SSRG International Journal of Electronics and Communication Engineering
ISSN: 2348-8549/ https://doi.org/10.14445/23488549/IJECE-V11I4P107

Volume 11 Issue 4, 60-67, April 2024

Original Article

Enhanced Security Measures for Medical IoT Communication through Biological Feature-Based Elliptic Curve Cryptography Authentication

Vijaya Kumar Vadladi[1], D Marshiana[2]

[1]*Department of ECE, Sathyabama Institute of Science and Technology (Deemed to be University), Tamil Nadu, India.*
[2]*Department Department of Electronics and Telecommunication, Symbiosis Institute of Technology, (Symbiosis International Deemed University), Maharastra, India.*

[1]*Corresponding Author : vijay20052009@gmail.com*

Received: 09 February 2024 Revised: 06 March 2024 Accepted: 06 April 2024 Published: 30 April 2024

Abstract *- Medical IoT devices often collect, transmit, and communicate sensitive patient health data. Ensuring robust security measures is essential to protect patient privacy and confidentiality during data transmission. Unauthorized access to this data can lead to privacy breaches, identity theft, or misuse of personal health information. Many researchers are trying to develop secure communication for medical IoT devices. Conventional methods, such as RSA-based authentication, require more data space and processing time, posing challenges for resource-constrained medical IoT devices. Additionally, the traditional system provides a single level of security and focuses only on internal control techniques. To overcome these limitations, a double level of security and external error control techniques-based authentication algorithm is proposed. The proposed authentication employs Elliptic Curve Cryptography (ECC) and DNA computing techniques combined to solve the memory space problem and processing time, respectively. Here ECC helps to encrypt the medical document using the private key and public key data to provide a double level of security while performing the authentication process. Also, the DNA computing technique is used to encode the original medical content since it has the capacity to store a large amount of data. From the simulation results, the proposed ECC-based double-level encryption process uses only a limited amount of time to execute both the encryption and decryption time. It also shows that the proposed authentication algorithm requires a lesser number of communication bits and a lesser storage amount of data compared with other traditional methods.*

Keywords *- Medical Internet of Things, IoT communication, Elliptic Curve Cryptography, DNA computing, Double level of encryption.*

1. Introduction

In the modern medical environment, it is necessary to collect and transmit sensitive patient health data in a secure environment. Researchers need to ensure robust security measures which very are essential to protect patient privacy and confidentiality. Unauthorized access to this data could lead to privacy breaches, identity theft, or misuse of personal health information [1, 4].

For example, in May 2017, one historical event happened that exemplifies the importance of ensuring robust security measures for protecting patient health data involves the cyberattack on the UK's National Health Service (NHS). During this incident, ransomware known as WannaCry infected thousands of computers within the NHS network, affecting hospitals and healthcare facilities across the country. The WannaCry ransomware exploited vulnerabilities in outdated Windows operating systems, encrypting data on infected computers and demanding ransom payments in exchange for decryption keys. As a result of the attack, many NHS hospitals were forced to suspend non-emergency services, divert patients to other facilities, and cancel appointments and surgeries.

The impact of the WannaCry attack on the NHS demonstrated the critical importance of cybersecurity in healthcare and the need for robust security measures to protect patient health data. The attack not only disrupted healthcare services but also raised concerns about the vulnerability of medical IoT devices and the potential risks associated with unauthorized access to sensitive patient information.

In response to the WannaCry incident, healthcare organizations worldwide have since heightened their focus on cybersecurity, implementing stronger security protocols, updating software systems, and investing in advanced

cybersecurity technologies to safeguard patient health data and mitigate the risk of future cyberattacks. There are so many cryptographic techniques, such as Rivest-Shamir-Adleman (RSA), Digital Signature Algorithm (DSA), Message Digest Algorithm, and Secure Hash Algorithm (SHA) are available to prevent the attack mentioned above. Especially, Rivest-Shamir-Adleman (RSA) (Rivest-Shamir-Adleman) based authentication methods are cryptographic techniques commonly used for secure communication and authentication.

While RSA encryption can provide security for data transmission and authentication, it may not directly help to avoid specific malware attacks like WannaCry. RSA encryption can be used to encrypt sensitive data transmitted over networks, including patient health data in medical IoT environments. Encrypting data ensures that even if intercepted by attackers, the information remains unreadable without the corresponding decryption key.

RSA encryption can establish secure communication channels between IoT devices and network servers. By encrypting data during transmission, RSA helps to prevent eavesdropping and man-in-the-middle attacks, thus enhancing the security of communication channels.

However, RSA-based authentication methods have their limitations for resource-constrained Medical IoT communication. RSA encryption operations can be computationally intensive, particularly for resource-constrained devices such as IoT devices with limited processing power and memory. This may impact the performance of devices and increase latency in communication. RSA-based authentication requires careful management of cryptographic keys, including key generation, distribution, and storage. Inadequate key management practices, such as weak key generation or improper key storage, can undermine the security of RSA encryption[5].

Considering this problem in mind, enhanced security measures for medical IoT Communication through biological feature-based elliptic curve cryptography authentication is proposed. It helps to maintaining the integrity of medical data is critical for accurate diagnosis and treatment. Security breaches or tampering with medical IoT devices could result in altered or corrupted data, leading to incorrect diagnoses, treatment errors, or compromised patient safety.

The proposed authentication algorithm helps to avoid unauthorized access to implantable medical devices or infusion pumps could result in harmful or even life-threatening consequences for patients to medical IoT devices or networks can pose significant risks, including unauthorized control or manipulation of medical devices, disruption of healthcare services, or even sabotage of critical medical infrastructure. The main contributions of the author are as follows:

- Development of an ECC-based authentication algorithm for authenticating Medical IoT users.
- Implementation of a double-level encryption process to enhance the security level of IoT devices.
- Utilization of external error control techniques instead of internal error control techniques.

The paper is organized as follows: Section 1 outlines the importance of security in medical IoT devices and discusses traditional RSA-based authentication algorithms. Section 2 presents recent research efforts in the field of authentication algorithms. Section 3 elaborates on enhanced security measures for IoT device communication through biological feature-based ECC authentication. Section 4 presents the simulation results and discusses the findings. Finally, the paper concludes.

2. Related Work

The following are the recent works carried out toward the proposed authentication algorithm:

X. Wang et al. [6] proposes a novel approach for enhancing security in medical IoT communication through biological feature-based authentication and analyze the limitations of traditional authentication methods in medical IoT environments and propose a biological feature-based authentication approach. They leverage biometric data, such as DNA sequences or physiological signals, as unique identifiers for authentication.

The authentication process involves integrating biological feature data with Elliptic Curve Cryptography (ECC) to establish secure communication channels between medical IoT devices. During the simulation phase, the proposed authentication method is implemented and evaluated using realistic medical IoT scenarios. The authors assess the performance of the authentication algorithm in terms of authentication accuracy, computational efficiency, and resource consumption. They analyze the robustness of the authentication mechanism against various security threats, including eavesdropping, data tampering, and unauthorized access.

R. Gupta et al. [2] introduce a novel approach for improving security in medical IoT environments using DNA-based cryptography. It proposes a methodology that leverages the unique properties of DNA sequences to enhance security in medical IoT communication. They first analyze the vulnerabilities of existing cryptographic methods and propose DNA-based cryptography as a potential solution.

The methodology involves encoding sensitive medical data into DNA sequences and using DNA manipulation techniques for encryption and decryption. The encoded DNA sequences serve as cryptographic keys for securing communication channels between medical IoT devices.

A. Aziz et al. [3] present a comprehensive review of security measures for Internet of Things (IoT) medical devices. It also provides an extensive overview of the security challenges and vulnerabilities associated with IoT medical devices. It examines the unique characteristics of medical IoT environments, such as the need for real-time data monitoring and the integration of heterogeneous devices, which pose significant security risks. The authors review existing security mechanisms and protocols employed in medical IoT systems, including authentication, encryption, access control, and intrusion detection. It provides valuable insights into the security challenges and solutions for IoT medical devices. It serves as a comprehensive reference for researchers, practitioners, and policymakers involved in securing medical IoT systems against evolving cyber threats.

R. Gupta et al. [7] propose a novel approach to enhancing security in medical IoT using DNA-based cryptography. This innovative method leverages the unique properties of DNA sequences to provide robust encryption and authentication mechanisms for securing medical data. With the increasing adoption of IoT devices in healthcare settings, the topic of securing medical IoT systems is highly relevant. It addresses an important aspect of IoT security and offers potential solutions that could contribute to improving the overall security posture of medical IoT environments.

It also likely provides a comprehensive analysis of DNA-based cryptography in the context of medical IoT security. It may cover various aspects such as encryption algorithms, key management, authentication protocols, and potential applications, providing readers with a detailed understanding of the proposed approach. The paper may make certain assumptions or have limitations that could affect the applicability of the proposed approach in real-world scenarios.

L. Zhang et al. [8] also present a novel methodology for biometric authentication in medical IoT devices using HRV, offering a promising approach to enhance security and user authentication in healthcare applications. It addresses the need for secure authentication mechanisms in medical IoT devices, considering the sensitive nature of health data and the potential risks associated with unauthorized access.

Instead of traditional authentication methods such as passwords or biometric fingerprints, the authors propose leveraging HRV as a biometric authentication modality. It involves collecting and analyzing HRV data from users to establish unique biometric profiles for authentication purposes. HRV refers to the variation in time intervals between successive heartbeats, which can reflect the autonomic nervous system's activity and the physiological state of an individual. By capturing and analyzing HRV signals, the authors extract distinctive features that can be used to identify and authenticate users. The paper proposes a DNA-based authentication protocol for securing communication in medical IoT (Internet of Things) environments. This approach leverages the unique properties of DNA sequences to provide robust authentication mechanisms for ensuring the security of medical data transmission [9].

S. Chen et al. [10] present a novel approach to ensuring secure communication in medical IoT (Internet of Things) environments using DNA-based authentication. It addresses the critical need for secure communication in medical IoT systems, where sensitive patient data is transmitted between interconnected devices. Traditional authentication methods may not provide adequate security for medical IoT due to vulnerabilities such as interception and unauthorized access.

In response to these challenges, the authors propose a DNA-based authentication protocol tailored specifically for medical IoT applications. So, it involves leveraging DNA sequences as cryptographic keys for authenticating users and securing communication channels in medical IoT systems. Finally, the paper presents a novel methodology for securing communication in medical IoT systems using DNA-based authentication. By leveraging the unique properties of DNA, the proposed protocol offers a promising approach to enhancing the security and privacy of sensitive medical data transmitted over IoT networks.

The above paper may overlook potential limitations or vulnerabilities of DNA-based authentication, such as the susceptibility to DNA sequencing errors, biological degradation, or the need for specialized equipment and expertise for DNA manipulation and analysis. Addressing these limitations and conducting further research to validate the protocol's effectiveness and address practical challenges would strengthen the paper's contribution to the field of medical IoT security.

3. Proposed Enhanced ECC Based Double Level Encryption and Authentication Algorithm

Conventional authentication algorithm involves RSA encryption techniques, which require more number of key lengths compared with the proposed ECC-based authentication algorithm. A lightweight biological feature-based authentication algorithm is proposed for IoT communication. This algorithm utilizes external error control coding techniques to enhance security.

By employing these error control codes, the authentication algorithm complicates the process of eavesdropping, as the decryption algorithm requires a valid error control bit to generate the plaintext. Even if an eavesdropper obtains the DNA code, it would be unable to generate the ciphertext without the correct error control bit. A novel Ex-OR operation-based DNA code generation method is introduced, playing a crucial role in ensuring message integrity and authentication. Elliptic Curve Cryptography (ECC) is utilized for encryption and decryption, maintaining

user confidentiality with a modest 160-bit key size for the cryptosystem process. Prior to encryption, the plaintext is converted into a plaintext point using the Koblitz method. The encoding process involves the following steps:

1. Choose the plaintext (m).
2. Convert the plaintext into ASCII code using a predefined table.
3. Transform the ASCII code into a plaintext point using the Koblitz method.
4. Translate the plaintext point (Pm) into binary digits (Bm).
5. Divide the binary digit blocks into four equal sub-blocks: M1, M2, M3, and M4.
6. Perform the Ex-OR operation between pairs of sub-blocks M1-M2 and M3-M4 to generate M12 and M34.
7. Complement both M12 and M34 and append them together to produce N = M12 || M34.
8. Map the appended binary digits to DNA strands using a conversion table.
9. Reduce the DNA strands using a DNA-XOR table to produce the final DNA code.

This comprehensive approach ensures robust authentication and confidentiality in IoT communication while leveraging biological features and encryption techniques to strengthen security measures.

Table 1. Conversion of plaintext into ASCII code

Alphabet	ASCII Code
A	65
B	67
C	68
D	69
E	70
f	71

Table 2. Map the binary digit into DNA strands

Binary Digit	DNA Strands
00	**A**
01	**T**
10	**G**
11	**C**

Table 3. DNA-XOR

DNA-XOR	A	T	G	C
A	**C**	**G**	**T**	**A**
T	**G**	**C**	**A**	**T**
G	**A**	**T**	**G**	**C**
C	**G**	**C**	**A**	**T**

3.1. External Error Control Code-Based Authentication Algorithm

3.1.1. Encryption Technique

The proposed authentication algorithm for IoT devices is carried out by employing the following process. Initially, a plaintext message (M) is converted into a plaintext point (Pm) by using the koblitz method [9]. Also, it generates the DNA code (Ma(M) by using a DNA mapping table, as shown in Table 1. The resultant DNA code is appended with plaintext point (Pm) and it produces the concatenated value [Pm‖ Ma(M)]. The concatenated value is encrypted by using the user A private key (Pra), and resultant ciphertext (Cm) values are transmitted by the source A, as shown in Figure 1.

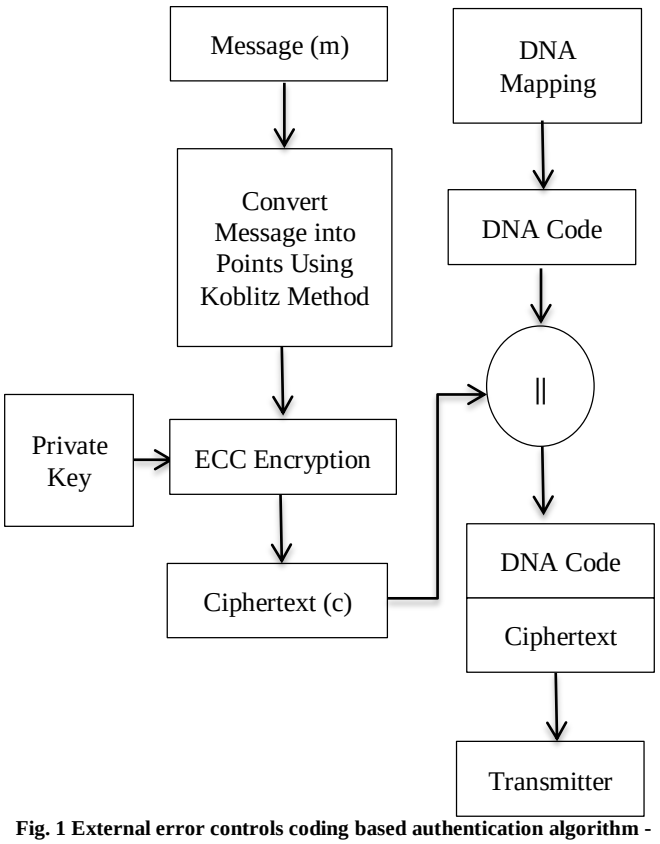


Fig. 1 External error controls coding based authentication algorithm - transmitter side

3.1.2. Receiver Side

At the receiver side as shown in Figure 2, the ciphertext value is decrypted by using the ECC decryption algorithm along with the user's public key. The decrypted value consists of both DNA code and plaintext point, as shown in Figure 1. The received plaintext point is again converted into a plaintext message by using the reverse process of the koblitz method. The converted plaintext point is allowed to convert into DNA code by using the same DNA mapping table mentioned on the transmitter side. Now, the encoded DNA code is matched with the received DNA code; it then matches "Authenticated Device "or "Unauthenticated Device".

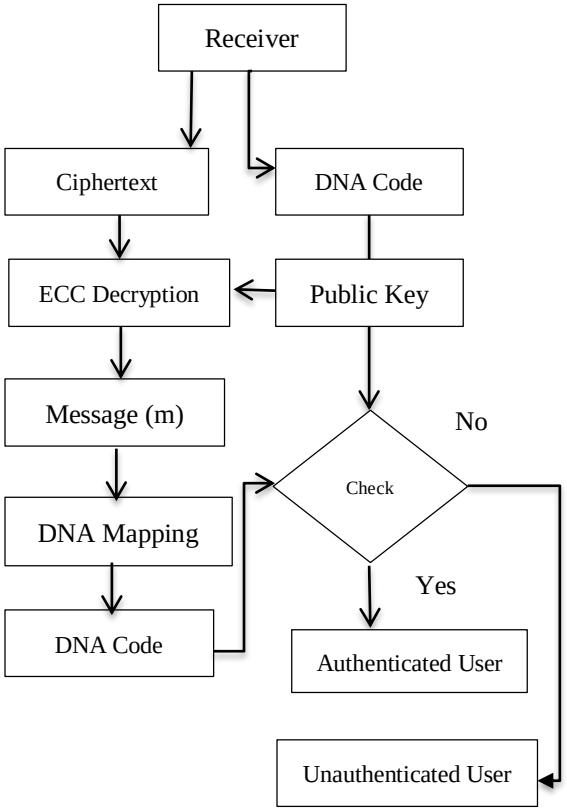


Fig. 2 External error controls coding based authentication algorithm - receiver side

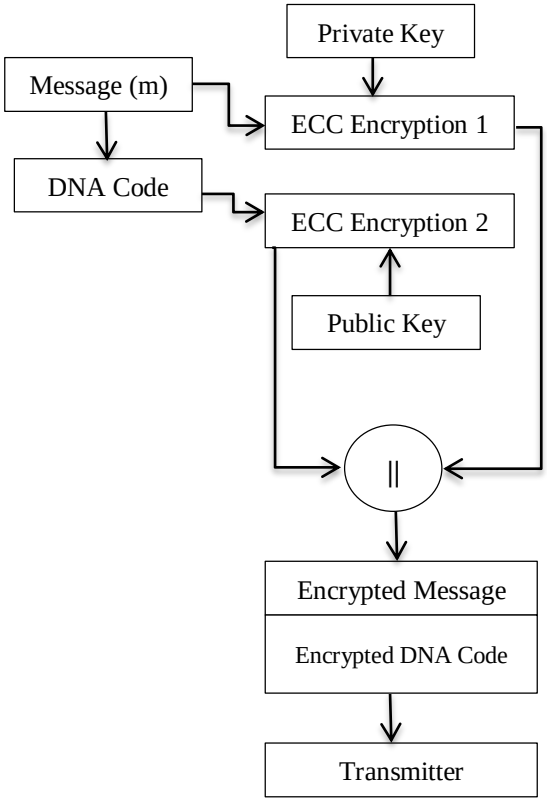


Fig. 3 Double level of encryption based authentication algorithm-transmitter side

3.2. Double Level Message Authentication and Integrity Checking Algorithm (DLMAIC)

Internal and external error control-based authentication algorithm provides authentication where user A uses its private key (KA) to encrypt the message in the form of plaintext point, and user B uses A's public key PUA to decrypt the message. User A signed the message by using its private key and it doesn't deliver confidentiality because anyone in possession of A's public key can decrypt the data.

In order to provide both confidentiality and authentication, user A encrypts the message using his own public key E(PUA, Pm) and encrypts the generated DNA code by using its own private key E(KA, D(m)). The encrypted message is appended with encrypted DNA code and transmitted as a block by using a transmitter, as shown in Figure 3.

At the receiver side, the encrypted message and DNA code are detached, as shown in Figure 4. The encrypted message is decrypted by using the user's private key and, similarly, decrypts the DNA code by using the user's public key. The decrypted message is converted into DNA code by employing the DNA code generation method. The calculated DNA code is compared with the received DNA code; it matches and then considers the data as authentic; otherwise, unauthenticated user.

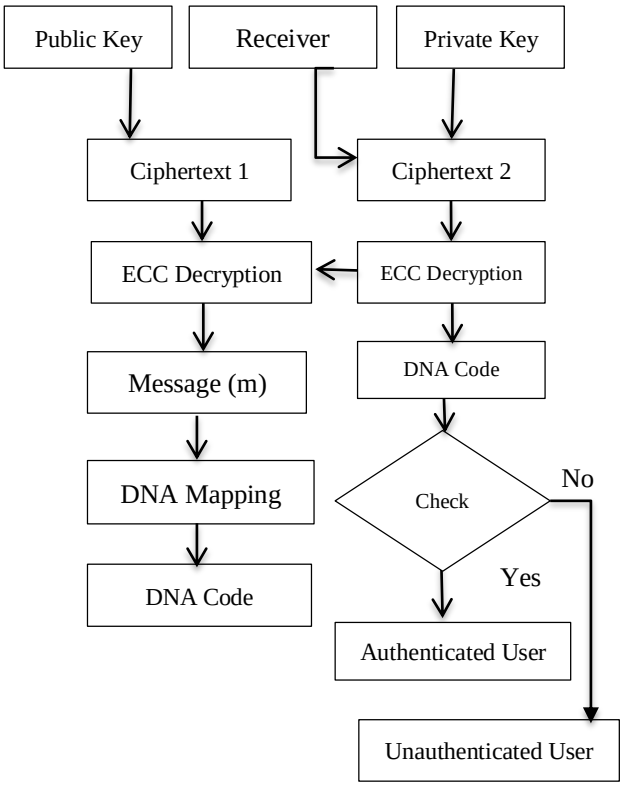


Fig. 4 Double level of decryption-based authentication algorithm – receiver Side

4. Results and Discussion

The simulation results obtained from MATLAB provide insights into the comparative processing times of ECC and RSA algorithms for different key sizes. The plotted results illustrated in Figure 5 show the comparative performance of ECC and RSA algorithms in terms of processing time for different key sizes. ECC generally outperforms RSA in terms of processing time, especially for smaller key sizes. This demonstrates ECC's efficiency in resource-constrained environments such as IoT devices, where faster processing times are essential. The results highlight the impact of key size on processing time for both ECC and RSA algorithms. While larger key sizes offer higher security levels, they also result in longer processing times, particularly for RSA. This trade-off between security and processing time is an important consideration in selecting cryptographic algorithms for specific applications.

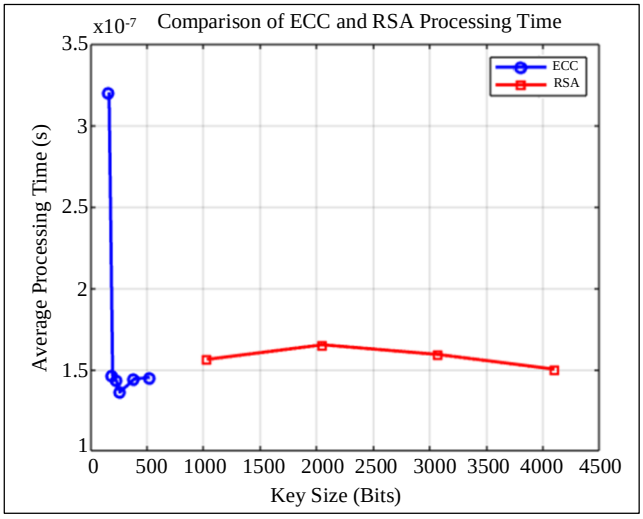


Fig. 5 Comparison of ECC and RSA with respect to key size and processing time

Table 4. Time taken to encrypt the data using ECC and RSA

RSA Key Size in Bits	Processing Time (us)	ECC Key Size in Bits	Processing Time (us)
1024	0.2270	160	0.4230
2048	0.1480	192	0.1650
3072	0.1510	224	0.1550
4096	0.1580	256	0.1440

Table 5. Time taken to encode the message using DNA nucleotide

Message Size in Bits	Processing Time for Encoding the Message (us)
100	0.0023
200	0.0007
300	0.0010
400	0.0003
500	0.0004

From the results shown in Table 5, we observe that as the message size increases, the processing time for encoding the message into DNA code also increases. This is expected because encoding a larger message requires more computational effort. The processing time approximately follows a linear trend with respect to the message size, indicating that the encoding process has a consistent time complexity. These results provide insights into the computational requirements of encoding messages into DNA code. They can be useful for assessing the performance of DNA encoding algorithms and optimizing them for different applications.

Table 6. Time taken to encrypt the encoded DNA message

ECC Key Size in Bits	Processing Time (us)
160	0.2480
192	0.0510
224	0.0230
256	0.0180
384	0.0080

Table 6 shows that As the ECC key size increases, the processing time for encryption may also increase. This is because larger key sizes typically involve more computational effort. The relationship between processing time and key size could vary depending on the ECC implementation, algorithm efficiency, and hardware/software optimizations. Generally, larger DNA-encoded message sizes may require more processing time for encryption. This is because encrypting larger messages involves more data manipulation and cryptographic operations. The processing time may scale linearly or exponentially or follow a different pattern with respect to message size, depending on the ECC encryption algorithm's complexity and efficiency.

Internal error control techniques may be preferable for real-time applications or systems with limited resources. In contrast, external error control techniques may be more suitable for reliable data transmission over unreliable channels. Ultimately, the selection of error control techniques should be based on a careful assessment of the trade-offs between complexity, performance, and reliability, as shown in Figure 6 and Table 7.

Table 7. Comparison table shows the total times taken to execute the control techniques

Data Size in Bits	Total Processing Time (us)	
	Internal Error Control Technique	External Error Control Technique
1000	0.8430	0.8956
2000	0.4650	0.4985
3000	0.3550	0.2985
4000	0.2440	0.2965

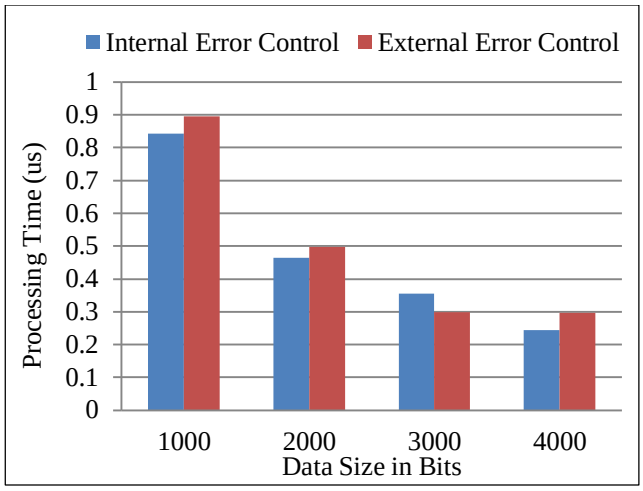
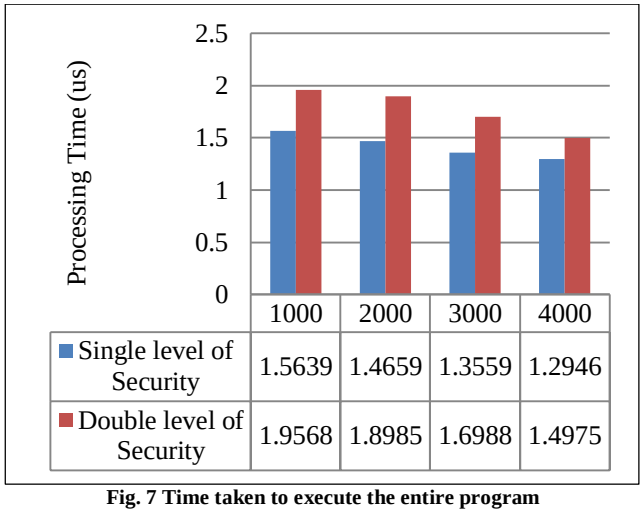


Fig. 6 Total times taken to execute the control techniques



	1000	2000	3000	4000
Single level of Security	1.5639	1.4659	1.3559	1.2946
Double level of Security	1.9568	1.8985	1.6988	1.4975

Fig. 7 Time taken to execute the entire program

In gneral, double-level security is considered more robust and effective in protecting against unauthorized access and security threats, especially for sensitive data or critical systems. However, it may come at the cost of increased complexity and potential user inconvenience. Single-level security may be sufficient for less critical systems or environments where the risk of unauthorized access is relatively low, and simplicity and convenience are prioritized, are shown in Figure 7.

5. Conclusion

In conclusion, the paper presents a cutting-edge approach to enhancing security in medical IoT communication through the utilization of biological feature-based authentication and elliptic curve cryptography. Elliptic curve cryptography provides a higher level of security with a 160-bit key size as compared with traditional RSA-based authentication algorithms. It helps to reduce the communication and computational overhead of the proposed authentication algorithm.

In proposed DNA-based computing techniques, more amount of data can able to held by the DNA sequences; in turn, it helps to store more data to provide the first level of security, and ECC-based encryption techniques provide a second level of encryption. Finally, simulation results prove that the proposed authentication algorithm requires a lesser processing time of only 0.8 ms for 1000 data bit sizes. It also proves that a double level of security requires very much lesser processing time of 1.95 ms compared with a single level of security algorithm for 1000 data bit size. Also, the integration of external error control techniques further enhances the security level of IoT devices, ensuring robust protection against unauthorized access and data breaches.

References

[1] Minhaj Ahmad Khan, and Khaled Salah, "IoT Security: Review, Blockchain Solutions, and Open Challenges," *Future Generation Computer Systems*, vol. 82, pp. 395-411, 2018. [CrossRef] [Google Scholar] [Publisher Link]

[2] Mahmud Hossain, Ragib Hasan, and Anthony Skjellum, "Securing the Internet of Things: A Meta-Study of Challenges, Approaches, and Open Problems," *2017 IEEE 37th International Conference on Distributed Computing Systems Workshops (ICDCSW)*, Atlanta, USA, pp. 220-225, 2017. [CrossRef] [Google Scholar] [Publisher Link]

[3] A. Aziz et al., "Securing Internet of Things (IoT) Medical Devices: A Review," *Journal of Network and Computer Applications*, vol. 136, pp. 22-39, 2019.

[4] Ala Al-Fuqaha et al., "Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications," *IEEE Communications Surveys & Tutorials*, vol. 17, no. 4, pp. 2347-2376, 2015. [CrossRef] [Google Scholar] [Publisher Link]

[5] A.H. Alvi, M.R. Khan, and S.G. Khandaker, "Security in the Internet of Things (IoT): An Overview," *International Journal of Computer Applications*, vol. 182, no. 20, pp. 22-28, 2018.

[6] X. Wang, Y. Liu, and Z. Zhang, "Biological Feature-Based Authentication for Secure Medical IoT Communication," *IEEE Transactions on Mobile Computing*, vol. 20, no. 5, pp. 1647-1658, 2021.

[7] R. Gupta, S. Sharma, and M. Gupta, "Enhancing Security in Medical IoT with DNA-Based Cryptography," *Sensors*, vol. 21, no. 7, 2021.

[8] L. Zhang, K. Wu, and H. Wang, "Biometric Authentication for Medical IoT Devices Using Heart Rate Variability," *IEEE Access*, vol. 8, pp. 206575-206583, 2020.

[9] S. Chen, W. Li, and J. Zhang, "DNA-Based Authentication Protocol for Secure Communication in Medical IoT," *Journal of Medical Systems*, vol. 44, no. 11, pp. 1-11, 2020.

[10] H. Kim, J. Lee, and S. Park, "Biometric-Based Security Solutions for Medical IoT Devices: A Review," *Computers, Materials & Continua*, vol. 63, no. 1, pp. 451-471, 2020.

[11] G. Chen, X. Wang, and Y. Liu, "Enhancing Security in Medical IoT Using DNA-Based Authentication," *IEEE Internet of Things Journal*, vol. 7, no. 11, pp. 11356-11364, 2020.

[12] S. Zhang, L. Wang, and C. Xu, "Biometric Authentication for Medical IoT Devices Using DNA Sequence Analysis," J*ournal of Ambient Intelligence and Humanized Computing*, vol. 11, no. 10, pp. 4343-4352, 2020.

[13] Z. Liu, Y. Li, and X. Chen, "Secure Communication in Medical IoT Using Voice Biometrics," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 2, pp. 1391-1400, 2019.

[14] W. Zhou, J. Yang, and Z. Li, "Biometric-Based Authentication Protocol for Wearable Medical IoT Devices," *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 2491-2500, 2019.