody can vote for someone else.

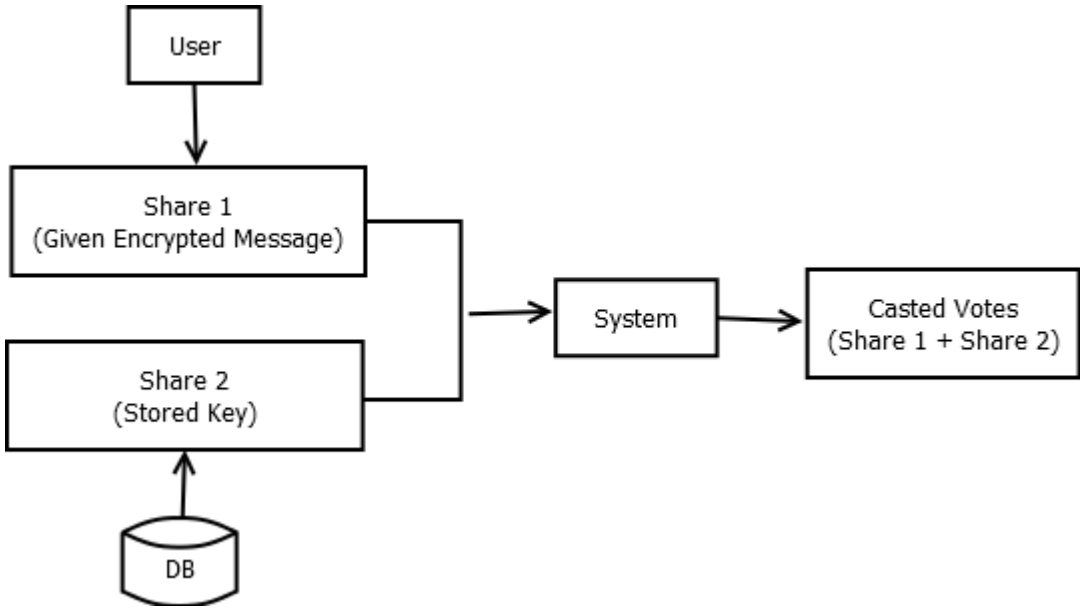

Fig. 1: System Architecture

V.MODULES

In the proposed method, election is held in full confidentiality by applying appropriate security measures to allow the voter to vote for any participating candidate.

Admin: admin can add candidate, voter, ward and election. He/she can perform update delete operation and declared result also.

Visual Cryptography: Administrator (Election officer) sends share1 to voter e-mail id before election and share 2 will be available in the voting system for his login during election. Voter will get the secret password to cast his vote by combining share 1 and share 2 using VC.

User: Voter can vote only if he/she logs into the system by entering the correct password which is generated by merging the two shares (Black & White dotted Images) using VC scheme.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 5, May 2019

VI.ALGORITHM

Visual cryptography is a cryptographic technique which allows visual information (pictures, text, etc.) to be encrypted in such a way that decryption becomes a mechanical operation that does not require a computer.
Such a technique thus would be lucrative for defines and security.
2 OUT OF 2 SCHEME
• Black and white image: each pixel divided in 2 sub-pixels
• Choose the next pixel; if white, then randomly choose one of the two rows for white.
• If black, then randomly choose between one of the two rows for black.
• Also we are dealing with pixels sequentially; in groups these pixels could give us a better result.

1. There is a (k,k)scheme with $m=2^{k-1}$, $a=2^{k+1}$ and $r=(2^{k-1}!)$
   We can construct a (5,5)sharing, with 16 sub pixels per secret pixel and, using the permutations of 16 sharing matrics.
1. In any (k,k) scheme, $m \geq 2^{k-1}$ and $a \leq 2^{1-k}$
2. For any n and k, ther is a(k,n)visual cryptography scheme with m=log n $2^{O(k\log k)}$, a= $2^{\Omega(k)}$

VII.RESULTS

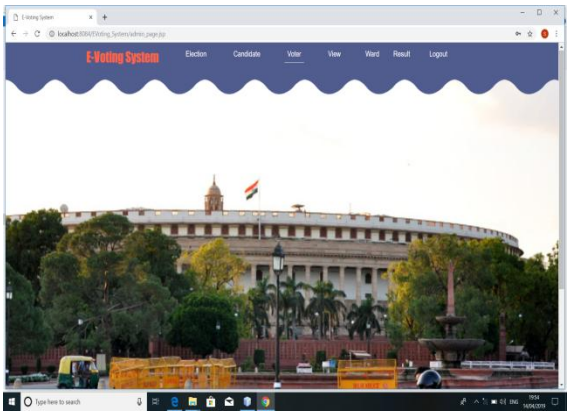

Fig. 2: Home Page

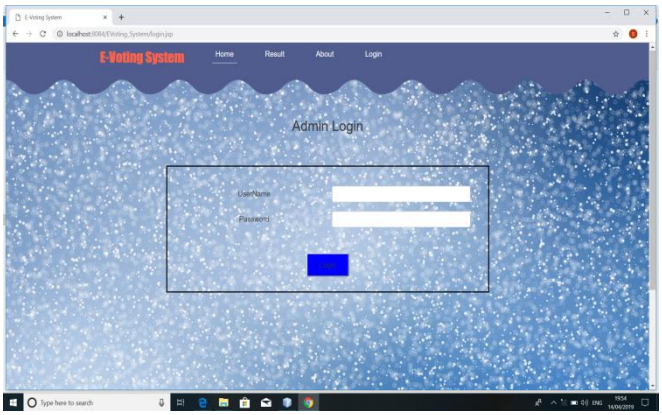

Fig. 3: Admin Login

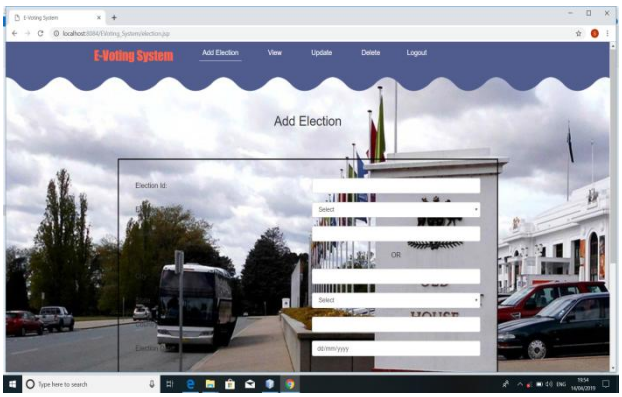

Fig. 4: Add Election

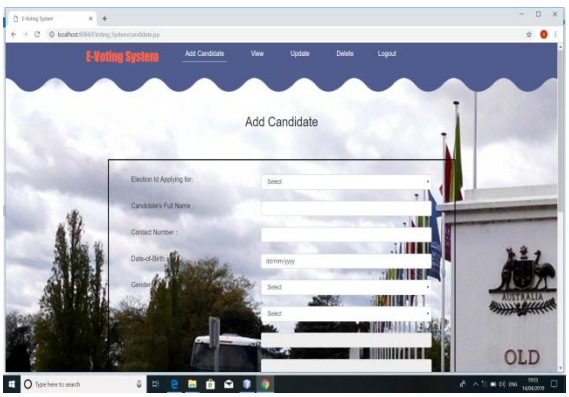

Fig. 5: Add Candidate

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 5, May 2019

VIII.CONCLUSION AND FUTURE WORK

In the proposed system internet-based voting offers many benefits including lowcost and increased voter participation. Voting systems must consider security and human factors carefully, and in particular make sure that they provide voters with reliable and intuitive indications of the validity of the voting process. Our propose system uses visual cryptography to provide mutual authentication for voters and election servers.

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. RifaHanifatunnisa, 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. Ali KaanKoç, EmreYavuz, Umut Can Çabuk, GökhanDalkilic," Towards Secure E-Voting Using Ethereum Blockchain",2018 IEEE.
5. 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.
6. Freya Sheer Hardwick, ApostolosGioulis, Raja NaeemAkram,KonstantinosMarkantonakis," E-Voting with Block-chain: An E-Voting Protocolwith Decentralisation and Voter Privacy",IEEE 2018,03 July 2018.
7. KashifMehboob Khan, Junaid Arshad, Muhammad Mubashir Khan," Secure Digital Voting System based on Block-chainTechnology",IEEE 2017.
8. Huaiqing Wang, Kun Chen and DongmingXu. 2016. A maturity model for block-chain adoption. Financial Innovation, Springer, Open Access, DOI 10.1186/s40854-016-0031-z
9. Buterin, Vitalik. 2015, On Public and Private Block-chains. [Online]https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains/
10. Zyskindet. al. 2015. Decentralizing Privacy: Using Block chain to Protect Personal Data, 2015 IEEE Securityand Privacy Workshops (SPW), San Jose, CA, USA, July 2015 [Online].Available: http://dx.doi.org/10.1109/SPW.2015
11. Thomas Monoth, Babu Anto P (2009), "Achieving optimal Contrast in Visual Cryptography schemes without pixel expansion". International Journal of Recent Trends in Engineering, Vol 1, No 1, pp. 468-471.
12. A B Rajendra and H S Sheshadri (2012), Study on Visual Secret Sharing Schemes Using Biometric Authentication Techniques, AJCST, Vol 1, pp.157-160.
13. Anusha MN and Srinivas B K (2012), "Remote Voting System for Corporate Companies using Visual Cryptography," vol. 2, pp. 250–251.
14. Pallavi V Chavan, Mohammad Atique, and Anjali R Mahajan, (2011) "An Intelligent System for Secured Authentication using Hierarchical Visual Cryptography-Review", ACCE Int J. on Network Security, vol. 02, No. 04.pp. 7-9 .
15. JianliangMeng, JunweiZhang,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