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

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

Research Article

Securing post-e-voting data through Blockchains

Pooja Patil and Prof. A. G. Phakatkar

Computer Engineering Pune Institute of Computer Technology, Pune, India poojakpatil3.pp@gmail.com

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

Abstract

Conducting fair and transparent elections is an integral part of any democratic country. Elections add more financial burden to the country as it includes more manpower, post voting security and counting of the same ballot papers. In electronic voting machines, all the process right from the conduction of elections, to providing security and counting votes, is seamless conduct without any hassle. So the biggest democratic countries like India also rely on Electronic voting machines, provided that the physical security of the voting machines has the same burden as of ballot papers. Securing the votes in the electronic voting machine is the most important task. Various techniques are implemented to secure the votes. Blockchain is one of the trending technology for securing the data in the distributed paradigm more efficiently. So this research paper provides a way to secure the post voting data using the reverse circle cipher technique. The whole process is powered by 16-byte hash keys obtained by processing the SHA 256 hashing algorithm and Bit mapping technology.

Keywords: *Blockchain, E-Voting, Reverse Circle Cipher, SHA 256, Multi Linear Pairing.*

Introduction

E-voting is one of the most important implementations of technology in governmental procedures[9]. This is because voting using ballot is archaic practices that are remnant of the last era. The ballot voting even though it is very old, is still being practiced across the world in one way or the other. It is the majority of the countries that are still using this old practice that is highly limited and filled with a lot of loopholes and is inefficient. Elections conducted by ballots are unsustainable as they use lots of resources and lead to the devastation of forests leading to degradation of climate[7]. The physical ballot is also subject to various environmental elements and can experience weather changes across the country. The ballots also need to be physically transported from one place to another, this leads to multiple cases of the voting data being tampered in transit. There are also possibilities that the ballot boxes will get damaged during transportation which would lead to the ballot being discarded. All the work in a physical ballot system is done manually, this will eventually introduce inconsistencies in the whole process, that is flawed from the beginning. The introduction of e-voting is necessary as there has not been a substantial improvement in the voting procedure over the years[1]. Many candidates have informed about their loss of faith in the secure nature of the Electronic Voting Machines which led the government analyzing the machines and putting them up for tampering to prove the machine's security. Many researchers have generated reports on the accuracy and the security of the Electronic Voting Machines that are being used by the government for the election process. Therefore, the application of the E-Voting paradigm is necessary as it would eliminate all these drawbacks and also increase the security, reliability, and efficiency of the whole process[9]. Due to the increase in demand for security, there has to be a significant increase in the number of solutions to match the demand. The conventional technique of encryption can be used in such a situation[3]. Encryption alone is not a viable solution, because if encryption is compromised, and the attacker modifies the database and encrypts it back again using the same procedure, any tampering will still not be evident to the election officials. Therefore, just the implementation of the encryption standard is not a comprehensive solution to the problem of security of the electronic voting data. There is a growing need for a technique that can keep track of the various modifications done on the data, like a digital notary ,etc. This is where the paradigm of blockchain comes into the picture. Blockchain is a platform that secures any data that is provided and ensures tamper-proof security of that data[3]. This tamperproofing is through the use of hash keys and block chaining. The first block in the blockchain is called as the genesis block. The subsequent blocks store the data in the block and the header stores the hash key of the current block as well as the hash key of the previous block. Every block is interconnected with each other through the use of

hash keys. This enables much better control over the whole data and the tampering done on the data[8]. Tampering on any of the blocks will change the hash key. This modified hash key will not be present in the next block and the chain will break. Therefore, the blockchain paradigm is one of the most efficient and secure applications that indicates there was any tampering done on the database. Along with blockchain, an efficient encryption algorithm is used to secure the data. Blockchain is a decentralized framework that utilizes a network, so AES and DES are not compatible as they perform multiple passes on the data. This makes the data incompatible for a real-time transfer. Other techniques such as RSA utilize a large number of bits that further increase the computational complexity of the system as well as the space complexity[6]. Therefore, an efficient encryption technique is needed to achieve functionality while keeping the complexities in check. Reverse Circle cipher encryption technique has all the properties that are needed to implement a secure electronic voting system. The reverse circle cipher is a block encryption technique that utilizes the effective combination of reversal transposition and circular substitution to achieve efficient encryption[6]. RCC along with the blockchain platform can be used which can achieve a high level of security in electronic voting machines. In this paper, section 2 is dedicated to the literature review of past work, section 3 provides motivation and finally, section 4 concludes the paper.

2. Literature Review

This section briefs us about the analysis, results, and work done by many authors as follows

H. Ge expresses concern over the fact that even after years of research there is no technique for the development of an effective E-voting system that is secure[1]. The authors have developed the Koinonia E-voting system that is highly secure against attacks. The main drawback of this technique is that the authors have not considered the practice of voteselling and voter coercion in the proposed methodology.

S. Desai explains that privacy risk is always a threat to the system. Blockchain paradigm is capable of reducing data tampering and leakage through secure sharing. Therefore, the authors in this paper extended the blockchain framework to EVoting that would enable much finer control over the security of the voting data, simplifying the counting of votes and transportation costs at the same time [2]. The main drawback of this paper is that the proposed technique has not experimented with performance evaluation.

L. Babenko states that it is about time for an E-Voting system to be developed to keep up with the world, upgrade the voting process, simplify and reduce the costs at the same time. The authors have designed a technique for E-voting that utilizes blind intermediaries and a parser that can understand the nature of the cryptographic protocols that are being used [3]. The technique has been verified using the Avispa automated verifier using the CAS+ language. The main drawback of this methodology is the increased computational complexity of the system.

M. Nassar explains that the process of conversion of the physical ballots into an E-Voting system is quite a difficult path. The authors have developed a toy voting scheme that utilizes the non-colluding parties and homomorphic encryption for preserving the privacy of the whole process [5]. The experimental results indicate that the proposed methodology maintains voter anonymity and election integrity throughout the voting process.

E. Issac has proposed a cryptographic technique known as Reverse Circle Cipher, which utilizes diffusion and confusion to implement reversal transposition and circular substitution [6]. The encryption is highly secure and effective in real-time. The main limitation of this paper is that the authors have implemented the technique only on the plaintext.

X. Yang utilized the ElGamal cryptosystem to secure the ranked-choice E-Voting paradigm [7]. This technique allows efficient verification of the votes. The experimental analysis conveys that the system is capable of conducting a highly secure election procedure. The main drawback of this system as that it assumes the honesty of one authority which can be its downfall.

K. Wang devised an architecture named SecNet that allows secure sharing of data with the help of blockchain and Artificial intelligence [8]. The main drawback of this system is that the authors have not utilized the blockchain framework for implementing secure access control mechanisms.

A. Qureshi tried to solve the problem of security by implementing SeVEP, a secure E-Voting system that authenticates voter, enables effective verifiability and prevents double voting [9]. The main drawback of the system is the increased computational cost for authentication.

Motivation

Conducting safe and secure elections is a challenging job because most of the electoral agencies are dealing with huge voting data. So the challenge to protect votes after the voting process becomes more tedious and a financial burden to the country. Thus to secure this in the most trusted manner blockchain is found useful. This motivated the use of blockchain in securing the voting data.

Proposed System

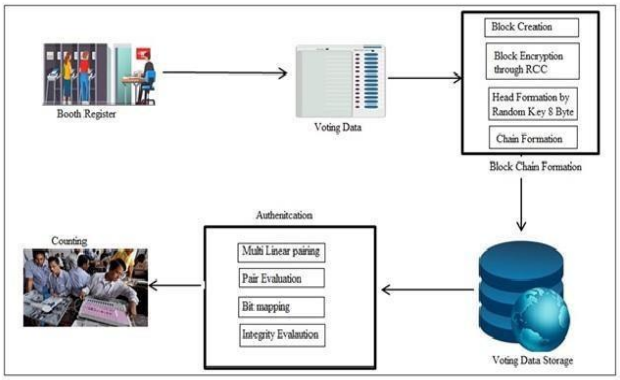

Figure 1: System Overview

The proposed model for securing the post voting data of election is depicted in the above figure 1 and the steps that are carried out to deploy the same are narrated below.

Step 1: *Simulation of Voting* - This is the very first step of the proposed model, where the whole model is simulated in an environment developed in Java. Initially, N number of booths are created randomly using the random function, so that a database table is allocated for each booth. Every voting booth is associated with a booth officer whose user name and passwords are created by the random selection of the names and password characters. Each booth database tables consist of fields like booth no, serial no, symbol name ,and vote.
On the other hand, all the candidate data is being entered in the provided interactive user interface along with the party name, symbol, candidate name, age, sex and other required attributes. Once all the candidates are nominated for carrying out the elections, then the voting process is triggered out using the random function. All the votes are encrypted using Reverse circle cipher encryption and then they are stored in the database.

Step 2: *Reverse Circle Cipher Encryption* – The casted votes in the past step is subjected to an encryption process using the reverse circle cipher encryption technique. Initially, this data is in the form of the string and subjected to create blocks to store in a list. Then, based on the indices of the blocks in the list their characters are being rotated to replace with the ASCII codes of the other characters which are obtained by the MOD function of the key. Then concatenation of these encrypted string yields the resulted in encrypted cipher String that will be stored in the database

Step 3: *Multi Linear Pairing* – In this process, the generated number of booths is divided into the fixed division. Then each and every division are subjected to parallel computation for the pairing process to estimate the data integrity using the blockchain technique.

Step 4: *Data Integrity through Blockchain*– This step uses the encrypted string of the stored booth tables based on the divided multi-linear divisions. Then it is subjected to hash generation using SHA 256 bit hashing algorithm. Random characters are selected using the hash key rotation and random character selection to form the moderate length of the keys.
This finally yields the blockhead and block body of the blockchain. The process is being continued for all the booth data of the particular division to get the final divisional head key. If there are N divisions then this method provides N divisional head keys which are then stored in the database for the purpose of Integrity evaluation.
In this process, previous and current divisional head keys are subjected to the integrity evaluation. If any inequalities between the current and previous head keys are encountered, then the integrity violations are identified to generate the required alert.

The Blockchain formation can be dipicted in the below shown algorithm 1

ALGORITHM 1: BlockChain Formation for Booths

// Input: Booth Set B_{SET}
// Output: Authentication Key A_{KEY}
1: Start
2: Initialize Previous Hash Key as P_K=NULL
3: **For** i = 0 to size of B_{SET}
4: BoothName= $B_{SET[i]}$
5: B_{CONT} = getBoothContent(BoothName)
6: CH_K = hashKey(B_{CONT}) [Current Hashkey]
7: $H_K = P_K + CH_K$
8: $P_K = CH_K$
9: $A_{KEY} = H_K$
10: **End For**
11: **return** A_{KEY}

Result and Discussions

The presented technique designed to facilitate electronic voting through the use of blockchain is developed using Java programming language on the NetBeans IDE. The machine used to develop this application has a Windows operating System equipped with 4GB of RAM and 500 GB of storage. The database responsibilities are handled by the MySQL database.
The proposed methodology has been tested extensively for its performance on various parameters. The experimental evaluation results have been detailed below.

Encryption and Decryption Time performance

The proposed model is subjected to encryption and decryption performance time evaluation and the obtained results are tabulated in Table 1 given below.

Table 1: Encryption and Decryption time performance

Number of Characters	Encrytion Time In Milliseconds	Decrytion Time In Milliseconds
15	2	2
1804	16	15
2707	30	31
3114	47	51
4939	53	50
5648	62	59
6516	63	62
8093	75	78
8770	78	78
9878	93	97

In below figure 2, it clearly indicates that time taken for encryption and decryption is not directly proportional to the number of characters. Thus it is a good sign about the encryption and decryption module, as it has been properly deployed in the selected domains

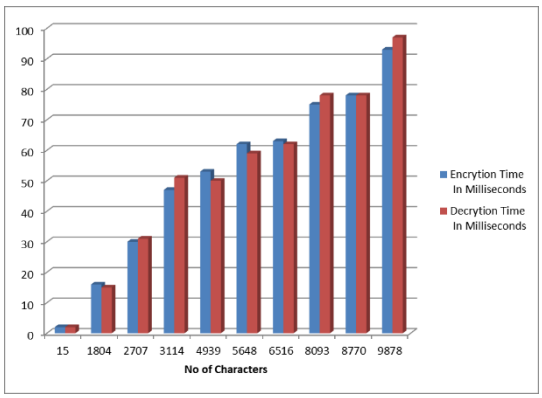

Figure 2: Encryption and Decryption Time

Conclusion and Future Scope

This paper successfully simulates the process of e-voting in a well-organized and designed, simulated environment system using Java programming language. To secure the EVoting data proposed model utilizes the reverse circle cipher encryption algorithm which outperforms than that of many traditional encryption algorithms like Elliptical cryptography techniques.

Whole E-voting data is being secured, the proposed model divides the number of booths into divisions to perform the parallel computation in order to increase the efficiency of the integrity evaluation through blockchain. This paper promises to achieve less time complexity due to parallel computation, data integrity evaluation process and thus is secured thoroughly.

In future , this research topic can be enhanced to work on real-time elections for Electronic voting machines at the village level or even in higher geographical areas.

References

[1] H. Ge et al, "Koinonia: Verifiable E-Voting with Longterm Privacy", Association for Computing Machinery, ACM, 2019.

[2] S. Desai et al, "Untampered Electronic Voting in Entertainment Industry: A Blockchain-based Implementation", The 20th Annual Conference on Information Technology Education SIGITE, 2019.

[3] L. Babenko et al, "Cryptographic Protocols Implementation Security Verification of The Electronic Voting System Based on Blind Intermediaries", Association for Computing Machinery, ACM, 2019.

[4] A. Goel et al, "Knapsack Voting for Participatory Budgeting", ACM Trans. Econ. Computing, Article 8, July 2019.

[5] M. Nassar et al, "sElect: Secure Election as a Service", 23rd International Database Engineering & Applications Symposium, IDEAS 2019).

[6] E. Issac et al, "Reverse Circle Cipher for Personal and Network Security", International Conference on Information Communication and Embedded Systems (ICICES), 2013.

[7] X. Yang et al, "A Secure Verifiable Ranked Choice Online Voting System Based on Homomorphic Encryption", IEEE Access, 2018.

[8] K. Wang et al, "Securing Data with Blockchain and AI", IEEE Special Section on Artificial Intelligence in Cybersecurity, 2019.

A. Qureshi et al, "SeVEP: Secure and Verifiable Electronic Polling System", IEEE Access, 2019