SecEVS : Secure Electronic Voting System Using Blockchain Technology

Ashish Singh
Computer Science & Engineering
National Institute of Technology Patna
Patna-800005, Bihar, (India)
Email: ashish.cse15@nitp.ac.in

Kakali Chatterjee
Computer Science & Engineering
National Institute of Technology Patna
Patna-800005, Bihar, (India)
Email: kakali@nitp.ac.in

***Abstract*—In todays digital environment, the voting system move from paper based to a digital system. A digital e-voting system have many properties such as transparency, decentralization, irreversibility, and non-repudiation. The growth in digital e-voting system arises many security and transparency issues. In this paper, we used the blockchain technology in digital e-voting system to solve the security issues and fulfill the system requirements. It offers new opportunities to deploy a secure e-voting system in any organization or country. The solution is far better as compared to other solution because, it is a decentralized system, contain the results in the form of bit-coins, having different locations. We will also analyze the security of our proposed voting system, which shows our protocol is more secure as compared to other solutions.**

***Keywords*—E-voting system, Block-chain, Hashing, Merkle hash**

I. Introduction

Recent days, electronic voting system is an interested research topic. Voters can give their vote from remote location with the help of some smart devices like smart-phones, tablet etc. to find out the best suitable candidate in an organization, country, or university. The movement from paper based voting system to electronic system brings new enhancement such as real time counting, instant result, environment friendly, transparent, anonymity, less error and decentralized. With the development in the digital voting system, there are a number of security issues, flaws, and attacks are coming [1]. In any electronic voting system the authentication, anonymity, accuracy, consistency, and verifiability are the basic system requirements [2]. It was first introduced by david shaum. This system used public key cryptography and blind signature to maintain the privacy and anonymity between the voters and ballots.

In the previous years, several research has been done regarding the electronic voting system by using the blockchain technology [3–10]. In 2015, Zhao and Chan [8] proposed a reward and penalty based e-voting system in which a good user get the rewards and bad behavior user get the penalty. But, this scheme has some limitations. To remove such limitations the author [11] proposed e-voting protocols using Trusted Third Party (TTP) to make system more easily implemented and controlled. But, the low security in TTP become system more vulnerable. The Estonia is the first country in the world to support the electronic voting system [12, 13]. In 2005 and 2007, the country used online voting and the primary criteria of the of the voting system is the secrecy of the whole system. But, in Estonian I-voting system faces the transparency issue during the election time [14]. These voting systems are centralized. Thus, the DDOS attacks are easily possible on the system. Some attacker and agencies are accessing the wide range of voter confidential data and computing power to analyze the voting results. Norwegian also implemented the electronic voting system similar to the Estonia voting system [15]. But, by using the cyber attack any attacker gets the information about the voting system and made the confidential information publicly available. The Scytl [16] design a new voting system which is different from the previous two Estonia and Norwegian electronic voting system. This system is implemented in 2015 in new south wales for the voting. In this process, the voter need to first register in the voting system. After the successful registration, the voters login into the system. After the login the voter check and ensure that the vote is completely entered into the voting database without alteration. Wolchok et al. [17] developed a new pilot electronic voting system by using the mail service. In this concept, the voter gives own vote by using the mail. The main specialty of this project is, it is a dummy project to test the security and robustness of the system. But, due to many critical security issues, the system is failed and never used for any official voting purpose [17].

From the above literature work, we have found many security issues, which are very common in the electronic voting system. Thus, to fulfill the security requirements, we have design more secure and robust electronic voting system for university election, which fulfill the following criteria:

- We have designed an electronic voting system in the university campus to find the best suitable candidate by using the concept of blockchain technology.
- This model not only conduct the voting procedure without human intervention, but also provide the security against all the major attacks.
- The proposed electronic voting system is validated by the system security analysis.

978-1-5386-4491-1/18/$31.00 ©2018 IEEE

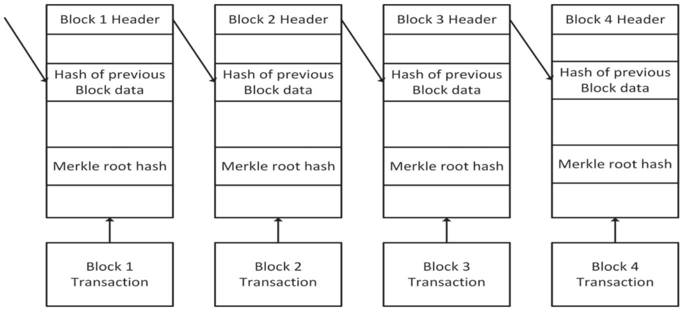

Fig. 1: Blockchain structure [5]

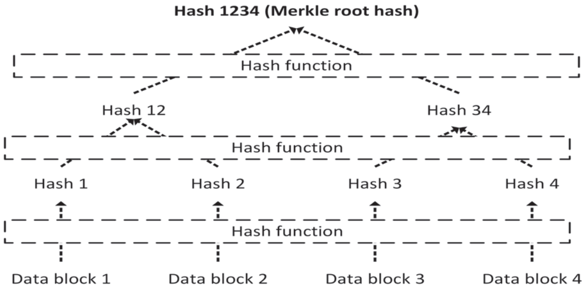

Fig. 2: Merkle root hash

The rest of the paper is organized as follows: the Section II describes the background of the work. The detail discussion of the proposed electronic voting system is describe in the Section III. In Section IV, we have discussed security analysis of the system. Finally, the paper is closed with the conclusion in Section V.

II. Background

In this section, we have discussed the background of the blockchain technology and other related terms, which is help to us to design a more secure and robust electronic voting system.

A. Participants

- **Voters:** It contain set of all eligible voters defined by V=$\{v_1, v_2, v_3.....v_n\}$, where n is the total numbers of eligible voters.
- **Organizers:** It contain set of all Election Organizer (EO)=1, which is responsible for managing and verifying the voter identity during the election.
- **Inspectors:** It is responsible for inspect the organizer behavior and limit the power of the organizer.

B. Blockchain

It was first introduced by Satoshi Nakamoto [18]. It was implemented on peer to peer payment system, where no need of a centralized authority. The first application of the blockchain is the Bitcoin, which is used as a currency in the Internet world. It is an ordered data structure, which contains set of transaction in the form of block. Each block is linked with the previous block to maintain the chain structure. The whole block is secured with the cryptographic algorithm, encryption technique and hash algorithm. The first block is the foundation of the chain. The block header is used for the identification of the block contain the hash by using Secure Hash Algorithm (SHA-256). The SHA-256 hash algorithm will take any size of plaintext as an input and produce a hashed output which is 256-byte binary value. Each block header contain the hash information of the previous block, merkle root hash, and signature. The block data contain the encrypted voter data [19]. The complete structure of the blockchain is shown in Figure 1.

C. Merkle root hash

The initial block of the blockchain is known as the “block 0”. It doesn’t contain any hash information about the previous block. When “block 0” is initialized the creation of “block 1” is started. After completion of the “block 1”, it is attached with the “block 0”. This process is continue until a single hash remains. This single hash is known as the merkle hash. The generation of merkle root hash in our proposed system is shown in Figure 2.

III. Proposed electronic voting system

A. Network model

The proposed network model is consider for an electronic voting system of a university campus. In the university, there are four zones: East, west, north, and south zone. Each zone contains number of colleges. The complete network model is shown in Figure 3. Now, the university administrator wants to elect one student leader from the contestants. Each college starts the voting process. Each vote under one college creates one block and each block join together to make a blockchain. After completion of the voting, blockchain of each college under one zone join together to make a zone level blockchain. Now, each zone level blockchain join together to make a university level blockchain. Now, we get the complete blockchain. The committee will consider this single blockchain for vote count.

B. Framework of digital voting system

The proposed electronic voting system uses the blockchain technology, which is explain in the Algorithm 1. This system is made based on the two concepts: hashing and encryption. The proposed structure of the blockchain is shown in Figure 4. The system contain the following components: participants=$\{$Voters$\}$, organizers=$\{$Colleges under the university$\}$, inspectors=$\{$university election commission$\}$, encryption algorithm=$\{$AES,DES$\}$, Hash algorithm=$\{$SHA-256$\}$, voting server. All the components of the proposed system is shown in Figure 5. The following steps are involved when a voter wants to give her/his vote during the election time.

Pre-voting steps*:*

1) The voters need to register with the voting system. In the first step, the voter choose a password for login and a private key for signing.
2) After the successful registration with the system, the voter receive a voter ID.

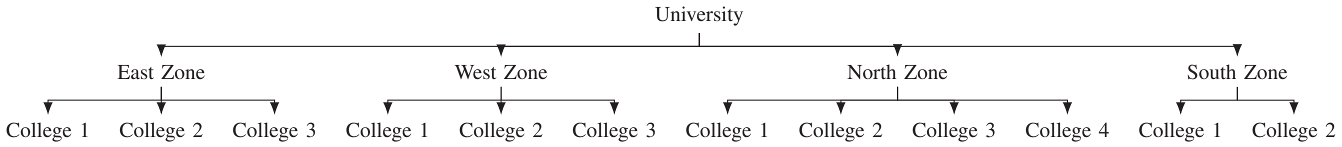

Fig. 3: University network model for electronic voting system

Algorithm 1 Electronic Voting System

```
procedure INPUT:(voter User Id, voter Password)
    OUTPUT: Complete vote in the form of blockchain
    BEGIN
    The voter registered with the voting system.
    Get the voter ID, choose the password and private key.
    if (voter Id == registered_voter Id) and (voter is eligible) then
        Enter your password.
    else
        voter is not registered or he is not eligible.
    if (Password is correct) then
        Open the candidate choosing page and choose the candidate.
    else
        Enter the correct password.
    Encryption of voting data- $ENCRYPT_{pubkeyUEC}(vote)$
    Signing the encrypted data - $SIGN_{Vprikey}(E_{pubkeyUEC}(vote))$
    Generation of the block BLOCK(block header+encrypted block data).
    Total no. of votes - $\sum_{i=1}^{n} zone_i = \sum_{i=1}^{n}\sum_{j=1}^{k} CL_{ij} = \sum_{i=1}^{n}\sum_{j=1}^{k}\sum_{p=1}^{v} BLOCK_{ijp}$, where n is the total number
of zone, k is the total number of college in a particular zone, v is the total number of blocks in a particular college.
    END
```

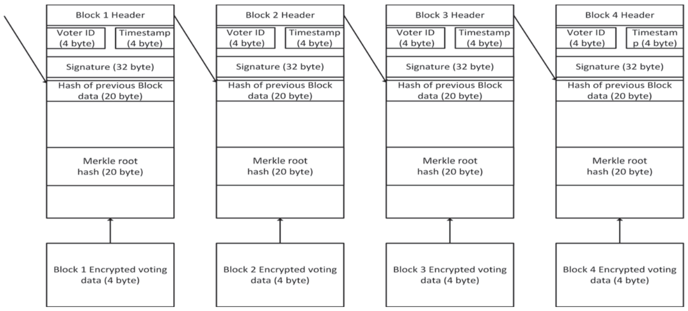
Block 1 Header
Voter ID (4 byte)
Timestamp (4 byte)
Signature (32 byte)
Hash of previous Block data (20 byte)
Merkle root hash (20 byte)
Block 1 Encrypted voting data (4 byte)
Block 2 Header
Voter ID (4 byte)
Timestamp (4 byte)
Signature (32 byte)
Hash of previous Block data (20 byte)
Merkle root hash (20 byte)
Block 2 Encrypted voting data (4 byte)
Block 3 Header
Voter ID (4 byte)
Timestamp (4 byte)
Signature (32 byte)
Hash of previous Block data (20 byte)
Merkle root hash (20 byte)
Block 3 Encrypted voting data (4 byte)
Block 4 Header
Voter ID (4 byte)
Timestam p (4 byte)
Signature (32 byte)
Hash of previous Block data (20 byte)
Merkle root hash (20 byte)
Block 4 Encrypted voting data (4 byte)

Fig. 4: Proposed Blockchain structure

Voting steps:

1) During the election time, the voter first need to login into the system with the help of voter ID and password.
2) After the successful login, the voter is verified by the college election organizers by using the eligible voter list (voter database).
3) If the voter is eligible for giving the vote, then the 2^{nd} page opens, which carry the details of contestants. Now, the voter will give her/his vote.
4) The vote are encrypted by using the public key of University Election Commission (UEC).
5) The encrypted vote are signed by the voter private key.
6) Now, the generated voter information is stored into the voter server through the Internet. This is the first block of the blockchain.
7) For generation of the block data, steps 3 to 6 repeated continuously until election time is over.

Post-voting steps:

1) After the election is over at the college level, blockchain of each college are joint together for preparation of the zone level blockchain.
2) The zone level blockchain comes together for preparation of the university level blockchain.
3) Now, the election committee check all the votes from the blockchain and declare the final result of the election.

IV. System security analysis

In this section, we have analyzed our proposed electronic voting system in term of security, privacy, and attacks. The proposed system is implemented on Netbean (Integrated Development Environment) using Java programming language. The following aspects we have are considered during the designing of the framework.

A. Privacy of the data transmission

According to the proposed e-voting system, the university level blockchain will be stored into the voting server. During the data transmission all the related information is stored in the block and this block is secure against different attacks and

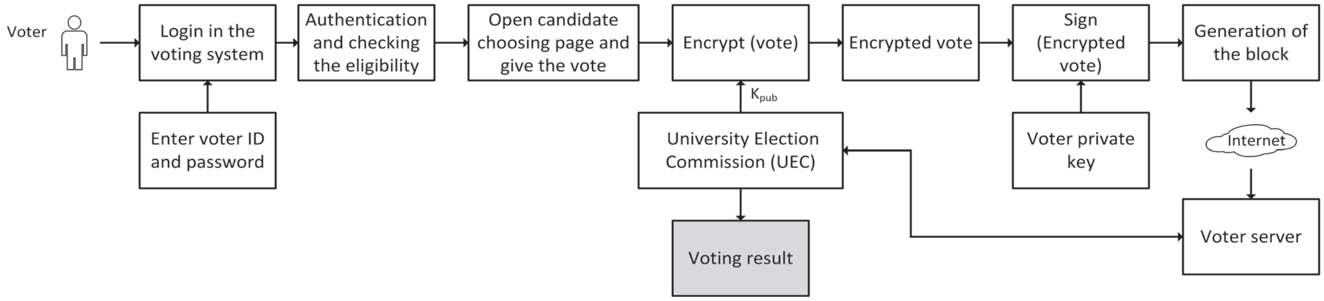
Voter
Login in the voting system
Enter voter ID and password
Authentication and checking the eligibility
Open candidate choosing page and give the vote
Encrypt (vote)
K_{pub}
University Election Commission (UEC)
Voting result
Encrypted vote
Sign (Encrypted vote)
Voter private key
Generation of the block
Internet
Voter server

Fig. 5: Framework of proposed electronic voting system

threats. Somehow, if any user gets the blocks, the attacker is not able to get any meaningful information because all the data will present in hashed and encrypted form.

B. Voter confidentiality

To provide the confidentiality of the voter identity, we have used the SHA-256 hash algorithm and encryption algorithm. The information related with the votes is kept in encrypted form. So, that if the block is tempered then also the attacker will not be able to know the vote. Thus, this protocol maintains the voter confidentiality.

C. Duplication and forgery into the system

We have created a blockchain to overcome the forgery and duplication cases during the voting. To ensure that no one will able to give two votes, we have used unique voter ID for unique identification. The blockchain contains the hash of the previous block, signature and merkle root hash. The signature is used to prove the authenticity and integrity of the transaction data. The hash of the previous block is used to maintain the data integrity in the blockchain. The merkle root hash tells the root (origin) of the voter data. Thus, our proposed e-voting system resist the duplication and forgery issue.

D. System level threats and attacks

As discussed before, the proposed e-voting system is based on the encryption and hashing. If an attacker performs any type of attacks into the system, the system will identify and block them. For instance, any attacker performs the data modification attack on one block. The hash of the modified block will change and it will reflect into the whole blockchain. The sybil attack is also not possible because the system will not allow to do duplicate registration or duplicate voting or multiple time voting.

E. Storage space

The simulation of the proposed system is done on the system level. The consideration of required storage space for conducting the e-voting is playing very important role in real world scenarios. During the voting, for storage of one voting transaction (block), we need 84 bytes. In this 84 bytes, the block contains voter ID, timestamp, signature, hash of previous data, merkle root hash, and encrypted voting transaction data.

V. Conclusion

We have mitigated all the possible threats and attacks into the electronic voting system. The proposed work is based on the blockchain technology, which remove all the threats from the communication link. It is a decentralized system, contain hashing and encryption concept for providing the security. Our proposed system ensures that only registered and eligible voter is able to give own votes. 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. The voter has facility to register only once into the system. The voter ID is used for unique verification and checking the eligibility of the user. Thus, our model ensures that one voter gives only one vote, no one will allow to give two votes. The system security analysis shows that the system is more robust and secure against existing attacks.

Acknowledgment

The author would like to acknowledge the Ministry of Electronics & Information Technology (MeitY), Government of India for supporting the financial assistant during research work through “Visvesvaraya PhD Scheme for Electronics & IT”.

References

[1] Douglas W Jones. Threats to voting systems. In *NIST workshop on threats to voting systems*, 2005.

[2] Yi Liu and Qi Wang. An e-voting protocol based on blockchain.

[3] Taher ElGamal. A public key cryptosystem and a signature scheme based on discrete logarithms. *IEEE transactions on information theory*, 31(4):469–472, 1985.

[4] Tadayoshi Kohno, Adam Stubblefield, Aviel D Rubin, and Dan S Wallach. Analysis of an electronic voting system. In *Security and Privacy, 2004. Proceedings. 2004 IEEE Symposium on*, pages 27–40. IEEE, 2004.

[5] Rifa Hanifatunnisa and Budi Rahardjo. Blockchain based e-voting recording system design. In *Telecommunication*

Systems Services and Applications (TSSA), 2017 11th International Conference on, pages 1–6. IEEE, 2017.

[6] Lijun Wu, Kun Meng, Shuo Xu, Shuqin Li, Meng Ding, and Yanfeng Suo. Democratic centralism: A hybrid blockchain architecture and its applications in energy internet. In *Energy Internet (ICEI), IEEE International Conference on*, pages 176–181. IEEE, 2017.

[7] Stefano Bistarelli, Marco Mantilacci, Paolo Santancini, and Francesco Santini. An end-to-end voting-system based on bitcoin. In *Proceedings of the Symposium on Applied Computing*, pages 1836–1841. ACM, 2017.

[8] Zhichao Zhao and T-H Hubert Chan. How to vote privately using bitcoin. In *International Conference on Information and Communications Security*, pages 82–96. Springer, 2015.

[9] Laure Fouard, Mathilde Duclos, and Pascal Lafourcade. Survey on electronic voting schemes. *supported by the ANR project AVOTÉ*, 2007.

[10] Jinn-Ke Jan, Yu-Yi Chen, and Yi Lin. The design of protocol for e-voting on the internet. In *Security Technology, 2001 IEEE 35th International Carnahan Conference on*, pages 180–189. IEEE, 2001.

[11] Kibin Lee, Joshua I James, Tekachew Gobena Ejeta, and Hyoung Joong Kim. Electronic voting service using block-chain. *The Journal of Digital Forensics, Security and Law: JDFSL*, 11(2):123, 2016.

[12] Ahmed Ben Ayed. A conceptual secure blockchain-based electronic voting system. *International Journal of Network Security & Its Applications*, 9(3), 2017.

[13] Ülle Madise and Tarvi Martens. E-voting in estonia 2005. the first practice of country-wide binding internet voting in the world. *Electronic voting*, 86(2006), 2006.

[14] J Alex Halderman, Harri Hursti, Jason Kitcat, Margaret MacAlpine, Travis Finkenauer, and Drew Springall. Security analysis of the estonian internet voting system. *Nr. May.*, 2014.

[15] Ida Sofie Gebhardt Stenerud and Christian Bull. When reality comes knocking norwegian experiences with verifiable electronic voting. *Electronic Voting*, 205:21–33, 2012.

[16] J Alex Halderman and Vanessa Teague. The new south wales ivote system: Security failures and verification flaws in a live online election. In *International Conference on E-Voting and Identity*, pages 35–53. Springer, 2015.

[17] Scott Wolchok, Eric Wustrow, Dawn Isabel, and J Alex Halderman. Attacking the washington, dc internet voting system. In *International Conference on Financial Cryptography and Data Security*, pages 114–128. Springer, 2012.

[18] Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system. 2008.

[19] Hiroki Watanabe, Shigeru Fujimura, Atsushi Nakadaira, Yasuhiko Miyazaki, Akihito Akutsu, and Jay Junichi Kishigami. Blockchain contract: A complete consensus using blockchain. In *Consumer Electronics (GCCE), 2015 IEEE 4th Global Conference on*, pages 577–578. IEEE, 2015.