DIGITIZED ELECTION CONTROL PROCESS USING BLOCKCHAIN TECHNOLOGY

Rashmi S
Asst Prof, Department of CSE,
Dayananda Sagar University
Bangalore
rashmi-cse@dsu.edu.in

Dr Anbunathan R
Researcher
Computer Society of India
Bangalore
anbunathan.r@gmail.com

Srinivasa Raju V
Director
Alykas Innovatiions(OPC) Pvt. Ltd
Visakhapatnam
director@alykasinnovatiions.com

Abstract:

The right to vote is said to be the most valued characteristic of any democratic country. In today's world, Automation has a huge impact in every aspect of life and so in the field of elections. However, common man has less trust in electronic based elections. This would also impact on the number of voters. Hence, a need for a digitized election process is realized, starting from the campaigning process, voting and counting process and analysis post-election process. The proposed voting system unite together three latest technologies namely, Blockchain , IOT and AI.

Keywords: Digital Voting, Blockchain , RFID, IOT, AI

1.   INTRODUCTION

In a republic self-governing nation, elections play a significant role. Any country is truly democratic, if the elections conducted to choose their representative are best characterized as "Free and Fair". Free elections means that an eligible citizen must feel free to take a decision on whether to vote or not. The citizen should also be able to choose their candidate without any force or fear. It is equally necessary that the citizen be ensured that his/her choice remains a secret. Furthermore, Fair Elections are associated with the campaigning, rallies and meetings by contesting political parties. All registered contestants must have equal rights to carry out the above. It also means that all votes are counted. Results announced are precise.

In a Traditional voting system, it is difficult to assure "Free and Fair" Elections [1]. Over decades, attempts are made to apply computer technology enhance its potential. Traditional voting system consists of Paper-based voting, Direct Recording Electronic (DRE) voting using Electronic Voting Machines (EVM)[2], Internet voting etc., In India, since 2004 EVMs developed by Bharat Electronics Limited (BEL) and Electronics Corporation of India Limited (ECIL) are being used. However, existing systems including Internet voting system are vulnerable to hacking, tampering and proved to be less secure.

EVM has two main components: a Ballot system and a control system. With the help of a control system, an electronic ballot is issued to the voter inside the booth so that he can secretly cast the vote. EVMs operate on batteries. They have the capability to record utmost 2000 votes.

However, the EVM system has been identified with some limitations [3]. Recent researchers have shown that EVMs can be hacked and tampered. It is vulnerable to virus attacks resulting is complete destruction of recorded data. EVM do not completely support physically challenged people as it uses touch screen technology. They are not manufactured in our country. It means that complete control of the unit does not lie with our country.

Over the past decades, one of the major concerns has been to ascertain an Electronic Election system using cryptography and other related techniques. Although some research work is carried out in this regard, there has been no

complete secure decentralized solution developed so far.

2.   PROPOSED SYSTEM

Blockchain[4] is the new technological development in the industry. Blockchain Technology is the union of key technologies that include cryptography, decentralized processing, distributed database and others that are most desirable for an electronic electoral system. Blockchain is an ordered data structure that holds a block of transactions. The sequence of blocks is linked to one another. Attempts have been made to take advantage of this technology in African and European countries although they do not provide a complete solution. However, in India, as already mentioned EVMs are still in use.

A digitized election system should desirable of the following qualities.

1) Authentication : Only eligible citizens of the nation should be liable to vote
2) Scam-free: Voter should be allowed to vote exactly once avoiding fake/multi votes
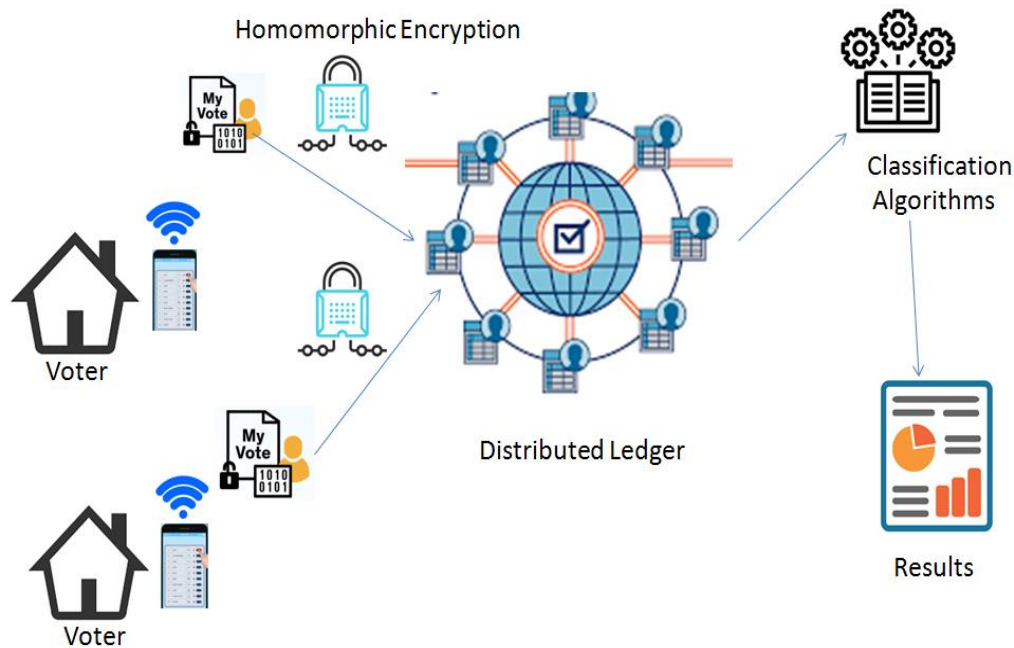3) Anonymous : The voting details of any voter should remain undisclosed

Figure 1: System Architecture of the Proposed Voting System

4) User-Friendly interface: Any common man should be able to understand the voting process easily
5) Transparency : The complete election procedure should be open to public to gain their trust

6) Secure :   Votes   should   be irreversible
7) Decentralized :   The   election process should support a democratic government
8) Recordable: After the elections, the entire process should be auditable to aid counting process

3.   METHODOLOGY

The proposed work plans to work in the area of Blockchain Technology [5] integrated with IOT and AI. to provide a secure electronic voting terminal. An Electronic voting System with the above listed objectives aims to use the below mentioned methodologies. The entire election system can be divided into three phases.

1.   Pre-Election Process
2.   Voting Process
3.   Post –Election Process

3.1   PRE-ELECTION PROCESS

The Pre-Election Process helps the political parties in the process of campaigning. Each of the registered candidates' profile appears in the voting device. The candidate can post their past achievements in the device. They can also display the list of proposals or promises of how they are going to serve for nation during their period. The citizens can 'like' their achievements or 'comment' on their negative deeds.

An overall rating for the candidate is computed by AI [6] based classification algorithm. The number of likes for each promise is analyzed by AI based classification algorithm [7]. The candidate profile is analyzed and classified based on the age group of the people 'liked', place/area of people 'liked', promises for which they have been 'liked' etc.,

AI based algorithms are used to identify right candidates based on candidates social

activities. The candidate information is collected from social media, media, news papers. The algorithm classifies the good things, bad things, educational qualification, speeches etc. automatically. It gives weight age to each good and bad thing what candidate has done in the past. The final credibility score is displayed against each candidate; this helps people to select the right candidate.

Also, AI algorithms help post analysis after election is completed. Based on the votes, algorithm identifies the promises of the candidate, development plans of the candidate, and parties' agenda on the development of country which are accepted by people. Each promise or agenda is rated by the algorithm and priority of the agenda can be identified from the agenda. This helps the new government to prioritize the implementation of the promises and agenda.

Based on this analysis, people can select the right candidate. The selected candidate information is stored in Blockchain

3.2 VOTING PROCESS

Authentication can be provided by employing a Security system that precisely identifies and verifies an individual using multifaceted system based on biometric and RFID [8,9] system. Such a system can be linked with the AADHAR or Voter ID of an individual. An IOT based voting device is provided to each individual home. Such a IOT based voting device allows interconnection of devices nationwide using internet. In a smart city, wifi is always available. This facilitates the citizens to cast their vote at home. The device is authenticated by voting commission. Each device is registered with a user name and password. Members of the family are authenticated by bio-metric and RFID based system.

Blockchain, the new trend in technology can be integrated with the IOT based voting that uses smart contracts. The IOT based device is connected to the voter

blockchain. The data is stored in blockchain technology using cryptography techniques in a merkle tree.

Homomorphic encryption can be ideally used as it retains the structure and relationship between the elements involved though encrypted. A Merkle tree aids to encode data in a blockchain safely and efficiently. It is even more secure as it validates transactions devoid of entire blockchain downloading. Each voter transaction is secured through private and public keys.

3.3 POST –ELECTION PROCESS

Post- Election Process consists of the counting process and result announcement. Each vote casted by the members of the family are securely transmitted and counted. Ideally, there should be no room for errors. Once validated by the election commission, results can be displayed in each machine location wise.

4.   ADVANTAGES OF THE PROPOSED SYSTEM

The following are the advantages listed for the proposed system.

- IOT enables the voting can be done from each home
- Blockchain enables the safety and security of the system
- Cryptography and RFID technology enables authentication of right voting person avoiding illegal votes
- AI based system enables to select right candidate to be selected

5.   CONCLUSION

The need for a secure, flawless decentralized digital voting system has been realized over decades, the reason being the limitations in currently used EVMs and cryptographic techniques. The latest technology advances in the area of Blockchain , IOT and Artificial Intelligence can be exploited to achieve the intended goals. IOT based device integrated with RFID technology confirms the authenticated voters. Blockchain Technology ensures secure transmission of each vote. AI algorithms can be used by voters to choose the right candidate for their nation.

References

[1] Md. Awal Hossain Mollah, University of Rajshahi, "Free, Fair and Credible Election and Democratic Governance in Bangladesh: How far the Dream of Success?" Review Pub Administration Manag, an open access journal, ISSN: 2315-7844, Volume 4 , Issue 2 , September 15, 2016

[2] http://kanglaonline.com/2012/03/how-can-electronic-voting-machines-evm-be-manipulated

[3] https://www.worldblaze.in/advantages-disadvantages-of-electronic-voting-machines-evm

[4] Mahdi H. Miraz, Maaruf Ali, "Applications of Blockchain Technology beyond Cryptocurrency", Annals of Emerging Technologies in Computing (aetic) Vol. 2, No. 1, 2018

[5] Ahmed Ben Ayed , "A Conceptual Secure Blockchain- Based Electronic Voting System", International Journal of Network Security & Its Applications (IJNSA) Vol.9, No.3, May 2017

[6] Sumit Das, Aritra Dey, Akash Pal, Nabamita Roy, "Applications of Artificial Intelligence in Machine Learning: Review and Prospect", International Journal of Computer Applications (0975 – 8887) Volume 115 – No. 9, April 2015

[7] Osisanwo F.Y. , Akinsola J.E.T. , A wodele O., Hinmikaiye J. O., Olakanmi O., Akinjobi J, "Supervised Machine Learning Algorithms: Classification and Comparison", International Journal of

Computer Trends and Technology(IJCTT) –Volume 48,Number 3, June 2017

[8]   Guangyu   Zhu ; Gul N.   Khan, "Symmetric   key   based   RFID authentication protocol with a secure key-updating scheme",   26th IEEE Canadian Conference on Electrical and Computer Engineering   (CCECE), 10.1109/CCECE.2013.6567741, Added to IEEE *Xplore*: 25 July 2013

[9] Inayat Ali , Sonia Sabir , Zahid Ullah, "Internet of Things Security, Device Authentication and Access Control: A Review", (IJCSIS) International Journal of Computer   Science   and   Information Security, Vol 14, No 8, August 2016