Managing E-voting Process through Blockchain

1.Prof.Shreesudha Kembhavi,Professor,IT Dept,G.S.Moze collage of Engineering,Balewadi, Pune
2.Anuja Pisal,Student,IT Dept,G.S.Moze collage of Engineering,Balewadi, Pune
3.Manasi Phadatare,Student, IT Dept,G.S.Moze collage of Engineering Balewadi,Pune
4. Rutuja Badhe,Student,IT Dept,G.S. Moze collage of Engineering, Balewadi, Pune

Abstract— **Conducting fair and transparent elections are the integral part of any democratic country. This exercise of conducting elections is a vital task for the election agencies of the countries along with the law enforcement agencies. Still now many countries are in the world is depending on ballot paper pattern for conducting the elections more efficiently. But this is not always the smart idea of conducting elections as using of ballot paper for conducting the elections may add more financial burden as it includes the more manpower in the process of conduction of elections, post voting security and counting of the same ballet papers. However, this is not the case in electronic voting machines, where all the process right from the conduction of elections, providing security and counting all the process is seamlessly conduct without much more hassle. The biggest democratic countries like India also rely on Electronic voting machines, providing the physical security of the voting machines is having the same burden as of ballot papers. Electronic voting machines are always having a threat of data tampering in mass numbers. So securing these votes in the electronic voting machine is a most important task in conduction of the elections. Blockchains are the trending technology for securing the data in the distributed paradigm more efficiently. So this research article provides a secured way to provide security for the post voting data in a controlled simulated environment using Blockchain. And the whole process is powered by the 16 byte hash keys obtained by processing the SHA 256 hashing algorithm and Bit mapping technology.**

Keywords— ***Blockchain, E-Voting, SHA 256, Bit mapping***.

I. Introduction

E-voting as a concept is one of the most important implementations of technology in governmental procedures. This is due to the fact that the voting mechanism using Ballot voting is one of the most archaic practices that is a remnant of the last era. The Ballot voting even though it is very old, is still being used 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 generally an inefficient process.

With physical ballots, the voters have to physically stand in a line and wait for their turn. With a large amount of population, the physical process takes a significant amount of time. Every year there are reports of various elderly people and others suffering from ailments have been waiting in the sun too long to have a sunstroke. Many elderlies get asphyxiated in the large crowds and ultimately succumb to their injuries. The process of physical ballots is highly troublesome and can be fatal for the physically disabled and the elderly.

The physical ballot is also subject to various environmental elements and can experience weather changes across the country. This is problematic as if the water during rains gets inside the box, it would ruin the votes and would need to be discarded, which would lead to a substantial loss to everyone involved in the voting process. 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.

The physical ballot votes also need to be counted in order to define the majority for the elections and declare a winner. The physical counting of votes is a long process that requires the votes to be segregated first into the different candidates and then the votes are physically counted. The possibility of an error being introduced is particularly high as there are humans counting the data and the segregation process also could lead to a wrong counting and the loss of some slips as the number of slips being counted is really large.

All the work in a physical ballot system is done manually, this is a great way to introduce inconsistencies in the whole process which is flawed from the beginning. The application of E-Voting is highly necessary as there has not been a single substantial improvement in the voting procedure over the years. Even though there has been a large growth in terms of electronics that are being manufactured nowadays, but they haven't allowed for an improvement in this sector.

There have also been various reports on the accuracy and the security of the Electronic Voting Machines that are being used by the government for the election process. Many candidates have informed about their loss of faith in the secure nature of the Electronic Voting Machines which led to the government analyzing the machines and putting them up for tampering to prove the machine's security. 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.

Due to an increase in the demand for increased 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, but just encryption is not a viable solution. This is due to the fact that even if the 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. This is a concerning fact as the encryption is considered a foolproof alternative to achieving security, but a determined attacker, after gaining access to the encryption keys can tamper the electronic voting data without a trace.

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. The blockchain technique was introduced by a group of researchers in the 1990s. Blockchain is a platform that secures any data that is provided and ensures tamper-proof security of the said data. This tamper-proofing is through the use of hash keys and block chaining.

The blockchain paradigm was designed for use in creating a digital notary or similar services where the time stamping of the documents of data is needed. This is due to the fact that the blockchain paradigm has the capability to prevent any modifications to the data once it's stored on the platform. This is through the clever use of hash keys. The blockchain did not gain as much popularity when it was introduced and was quickly forgotten. Until Satoshi Nakamoto utilized the blockchain platform and its immense security to introduce bitcoin - a crypto currency, which got increasingly popular and pushed blockchain into the limelight.

This reignited the interest of the researchers in the blockchain platform. The data stored on the blockchain is encrypted into the form of a block and ahead, where the block contains the actual data and the head contains the hash key of the stored data. The hash key is nothing but the data about the data that is stored in the block.

The first block in the blockchain is called as the genesis block. The subsequent blocks store the data in the block and the head stores the hash key of the current block as well as the hash key of the previous block. This way 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. As any 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.

II. Literature Review

This section of the literature survey eventually reveals some facts based on thoughtful analysis of many authors work as follows.

H. Ge expresses concern over the fact that even after years of research there hasn't been a technique for the implementation of an effective E-voting system that is secure [1]. Most of the approaches that have been proposed have been concentrated on achieving the privacy of the immediate data. Therefore, the authors have proposed a technique that utilizes the adversary models and analyses the various different threats to the e-voting systems. After the analysis, 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 including the practice of vote-selling and voter coercion in the proposed methodology.

S. Desai explains that there has been a large-scale increase in the number of electronic devices in this decade. But the privacy risk is always maintained, therefore, the Blockchain paradigm is capable of reducing data tampering and leakage through secure sharing. Therefore, the authors in this paper extend the blockchain framework to the E-Voting paradigm to enable much finer control over the security of the voting data and also simplifying the counting of the votes as well as transportation costs at the same time [2]. The main drawback of this paper is that the proposed technique has not been experimented on for the purpose of performance evaluation.

L. Babenko states that it is about time for an E-Voting system to be developed to keep up with the world as well as upgrade the voting process and simplify and reduce the costs at the same time. As physical voting has not been upgraded for a long time and the E-voting system can help save a lot of resources. Therefore, to ameliorate this effect 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.

S. Bag describes that the use of an E2E or End to End encrypted E-Voting system is highly useful in implementing higher security and also maintaining the integrity of the voting process. This is the motivation for the authors for presenting an innovative technique for a Borda count based voting system using DRE named DRE-Borda [4]. The presented technique eliminates the use of Tallying authorities and can be a highly convenient implementation of the E-Voting paradigm. The system addresses security concerns by implementing an E2E system that is verifiable. The limitation of the system is that it does not support complicated rank-based voting schemes.

A. Goel expresses that there has been a shift in the people's mentalities over the past decade, where the concept of direct democracy, wherein the citizens vote on the various different policy-making decisions and express their opinions to the government. Therefore, to implement a convenient, secure and cost-effective voting scheme, the authors have presented Knapsack Voting, which has the capabilities to provide various different settings such as surpluses, deficits, and revenues that can help the voters understand the policy that they are going to vote for by using a strategy proofness result [5]. The experimental results provide empirical results that demonstrate the superiority of the presented concept.

M. Nassar explains that the process of conversion of the physical ballots into an E-Voting system is quite a difficult path. This is due to the reluctance of the voters to shift to another unfamiliar concept as there is a lower amount of trust in a newly developed scheme. Therefore, 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 [6]. the experimental results indicate that the proposed methodology maintains voter anonymity and election integrity throughout the voting process. The main drawback of this paper is that the authors have not utilized the Blockchain framework to secure their voting data efficiently.

R. Raghunandan explains that the most important feature to be considered while sharing information is the security of that information. Therefore, the author state that there are a plethora of ways to secure information and most of the techniques revolve around the paradigm of cryptography and mainly RSA algorithm which has a slew of limitations such as Weiner's attack and integer factorization [7]. Therefore, the researchers utilize Pell's equation variables and prime numbers for the purpose of key generation. The experimental results conclude that the proposed key generation technique has improved upon the RSA algorithm to improve the security and reliability of the key generation algorithm.

X. Yang introduces the various different techniques that are being used the world over for the purpose of conduction Electronic voting on various elections. The authors declare that this is one of the most efficient ways to conduct an election as it reduces the need for extensive amounts of paper this is basically wasted. The election process also increases pollution across the city by a large margin. Therefore, the author shave utilized the ElGamal cryptosystem to secure the ranked-choice E-Voting paradigm [8]. This technique also allows for efficient verification of the votes obtained. The experimental analysis conveys that the system is capable of conducting a highly secure election procedure. The Amin drawback of this system as that it assumes the honesty of one authority which can be its downfall.

Fridrick P. states that there is a growing need for the implementation of an effective and secure E-Voting application as the physical ballot process is very old and desperately needs an upgrade. The Physical ballot voting is also very limited and contributes greatly to the environmental degradation, therefore an alternative E-Voting Paradigm must be ventured. Therefore, to ameliorate these effects, the authors have proposed a methodology of utilizing a distributed ledger scheme called Blockchain to secure the E-Voting system [9]. The methodology has not been implemented to perform an experimental analysis yet. The authors state that the proposed methodology has the potential to reduce costs while increasing the security of the system.

K. Wang elaborates on the various different techniques that have been used traditionally for the purpose of securing data. Due to the large advancements in the electronics industry, there is a large influx of electronic devices in the market. This leads to a large number of users that are generating useful data every day that can be used for various artificial intelligence applications. But most of the times the users do not wish to share their data with the concerns over safety. Therefore, the authors have devised an architecture named SecNet that allows for the secure sharing of data with the help of Blockchain and Artificial intelligence [10]. The main drawback of this system is that the authors have not utilized the blockchain framework for implementing secure access control mechanisms.

A. Qureshi explains that the E-Voting paradigm is one of the most essential concepts that need to be applied to the various paper ballot elections, this is due to the fact that this paradigm allows for greater convenience to the users and also decreases the impact of the voting process on the environment. The main concern of the E-Voting system is the security; therefore, the authors try to solve this problem by implementing SeVEP, a secure E-Voting system that authenticates the various voters and also enables effective verifiability and prevents double voting [11]. The main drawback of the system is the increased computational cost of the authentication technique in the proposed system.

B. Shahzad states that the E-Voting paradigm has gained a lot of traction in recent years as a substitution for the traditional paper-based ballot elections. this is due to the large environmental impact and also the logistic difficulties in the transportation and counting of a large number of votes [12]. An E-Voting system is highly capable of eliminating these problems with ease but it comes with its own concerns over the security of the voting data. therefore, the authors in this paper have devised an innovative scheme for a Trustworthy E-Voting platform that utilizes an Adjusted Blockchain for securing the voting data which also prevents any tampering done from any person. The experimental analysis details the superiority of the proposed methodology.

III PROPOSED SYSTEM

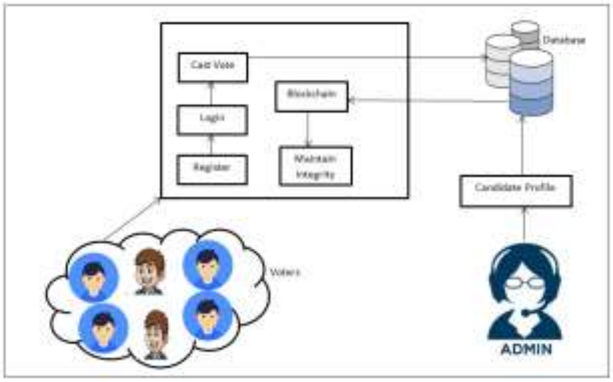


Figure 1: System Overview

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

Step 1: *Candidate Profile creation* – This is the initial step of the proposed model, where the interactive model is developed in the form of a web application. The admin log into the system and is given the ability to register the election candidates. The candidate data that is being entered in the provided interactive user interface consists of the party name, symbol, candidate name, age, sex and other required attributes to store in the database. Once all the candidates are nominated for the carrying out the elections, then voting process is initiated by the voters.

Step 2: Voting process and Blockchain formation – The voters also log into the system through the web application. The voter provides the login credentials that are authenticated before providing the access to the voter. Once the voter logs into the system, they are presented with the various candidates and their profiles according to the political party or affiliations. The voter can then choose between the candidates which belong to the party of their preference. After the selection of the candidate, the voter's vote is accepted along with the aadhar card number and the Blockchain framework is initiated.

There is a need for an effective approach to establish some type of accountability after the vote has been given to the candidate in order to prevent vote manipulation. As a result, the Blockchain framework was created for this purpose. The voter's aadhar card number is retrieved once the first vote on the proposed system is casted. The SHA256 hashing technique is used to generate the key for this vote. The key created through this method is then transformed into a shorter key by the application of the mod operation which randomly picks 7 characters from the key. Thus, this achieved key is referred to as the Head Key. The procedure of key generation is detailed in algorithm 1 below.

Algorithm 1: Block Head Key Generation

```
// Input:  Vote Attributes $V_{AT}$
// Output: Head Key $H_{KEY}$
Function: headKeyGenerator($V_{AT}$)
Start
HKEY =Ø
$SH_{KEY}$=SHA256 ($V_{AT}$)
    N=$SH_{KEY}$ MOD 7
  If N<7, then
  P=N+1
      for i=0 to $H_{KEY}$ length < 7
          i=i+P
          if i < $H_{KEY}$ length, then
              $H_{KEY} = H_{KEY} + SH_{KEY}$ [i]
              $SH_{KEY} =$ rotate ($SH_{KEY}$)
          end if
          else
                i=0
      end for
  end if
return $H_{KEY}$
Stop
```

When the next votes are casted, the same parameters are picked and concatenated with the previous transaction's head key, and the whole hash key creation procedure using SHA256 is repeated to obtain the current transaction's head key. This is repeated for all votes cast and the key of the final transaction or vote is called as the terminal key which is stored in another database for security reasons. The Blockchain formation process is illustrated in the algorithm 2 below.

ALGORITHM 2: Blockchain Formation

```
//Input : Vote Information list $V_L$
//Output: Terminal Key $T_K$
blockchainFormation($V_L$)
Start
$P_K$ =" " [Previous Key]
  for i=0 to size of $V_L$
    $T_P=B_{L[i]}$ [$T_P$ = Database Tuple]
    $P_K$= getBodyKey($T_P$)
     $T_K=P_K$
  end for
  return $T_K$
Stop
```

Step 3: Data Integrity through Blockchain– This step uses the input string of the stored vote from the database table. And then this 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 is finally *yielding* the block head and *block* body of the block chain. This process is being continued for all the voting data of the application to get the final head key.

In the process of Integrity evaluation previous and current head keys are subjected to the integrity evaluation process. If any inequalities between the current and previous head keys are encountered, *then* the integrity violations are identified to generate the required alert.

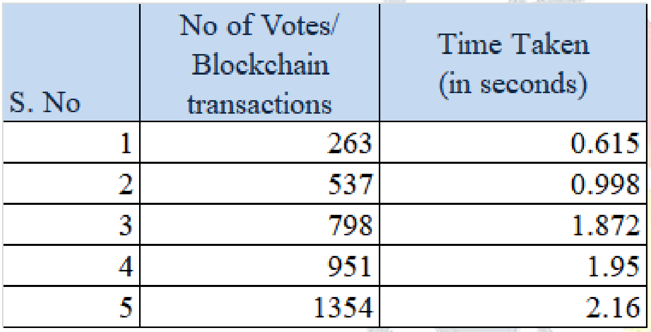
IV RESULT AND DISCUSSIONS

The presented technique designed to facilitate Electronic voting through the use of Blockchain has been developed using Java Programming language on the Netbeans IDE. The web application utilizes glass Fish web server for the hosting purpose. The development machine is running on 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 different parameters. The experimental evaluation results have been detailed below.

Scalability Analysis of Blockchain Transaction

The presented technique for securing voting data and its integrity through the Blockchain is calculated for the scalability of Blockchain transactions. For this purpose an elaborate experimentation is being performed by implementation of a secure web application for voting process. The number of Blockchain transactions are counted and listed in the table 1 given below.



S. No	No of Votes/ Blockchain transactions	Time Taken (in seconds)
1	263	0.615
2	537	0.998
3	798	1.872
4	951	1.95
5	1354	2.16

Table 1: Blockchain Transaction Time Estimation Table

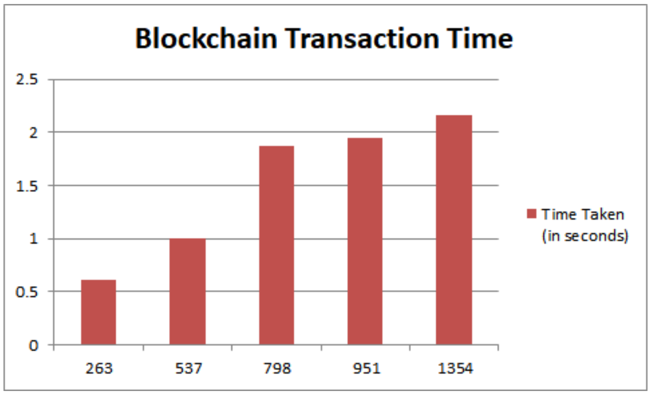


Figure 2: Blockchain Transactions

The tabulated results are then used to plot the graph given in the figure 2 given above. The graphical representation has been effective in realizing the relationship between the number of transactions and the time taken for these transactions on the Blockchain platform. The analysis of the results provides a greater understanding of the procedure and the implementation of the Blockchain framework to achieve the security of the voting data. It can be understood that the number of votes or the Blockchain transactions is not proportional to the time taken for the transaction. This indicates that the Blockchain approach has been accurately deployed. The results have been fruitful in describing the improved security of the entire election procedure.

V. CONCLUSION AND FUTURESCOPE

This paper successfully deploys in web application the process of E-voting in a well-organized and designed system using Java programming language. To secure the E-Voting data proposed model utilizes the Blockchain Platform which outperforms large number of many traditional Electronic voting approaches by a large margin. Whole E-voting data is being secured using the Block chain technique, The proposed methodology stores the voting data throguh the blockchains to secure the same. These blockchain transaction are used for the evaluation purpose in the pre-counting process through the use of previous and the current terminal head keys. The process of blockchain is evaluated for its time performance and it is proved that it is not directly proportional with the time. Hence, the deployment of the blockchain outperforms in the measurement of time sequence with respect to the number of transactions. This paper promises to achieves less time complexity due to parallel computation technique in E-Voting data integrity evaluation process, so that it can be secured thoroughly.

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

References

[1] H. Ge et al, “Koinonia: Verifiable E-Voting with Long-term 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] S. Bag et al, “E2E Verifiable Borda Count Voting System without Tallying Authorities”, 14th International Conference on Availability, Reliability, and Security, ARES 2019.

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

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

[7] R. Raghunandan et al, “Key Generation and Security Analysis of Text Cryptography using Cubic Power of Pell’s Equation”, International Conference on Intelligent Computing, Instrumentation and Control Technologies (ICICICT), 2017.

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

[9] Fridrik P. et al, “Blockchain-Based E-Voting System”, IEEE 11th International Conference on Cloud Computing, 2018.

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

[11] A. Qureshi et al, “SeVEP: Secure and Verifiable Electronic Polling System”, IEEE Access, 2019.

[12] B. Shahzad and J. Crowcroft, “Trustworthy Electronic Voting Using Adjusted Blockchain Technology”, IEEE Access, 2019.

[16] Iuliia Tkachenko, William Puech, Christophe Destruel, Olivier Strauss, Jean-Marc Gaudin, and Christian Guichard, “Two-Level QR Code for Private Message Sharing and Document Authentication”, IEEE Transactions on Information Forensics and Security, Vol. 11, No. 3, March 2016.