IoT Enabled Secure Voting System utilizing Fingerprint Authentication for Enhanced Security using Blowfish cipher

Dr. Somu. K[1], Mr. Pandiyan.K. S[2], Arivumani.P[3], Arul.A[4], Sathish Kumar.A[5]
[1]*Professor, Department of Electronics and Communication Engineering, Maha Barathi Engineering College, (Affiliated to Anna University), Chinnasalem (Tk), Kallakurichi (Dt)-606 201.*
[2]*Assistant Professor, Department of Electronics and Communication Engineering, Maha Barathi Engineering College, (Affiliated to Anna University), Chinnasalem (Tk), Kallakurichi (Dt)-606 201.*
[3,4,5] *UG Students, Department of Electronics and Communication Engineering, Maha Barathi Engineering College, (Affiliated to Anna University), Chinnasalem (Tk), Kallakurichi (Dt)-606 201.*

***Abstract*—Over the years, the voting process has faced issues with data security. Voting data can be easily exploited using the Internet of Things (IoT), yet the security of the prediction process is insufficient. To address the problems associated with the Blowfish cipher, encrypted and decrypted data from the voting process are considered. Furthermore, the Rivest–Shamir–Adleman cryptography is crucial for identifying sensitive and non-sensitive data and assessing key generation for public and private data within the individual process. Additionally, the Automated Fingerprint Identification System (AFIS) analyzes the pixels of the voting data. Calculating the height and width of the data enables automatic performance detection. Ultimately, the proposed method shows that these values relate to the voting data regarding security and performance efficiency. The voting data is a test and validation, ensuring more reliable and trustworthy results. To prevent multiple data entries for the same individual, verifying all votes in the database and maintaining a standardized, stable, and secure process is essential, making it applicable for broader performance use. The process is more reliable with a high level of performance, and the proposed method ensures standard scalability. The suggested techniques reduce time complexity and power consumption, achieving performance within an accurate range of 90%.**

I. INTRODUCTION

The voting counting process maintains security by using IoT technology. It is a highly reliable method with a standard performance stability level. Fingerprint scanning is one of the most advanced techniques to capture biometrics, focusing on reducing multiple votes from the same individual [1]. Blockchain technology ensures encryption and decryption, with each data point collected securely. The EVM evaluates secure features regarding reliability, performance metrics, scalability, and usability of the process, addressing issues such as poll violence and long queues to cast votes [2]. The online voting process also maintains a higher level of security and lower complexity in its techniques, assisting all citizens in voting. The presented method increases trust, security, and transparency among member organizations by enhancing the traceability of data shared across a network.

The e-voting process maintains trustworthiness and high scalability to reduce integrity and time complexity. The ECC prevents data corruption and ensures system stability by automatically detecting and correcting errors. Multifactor authentication minimizes issues like voting rigging, impersonation, and falsification [3]. The presented techniques analyze multiple data points within a specific timeframe and complete internal tasks seamlessly. Critical situations are handled effectively, making them suitable for various process applications. The RSA secure communication method delivers high performance and greater efficiency in the outcomes of the techniques.

The secure voting system presents challenges in maintaining secure processes at all times, and the military-level factors involved are impacted by the high computational costs associated with them [4].

IoT technology utilizes collected data stored in the cloud; occasionally, data may be overlooked due to substantial implementation costs in practical processes. The proposed method is essential for enhanced consumption while maintaining high energy efficiency. The most advanced fingerprint technology uses digital platform ID, or unknown data, for the voting process, allowing multiple voter data points from the same individual [5]. A lack of transparency and limited application can sometimes signal issues with performance. The presented method frequently encounters integrity concerns due to the high level of interference in the process.

The main contribution involves using distinct keys for encryption and decryption and a computer database that stores and compares fingerprints quickly and accurately to identify individuals. The process enhances the security of the voting data during performance evaluations. The decryption maintains the voting data's privacy to uphold the voting data's privacy.

II. LITERATURE SURVEY

According to the traditional method, Electronic Voting Machines (EVMs) are used for counting votes; however, the presented method is unreliable and prone to misuse in the voting process [6]. The proposed system captures and stores voters' fingerprints in a database during registration, preventing multiple registrations by the same individual. However, this process poses risks of data theft, false negatives, and positives and incurs high-performance costs.

The Internet of Things (IoT) technology involves collecting voting data stored in the network connection of the process. This technology focuses on poll violence and the long waits in queues to cast votes due to low security and data loss [7]. The proposed method uses Blockchain technology that maintains a standard level of reliability in voting performance. However, the process consumes more power and sometimes encounters signal issues with the techniques.

The encryption and decryption techniques ensure the security of the data in the voting process, reduce signal issues, and maintain performance scalability [8]. The proposed method, Rivest-Shamir-Adleman, enhances accessibility and convenience, ultimately contributing to the evolution of online voting systems. However, the process has slow performance levels, low reliability, and is more computationally costly.

The EVM techniques ensure accurate vote counting and prevent multiple voting by the same individual. However, the process has low accuracy and significant complexity [9]. The proposed method involves biometric fingerprint detection, analyzing performance, and achieving high effectiveness. However, the process faces scanner issues and environmental impacts on performance.

Convolutional Neural Elliptical Curve Blockchain (CbECB) enhances security in the voting process and offers a multi-secret image-sharing security system. However, the method presented is not suitable for all types of applications [10]. The proposed method utilizes Elliptic Curve Cryptography (ECC), a reliable and versatile approach that significantly impacts performance metrics, including time, memory usage, and cost reduction. Nevertheless, the implementation process is complex and depends on random number generators.

The EVM technology uses polling places, its analysis in the voting counts, and maintaining security in the voting process, but the easy misuse of the electoral machine in the performance [11]. The proposed method is a fingerprint sensor that detects the face and fingerprint and evaluates the secure feature of a high level of authenticity, dependability, and usability. However, the process is a high-cost range, and implementation in the stability is complex in the performance.

Multifactor authentication (MFA) is a distributed e-voting system that addresses the issues of vote rigging, voter impersonation, and vote falsification while enhancing stability despite its slow performance levels [12]. The proposed method, Blockchain, reduces integrity and authentication concerns, promoting credible e-democratic decision-making in digitally enabled voting scenarios. However, these techniques cause network issues and high power consumption.

Aadhar-linked biometrics, such as fingerprint and facial scans, Secure Vote offers a novel way to strengthen the democratic process. Still, it faces issues with biometric authentication failures and data mix-ups [13]. The proposed method is a Local Binary Pattern Histogram (LBPH), reducing privacy protection, safeguarding data, and accommodating individuals without Aadhar presents significant challenges. However, the process involves limited global information and high computational costs of the techniques.

Blockchain technology is a distributed mechanism based on a consensus process for storing and securing information; however, this process has scalability limitations and high energy consumption [14]. The proposed method, homomorphic-assisted hash-based encryption (HAHE), ensures the performance of every individual voting data encryption. However, the process is at a slow level of performance speed and has limited practical implementations.

The Data Encryption Standard (DES) is a form of encryption; however, in the case of online voting, the data transferred between the client (in this case, the voter) and the server is highly sensitive. DES cannot provide sufficient security [15]. The proposed method is the Advanced Encryption Standard (AES), which securely encrypts voter data, making online voting much more reliable and secure. However, the process has limited storage capacity, increased time complexity, and a high computational cost.

III. PROPOSED METHODOLOGY

The section decrypts the voting data, while encryption represents a public key view of the voting data. It calculates each individual's fingerprints and tests validation in the pixel values of the process. It is divided into two separate values: left and right. These values correspond to the voting data related to is efficient of the secure performance.

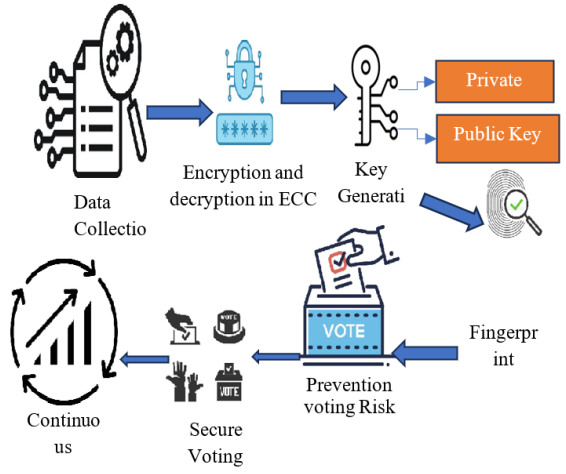

Fig .1. Secure Voting System Using Blowfish Cipher

Figure 1.1 shows a process that enhances the security of voting data during performance evaluations. The decryption maintains the privacy of the voting data.

A. Dataset Description

The section includes voter details, the security system, status, exits, names, and passwords and generates reports. "Add Citizens" and "Generate Report" are displayed, and the election results, along with the reset database, are shown after the report is generated.

	A	B	C	D	E	F	G	H	I	J	K	L
1	Council	Date	Title	Resolutio	TOTAL VO	NO-VOTE	ABSENT O	NO COUN	YES COUN	Link	token	SENEGAL
2	Security C	########	Security C	S/RES/232	15	0	0	0	15	https://di	852025	Y
3	Security C	########	Security C	S/RES/252	15	0	0	0	15	https://di	3866679	
4	Security C	########	Security C	S/RES/232	15	0	0	0	15	https://di	852028	Y
5	Security C	########	Security C	S/RES/232	15	0	0	0	15	https://di	852020	Y
6	Security C	########	Security C	S/RES/162	15	0	0	0	15	https://di	557118	
7	General A	########	Reducing	A/RES/76/	193	4	14	50	125	https://di	3950570	Y
8	General A	########	Reduction	A/RES/58/	191	16	43	4	128	https://di	508018	Y
9	General A	########	Implemer	A/RES/76/	193	5	19	0	169	https://di	3950569	Y
10	General A	########	Nuclear-w	A/RES/58/	191	12	8	3	168	https://di	508016	Y
11	General A	########	Implemer	A/RES/76/	193	10	21	8	154	https://di	3950571	Y
12	General A	########	Transpare	A/RES/58/	191	14	27	0	150	https://di	508023	Y
13	General A	########	Implemer	A/RES/58/	191	15	23	0	153	https://di	508021	Y
14	General A	########	Establishr	A/RES/76/	193	12	2	1	178	https://di	3950572	Y
15	General A	########	Illegal Isra	A/RES/ES-	188	9	5	2	172	https://di	426078	Y
16	General A	########	A path to	A/RES/58/	191	11	14	2	164	https://di	508027	Y
17	General A	########	Rights of t	A/RES/61/	192	6	0	1	185	https://di	589951	Y
18	General A	########	Conclusio	A/RES/76/	193	8	59	0	126	https://di	3950573	Y
19	Security C	########	Security C	S/RES/132	15	15	0	0	0	https://di	426132	
20	General A	########	Comprehe	A/RES/58/	191	13	4	1	173	https://di	508032	Y

Fig .2. Voting Dataset

Figure 1.2 measures the security and enhances the efficiency of the process while maintaining state stability and trustworthiness of the performance, which can be used for more applications of the performance dataset.

B. Cryptography Rivest–Shamir–Adleman algorithm

The section key generation is separate from the encryption and decryption of the voting data. The encryption is a public key view of the voting data, and the decryption maintains its privacy.

Equation 1 represents an encryption that is a public key generated in the voting data, and it reduces the unknown voting data. Let's assume the z-public key, m, n-encryption voting data.

$$z = m \times \mathrm{n} \qquad (1)$$

Equation 2 represents a decryption using a private key generated within the voting data, which enhances the maintenance of privacy in that data. Let's assume the q-private key, p,q-Decryption voting data

$$\mu(p) = q_{ij}(p-1, q-1) \qquad (2)$$

Equation 3 measures the overall data encryption in voting performance, and let's assume the Si-total encryption voting data, q, s- input voting data.

$$s_i = k^t (mod\ f) \qquad (3)$$

Equation 4 measures the overall decryption of data in voting performance, and let's assume the Sj-total decryption data.

$$s_j = t^e (mod\ f) \qquad (4)$$

C. Automated Fingerprint Identification System *(AFIS)*

The section measures the height and weight of fingerprints, calculates each fingerprint, and testing

validation in the pixel values of the process, and determines to detect the performance automatically. Equation 5 is a measure in the direction of the fingerprint of the voting data in the multiple databases of the process, and let's assume the Kp-direction of pixels, Hj-multiple data

$$k_p = (max\ h_j) \quad (5)$$

Equation 6 is the total number of the height and width of the measurements in all voting data of the fingerprint values; let us assume the l-height-width

$$h_j = \sum_{(p,q)\in N} s_j(l,w) \times y(l,w) \quad (6)$$

Equation 7 is calculated based on each pixel of the performance fingerprint data; let's assume the p, q—voting data values and the Sj-Total number of pixels.

$$k_p = \left(\frac{\sum_{(p,q)\epsilon block(p,q)}}{M}\right) \quad (7)$$

D. Blowfish Cipher Algorithm

The section refers to all essential validation for a secure and efficient process. It is divided into two separate values: left and right. These values correspond to the voting data concerning security and performance efficiency.

Input: No of Voting Data
Output: Secure Efficient Voting Data
Start
Divide the section values in Xleft and XRight.
for i=1
XLeft=XLeft XOR Pi;
XLeft and XRight should be efficient;
END
XRight=Y(XLeft)XOR XRight:
XLeft and XRightXOR Pj;
XLeft=XLeft XOR pi;
XLeft and XRight should not be efficient;

The section represents a change in the voting data values, representing a new sequence in the process. The performance is more secure and reliable due to the implemented techniques. Let's assume x and y are input variables, Pi is secure voting data, and Pj is low-efficient voting data.

IV. RESULT AND DISCUSSION

This section assesses the encryption, decryption, security analysis, throughput, and time complexity across multiple parameters and methods. The proposed approach can also be applied to secure and efficient IoT technology, utilizing 7,856 data points in the attack dataset.

Table 1. Simulation Parameter

Simulation process	Parameter Name
Dataset	Secure Voting Dataset
No of Dataset	7856
Testing Data	4,856
Training data	3000
Language	C program

As illustrated in Table 1, the simulation parameters were evaluated through 7856 data collected in the feature selection process. 4,856 is a training dataset, and 3000 is a testing dataset.

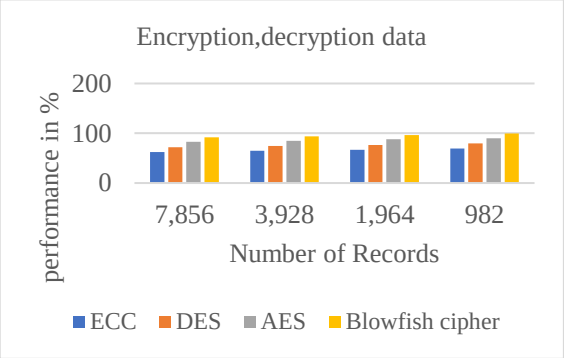

Fig .3. Analysis of Encryption and Decryption Data

Figure 1.3 illustrates using precision analysis for secure voting data exchange through IoT technology. This review assesses previous methods, including ECC and AES DES, and contrasts them with the proposed Blowfish cipher data method. The precision levels of the performance ratings for these methods are 85.6, 89.9, and 99.2, respectively, for the various performance levels in data protection.

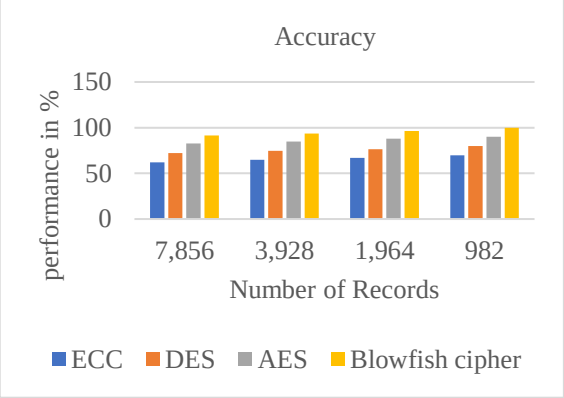

Fig .4. Analysis of Accuracy

Figure 1.4 illustrates using accuracy analysis for secure voting data exchange through IoT technology. This review assesses previous methods, including ECC and AES DES, and contrasts them with the proposed Blowfish cipher data method. The precision levels of the performance ratings for these methods are 85.6, 89.9, and 99.2, respectively, for the various performance levels in data protection.

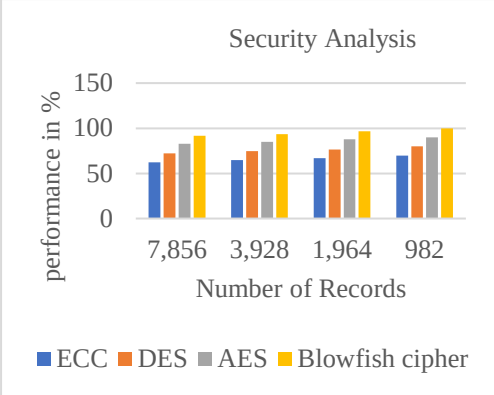

Fig .5. Analysis of Security

Figure 1.5 illustrates using reliability analysis for secure voting data exchange through IoT technology. This review assesses previous methods, including ECC and AES DES, and contrasts them with the proposed Blowfish cipher data method. The precision levels of the performance ratings for these methods are 85.6, 89.9, and 99.2, respectively, for the various performance levels in data protection.

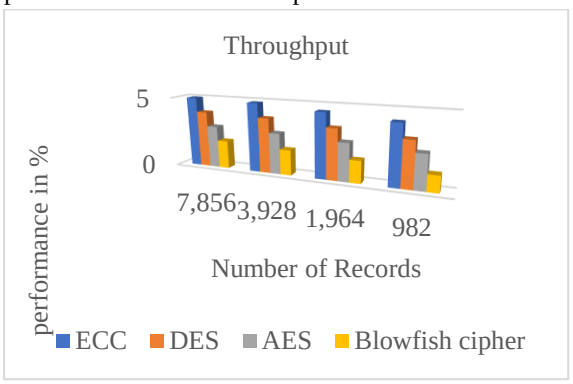

Fig .6. Analysis of Throughput

Figure 1.6 illustrates using Throughput analysis for secure voting data exchange through IoT technology. This review assesses previous methods, including ECC and AES DES, and contrasts them with the proposed Blowfish cipher data method. The precision level of the performance ratings for these methods is 4.65, 3.95, and 1.25, respectively, for the various performance levels in data protection.

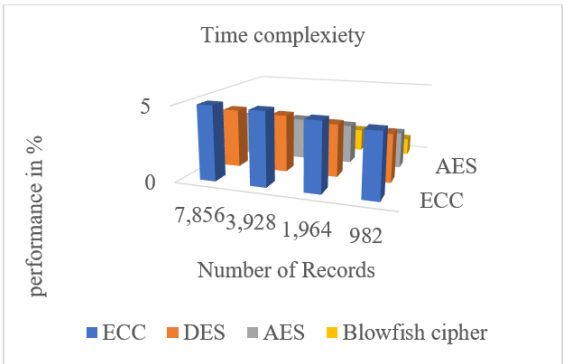

Fig .7. Analysis of Time Complexity

Figure 1.7 illustrates using time complexity analysis for secure voting data exchange through IoT technology. This review assesses previous methods, including ECC and AES DES, and contrasts them with the proposed Blowfish cipher data method. The precision levels of the performance ratings for these methods are 4.65, 3.95, and 1.25, respectively, for the various performance levels in data protection.

V. CONCLUSION

This study analyzes the crucial role of IoT techniques in enhancing throughput, security, time complexity, and accuracy. Prediction analysts respond to voting data, which is more secure in the process, and maintain standard scalability and high trustworthiness performance. To identify the sensitive and non-sensitive aspects of the data, measure the public and private key generation performance. All voting data is collected through the encryption and decryption techniques. The presented method is measured in fingerprint height and weight, along with the validation and testing of the voting data. The process effectively handles any critical situation, is completed within a specific time frame, and performs with multitasking efficiency while maintaining reliability. The process has achieved a 90% accuracy rate in fraud detection.

REFERENCE

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

[2] Ahmad, Masood, et al. "Security, usability, and biometric authentication scheme for electronic voting using multiple keys." *International Journal of Distributed Sensor Networks* 16.7 (2020): 1550147720944025.

[3] Hossain Faruk, Md Jobair, et al. "Transforming online voting: a novel system utilizing blockchain and biometric verification for enhanced security, privacy, and transparency." *Cluster Computing* 27.4 (2024): 4015-4034.

[4] Gowtham, R., A. Mohankumar, and B. Gokul. "Enhancing Electoral Integrity: A Fingerprint-Verified Voting System for Fair and Secure Elections." *Asian Journal of Applied Science and Technology (AJAST)* 8.1 (2024): 33-46.

[5] Gangadurai, E., R. Divakaran, and U. Aruneshwaran. "Fingerprint-Based Voting System." *Journal of Telecommunication Study* 8.2 (2023): 30-38.

[6] Kumar, C. Ashok, et al. "Ensuring trustworthy elections with dual biometric verification using facial and fingerprint recognition." *Integrated Technologies in Electrical, Electronics and Biotechnology Engineering*. CRC Press, 2025. 256-261.

[7] Krishnamurthy, R., Geetanjali Rathee, and Naveen Jaglan. "An enhanced security mechanism through blockchain for E-polling/counting process using IoT devices." *Wireless Networks* 26.4 (2020): 2391-2402.

[8] Rahman, Kazi Naimur, et al. "Highly secured and effective management of app-based online voting system using RSA encryption and decryption." *Heliyon* 10.3 (2024).

[9] Chakraborty, Shubhranil, et al. "Designing a biometric fingerprint scanner-based, secure and low-cost electronic voting machine for India." *International Journal of System of Systems Engineering* 12.4 (2022): 354-370.

[10] Samayamanthula, Venkata Chinnaiah Gupta, and Satya Prasad Kodati. "An effective E-voting enhancement system through multi secret image sharing security system." *Knowledge-Based Systems* 315 (2025): 113239.

[11] Tuptewar, Piyush, et al. "Enhanced Security with Biometric Authorization in Smart Voting Machine." *Available at SSRN 5040474* (2024).

[12] Olaniyi, Olayemi Mikail, et al. "A secure electronic voting system using multifactor authentication and blockchain technologies." *Blockchain Applications in the Smart Era*. Cham: Springer International Publishing, 2022. 41-63.

[13] MOLINA, Walter M., and Daniel SUBAUSTE. "Improving the Integrity of a Voting Process with Biometric Authentication and Data Encryption." *Journal of Systemics, Cybernetics and Informatics* 21.2 (2023): 39-46.

[14] Elhoseny, M., et al. "An efficient and secured voting system using blockchain and hybrid validation technique with deep learning." *Peer-to-Peer Networking and Applications* 18.2 (2025): 1-21.

[15] Lalit Kumar Gupta "AES Based Online Voting System", March 2019International Journal of Computer Sciences and Engineering 7(3):915-918 DOI:10.26438/IGCSE/v7i3.915918