EAI Endorsed Transactions
on Internet of Things

Research Article EAI.EU

Blockchain Based Cryptographic Algorithm for Data Protection in Electronic Voting System

Vinayachandra[1,*], Krishna Prasad K[2]

[1,*]Institute of Computer Science and Information Science, Srinivas University, Mangalore, Karnataka, India

[2]Cyber security and Cyber Forensics in the Institute of Engineering and Technology, Srinivas University, Mangalore, Karnataka, India.

Abstract

The development of digital world created advancement of technology, by which the data services are electronically transacted. Electronic voting is used to improve the election system in several ways. But technical issues associated with protection of data, is considered as a major concern leading to illegal activities and threats. Some of the conventional methods used in securing e-votes are matching finger prints of individual, control unit accessibility, which provides decreased capability of attaining proper authenticity and security. Even several cryptographic methods are used for data security, but produced limited accuracy. So, to improve the reliability and accuracy of data protection in e-voting, combination of AES (Advanced Encryption System) and RSA (Rivest, Shamir, Adleman) combined with blockchain technology is implemented. AES uses larger key size which makes the data privacy robust. But encryption and decryption time produces decreases computational speed. So, AES is combined with RSA, as it uses shorter key length and easy to implement with block-chain algorithm, it is deployed to decrease encryption and decryption time, thus producing highly sensitive data security. The performance of the system is validated by calculating the encryption and decryption time, block size and verification time of original data with output data.

Keywords: Electronic Voting System, Cryptography, Data Protection, Encryption, Decryption, Blockchain

Received on 28 10 2024, accepted on 26 11 2024, published on 08 01 2025

doi: 10.4108/eetiot.7680

1. Introduction

Data security plays a significant role in protecting the digital information from unauthorised access, corruption and theft. The election commission introduced EVM (Electronic Voting System) [1], to cast votes and secure the votes from anonymous threats. One of the major concern in online voting mechanism, is security. The security requirements are verifiability, integrity, authentication, and privacy. Elections done by paper votes, are unsustainable since it intakes large number of resources, whereas the e-voting enables people to cast votes from anywhere with improved security. There are two kinds of casting votes, namely, presence voting and distance voting. So, reliability, accuracy, security and confidentiality are the important key factors to ensure while using online voting system. Concurrently, cryptographic methods [2], are associated in the process of verifying the casted votes, to prevent illegal voting. This technique involves encoding the plain text into cipher text and vice-versa for data protection. Here, the information cannot be altered and there is less chance of alteration. In addition, a robust data security, is needed to maintain and process data against illegal activities. There are various

[*]Corresponding author. Email: veeciashu@gmail.com

approaches used in data security in EVM. One among the methods is using blockchain [3] along with its attributes like, faster settlement, distributed ledgers, decentralised, consensus and optimised security. Integrated blockchain represents that the stored votes are secured with reliability and is implemented in remix IDE [4]. This approach targets to easily identify the replaced votes with correct ones. Likewise, a secured e-voting in a IoT embedded system can also be achieved using blockchain technology [5]. It ensures end-to-end security for entities intricate in electronic voting method. The D-App (Decentralised Voting Application) [6] associated with blockchain approach, uses the decentralisation network to secure casted votes. It allows ballot reliability, safeguarding of voter identification, validity and data transmission privacy [7, 8]. Additionally, the hybrid AES-RSA algorithm along with blockchain technology to secure voter information. The confidentiality of voter data while improving the speed to encryption and decryption processes in the method of tamper proof ledger for storing voter data, which is crucial for maintaining the integrity of the voting process [9]. Similarly, the hybrid encryption schemes, including AES-ECC, AES-RSA and AES-ElGamal, focusing on the performance in terms of encryption and decryption times as well as throughput [10].

Several e-voting systems are prevailing in order to overcome the security issues prompted while checking the valid votes. However, existing methods fall short in producing efficient reliability and integrity, leading to vulnerabilities such as vote tampering, data breaches, and lack of transparency. For instance, traditional e-voting systems have faced significant security incidents, including unauthorized access and manipulating of vote data, which undermine public trust in electoral processes. So, the proposed system implements cryptographic methods to ensure if there is any invalid or altered data of votes to protect from fault and inaccuracy. So, the AES with RSA using blockchain technology is used to secure the casted votes. AES is used to speed up the encryption and decryption time, as it is suitable for encryption huge volume of data. It uses large key sizes for encryption, which makes it robust against threats. But it decreases the computational speed as it generates increased encryption and decryption time. So, AES is combined with RSA, as it uses shorter key length and less key generation, by which the data's are processed quickly. Further, blockchain is a technology, which is completely decentralised with stored data instead of using single database. It is sustained by peer-to-peer network which leads to next level integrity and security. This specifies the problem with existing e-voting systems and highlights how the proposed work addresses the issues effectively.

The main contribution of the proposed algorithm is as follows,

- To combine AES and RSA offers Dual layered encryption, significant improving data protection compared to traditional methods.
- To use blockchain to verify the login details of voter and validate the mismatching data's.
- To evaluate performance with respect to encryption and decryption time, block size and verification time.
- To synergy of AES's string encryption and RSA's efficient Key managements reduce computational load, resulting in faster processing during high volume voting events.
- The blockchain integration ensures tamper resistance vote verification, providing transparency and scalability. Also different voting ensures both large and small-scale electrons
- The mechanism protects against coercion by ensuring voters cannot prove how they voted. And allowing the voter to track their votes

1.1. Paper Organisation

The paper is characterised based on the security analysis of voter details to prevent illegal activities. Whereas, analysis of the existing works is done on similar domain with several approach and shown in Section II. Further, Section III signifies the methodology executed in the proposed system. Sequentially, the outcomes and comparative analysis of existing methods are shown in Section IV. Lastly, the conclusion and future work of the proposed model is determined in Section V.

2. Review of the Literature

Diverse procedures obtained by existing studies for data security in EVM, are reviewed and discussed in this section.

AES is determined as the widely used block cipher. A low power consumed AES [11] has been implemented, called as LPADA (Low power AES Data Encryption Architecture) to decrease the power consumed for data encryption, by AES with power management method, power gaining approaches, and low power S-Box. Further, a key updating algorithm has also been deployed, to improve the session-key renewal security. As a result, the security analysis has represented that the key updating algorithm, has allowed mutual authentication. Most of the people use mobile phones for several applications such as internet voting, banking, e-mails and others. A secured mobile internet voting system using biometric approach authentication [12], has been deployed. The wavelet-based AES method, has been used to haste the encryption process and decrease mobile device CPU consumption. From the analysis of three methods, such as biometric template generation, AES encryption and wavelet based AES encryption, it has been found that the wavelet based AES encryption has performed better than other two algorithms. From the study, it has been identified that the internet voting system works better on all mobile based spasms. An issue of voter's information and storage of data processing is a threat in data security and privacy, during election.

The post-election auditing problems and its confidentiality in electronic voting system, has been detected using cryptographic algorithms [13]. The auditing problems of the electronic ballot, has been predicted using SHA-256 cryptographic hash functions whereas, the confidentiality has been enriched by employing combination of E-AES (Enhanced-AES) and Space Insertion Text Semagram. As a result, post-election auditing verification problems and its confidentiality of electronic ballot has performed better with improved security. Voting process through mobile or PC, is an alternative way for organising online voting from any place. A method called, CryptDB has been used, to detect reliability and security in electronic voting procedure. Here, the candidates data, voters information, and votes has been encrypted and stored in database and follows several encryption levels. Therefore, the voting process, has been achieved with integrity, security and confidentiality, as the intruders cannot gather any information of voting from the polling system.

Similarly, a visual semagram approach, has been implemented to protect the election results against deformity, suspicion and threats. By using bits of original image, the "semagramming" [14] process, has been held and thus the image obtained is called as "Vimago". In the visual semagram method, any image regardless to shape and appearance has been produced, by which the information cannot be changed by the fraudsters. These vimago's are generated, depending on alphabetical characters of political parties and contestants as well as numerical values of election results that has been encoded in matrix T. It has resulted that, the implied method has resolved jargon codes, encryption methods and grille-cipher to prevent illegal modification of hidden information. Likewise, a blockchain [15] based decentralised electronic voting system, has been used for transparency and data integrity.

The blockchain, has used hash functions and encryption methods, to verify security of each and every vote of the people. It has been constructed such that no intrusion and alteration of data is performed without the accordance of entire network. Thus, the insisted system [16], has made the voting process reliable and fully secured. A compatible voting system, has been produced by using encryption and decryption methods. And a blockchain e-voting procedure with audit function has been introduced [17]. The system has also been adopted for quantum attacks. The anonymous of voters has predicted by certificate less cryptosystem. It also produced feature of audit with traceable ring signature approach. Correspondingly, an electronic voting system based on RSA and altered classical cipher has been deployed.

The memory allocation and time management has been investigated and compared with other existing methods. It has produced better universal verifiability, privacy and anonymity. A modified voting system [18], has been produced by using firewall system, biometric authentication, and voting data encryption to overcome malicious threats. An inimitable serial ID, has been produced and stored in database making auditing, counting and tallying easier. Thus the system has enhanced better in accuracy, security and transparency.

2.1. Problem Identification

The major issues found by the analysis of conventional studies are,

- The visual cryptography algorithm used in privacy protection lacked in providing adequate security system [2].
- A hybrid method of RSA and ECC (Elliptical Cryptographic Curve) based on post quantum cryptography is not capable of producing optimised security [5].
- In the study, the EVM is dearth in producing security against attacks such as DoS and DDoS [13].

3. Proposed Methodology

E-Voting system has a great potential to decrease organizational costs with improved voter turnout. Effective caution is needed to avoid vulnerabilities. Though conventional algorithms thrived to attain secured voting mechanism, they are deficient with limited integrity and computational speed. Therefore, the proposed model employs hybrid AES-RSA algorithm with blockchain for the secured local-E voting mechanism with Manual dataset. The Figure.1 signifies the overall process of secured voting mechanism.

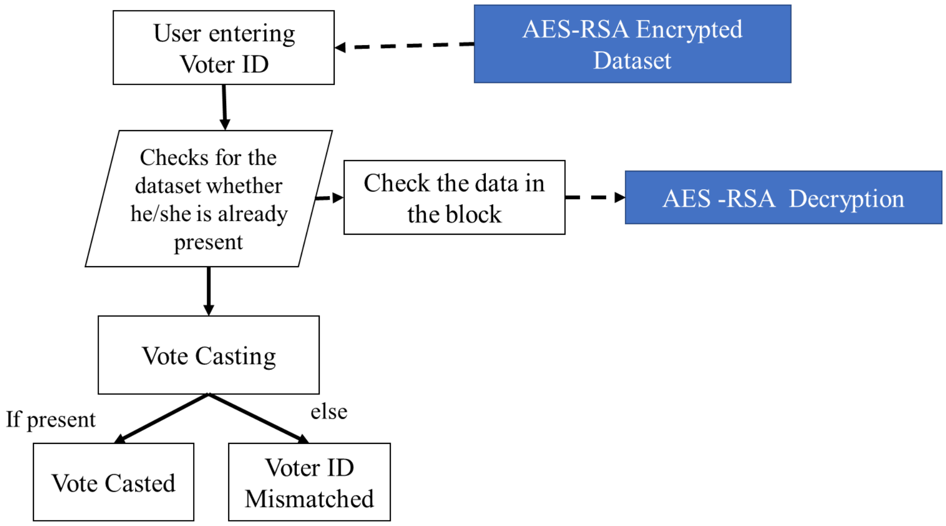

User entering Voter ID
AES-RSA Encrypted Dataset
Checks for the dataset whether he/she is already present
Check the data in the block
AES -RSA Decryption
Vote Casting
If present
else
Vote Casted
Voter ID Mismatched

Figure 1. Overall Process of Secured Voting Mechanism

Fundamentally, the admin and voter is the window in the respective mechanism. The data of the voter is stored in the local dataset (CSV file). When the voter enters the data, it will be encrypted by using AES-RSA algorithm. The proposed AES-RSA and blockchain e-voting system show great potential for secure, transparent, and scalability in digital voting. By addressing the infrastructure needs, selecting appropriate with pilot projects in controlled environments would allow for iterative improvements before scaling up for larger electronics. It enhances the significantly enhance e-voting reliability and security, setting a new standard for digital election platform. The figure.2 shows the methods involved in voting process using AES-RSA based on blockchain.

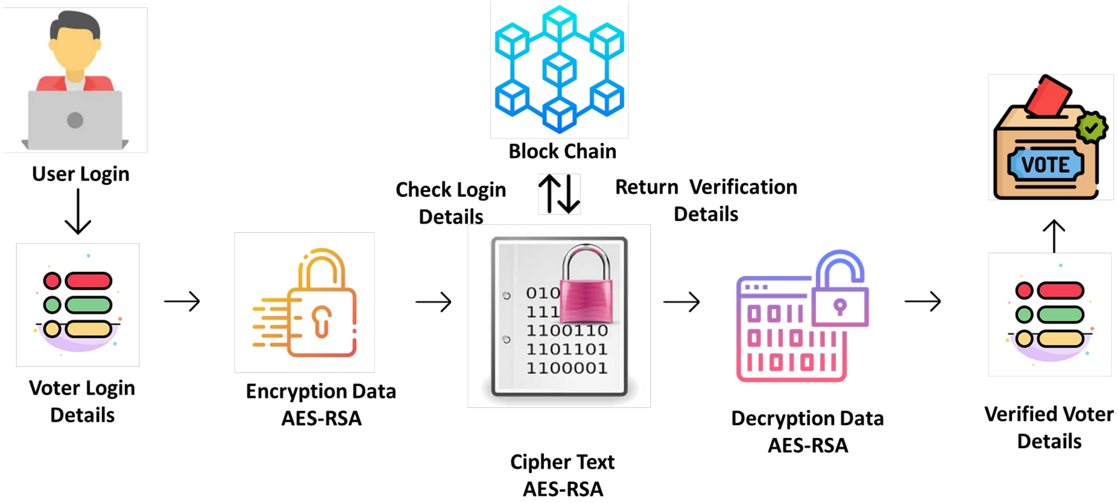


Figure 2. Methodology Involved in Secured Voting Process

This encrypted data will be pass through the Blockchain where the data is verified in the block. The verified data will be decrypted using AES-RSA algorithm. The resulted verified data will be sent to the voting progression. Once the data gets matched with the stored data, the vote will be casted. If it's not matched with the stored data, the vote will not be casted. The two step encryption and decryption process will strengthen the security in the voting mechanism.

The innovative combination of AES-RSA encryption and blockchain technology present a significant advancement in electronic voting systems, enhancing security, efficiency, and transparency. The AES-RSA hybrid encryption combines both symmetric and asymmetric techniques for robust data protection, while blockchain techniques ensure tamper-proof verification. Similarly, the method streamlines data processing and enable real time verification, which is essential for managing high volume voting events. In scalability the system handle large volumes of vet's effectively, making that ideal for national and international electronics.

Whereas, in adaptability the design is compatible with IoT environments, securing data exchanges across decentralized nodes, application in sector like smart cities. The security of government is enhanced in public sector by allowing citizens to safety access and verify personal information while promoting transparency. As well as in private sector, the secures sensitive transaction and supports real time data handling across network, benefiting the industries like finance, logistic.

3.1. AES-RSA

The voter's data is initially encrypted by using AES-RSA algorithm in the respective model. It is a symmetric cipher block algorithm with 128 bits block-size. AES performs operations like permutations and substitutions and capable of encrypting larger bits size data. AES has numerous compensations compared to the other encryption protocols. It has good speed in the process. It acquires only few memory space and the resource system. Figure.3 signifies the hybrid AES-RSA mechanism.

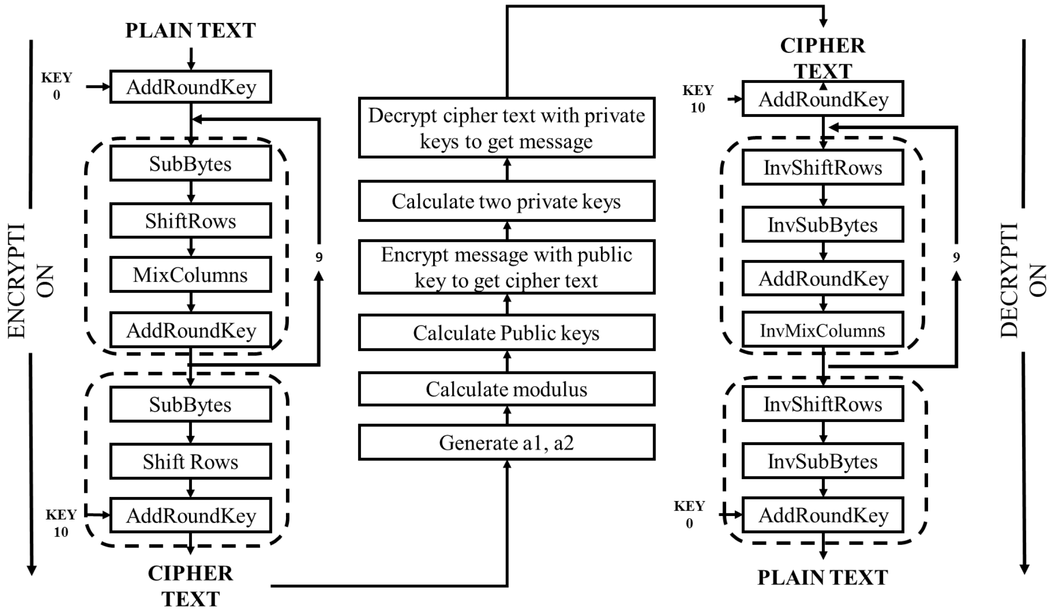


Figure 3. AES-RSA Process in Secured Voting Mechanism

AES can be combined with other security protocols when it needs an extra security layer. Implementation is easy in this algorithm. The encrypted data from the AES algorithm is further encrypted and decrypted by using RSA algorithm. RSA is the asymmetric algorithm that works with two diverse keys such as private key and public key. In the cryptography process, both the keys is utilised for encrypting the data. The contradictory key utilised for encryption is used for decryption of the data. The resulted data is further decrypted, once the data is verified, it sent for the casting of vote. This mechanism is secured against the attack in the voting system. Algorithm. I signifies the cryptography process with AES-RSA algorithm.

Furthermore, in depth cryptographic analysis, a detailed comparison of AES, RSA, and other encryption standards will clarifies the rationale behind choosing AES-RSA. This analysis examine the key sizes, computational complexity, and potential vulnerability, thereby providing a clear understanding of the performance in a security voting. Similarly, to ensure the reproducibility, it is essential to document all algorithm steps comprehensively. This includes specifying the exact parameters used for AES and RSA, detailing the encryption and decryption processes.

Algorithm. I: AES-RSA Encryption and Decryption

```
Initialization
input (text)
Encryption
Input Values: a1 and a2
Pr = a1xa2
```

```
$Pr = (a1 - 1)\ (a2 - 1)$
Select Integer values: $e\ [(gcd\ (), e) - 1;$
$1 < e < Ø(Pr)]$
Compute: $d\ de\ mod\ Ø\ (Pr) = 1$
$C = Cg\ 1\ mod\ (z)$
$Num_{block} = 4$  block_size of 128 bits
$CipherText(byte_{in}\ [4 * Num_{block}], byte_{out}$
 $[4 * Num_{block}], word\ w[Num_{block}$
$* (Num_{row} + 1)])$
begin
byte state $[4, Num_{block}]$
$st = in$
$AddRoundKey(state, w[0, Num_{block} - 1])$
for round 1 step 1 to $Num_{row} - 1$
    SubBytes (st )
    ShiftRows (st )
    MixColumns (st )
   $AddRoundKey(state, w[round * Num_{block},$
   $(round + 1) * Num_{block} - 1])$
 end for
 SubBytes (st )
 ShiftRows (st )
 $M =$  AddRoundKey
 $(st\ , w[Num_{row}\ Num_{block}, (Num_{row} + 1)$
                  $* Num_{block} - 1])$
 Encryption: $M < n$ ,
                  $chipertext = M\ (mod\ n)$
  out state chipertext
Decryption
plaintext → decrypt (chipertext, key)
begin
Decryption: $CM = chipertext(mod\ n)$
byte state $[4, N_{block}]$
$state = CM$
$AddRoundKey(state, w[0, N_{block} - 1])$
for round 1 step 1 to $N_{row} - 1$
      InvMixColumns (st )
     InvShiftRows (st )
     InvSubBytes (st )
    $AddRoundKey(state, w[round$
                 $* N_{block}, (round + 1)$
                 $* N_{block} - 1])$end for
 End for
 SubBytes (st )
 ShiftRows (st )
 output(plaintext)
end
```

Similarly, the implementation of AES-RSA encryption consists of several key processes to secure voting data. The key generation involves the generating AES symmetric key typically 256 bits, and RSA public and private key pairs of 2048 bits. Secure distribution is critical, and the AES keys can be encrypted with the recipient's RSA public key for safe transmission. And AES encryption uses a block size of 128 bits, requiring data to be splits or padded to fit these blocks, ensuring handling of varying amount of voter data. The process begins with the AES key by encrypting voter's data, followed by encrypting the AES key with RSA for added security. During decryption, the RSA private key retrieves the key, which then decrypts the voter data. This layered approach enhances security by combining symmetric and asymmetric encryption methods. In addition to these election authorities and auditors to verify the election's integrity at any stage, established transparent log mechanisms that record every voter action without revealing private information. This ensures that voters can be independently verified while maintaining voter privacy. This integration maintains the original meaning and content while adding the new information about real time voting audits.

3.2. Blockchain

The blockchain is utilised in the respective method to store the encrypted data that can comprehend data security with supple alteration of policy in accessing control. It is primarily a connection of blocks that is joint with cryptographic networks. Every block in the blockchain comprises of timestamp, transaction and hash from the preceding data. Each block contains a hash, timestamp, and transaction data from the previous block.

The respective study is proposed to develop a secured voting mechanism on the AES-RSA algorithm with Blockchain technique. The manual dataset is encrypted and decrypted by the hybrid AES-RSA algorithm and validated with the data utilised by the Blockchain technique. By utilising the hybrid AES-RSA algorithm, voting process can be secured with cryptography mechanism that validate the data of the user which enhance the overall security of the voting mechanism.

The consensus mechanism, chosen blockchain consensus mechanism is proof of work, tailored for a permissioned private blockchain network, which ensures secure vote validation. Also the data flow and verification passes through blockchain nodes for validation before proceeding to the vote casting and counting stage. An each blocks comprises encrypted data, anonymised voter IDs, timestamps, and has values. The element are cryptographically linked to maintain data integration throughout the voting process.

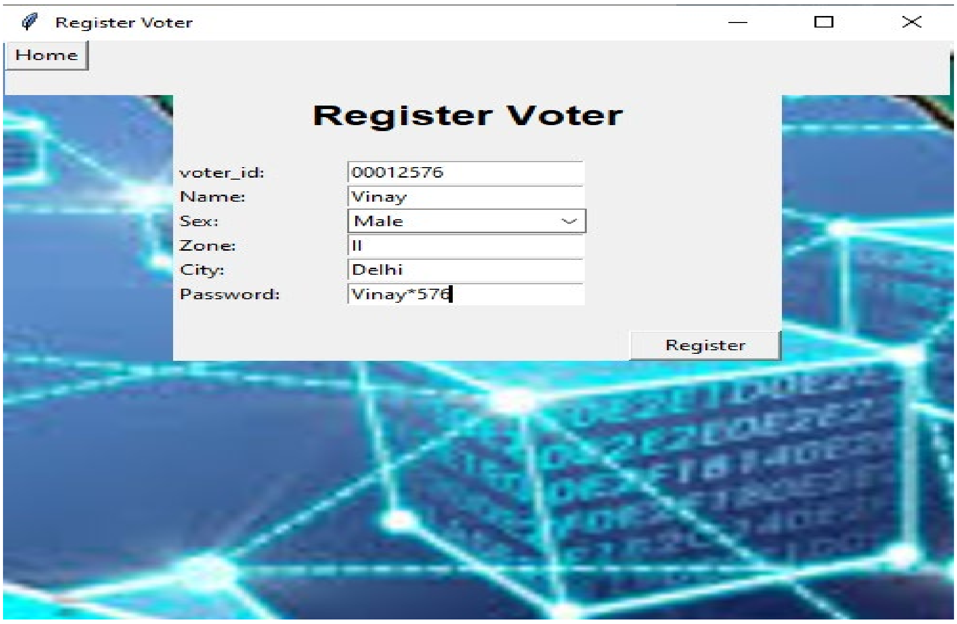
The process of casting a voting begins with the user entering their "VoterID" with a value of "12345". This voter ID is crucial for verifying or casting the vote. Once entered, the voter data is encrypted using AES-RSA encryption, resulting in an encrypted dataset denoted as “encryptedData”, which the byte as a string for example (“b’…5e4e9f8d21a…”). Following this, a check is performed on the dataset, indicated by dataSetCheck, which returns a Boolean values namely true or false to determine the voter ID data is present in the checks are successful, AES-RSA decryption is applied to retrieve the original data, resulting in decryptedData, which confirms the user’s identify and their voting data (b'User data: ID 12345, Vote data...'). Next the voter will submit their vote using voterData for instance b’vote: Yes’. During this procedure, a verification is made to check for any discrepancies in the Voter ID, shown as voterIDMismatch, which provides a Boolean value indicating if there is a difference between the input Voter ID and the expected information. Ultimately, the system verifies if the vote has been effectively submitted with voteStatus, which also provides a True/False Boolean value to show the result of the voting process. This helps to increase the practical applicability

4.0. Proposed Methodology

The results obtained from the execution of the proposed hybrid AES-RSA algorithm with Blockchain is shown in this section. The performance metrics used for analysis is described. Experimental and comparative analysis results are finally declared. Dataset utilised in the respective approach is the manual dataset.

4.1. Experimental results

The experimental results attained by the respective model in the manual dataset is used for secured voting mechanism. The result of overall performance is validated in terms of time in encryption and decryption process, block size and verification time attained by the proposed mechanism. The dataset is analysed and predicted for secured voting system. Figure.4 represents the information of voter such as voter id, name, sex, zone, city and password.



Register Voter

voter_id:	00012576
Name:	Vinay
Sex:	Male
Zone:	II
City:	Delhi
Password:	Vinay*576

Figure 4. Voter’s Information

The encryption and decryption time of the proposed model is signified in table 1. and the figure 5. represents the processing time of the proposed secured voting mechanism.

Table 1. Processing Time of the Proposed Mechanism

Input Size	Encryption Time	Decryption Time(ms)
512	0.017	0.018
1536	0.025	0.028
3345	0.046	0.046
4096	0.068	0.054

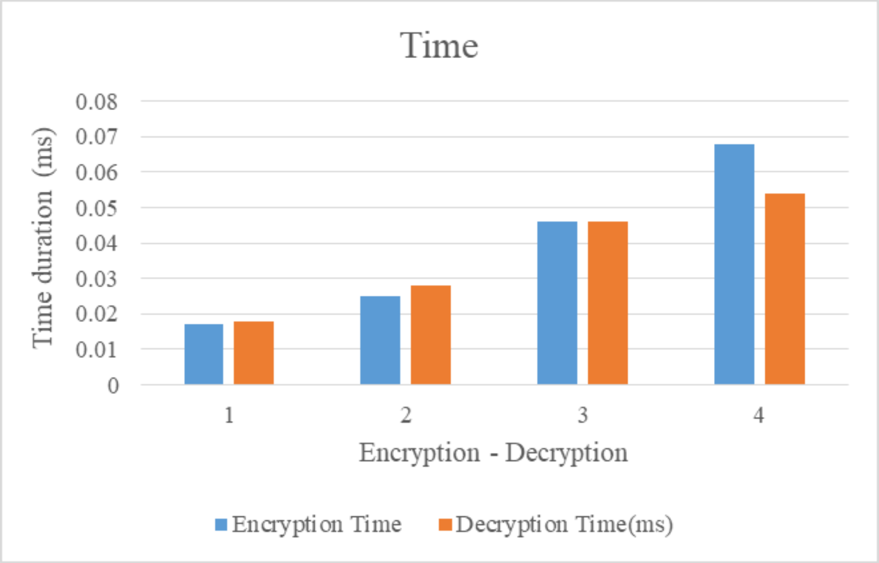


Figure 5. Processing Time of Proposed Secured Voting Mechanism

The time taken for the encryption and decryption is based on the key length. From table 1. it is inferred that as the input size increases, the processing time is also increased. It produced 0.068ms for encryption time and 0.054ms for decryption time for 4096 input key size. The table 2. signifies the time taken for the AES-RSA cryptography process in terms of key length and the figure 6 represents the AES-RSA processing time with the key length in the proposed secured voting mechanism.

Table 2. Processing Time of AES-RSA with Key Length

Key Length	Time by AES - RSA
1024	0.359
2048	3.32
3072	17.52
4096	28.98

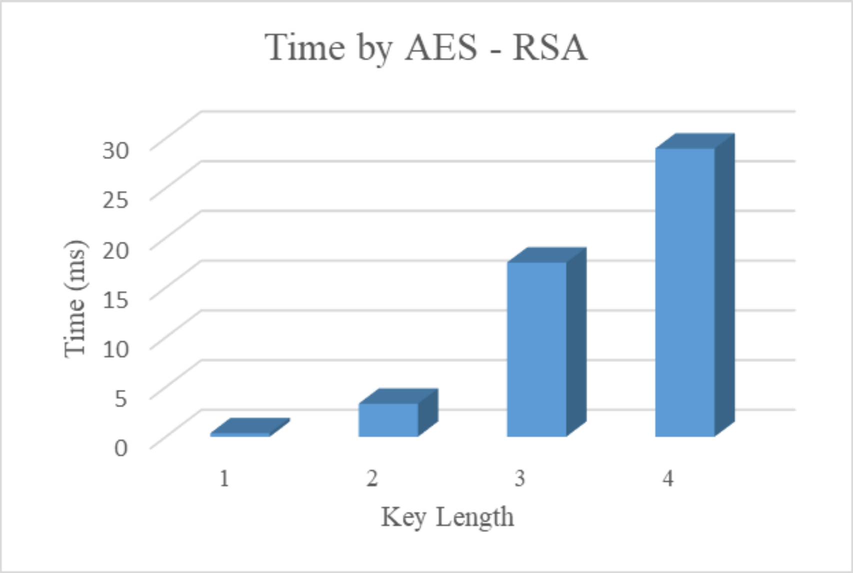


Figure 6. AES-RSA Processing Time with Key Length

The table and graphical representation denotes the processing time taken by AES and RSA. Here the time increases as the key size increases. For input key size 4096, the processing time taken by AES-RSA is 28.98ms. The sample text used in the system and their corresponding encoded format is shown in table 3.

Table 3. Encoded Text

Text	Encoded
12232	efa8ae
Vinay	9e751ee7d117
male	dsa8a
MP	895e1fd4060d6c
Bhopal	77e702
156	fef
5	8375
32	6a80d5f3a4

The vote details taken as input for data privacy are encoded by converting plain text into cipher text, as shown in table.

4.2. Comparative Analysis

Numerous algorithm and mechanism used by the Conventional methods and the produced results thus attained are compared with the respective method. Different existing methods and the time duration is represented in the table 4. and the figure 7. signifies the encryption time of the different existing methods.

Table 4. Performance Analysis Based on Time [19]

	Encryption time duration(ms)	
Voters	Existing Model	Proposed Model
Voter 1	94	80
Voter 2	89	78
Voter 3	91	80.4
Voter 4	87	78.8
Voter 5	90	79.8

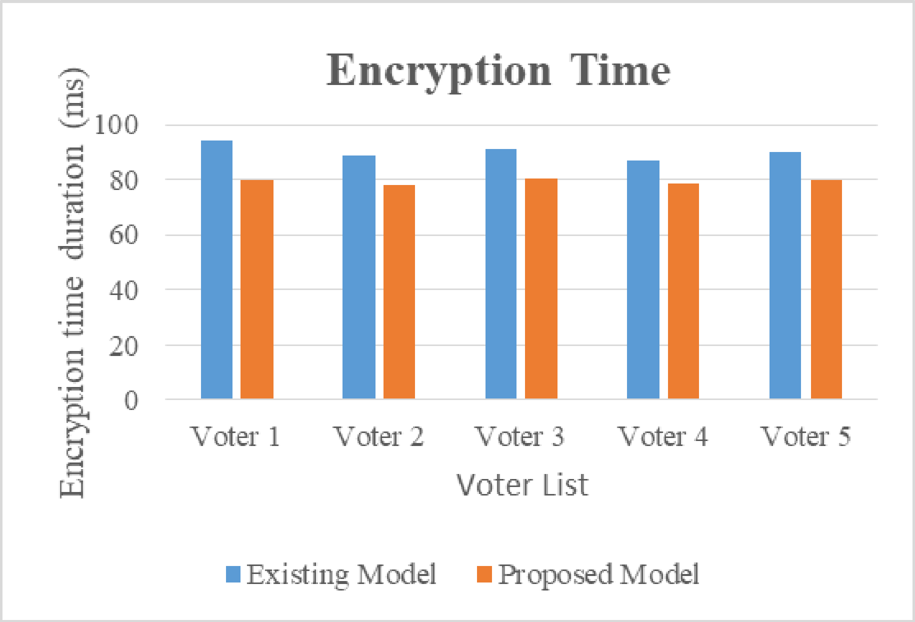


Figure 7. Performance Analysis of the Secured Voting Mechanism in Terms of Encryption Time

The encryption time taken by the existing method are high when compared with proposed system. The time taken for process for voter 5 by existing method is 90ms, but the proposed system uses only 79.8ms for encryption. The comparison of the proposed mechanism, with the existing method for the secured voting mechanism is show in the figure 5. It signifies the running time of the each voter. The table 5. represents the comparative analysis of the proposed model with the existing model in terms of processing time.

Table 5. Comparative Analysis of the Proposed Model with Existing Model [20]

Number: Operation	Existing Model		Proposed Model
A. Generate Public / Private Keys	36.19		28.34
B. Verify f(i,j) other voters	0.23		0.1
C. Compute Public key	4.01		2.6
D. Sub Secret Reconstruct	0.08		0.02
Total Time Taken	40.51		31.06

The comparative analysis of the proposed model performance with the existing model are based on the time taken for the encryption, decryption process and verification process. The AES-RSA with blockchain increases computational speed with decreased time consumption.

Table 6. Proposed AES-RSA Blockchain System

Metric	Proposed AES-RSA Blockchain System
Encryption Time (per vote)	100ms
Decryption Time (per vote)	80ms
CPU Usage during Encryption/Decryption	25% (average), 65% (peak under load)
Memory Usage (per vote)	100MB - 150MB
Throughput (votes per second)	200 votes/sec (with 50 active users)
Blockchain Bloc Verification Time	200ms (average), 500ms (peak under load)
Time to Create a Block	250ms (average), 500ms (peak under load)
Vote Casting Time	50ms - 100ms
Scalability	Decreases in throughput under high load; could benefit from optimization (sharding, PoA)
Security .	Enhanced by AES-RSA and verified by blockchain
Blockchain Integration	Integrated for vote verification and data integrity

Table 6. Summarized by addressing the aspects, the evaluation of the AES-RSA and block chain system can be significantly enriched, the demonstrating the potential area for improvement within the evolving landscape of e-voting technology.

5. Conclusion

Security measures for digitally casted votes are crucial to prevent large scale embezzlement and fraudulent. The proposed system employed AES and RSA cryptographic algorithms along with blockchain approach, to ensure privacy with increased accuracy and integrity. The original data of voting individual was verified with the output data from the EVM. Mismatching of votes were identified and was not casted. The precision of the proposed system was compared with other conventional methods. Further the performance metrics of the system was evaluated with encryption and decryption time, block size and verification time. The results produced better reliability and integrity of security in EVM, as the proposed system consumed less time when compared with existing methods. It provided 0.068ms for encryption and 0.054ms for decryption for 4096 key size which is less when compared with existing methods. It can also be enhanced by deploying different cryptographic algorithms. The societal implication of robust data privacy and election integrity are significant for maintaining public trust in democracy. By demonstrating the effectiveness of the hybrid cryptographic approach and utilizing decentralised validation, proposed systems can enhance confidence in digital elections, potentially increasing voter participation, this approach may also facilitate global adoption of secure online voting, making the electron process more accessible and efficient. The practical implementation of the proposed e-voting system faces challenges, including the need for robust infrastructure, secure voter devices, and integration with existing electoral systems. The compliance with regulation like GDPR and HAVA is essential. The limitation include, potential latency from blockchain consensus mechanisms must be recognised, particularly, in large decentralized networks, as this may impact real time voting scenarios and required optimizations. Moreover a balance between enhanced security and potential delays in encryption, decryption times should be discussed as the trade-off, could affect the voter experience during large-scale elections. The future work is to emphasize real world testing through pilot programs, optimizing blockchain architecture with improved consensual algorithm and enhancing cryptography with post quantum solutions and light-weighted algorithms such as elliptic curve cryptography (ECC). Additionally, ensuring regulatory compliance and integrating the decentralized identity solution for voter authentication will be crucial for successful deployment.

References

[1] A. Solankar, "Secure E-Voting System Using Visual Cryptography & Block Chain Ledger," *Turkish Journal of Computer and Mathematics Education (TURCOMAT),* vol. 12, no. 1S, pp. 7-12, 2021.

[2] A. Alotaibi, L. Alhubaidi, A. Alyami, L. Marghalani, B. Alharbi, and N. Nagy, "Preventing Phishing Attack on Voting System Using Visual Cryptography," *Journal of Computer and Communications,* vol. 10, no. 10, pp. 149-161, 2022.

[3] S. Priya, G. Srivastava, and S. Kumar, "Secured Electronic Voting Transactions Integrated with Blockchain," 2021.

[4] S. Tanwar, N. Gupta, P. Kumar, and Y.-C. Hu, "Implementation of blockchain-based e-voting system," *Multimedia Tools and Applications,* vol. 83, no. 1, pp. 1449-1480, 2024.

[5] C. Toma, M. Popa, C. Boja, C. Ciurea, and M. Doinea, "Secure and Anonymous Voting D-App with IoT Embedded Device Using Blockchain Technology," *Electronics,* vol. 11, no. 12, p. 1895, 2022.

[6] B. Ali, F. Iqbal, I. Hussain, and M. Younas, "An Efficient E-Voting Algorithm and Dapp Using Blockchain Technology," *Multidisciplinary International Journal of Research and Development (MIJRD),* vol. 1, no. 03, pp. 60-69, 2022.

[7] K. N. Rahman, M. W. Hridoy, M. M. Rahman, M. R. Islam, and S. Banik, "Highly secured and effective management of app-based online voting system using RSA encryption and decryption," *Heliyon,* vol. 10, no. 3, 2024.

[8] E. Daraghmi, A. Hamoudi, and M. Abu Helou, "Decentralizing Democracy: Secure and Transparent E-Voting Systems with Blockchain Technology in the Context of Palestine," *Future Internet,* vol. 16, no. 11, p. 388, 2024.

[9] S. Gupta, K. K. Gupta, and P. K. Shukla, "Improving the End-to-End Protection in E-Voting Using BVM—Blockchain-Based E-Voting Mechanism," *Concurrency and Computation: Practice and Experience,* p. e8324, 2024.

[10] R. K. Muhammed, K. H. A. Faraj, J. F. Gul-Mohammed, T. N. A. Al Attar, S. J. Saydah, and D. A. Rashid, "Automated Performance analysis E-services by AES-Based Hybrid Cryptosystems with RSA, ElGamal, and ECC," *Advances in Science, Technology and Engineering Systems Journal,* vol. 9, no. 3, pp. 84-91, 2024.

[11] K.-L. Tsai, F.-Y. Leu, I. You, S.-W. Chang, S.-J. Hu, and H. Park, "Low-power AES data encryption architecture for a LoRaWAN," *IEEE Access,* vol. 7, pp. 146348-146357, 2019.

[12] S. Ajish and K. AnilKumar, "Secure mobile internet voting system using biometric authentication and wavelet based AES," *Journal of Information Security and Applications,* vol. 61, p. 102908, 2021.

[13] B. A. Oke, O. M. Olaniyi, A. Aboaba, and O. T. Arulogun, "Securing electronic voting system using crystographic technique," 2019.

[14] O. S. Adewale, O. K. Boyinbode, and E. A. Salako, "Visual semagram: An enhanced technique for confidentiality requirement of electronic voting system," *International Journal of Computer Network and Information Security,* vol. 12, no. 4, pp. 51-59, 2020.

[15] S. Latif and T. Anees, "Blockchain based Decentralized Electronic Voting System: A Step towards Transparent Elections," *IJCSNS,* vol. 19, no. 12, p. 165, 2019.

[16] K. G. Houlder, P. Nithishwar, G. Santhosh, and E. Venkatesh, "A Secure Verifiable Internet Voting System Using Identity Based Encryption And Decryption."

[17] S. Jayanti, K. Chittibabu, P. Chaganti, And C. Sekhar, "A Novel Cryptosystem Of An Upgraded Classical Cipher And Rsa Algorithm For A Secure And An Efficient Electronic Voting System," *Journal of Theoretical and Applied Information Technology,* vol. 101, no. 4, 2023.

[18] J. Bhatti, S. Chachra, A. Walia, and A. Vishal, "Secure electronic voting machine using multi-modal biometric authentication system, data encryption, and firewall," *International Journal of Performability Engineering,* vol. 15, no. 10, p. 2570, 2019.

[19] R. Taş and Ö. Ö. Tanrıöver, "A manipulation prevention model for blockchain-based e-voting systems," *Security and communication networks,* vol. 2021, pp. 1-16, 2021.

[20] J. Lyu, Z. L. Jiang, X. Wang, Z. Nong, M. H. Au, and J. Fang, "A secure decentralized trustless E-voting system based on smart contract," in *2019 18th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/13th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE)*, 2019: IEEE, pp. 570-577.