# Managing EVM Data through Blockchain

AniketHingane[1], Pratik Shah[2], Sandhya Chavan[3], Shashank Borkar[4],
Archana P. Kale[5]
[1-5]Computer Department, Modern Education Society's College Of Engineering, Pune

***Abstract* – Elections are one of the most important events in any democratic country. As the elections can have a large impact and can change the course of the government and the country. Elections are usually done manually through the use of physical ballots distributed across the country in the form of constituencies. The procurement of the votes of the citizens is a humongous task that is fulfilled by the election commission. It is a very expensive procedure to conduct an election in this manner, it also creates a lot of paper waste and harms the environment to a great degree. Therefore, a shift towards an E-voting approach is one of the most viable solutions to such problems but then there is low trust and security offered on the E-Voting approach that needs to be solved. Therefore, the methodology proposed in this publication secures the E-Voting data through the use of the RSA encryption technique and the implementation of the Distributed Blockchain Framework. The implementation of such algorithms guarantees the security and integrity of the E-Voting data which can enable a far more convenient alternative to the Election procedure. The presented methodology has been tested extensively to realize the performance metrics and assert the Tamper-proof nature of the Blockchain Platform.**

***Keywords:****Access Control Mechanism, Blockchains,E-Voting, RSA, Data Integrity.*

## I. INTRODUCTION

In a democracy and representative is selected from the citizens of the country for leadership and taking important and functional decisions. The representative is also selected from the citizens itself and it is usually done through the means of an election. The election process is highly complicated and has to take into account all the legal voters that are above 18 years of age. For this purpose, an election commission is established independently of the government. This is because some government corruption might creep into the election process. Therefore, and independent authorities like the election commission is devoid of any corruption add to start with the fair and just conduction of the election process. The election commissioner is the authority that has the decision-making capability in the election process.

The process by which India conducts elections is a highly manual one called the ballot process. Through this process, various constituencies establish all across the country and its respective States. These constituencies have their voter list comprising of the voters in that area. For this process, the election commissioner appoints various booth officers that are in charge of a particular constituency. Depending on the size of the constituency multiple boots can be assigned to a single constituency. The booth officer conducts elections on a particular date where a holiday is given to the various working people to cast their votes. The voters physically cast their votes to a particular party through the means of a ballot. This is the time-consuming process through which booth officers seal the ballot boxes which are then transferred to a safe location where the votes are counted.

This whole process is laborious and time-consuming which also creates a lot of environmental pollution the ballot boxes require paper and a lot of transportation from one place to another which requires a lot of fuel which pollutes the environment even further. Therefore, there is a need to streamline this process and effectively achieve the whole election process with the least amount of damage done to the environment. For this purpose, Technology can be used for our benefit as the whole process of election can be converted into an electronic system. This has been the goal for a long time but one of the biggest problems that are faced for this implementation is the lack of security in the whole process and the east by which an electronic system can be attacked nowadays. Therefore, for this purpose and innovative platform called blockchain can come to the rescue.

The blockchain was introduced in late 1900 for the creation of a digital notary. The blockchain is a distributed ledger system that time stamps the document and prevents any changes after that period. This platform did not gain much popularity with researchers at that time and was forgotten for a long time. Up until the blockchain platform was used to create an electronic currency or cryptocurrency called Bitcoin. The blockchain platform gained immense popularity with researchers after this point as the robust security of the blockchain platform was established with certainty. The

blockchain platform utilizes A block and chain method which chains the blocks of data with the help of hash keys. This makes the blockchain a tamper-proof distributed storage that can be easily utilized to store e-voting data with utmost security.

To provide security to the data blocks in the blockchain the RSA algorithm has been utilized for this purpose. The RSA encryption is one of the most popular cryptographic security systems that have been utilized almost ubiquitously everywhere. The RSA encryption system was designed by 3 scientists which utilize large prime numbers to encrypt the data blocks asymmetrically. This provides robust security to the important data which is successfully protected by a combination of these two methodologies.

In this publication section 2 discusses about the Literature survey of the earlier publications. Whereas section 3 deeply explains the Proposed methodology techniques, whereas section 4 Discusses the obtained results. The future traces and conclusion of this publication is described in section 5.

## II. LITERATURE SURVEY

E. Belanger explains that due to various technological advancements and the adoption of these technologies in the automotive industry has led to several improvements. Most of these improvements due to the creation of autonomous cars that are being disruptive to Maintenance Services, insurance, manufacturing, and government regulations. Therefore, the authors address these issues in this Publication proposing a distributed Framework based on blockchain for implementation in a smart City automotive industry [1]. The proposed methodology has been implemented in a simulation environment using the Ethereum platform and produced satisfactory results.

P. Sharma elaborates on the various parameters through which the effectiveness of government websites has been evaluated. Government websites are one of the most important websites that are used for various purposes such as the implementation of government policies and interaction with the citizens of the country. Therefore, the website should be highly user-friendly and should be clear in their representation. Therefore, various government websites have been evaluated for the New Zealand government on these parameters [2]. The extensive survey concluded that there are high discrepancies that are noticed in the websites which need to be addressed immediately.

R. Cullen introduces the EVM for electronic voting machines that are used to conduct elections in India. Electronic voting machines have been the center of a lot of controversies due to various irregularities that are being exposed by various organizations. There are various claims that electronic voting machines have been compromised and cannot be used as a fair means of conducting the elections [3]. Therefore, for this purpose and extensive security valuation has been performed by the authors in this paper. The analysis has concluded that there are two types of attacks that can be performed the electronic voting machines which need to be safeguarded and prevented to perform fair election procedure.

S. Wolchok states that there voting is one of the most important aspects of a democracy's success in India which helps in the election of various representatives and government officials. The elections from the center of a democratic country as they are one of the most essential aspects of maintaining law and order in the country [4]. As various other procedures have been enhanced by the use of Technology the voting process also needs an uplift in the form of an electronic voting system. Hotels in this paper propose an ineffective executive e-voting system through the use of the blockchain decentralized platform. The major drawback of this paper is that the authors have already discussed and not implemented a decentralized system for E-voting.

S. Aggarwal explains that due to various technological advancements a lot of procedures have been getting highly automated and revolutionized. This has been noticed in various sectors that have been improved by the addition of Technology and electronic assistance. One of the techniques that have not been improved in such a long time is the process of voting, as e-voting can be subject to a lot of denial-of-service attacks and cyber-attacks which is very difficult to provide a fair voting procedure [5]. Therefore, the authors in this paper propose an innovative technique for e-voting by introducing a decentralized blockchain for managing the security and providing a fair and just voting system. The experimental results conclude that the blockchain provides a temple proof security that is highly reliable in the voting system.

H. Wu elaborates on the various techniques that are utilized for the performance of an effective online voting system. Most of the elections are conducted using the ballot system which generates a lot of waste in the form of paper which can be highly detrimental to the environment. Therefore, the authors to reduce the wastage and implementation of an online voting system propose homeomorphic encryption assisted by the verifiable rank choice voting system. The proposed methodology has been experimented to analyze the performance and security of the whole system [6]. The experimental results conclude that they have been significant improvements that have been noticed in the security and the performance of an online voting system compared to a physical system.

X. Yang introduces an electronic voting system which has been elected as the replacement to the physical voting systems that are in place in various countries and institutions all over the world. This is because the physical voting system

is highly time-consuming and produces a lot of wastage that can hurt the environment on a large scale. The electronic voting system also provides an increasing amount of privacy and promotes fairness in the whole voting scheme. Electronic voting systems are also highly flexible and transparent for various users. Therefore, the authors in this paper proposed the utilization of a blockchain Framework for securing the voting data effectively [7]. A distributed ledger system that is blockchain provides enhanced security the electronic voting system which is quite valuable implementation.

Fridrick P. states that data has been one of the most important aspects that provide effective utilization of various Artificial Intelligence and mining algorithms. But the authors state that most of the data that is highly useful for these applications are scattered all over the internet and is difficult to aggregate for effective implementation [8]. Therefore, where is data stakeholders are in charge of aggregating the data and providing it to the various vendors that can utilize this data effectively. The photo provided a tamper-proof method of sharing and securing the data the others introduce utilization of artificial intelligence along with the implementation of the distributed ledger system called a blockchain. The experimental results conclude that SecNet is highly reliable and Secure and achieve its goals effectively.

K. Wang explains that the election procedure is one of the most important aspects of a democratic country that is being utilized to implement the basic tenants of democracy [9]. But it has been noticed that an increasing number of people have not been casting their votes for being a part of the election due to inaccessibility issues. Therefore, to provide an effective solution to this problem electronic voting can be utilized as a means of casting their votes from the comfort of their homes. For this purpose, the others propose SeVEP which is a secure and verifiable electronic polling system. The Proposed methodology is highly secure through the use of cryptography the experimental results conclude that it performs as expected.

A. Qureshi elaborates on the various aspects of the election procedure that are highly physical because of the use of the ballots system. The physical nature of the election procedure and makes most of the citizens skip the election as they have to travel to a certain location for Casting their votes. Therefore, a solution to this problem is the effective implementation of an electronic voting system. The authors in this paper propose an effective utilization of the distributed blockchain platform to implement a trustworthy electronic voting system [10]. The experimental result concludes that the implementation of the blockchain platform has increased the security of the voting data considerably.

B. Shahzad introduces the various advancements that have been made in the Election System out of which the most important is the implementation of Technology in replacing the physical voting system [11]. The technology allows for the implementation of an electronic voting system that can help save a lot of time and physical resources that are required for conducting paper-based elections. They have been significant growth in various electronic procedures that implement a voting system but most of these are related to security lapses and concerns that are noticed significantly. Therefore, the authors in this paper propose an effective solution for providing security to the voting data by the use of the distributed blockchain system. The experimental result concludes that the blockchain system effectively provides security to the voting data.

## III PROPOSED SYSTEM

The presented system for secure E-Voting data of an election process is outlined in the figure 1 below and the steps that are performed for the implementation of the same are explained below.

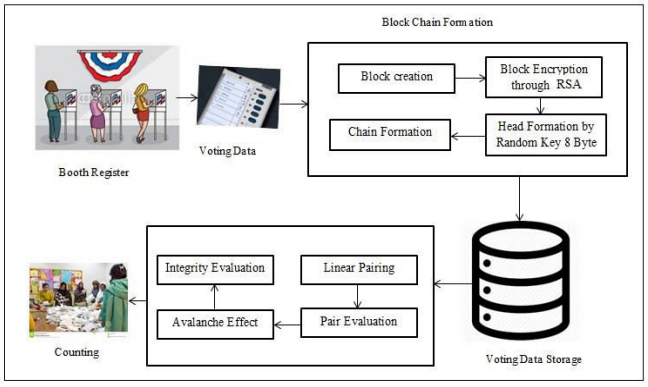


**Figure 1: System Overview**

***Step 1:*** *Simulation of Voting* – The simulation of the voting process is the initial step in the proposed system. The simulation procedure is performed in the Java programming language. First, a number of booths (N) are generated randomly through the random function using the Java Library. For every booth created a database table is allocated to store the details of voting. Each of the booths created is authenticated through the use of a particular booth officer. The login credentials such as the username and the password are generated through the random selection. The password characters and the names for password and username generation respectively are chosen randomly through a provided spread sheet. The voting booth database tables contain various attributes such as vote, Symbol, Serial no, name, and booth no.

The candidate data is being supplied to the system using the interactive user interface created for this purpose. The attributes of the candidate consist of sex, age, candidate name,

symbol and, party name and many more which are then subsequently stored in the database. After the completion of the nomination process of all the candidates, the random function is utilized once again to trigger the voting process. The votes received during this execution are then encrypted using the RSA encryption standard before storing them in the database.

***Step 2:*** *RSA Encryption* –The votes cast in the previous step are subjected to the encryption procedure utilizing the RSA encryption approach. The voting data is in the string format which is subjected to the asymmetrical encryption methodology of the RSA encryption approach. As RSA is an asymmetrical encryption technique, there is a need for the generation of a public key for encryption and a private key for decryption. The public key generation relies on prime numbers and their co primes to generate the values of N and Φ(N).

The values generated namely, N and Φ(N) form the boundaries for the creation of the public key of the form (e, N). This public key is then used to encrypt the votes. Firstly, the data is converted into a numerical format from the string format. Then the data is subjected to the equation $C = M^e \bmod N$. Where C is the resultant ciphertext and M is the original data to be encrypted. Once encrypted the resultant ciphertext is converted into a string format that is stored in the database.

Decryption – When the cipher data obtained from the RSA is required to be converted back into its original form the decryption key is utilized. The encrypted E-voting data needs to be decrypted back to its original form for the counting process. The decryption key is of the form (d, N), which is a private key different from the encryption key as the RSA platform is an asymmetrical encryption paradigm. $M= C^d \bmod N$ is utilized to achieve the original data back, where M is the original data, and C is the cipher data obtained in the previous step. The cipher data and all the operations are performed on a numerical value. Therefore, the obtained original data must be then converted to its requisite format to decipher the entire contents in the original form.

The algorithm for the RSA encryption is illustrated in algorithm 1 below.

ALGORITHM 1: RSA ENCRYPTION AND DECRYPTION

// Input: Voting data String $V_S$, public ( N,E),private(N,D)
// Output: Cipher Data $C_D$ , Plain Data$P_D$
1: Start
2: $C_D = \emptyset$
3: $P_D = \emptyset$
4: **For** i = 0 to size of $V_S$
5: char ch=$V_{S\,[i]}$
6: int A=ch
7: int C=A^E MOD N
8: char cipher=C
9: $C_D = C_D$+ cipher
10:**End For**
11: **For** j = 0 to size of $C_D$
12: char cch= $C_{D\,[j]}$
13: int CI=cch
14: int $P_T$= CI ^D MOD N
15: char plain=$P_T$
16: $P_D = P_D$ + plain
17:**End For**
18: **Stop**

*Step 3: Multi Linear Pairing* – The voted booths generated in the previous steps are segregated into a definite division in this step of the procedure. The resultant segregations are then administered into the parallel computation that evaluates the pairings for the measurement of the data integrity through the distributed blockchain framework.

*Step 4: Data Integrity through Blockchain* – This is the final step in the proposed methodology that utilizes the encrypted and segregated booth tables according to the multi-linear divisions, obtained from the previous step. The MD5 hashing algorithm is utilized for the generation of the hash key. To reduce the hash key length, it is subjected to random character selection through the rotation.

This achieves the creation of the Blockhead as well as the Block body for the formation of the blockchain. This procedure is repeated for creating the blockhead and the block body for all the booths to achieve the final divisional head key. These head keys are generated for all the divisions performed. The N division yields N heads keys which are subsequently stored in a database for the integrity evaluation.

The head keys generated previously and currently are utilized and compared for the purpose of executing the Integrity evaluation mechanism. Integrity violations are identified if there are any discrepancies or inequalities are found between the previous and current head keys, and a suitable alert is generated.

## . IV RESULT AND DISCUSSIONS

The presented technique for the implementation of a secure E-Voting approach through the distributed framework of the Blockchain platform is coded using the Java platform through the utilization of the NetBeans IDE. A standard configuration for a development computer is utilized for the execution of the system which contains the Intel Core i5 processor along with 4GB of RAM and 500GB of storage. MySQL database server is utilized for fulfilling the database requirements. The presented technique also utilizes the D-Link WiFi router for enabling network integration and connection for the process of Emailing and Messaging.

For the calculation of the execution performance of the proposed system for the implementation of a secure E-voting mechanism through Blockchain, extensive experimentation is

conducted. The proposed system has been evaluated for the prevalence of errors that are confronted while securing the E-Voting data and performing the integrity evaluation through the use of Mean Absolute Error (MAE).

**Performance Evaluation based on Mean Absolute Error**

The Mean Absolute Error approach measures the errors which are encountered in the system in the form of a percentage. The results are implemented in the form of a percentage as the percentages are easy to comprehend and allow for ease in interpreting the data. The attribute observed in regards to this measurement is the inability in achieving integrity evaluation through the prescribed technique. The error percentage for not achieving successful integrity evaluation is measured through the implementation of the Mean Absolute Error. The mathematical form of the approach is given below.

$$\text{MAE} = \frac{(\sum_{i=1}^{n} | xi - yi |)}{n}$$

Where,
xi - Number of Expected Integrity Evaluation.
yi - Number of Achieved Integrity Evaluation.
n - Number of Trials Conducted.

| Experiment Number (n) | Number of Trials | Expected No. of Integrity Evaluation (xi) | Achieved No. of Integrity Evaluation (yi) | Difference (xi-yi) |
|---|---|---|---|---|
| 1 | 10 | 9 | 7 | 2 |
| 2 | 10 | 8 | 7 | 1 |
| 3 | 10 | 9 | 8 | 1 |
| 4 | 10 | 10 | 10 | 0 |
| 5 | 10 | 6 | 6 | 0 |
| 6 | 10 | 7 | 6 | 1 |
| 7 | 10 | 9 | 6 | 3 |
| 8 | 10 | 10 | 9 | 1 |
| 9 | 10 | 8 | 8 | 0 |
| 10 | 10 | 7 | 7 | 0 |
| | | | MAE | 0.9 |

**Table 1: Experimentation and Calculation of MAE.**

The Integrity evaluation results obtained from the presented technique are listed in table 1 above. The results tabulated in the table above are plotted in the form of a bar graph for easier comprehension in figure 2 given below.

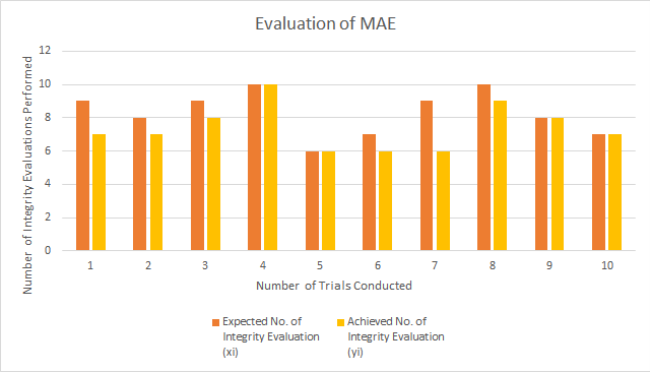


**Figure 2: Evaluation of MAE.**

The results of the experimentation demonstrate the accuracy of the proposed methodology in evaluating the integrity of the E-Voting Data. The experimental assessment illustrates that the approach for evaluation of the integrity attains a Mean Absolute Error of 0.9. This much of low MAE is just because of hardware or software error that may occur during the performance of the model otherwise system might yield a absolute Zero error under the constrained environment. This depicts that the secure E-Voting mechanism is executing as expected and the integrity evaluation is in the prescribed limits of the proposed methodology.

## V CONCLUSION AND FUTURE SCOPE

E-Voting paradigm is one of the most innovative approaches that can be enabled for far more efficient, transparent, and secures conduction of the election procedure. The E-Voting can enable the physically disabled or the elderly to cast their votes in increased convenience and improve the voter turnout of the constituencies. The main cause of concern preventing a shift towards the E-Voting paradigm is the security concerns over the integrity of the E-voting data. Thus, the proposed methodology has been implemented to provide effective security to the E-voting data through the use of the distributed blockchain platform and the RSA encryption standard. The Blockchain is a tamper-proof framework that can effectively secure the data in a distributed network that enables the integrity evaluation of the E-Voting data effectively. The RSA encryption is one of the most widely used and highly secures encryption technique that has been implemented to secure transmission of the E-Voting data. Extensive Experimentation of the proposed methodology has been conducted to evaluate the performance of the approach. The Integrity evaluation has been tested to achieve significantly low levels of error which proves the superiority of the presented system in comparison to the conventional E-voting techniques.

For the Future research direction, the proposed methodology can be implemented in a real-world scenario for conducting the elections electronically in a secure and efficient manner.

## REFERENCES

[1] E. Belanger and R. Nadeau, "Political trust and the vote in multiparty elections: The Canadian Case", European Journal of Political Research, 2005.

[2] P. Sharma, N. Kumar and J. Park, "Blockchain-based Distributed Framework for Automotive Industry in a Smart City", IEEE Transactions on Industrial Informatics, 2019.

[3] R. Cullen and C. Houghton, "Democracy Online: An Assessment of New Zealand Government Web Sites", Government Information Quarterly, Volume 17, Number 3, 2000.

[4] S. Wolchok et al, "Security Analysis of India's Electronic Voting Machines", Proceedings of the 17th ACM conference on Computer and communications security, 2010.

[5] S. Aggarwal et al, "A Comparative Analysis on E-Voting System Using Blockchain", 4th International Conference on Internet of Things: Smart Innovation and Usages (IoT-SIU), 2019.

[6] H. Wu and C. Yang, "A Blockchain-Based Network Security Mechanism for Voting Systems", 1st International Cognitive Cities Conference (IC3), 2018.

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

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

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

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

[11] B. Shahzad and J. Crowcroft, "Trustworthy Electronic Voting Using Adjusted Blockchain Technology", IEEE Access, 2019.

*****