International Journal of Current Engineering and Technology
E-ISSN 2277 – 4106, P-ISSN 2347 – 5161

Available at http://inpressco.com/category/ijcet

Research Article

Smart E-Voting System using Block Chain

Mr. Santosh Kumar and Prof. Abhijit Patankar

Department of Computer Engineering Alard College of Engineering & Management, Marunji

Received 10 Nov 2020, Accepted 10 Dec 2020, Available online 01 Feb 2021, **Special Issue-8 (Feb 2021)**

Abstract

India is the world's largest democracy with a population of more than 1 billion. India is having voters of more than 668 million and covers 543 parliamentary constituencies. Voting is the bridge between the ruled and government. The previous couple of years have brought a renewed focus on to the technology used in the balloting process. The current vote casting machine has many protection holes, and it is tough to show even easy security properties about them. The current vote casting machine has many protection holes, and it is tough to show even easy security properties about them. A vote casting system that can be proven accurate has many concerns. There are a few motives for a central authority (government) to use electronic systems are to increase elections activities and to reduce the elections expenses. Still there's some scope of work in electronic voting system because there may be no way of identification by the electronic voting machine whether the consumer is authentic or now not and securing electronic vote casting device from miscreants. The proposed System is to develop a Compatible vote cast machine with excessive safety through the usage of Blockchain technology in order increase security and transparency among the users.

Keywords: *Electronic Vote cast System, voter ID,Vote, Security, Block Chain;*

Introduction

A block-chain is a decentralized, distributed and public digital ledger that is used to record transactions across many computers so that any involved record cannot be altered retroactively, without the alteration of all subsequent blocks.

A block-chain is a database that is shared across a network of computers. Once a record has been added to the chain it is very difficult to change. The records that the network accepted are added to a block. Each block contains a unique code called a hash. It also contains the hash of the previous block in the chain.

Voting, whether traditional ballet based or electronic balloting (e-vote casting), is what modern democracies are build upon. In recent years voter apathy has been increasing, mainly among the more youthful computer/tech savvy generation. E-balloting is pushed as a potential solution to attract young voters.

For a robust e-balloting scheme, a number of functional and security requirements are specified which include transparency, accuracy, audit-ability, machine and data integrity, secrecy/privacy, availability, and distribution of authority. Block-chain technology is supported by a distributed network consisting of a large number of interconnected nodes. Each of these nodes have their own copy of the distributed ledger that contains the full records of all transactions the network has processed. There is no single authority that controls the network.

B. Motivation

By developing e voting through block-chain technology we can take care of chores of casting and counting votes. By developing this E-voting help us in many different levels of usability, security, efficiency and accuracy. This innovative type of E voting can increase voter participation either from increase accessibility, decrease cost and difficulty or any other method clearly as it benefit to the larger community through the E-voting system. E-voting system also has ability to reduce fraud by eliminating the opportunity for ballot tampering.

Objectives

1. To overcome the problem of multiple votes to same candidate.
2. To reduce the man power for counting the votes.
3. Helps to generate digital counting

Review of Literature

This paper, proposed secure voting system with fast voting results through RFID based biometric voting system. In this paper, there are two verification steps involved. First, RFID tag is used which contains the verification data which is already stored in LPC 2148. Second, the Fingerprint scanner is used to check whether the RFID is belonging that particular person

or not. The drawback of this paper is cost maximized due to use of RFID method. [1].
In this paper, used of Aadhaar card provided by UIDAI with QR code present in it. Online instead of offline mode and storing the voting data to secured online server. Results can be displayed by admin after entering user id and password [2].
The proposed method is to build a Smart voting system using fingerprint recognition technology that allows any voter in INDIA to cast the vote to their respective constituency from anywhere in INDIA by going to their nearest voting booth in the place of stay. Also to develop a secure smart voting system based on biometric recognition. Provides the voter to vote from any region with in India to their Residential Constituency from the nearest Voting Booth with a secure voting process without neglecting to vote. [3].
This paper, proposes protected voting system to avoid the unlawful voting. The authentication of an individual are made using biometric and capability of the voter is affirmed using the Aadhaar. In this system the data stored in the Aadhaar card act main criteria for authentication and conformation. The security is provided through biometrics such as fingerprint. The fingerprint information stored in the Aadhaar is taken as the reference and used for authentication at the time of voting [4].
Basic electronic machine which is used nowadays has some laggings like multiple vote casting from one member and invalidity of votes are checked automatically. To reduce these disadvantages the smart automatically and fingerprints are used to reduce multiple vote casting in simple way [5].
This paper has shown the possibility of establishing EVoting protocol based on public-key encryption cryptosystem. The security of the proposed E-Voting depends on RSA public key encryption protocol. It allows the voter to vote from his/her own personal computer (PC) without any extra cost and effort. This protocol is proposed to replace the unreliable previous voting system, since voters feel justifiably confident that their votes will be counted [6]. This system provides security from all type of attacks, when vote is travelling from voting client to voting server from their experimentation. These attacks include security threats from passive as well as active intruder. For authentication of voter instead of USERNAME, if we can use thumb impression of voter or capture photo of his/her face and compare it with photo stored in our database, it will be more secure [7]. In this paper, a block-chain-based voting system. It needs time to popularize block-chain for a voting system as it is a novel idea and voting itself is a crucial matter in a democratic country [8]. The proposed model is more secure than other models and it is suitable for use in major elections on a large scale. After casting a vote with NCVVS system, the voter receives a confirmation email containing the ballot fingerprint (and also the fingerprint of the election) calculated by standard hash function SHA (256) [9].
The proposed work is based on the block-chain technology, which remove all the threats from the communication link. It is a decentralized system, contain hashing and encryption concept for providing the security [10].

Proposed Methodology

The proposed work is based on the Blockchain technology. It is a decentralized system, contain hashing and encryption concept for providing the security.In our system Blockchain Concepts are applied to Online Voting System when we are developing an online voting system by taking advantage of block Chain concepts with web interface.

Advantages of Proposed System:

1. Time Saving Working load reduced.
2. Information available at time and Provide security for data.3. This is simple, safe secures methods that minimum of time.
4. Using Blockchain Concepts the calculated time is reduces. 5. Integrity of result is granted, preventing the chance of false voting.

A. Architecture

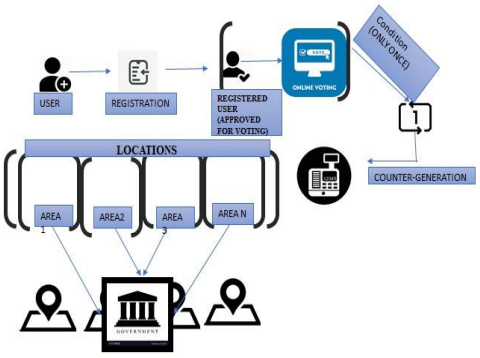

Fig. 1. Proposed System Architecture

Explanation:
1) Registration:- Register a new voter/candidate with their legitimate id i.e.(government identification proof).
2) Verification:- Confirmation of the Voter/Candidate which can be connected to system.
3) Conditions:1. The voter can cast only once.
2. The timing of casting the vote are between (7 A.M. To 5 P.M).
4) Counting:- Generation of votes in terms of counting the votes one by one without fail.
A. Module Explanation
Module 1 - Administrator (Admin):- Admin Add new Candidate, modify Candidate details and check user(Voter) are legal or not
Module 2 - User (Voter):- Voter can cast the vote to the candidate.
B. Algorithms explanationAdvanced Encryption Standard:

1) Input:
2) 128 bit /192 bit/256 bit input(0,1) 3)secret key(128 bit)+plain text(128 bit).
4) Process:
5)10/12/14-rounds for-128 bit /192 bit/256 bit input
6)Xor state block (i/p)
7)Final round:10,12,14
8)Each round consists:sub byte, shift byte, mix columns, add round key.
9)Output:
10)cipher text(128 bit)

C. Mathematical Model

1. Mathematical equation in Advanced Encryption Standard:

Initialization: password,key,time,salt:string time ←− *get time input* ←− (*password*) *key* ←− *salt* + *time*
Encryption:
Ciphertext ←− *AESEncrypt*(*password,key*) *output*(*ciphertext*) Decryption:
key ←− *salt* − *time*
$forasmuchtolerancegiventime$
$ifkey = get\_time$
$key \longleftarrow salt + time$
plaintext ←− *AESDecrypt*(*ciphertext,key*) *endif endfor output*(*plaintext*)

D. System Requirements

1. Hardware Requirement:

Processor:- Dual core/Intel i3
Speed:- 1.8 GHz
RAM:- 2 GB (Min)
Hard Disk:- 100 GB
Key Board:- Standard Windows Keyboard
Mouse:- Two or Three Button Mouse
Monitor/LCD:- SVGA/LED

2. Software Requirement:

Operating System:- Windows 7/8/10
Application Server:- Apache Tomcat7
Front End:- HTML, JSP, CSS
Scripts:- JavaScript
Database:- My SQL 5.0
IDE:- Eclipse Oxygen
Coding Language:- Java 1.8

Result and Discussion

Experiments are done by a personal computer with a configuration: Intel (R) Core (TM) i5-6700HQ CPU @ 2.60GHz, 16GB memory, Windows 7, MySql Server 5.1 and Jdk 1.8.

In our system, The first aspect of our design is the registration process, verifying a voter is essential in establishing security within the system.

Once any voters completed her/his vote, the block will be created, which will be publicly verifiable and spread over the network.

After completion of the Blockchain no one will do any modification into the block. If an attacker wants to do any modification into the block, the hash value of the block will change and the effect of the modification will reflect into the whole Blockchain. Our model ensures that one voter gives only one vote, no one will allow to give two votes.

Lastly, the vote count automatically generates.

Result between Algorithms:

S.No	Algorithm	No. of Voters	Rate of Vote counts	Result
01	Proposed System	30	30	90%
02	Existing System	30	24	83%

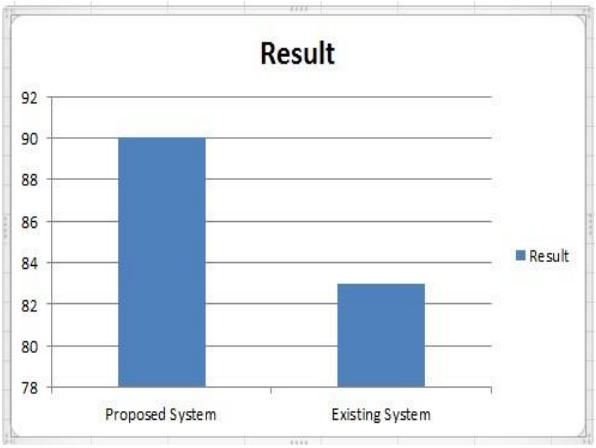

Fig. 2. Comparison graph

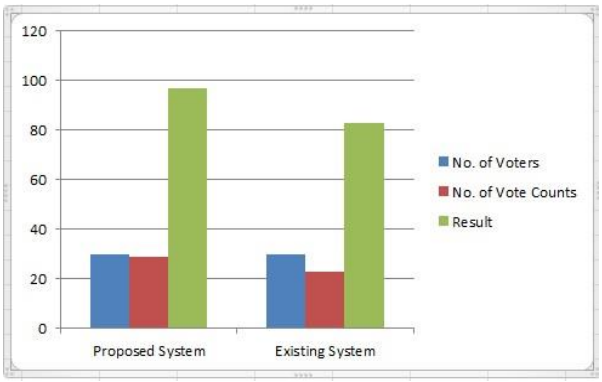

Fig. 3. Algorithm Comparison graph

Conclusion

This paper described, an virtual Voting device for small to medium sized Internet-based public opinion systems that gives privacy of vote, voter's authentication, auditability, security, double-balloting prevention, fairness vote casting device from manipulating the authenticated voters voting choices.

Acknowledgment

The authors would like to thank the researchers as well as publishers for making their resources available and teachers for their guidance. We are thankful to the authorities of Savitribai Phule University of Pune and concern members of CPGCON2020 conference, organized by, for their constant guidelines and support. We are also thankful to the reviewer for their valuable suggestions. We also thank the college authorities for providing the required infrastructure and support. Finally, we would like to extend a heartfelt gratitude to friends and family members

References

[1] J.Deepika, S.Kalaiselvi, S.Mahalakshmi, S.Agnes Shifani, "Smart Electronic Voting System Based On Biometric Identification-Survey", International Conference on Science Technology Engineering Management (ICONSTEM).
[2] Ravindra Mishra, Shildarshi Bagde, Tushar Sukhdeve, J. Shelke, "Review on Aadhaar Based Voting System using Biometric Scanner", International Research Journal of Engineering and Technology(IRJET)
[3] Girish H S, Gowtham R, Harsha K N, Manjunatha B, "Smart VotingSystem", International Research Journal of Engineering and Technology(IRJET).
[4] K. Lakshmi, R. Karthikamani, N. Divya "Aadhar Card based smart e-voting system", International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 8958, Volume-8, Issue-2S, December 2018.
[5] G.Saranya, R.Mahalakshmi, J.Ramprabu, "Smart Electronic Voting Machine survelliance", International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 8958, Volume-8, Issue- 2S, December 2018.
[6] Ashish Singh, Kakali Chatterjee, SecEVS : Secure Electronic Voting System Using Blockchain Technology, International Conference on Computing, Power and Communication Technologies (GUCON)Galgotias University, Greater Noida, UP, India. Sep 28-29, 2018.
[7] Cosmas Krisna Adiputra, Rikard Hjort, and Hiroyuki Sato, A Proposal of Blockchain-based Electronic Voting System, Second World Conference on Smart Trends in Systems, Security and Sustainability.
[8] Mr. Abhijit Janardan Patankar, Dr. Kshama V. Kulhalli, Dr. Kotrappa Sirbi, "Emotweet: Sentiment Analysis tool for twitter", 2016 IEEE International Conference on Advances in Electronics, Communication and Computer Technology (ICAECCT) Rajarshi Shahu College of Engineering, Pune India. Dec 2-3, 2016.
[9] Abhijit J. Patankar, Kotrappa Sirbi, Kshama V. Kulhalli, "Preservation of Privacy using Multidimensional K-Anonymity Method for Non-Relational Data", International Journal of Recent Technology and Engineering (IJRTE) ISSN: 2277-3878, Volume-8 Issue-2S10, September 2019.
[10] Jena Catherine Bel.D, Savithra.K, Divya.M, "A Secure Approach for E-Voting Using Encryption and Digital Signature, International Journal of Engineering Development and Research.
[11] Ashraf Darwish and Maged M El-Gendy, "A New Cryptographic Voting Verifiable Scheme for E-Voting System Based on Bit Commitment and Blind Signature", International Journal of Swarm Intelligence and Evolutionary Computation.
[12] Hayam K. Al-Anie, Mohammad A. Alia and Adnan A. Hnaif, Evoting protocol based on public-key Cryptography, International Journal of Network Security & Its Applications (IJNSA),Vol.3, No.4, July 2011.