International Journal of Computational and Experimental Science and ENgineering (IJCESEN)

Vol. 10-No.4 (2024) pp. 1528-1540
http://www.ijcesen.com

ISSN: 2149-9144

Research Article

Hybrid Ensemble Lightweight Cryptosystem for Internet of Medical Things Security

M. Swetha[1,*], G. Appa Rao[2]

[1]Research Scholar, Department of Computer Science and Engineering, GITAM (Deemed to be University), Vishakhapatnam, A.P., India
* **Corresponding Author Email:** mugadaswetha9@gmail.com - **ORCID:** 0009-0008-8806-8929

[2]Assistant Professor, Department of Computer Science and Engineering, GITAM (Deemed to be University), Vishakhapatnam, A.P., India
Email: agodi@gitam.edu - **ORCID:** 0009-0007-5169-6262

Article Info:

DOI: 10.22399/ijcesen.625
Received : 14 November 2024
Accepted : 18 November 2024

Keywords :

Internet of Medical Things,
Hybrid ensemble lightweight, cryptosystem,
Probabilistic rivest cipher 6,
Modified MFBC.

Abstract:

Internet of Medical Things (IoMT) is a fast-developing area that includes the use of connected medical devices to enhance patient care and expedite the procedures involved in the delivery of healthcare. Concerns about the safety and confidentiality of patient information are a roadblock to the broad use of telemedicine technologies like IoMT. Encryption is an essential part of IoMT security, and there is a wide variety of encryption methods that are used to safeguard sensitive patient data. This work implemented a hybrid ensemble lightweight cryptosystem (HELC) using probabilistic rivest cipher 6 (PRC6) encryption and modified feistel block cipher (MFBC) approaches. Initially, the data from users are applied to PRC6 encryption, which is symmetrical encryption and provides security at in abstract level. So, to provide more security to data, the MBFC is applied to PRC6 outcome. Then, the resultant data transferred over the IoMT environment to the destination. Finally, the MBFC decryption and PRC6 decryption operations are performed at receiver side, which resulted in decrypted outcome. The simulations results show that the proposed HELC consumed 0.0021 seconds of encryption time, and 0.000276 seconds of decryption time, which are lesser as compared to other approaches.

1. Introduction

The IoMT is a rapidly growing field in healthcare, where medical devices, sensors, and systems are interconnected to enable remote monitoring, data collection, and real-time healthcare management [1]. The IoMT offers numerous benefits, such as improved patient care, enhanced efficiency, and cost savings. However, the increasing connectivity and reliance on technology in healthcare also give rise to significant security challenges [2]. Protection of sensitive medical data in terms of confidentiality, integrity, and availability; and IoMT device functionality assured with security requirements to preserve patient safety and trust in the health care ecosystem is a critical issue. IoMT devices generate and transmit an enormous amount of sensitive patient data pertaining to personal health information, vital signs, and medical records. This information must be protected to ensure the privacy of patients and to abide by statutory laws such as Health Insurance Portability and Accountability Act [3] and General Data Protection Regulation [4]. Unauthorized access, intercepts, or alteration of this data will bring about serious consequences like identity theft, fraud, and compromised quality of patient care. IoMT devices, including implantable medical devices, wearable health trackers, and even hospital equipment, can become security vulnerable. Most of these devices lack great security-based mechanisms that make them an attractive target for cybercriminals [5,6]. Vulnerabilities like weak authentication, outdated firmware, and unencrypted communication channels expose a space to gain unauthorized access or disrupt the device's functionality or inject malicious code into it, thus posing risks to patient safety and integrity of medical procedures. The accuracy and reliability of medical data must be very high in IoMT systems 6 because improper manipulation or interference with data can cause improper diagnosis, wrong dosage of some medication, and compromised treatment programs.

The integrity of the transmitted and stored data within the IoMT should be ensured to protect patients and advance good healthcare quality. Healthcare organizations rely on stakeholders who are healthcare professionals, administrators, and third-party vendors accessing the IoMT systems that possess patients' information.

Several recent data breaches and violated privacy incidents [7] have also led to the disruption of healthcare operations due to unauthorized access, data leakage, or even intentional sabotage by malevolent insiders. Strong mitigation requires comprehensive approaches in controlling access controls, robust mechanisms for authentication, and continuous monitoring of users' activities. There are many IoMT devices and systems that come from different manufacturers, making them diverse in both communication protocols and data formats used [8]. The lack of interoperability and standardization makes it more challenging to establish uniform and effective security measures. Poor integration of different components of IoMT may lead to opening security gaps and compatibility problems as well as issues related to management and security for the interconnected network of devices and systems. IoMT relies heavily on appropriate and secure network infrastructures to ensure unobstructed communication between devices, healthcare providers, and other stakeholders involved.

Here, vulnerabilities of the network, such as weak encryption protocols, unsecured wireless networks, and the lack of network segmentation, leave these pieces of medical data susceptible to unauthorized access and eavesdropping. Therefore, secure network infrastructure, including the strong mechanisms of encryption, an intrusion detection system, and firewalls, is critical for protecting the privacy and integrity of data transmitted within the IoMT environment. The healthcare industry has stringent regulatory and conformity standards regarding data privacy and security. These standards include HIPAA and GDPR. With this, compliance becomes inevitable to avoid legal repercussions and to avoid the loss of trust due to the patients. Achieving compliance, however, in such a complex dynamic IoMT environment is even more complex because of elements that may include the ever-changing technology landscape and the element of efficient operation. Effective navigation of the required regulations will help healthcare organizations ensure the secure deployment and operation of IoMT systems. Human factors are one of the most critical elements related to IoMT security. Healthcare professionals, device users, and administrators may lack proper training in the best practices and protocols associated with IoMT systems. With a lack of awareness, security vulnerabilities will tend to occur due to unsuspecting users clicking on phishing emails, misplaced sensitive information, and poor usage in password management. Addressing these security issues of IoMT requires a comprehensive approach involving strong cryptographic algorithms [9], secure communication protocols, access control mechanisms, device authentication, security audits, and continuous monitoring. Proactive identification and mitigation of the threats will assist health care organizations in reaping the transformative power of the IoMT with increased safety for patients, such as privacy and data security [10]. Therefore, to solve these problems, this work defines novel contributions as follows:

- The work introduces a new encryption system called HELC that combines two encryption techniques, PRC6 and MFBC, to provide strong security while keeping resource usage low.
- Development of PRC6 encryption to protect user data, ensuring that it remains confidential and tamper-proof in the IoMT environment.
- Development of MFBC, a modified version of a widely used encryption structure called the FBC, to enhance the security of the encrypted data obtained from PRC6 encryption.
- The system enables authorized recipients to retrieve the original data by performing the reverse processes of MFBC and PRC6 encryption, ensuring data integrity and allowing secure access to the decrypted information.

The rest of the article is organized as follows: section 2 contains a detailed analysis of existing methods such as related work. Section 3 illustrates the operation details of HELC with PRC6 and MFBC methods. Section 4 gives the detailed results analysis of the proposed HELC approach. Finally, section 5 concludes the article with possible future scope.

In their paper [11], Salim et al. proposed a method that protected users' privacy while encrypting medical plaintext data using homomorphic encryption to prevent malicious parties from accessing the data. By concealing the results of all mathematical operations and distributing computations among several different virtual nodes on the edge, secret sharing prevented untrusted cloud services from gaining knowledge of the operations carried out on encrypted patient data. An EMOEUA approach was presented by Riya et al. [12] to perform mutual authentication as a means of resolving the security challenges and minimizing computational complexity. In addition to this, the EMOEUA method encrypted the IoMT data using the optimum multikey homomorphic encryption (OMKHE) method. Furthermore, the improved social spider optimization algorithm (ISSOA) was

used to generate the best possible multikey for use with the OMKHE method.

Liu et al. [13] heavily depended on high-consumption bilinear pairing, and some of them were susceptible to Inside Keyword Guessing Attacks (IKGA). They built a lightweight encryption scheme for the IoMT. It has been shown that our technique is safe within the paradigm of the random oracle. Ravi et al. [14] suggested a new algorithm for the encryption of medical images, specifically for use in IoMT applications. The key space of the new approach was large enough, and both the encryption and decryption processes were sensitive to the key.

The sparse-learning-based encryption and recovery method presented in [15] provided an approach to a privacy-aware sensing and transmission technique. In the encryption procedure, the sparse learning-based approach compressed and encrypted the sparse sensing signal before data transmission to the network coordinator or edge devices. The sparse signal is retrieved using appropriate sparse learning at the decryption stage. Raj et al. [16] suggested hardware-oriented ASCON-128 encryption that was a lightweight cipher for data encryption. One part of the permutation block of the cipher was an FPGA implementation of a substitution box based on LUT6. Saif et al. [17] presented a revolutionary lightweight symmetric encryption algorithm for low-powered IoMT devices. The recommended approach used a block ciphering of 8-bits and had secret keys that were 2 and 8-bit each in size. Physiological parameters such as the human body pulse rate were considered while designing the algorithm as one among the secret keys that needed to be hidden. Ravikumar et al. [18] described the smart safety of the patient's data along with diagnosis of a sleep alarm using deep learning methods in detail. However, this system was affected by higher losses, as well as security issues. Wang et al. [19] proposed an efficient searchable encryption scheme using weighted keywords. In this architecture, they designed a weighted keyword model that was used to enhance the precision of their search results while reducing computational and storage overhead.

A secure cryptosystem El-Shafai et al. [20], for encrypting medical images, with the potential to be compatible with the IoMT and cloud services, was proposed in this work using a three-dimensional chaotic map. Here, encryption technique is based on a three-dimensional chaotic map; the nonlinear ciphering method is introduced by using this map for diffusion of pixel values and positional permutation. AES was first proposed by Guitouni et al. [21]. It is one of the most widely used standards in digital picture security systems and offers five different types of encryptions. However, this method had high computational complexity. Bhuvaneswari et al. [22] suggested a group key management strategy that ensures secure group communication using a dual encryption scheme (AES and RSA). Patients could also be considered members of the network. In this case, both the group key and the identity key were used to enable members of the group to communicate securely with one another. Bhushan et al. [23] presented a hybrid encryption system for the protection of IoMT systems in their research. Although widespread and low-cost sensing devices like these have the potential to bring about major improvements in the healthcare industry, these devices are susceptible to a wide variety of privacy and security concerns.

Adil et al. [24] proposed a hybrid lightweight authentication scheme that leveraged a supervised machine learning technique followed by a Cryptographic Parameter Based Encryption and Decryption (CPBE&D) scheme to ensure the validation of legal patient wearable devices with secure transmission over the wireless communication channel. Ravi et al. [25] suggested an effective and low-overhead technique for encrypting data. The proposed lightweight encryption technique first divided the picture into many clusters and then used cluster-based permutations. Additional processes such as modulation or diffusion could be applied as well. Singh et al. [26] presented a region-based hybrid Medical Image Watermarking strategy to ensure the integrity of IoMT. The region of interest was watermarked via adaptive Least Significant Bit replacement based on the hiding capacity map. This ensured a lower level of RoI imperceptibility and improved accuracy in tamper detection and recovery. Nie et al. [27] introduced a unique data sharing strategy aided by blockchain. The reliability of keyword ciphertext was ensured using a bloom filter equipped with hash functions. Key-policy attribute-based encryption (KP-ABE) and smart contracts were used for secure profile matching. To protect sensitive information, Sutradhar et al. [28] developed a dynamic stepwise tiny encryption algorithm with fruit fly optimization algorithm. The Energy Efficient Routing Protocol was used to send data in an encrypted form, and decryption occurred upon user request for data access. Ktari et al. [29] suggested an IoMT-based platform for monitoring the health of patients, employing distributed ledger technology, also known as blockchain, as a secure and reliable solution for maintaining medical confidentiality. Karam et al. [30] conducted research on the significance of ethics and security in relation to IoMT. They proposed an identity-based cryptography cornerstone management strategy that protected the data translation between any health

device and any other entity from a different firm or domain.

Problem analysis: Based on the survey of the research papers mentioned above, several problem areas in IoMT security could be identified, which researchers aimed to address. Ensuring privacy in medical data is a major problem in IoMT. Sensitive patient information breaches and data misuse can occur due to unauthorized access. Several techniques and methods that proposed encryption to protect the privacy of patients and prevent malicious parties from accessing their confidential medical data. IoMT devices are usually characterized by limited computing resources as well as limited power. Therefore, designing lightweight encryption algorithms that could have the potential of strong security with minimal computational complexity is difficult. Research has been focused on designing optimized resource-constrained IoMT devices for encryption schemes.

2. Material and Methods

The IoMT has revolutionized the healthcare sector because now all medical devices and systems can become Internet-connected [31,32]. In this process, security risks come into being because patients' sensitive information as well as critical operations about medical emergencies become prone to unauthorized access and malicious misuse. Such risks require robust security systems.

Figure 1 shows the design of the proposed HELC method focusing on the security of IoMT and proposed usage of PRC6 and MFBC data encryption for IoMT systems. First, the plaintext is applied through the PRC6 method, which is a symmetric block cipher of the latest generation known for its high security and flexibility. It has a variable key size. Therefore, it could offer to help with the variety of IoMT devices with diverse calculating powers. With PRC6 encryption, sensitive data related to medical care flow from various devices to systems or vice-versa may be safely safeguarded against eavesdropping and unauthorized access. Then, this PRC6 encrypted result is used in MFBC process. The MFBC structure is used here as an effective framework for encryption and decryption processes. The rounds of iteration involving data splitting, substitution, permutation, and recombination enhance the secrecy of the cryptographic operation performed. Combining the Feistel structure with PRC6 encryption further gives security to the system. Subsequently, the proposed work discusses the decryption operation at the receiver end for effective retrieval of the original data [33]. The operations of decryption consist of the inverse operation of MFBC and PRC6 encryption in reverse.

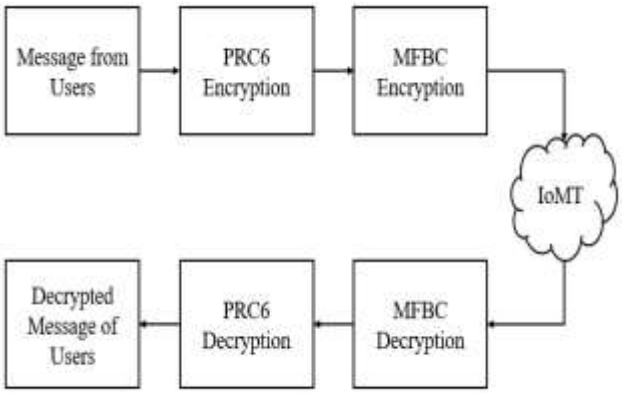

Figure 1. *Proposed hybrid ensemble lightweight cryptosystem block diagram.*

Hence, the system can gain the reversibility of the original data of the transmitted ciphertext through the execution of MFBC decryption along with PRC6 decryption. This contribution ensures data integrity and allows the intended recipients to use and utilize the decrypted information.

2.1 Probabilistic rivest cipher6 encryption

The algorithm shall ensure safe encryption and decryption of digital data. The PRC6 technique is an advanced form of the RC6 algorithm [34], and it was designed to provide a higher level of security by utilizing a variable block size and variable key size. Figure 2 indicates the block diagram of the PRC6 encryption process. A thorough mathematical analysis of the PRC6 encrypting and decrypting processes is going to be provided in this chapter. To

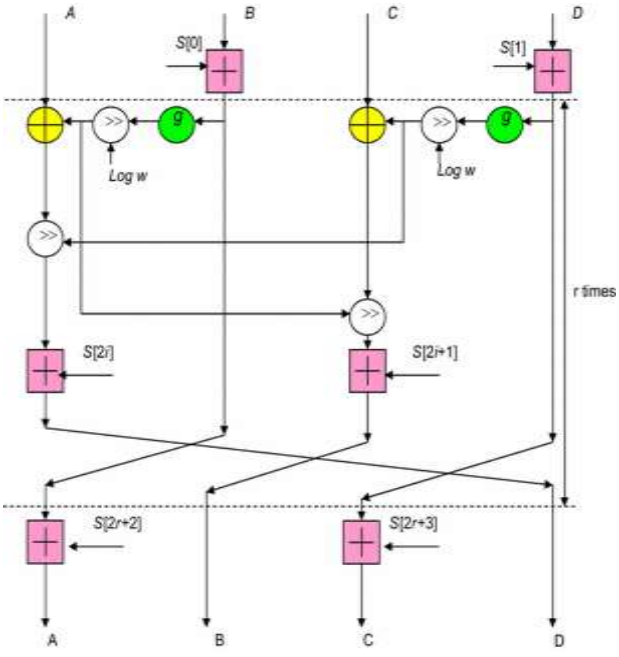

Figure 2. *Proposed probabilistic rivest cipher6 encryption operational diagram.*

come up with the ciphertext, the process of PRC6 encryption executes several steps that must be carried out in some specific sequence. The steps involved include expansion of keys, initialization, rounds of encryption, and output ciphertext generation [35].

Step 1: Key Expansion: The first stage execution in the encryption process using PRC6 is key expansion as the first step. Key expansion" is the term used for key expansion, which expands the user-provided key to a grid of round keys. The round keys serve for modification of plaintext in subsequent encryption rounds. In a way, the key provided by the user is implemented through the key expansion algorithm, which then proceeds to generate a list of the round keys. The PRC6 key expansion process generates a list of round keys based on the key given by the user. The following equations are used to generate the round keys

$$w = ceil(log2(r)) \tag{1}$$

$$b = 4 * max(c, 1) \tag{2}$$

$$L = [key[i]\ for\ i\ in\ range(b)] \tag{3}$$

$$S = [Pw] * t \tag{4}$$

for i in range (2 * t):

$$S[i] = (S[i-1] + Qw)\ \%\ 2 ** w \tag{5}$$

$$A = B = i = j = 0 \tag{6}$$

For k in range $(3 * max(t, b))$:

$$A = S[i] = rol((S[i] + A + B), 3, w) \tag{7}$$

$$B = L[j] = rol((L[j] + A + B), (A + B)\ \%\ w, w) \tag{8}$$

$$i = (i + 1)\ \%\ (2 * t) \tag{9}$$

$$j = (j + 1)\ \%\ b \tag{10}$$

The round keys are produced by using several different bitwise operations in conjunction with modular arithmetic. The following is an example expression of the PRC6 key expansion algorithm. Create the initial values for an array of round keys denoted by $R[0 \ldots 2r + 3]$, where r is the total number of rounds. Set $R[0]$ to a constant value. Put a P value of 0 in the array variables A and B, then save the changes. Set the loop counter i to 1, while i is less than $2r + 3$, carry out the following operation

- Set R[i] = (R[i-1] + A + B) mod $2w$, where w is the word size (in bits).
- Set A = R[i]
- Set B = A + B
- Increment the loop counter i by 1.

The key expansion algorithm is responsible for producing a collection of round keys, which are then used in the succeeding stages of the encryption process.

Step 2: Initialization: After the key expansion process is complete, this is then followed by the initialization process. The round keys and the ciphertext are used to initialize the cipher in the process called "initialization." The initialization algorithm is defined below: Set the variables $A, B, C,$ and D to be the first four words of the ciphertext. This is for initialization. Set the value Q as the initial state of the array variable $[0.2r + 3]$ before doing so. Use the round keys created in key expansion to modify the array variable S.

Step 3: Rounds of Encryption: The more significant part of the encryption of PRC6 is called the rounds of encryption. Based on its parameter, the value of r determines how many rounds will be executed. This PRC6 technique uses a type of cryptographic network known as a Feistel network. A Feistel network is a transformation network in which the plaintext is transformed using both substitution and permutation. It is used for encrypting as well as decrypting messages. Each round of PRC6 algorithm consists of the following operations: Carried out modular addition of the working variables A and B by the round key $R[2i - 1]$. Perform a bitwise rotation of the mixed value by some predefined number of bit positions. Through the modular addition process, combine working variables C and D along with the round key $R[2i]$. Perform a left-right bitwise rotation of the resulting value by a certain number of bit positions. Based on the new values, effect adjustments in the working variables. The round function can be described as:

- Mix A and B with the round key R[2i-1]: A = ((A + B) XOR R[2i-1]) <<< s
- Mix C and D with the round key R[2i]:

To encrypt data using PRC6, the plaintext must first be segmented into blocks, after which the round keys are used to perform a sequence of operations on each individual block. The process of encrypting data is described with the help of the following equations:

$$w = ceil(log2(r)) \quad (11)$$

$$b = 4 * max(c, 1) \quad (12)$$

$$L = plaintext[0] \quad (13)$$

$$R = plaintext[1] \quad (14)$$

$$L = (L + S[0]) \,\%\, 2w \quad (15)$$

$$R = (R + S[1]) \,\%\, 2w \quad (16)$$

2.2 Modified feistel block cipher encryption

A Feistel network [36] is the primary element that is used in both the encryption and decryption processes when working with MFBCs, which belong to the category of symmetric key block ciphers. Figure 3 shows the block diagram of MFBCs encryption process. A cryptographic network is said to be of the Feistel variety if it modifies the plaintext using a mix of substitution and permutation, as is the case with a Feistel network, which consists of numerous rounds of operations. Each round is divided into two stages: the first stage is the substitution step, and the second stage is the permutation step [37]. A piece of plaintext is split into two equal halves and used as the basis for the operation of the Feistel network. During each round, the right portion of the plaintext is altered in a manner that is determined by the left portion of the plaintext in conjunction with a round key. Following this step, the new plaintext is

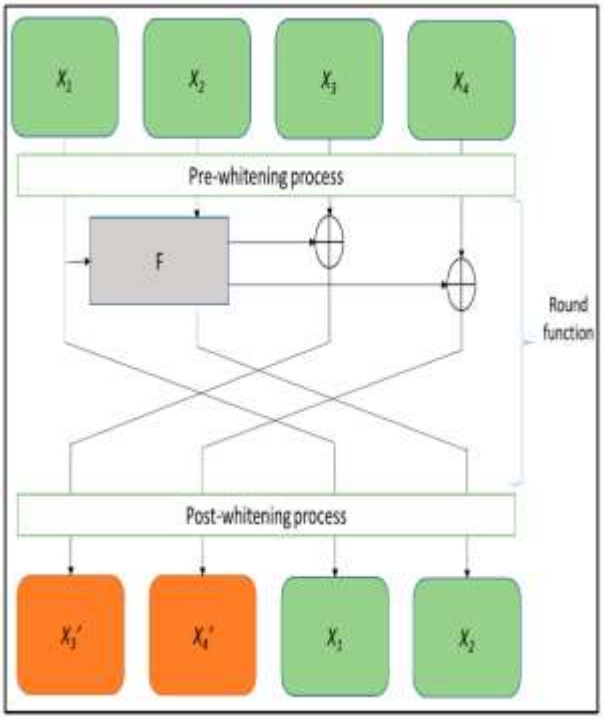

Figure 3. *Proposed modified feistel block cipher encryption operational diagram*

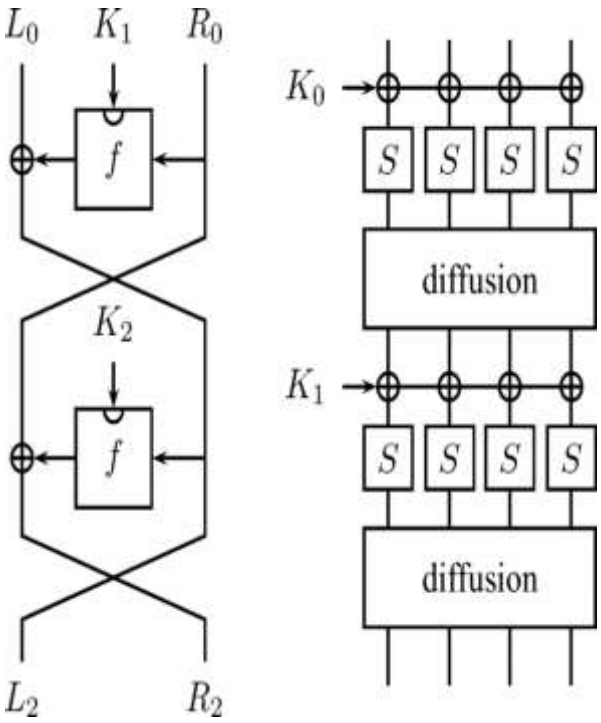

Figure 4. *Proposed feistel network architecture*

constructed by combining the changed right component with the unaltered left part. After a certain number of iterations of the procedure have been completed, the final ciphertext is produced. The Feistel network is intended to result in confusion and diffusion of information as shown in figure 4. The term "confusion" refers to the quality of having a connection between the plaintext and the ciphertext that is difficult to understand and convoluted in nature. The term "diffusion" refers to the condition that even a little modification to the plaintext should result in a significant alteration to the ciphertext [38]. The processes of encrypting and decrypting data using a MFBC are quite similar and is explained in the following way:

Step 1: Key Expansion: Key expansion is necessary for both encryption and decryption. Key expansion is generating a sequence of round keys based on the key provided by a user. In Feistel network's later rounds [39], plaintext is modified using the round keys.

Step 2: Initialization: Following the expansion of the keys there comes the initialization process. Round keys and the plaintext are used to start the cipher in the process called "initialization". Most "initialization" methods for an MFBC differ from others; each cipher might have extra operations like padding or whitening.

Step 3: Rounds of Encryption/Decryption: The two main stages that constitute the core part of the MFBC are the rounds of encryption and decryption. The number of rounds is determined by the design of

the cipher, and the rounds used may depend on the desired level of security [40]. Table 1 represents each round of Feistel network algorithm.

Table 1. *Modified feistel block cipher encryption Rounds of Encryption/Decryption Algorithm.*

Step 1: Divide the block of plaintext into two equal parts, L and R.
Step 2: Apply the Feistel network function to R using a round key. The Feistel network function involves applying a substitution function and a permutation function to R.
Step 3: XOR the result of the Feistel network function with L.
Step 4: Swap L and R.
Step 5: Repeat steps 2-4 for the desired number of rounds. The modification of the plaintext is the province of the Feistel network function, which serves as the central component of the MFBC. The following is an expression that is used to describe the Feistel network function.
Step 6: Split the input into two parts, X and Y, each of which is equal in size.
Step 7: Use the round key to apply a replacement function to the letter Y. The replacement function is intended to cause confusion by making it difficult to discern the connection between the input and the output. This is the intended purpose of the substitution function.
Step 8: Using the result of the substitution function, apply a permutation function to the output. The permutation function's purpose is to provide dispersion by dispersing the changes brought about by the substitution function over the whole block.
Step 9: Perform an XOR operation on the output of the permutation function and X.
Step 10: Publish the updated versions of X and Y.
Step 11: The substitution and permutation functions used in the Feistel network function are often based on cryptographic primitives such as S-boxes and P-boxes. These primitives are utilized to ensure the security of the Feistel network function.

3. Results and Discussions

This section explains the simulation results in detail with several performance metrics. Here, the performance of the proposed approach is compared with other encryption standards in terms of the same metrics.

3.1 Performance metrics

In general, the encryption and decryption time for a given cryptographic algorithm may be expected to be significantly affected by many factors including key size, message size, hardware/software implementation, and even facets of algorithmic complexity. The mathematical formulas applied to represent encryption and decryption time are based on these factors as well as on the actual algorithm under consideration. For example, let's describe a very simple example if the encryption and decryption time (T) is proportional to the message size (M) and the algorithmic complexity (C). The relationship was represented with the following formulas:

$$T_{encryption} = k_{encryption} * M * C \quad (17)$$

$$T_{decryption} = k_{decryption} * M * C \quad (18)$$

In these formulas, $k_{encryption}$ and $k_{decryption}$ are proportionality constants that account for the specific hardware or software implementation, as well as any additional factors that might affect the processing time (e.g., algorithm optimizations, parallelism, etc.).

3.2 Performance evaluation

Table 2 compares the encryption time for various users for various methods. Here, the proposed HELC resulted in reduced encryption time as compared to existing OMKHE [12], SLER [15], and LSEA [17] methods. Figure 5 shows the graphical representation of encryption time for various users. For User 1, the proposed HELC algorithm shows a 49.41% improvement compared to OMKHE, a 45.35% improvement compared to SLER, and a 51.02% improvement compared to LSEA. For User 2 experiences a 46.34% improvement with the proposed HELC algorithm compared to OMKHE, a 55.10% improvement compared to SLER, and a 58.49% improvement compared to LSEA. In the case of User 3, the proposed HELC algorithm exhibits a 51.06% improvement compared to OMKHE, a 47.17% improvement compared to SLER, and a 55.32% improvement compared to LSEA. User 4 benefits from a 43.02% improvement with the proposed HELC algorithm compared to OMKHE, a 45.35% improvement compared to SLER, and a 44.19% improvement compared to LSEA. For User 5, the proposed HELC algorithm demonstrates a 54.90% improvement compared to OMKHE, a 46.08% improvement compared to SLER, and a 50.61% improvement compared to LSEA. User 6 observes a 47.83% improvement with the proposed HELC algorithm compared to both OMKHE and SLER, and a 53.19% improvement compared to LSEA. User 7 experiences a 45.88% improvement with the proposed HELC algorithm compared to OMKHE, a 48.89% improvement compared to SLER, and a 43.75% improvement compared to LSEA. In the case of User 8, the proposed HELC algorithm exhibits a 61.54% improvement compared to OMKHE, a 56.86% improvement compared to SLER, and a 63.64%

improvement compared to LSEA. User 9 benefits from a 49.02% improvement with the proposed HELC algorithm compared to OMKHE, a 50.00% improvement compared to SLER, and a 51.92% improvement compared to LSEA. For User 10, the proposed HELC algorithm demonstrates a 53.33% improvement compared to OMKHE, a 50.00% improvement compared to SLER, and a 55.71% improvement compared to LSEA.

Table 2. *Performance evaluation of encryption time for various users.*

Users	OMKHE [12]	SLER [15]	LSEA [17]	Proposed HELC
User 1	0.0054	0.0047	0.0049	0.0026
User 2	0.0041	0.0049	0.0053	0.0022
User 3	0.0043	0.0053	0.0047	0.0021
User 4	0.0043	0.0041	0.0043	0.0024
User 5	0.0051	0.0045	0.0041	0.0023
User 6	0.0046	0.0045	0.0049	0.0024
User 7	0.0050	0.0044	0.0048	0.0027
User 8	0.0052	0.0045	0.0055	0.0020
User 9	0.0051	0.0050	0.0052	0.0025
User 10	0.0045	0.0048	0.0042	0.0021

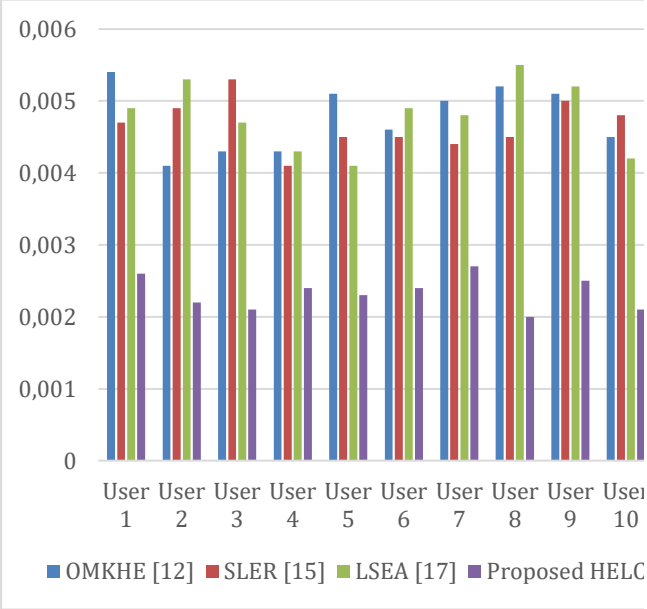

Figure 5. *Graphical representation of encryption time for various users.*

Table 3 compares the decryption time for various users for various methods. Here, the proposed HELC resulted in reduced decryption time as compared to existing OMKHE [12], SLER [15], and LSEA [17] methods. Figure 6 shows the graphical representation of decryption time for various users. For User 1, the proposed HELC algorithm shows a 48.27% improvement compared to OMKHE, a 40.78% improvement compared to SLER, and a 39.85% improvement compared to LSEA. User 2 experiences a 23.73% improvement with the proposed HELC algorithm compared to OMKHE, a 46.46% improvement compared to SLER, and a 37.13% improvement compared to LSEA. In the case of User 3, the proposed HELC algorithm exhibits a 32.43% improvement compared to OMKHE, a 43.02% improvement compared to SLER, and a 29.53% improvement compared to LSEA. User 4 benefits from a 13.04% improvement with the proposed HELC algorithm compared to OMKHE, a 30.26% improvement compared to SLER, and a 23.77% improvement compared to LSEA.

For User 5, the proposed HELC algorithm demonstrates a 26.07% improvement compared to OMKHE, a 19.82% improvement compared to SLER, and a 29.08% improvement compared to LSEA. User 6 observes a 28.47% improvement with the proposed HELC algorithm compared to OMKHE, a 40.19% improvement compared to SLER, and a 24.34% improvement compared to LSEA. The proposed HELC algorithm shows a 30.58% improvement compared to OMKHE, a 36.73% improvement compared to SLER, and a 10.06% improvement compared to LSEA for User 7. In the case of User 8, the proposed HELC algorithm exhibits a 26.86% improvement compared to OMKHE, a 46.16% improvement compared to SLER, and a 42.85% improvement compared to LSEA. User 9 benefits from a 55.63% improvement with the proposed HELC algorithm compared to

Table 3. *Performance evaluation of decryption time for various users.*

User	OMKHE [12]	SLER [15]	LSEA [17]	Proposed HELC
User 1	0.000431	0.000378	0.000371	0.000223
User 2	0.000335	0.000480	0.000409	0.000257
User 3	0.000426	0.000344	0.000409	0.000288
User 4	0.000345	0.000380	0.000324	0.000265
User 5	0.000437	0.000333	0.000381	0.000270
User 6	0.000361	0.000428	0.000341	0.000257
User 7	0.000412	0.000452	0.000327	0.000286
User 8	0.000323	0.000442	0.000413	0.000236
User 9	0.000469	0.000355	0.000420	0.000208
User 10	0.000322	0.000391	0.000410	0.000276

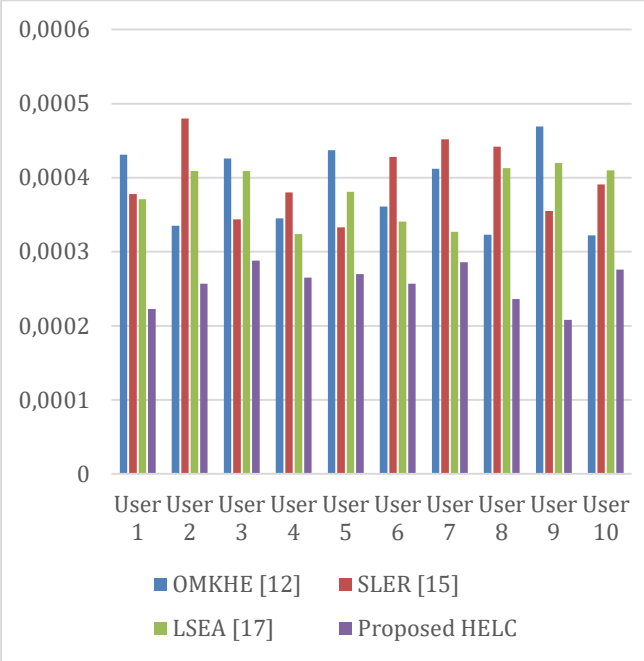

Figure 6. *Graphical representation of decryption time for various users.*

OMKHE, a 41.41% improvement compared to SLER, and a 50.48% improvement compared to LSEA. For User 10, the proposed HELC algorithm demonstrates a 14.29% improvement compared to OMKHE, a 29.61% improvement compared to SLER, and a 32.68% improvement compared to LSEA.

Table 4 compares the encryption time for various message sizes for various methods. Here, the proposed HELC resulted in reduced encryption time as compared to existing OMKHE [12], SLER [15], and LSEA [17] methods. Figure 7 shows the graphical representation of encryption time for various message sizes. For message size 100, the proposed HELC algorithm shows a 16.90% improvement compared to OMKHE, a 13.97% improvement compared to SLER, and a 14.12% improvement compared to LSEA. For message size 200, the proposed HELC algorithm demonstrates a 9.42% improvement compared to OMKHE, a 19.79% improvement compared to SLER, and an 11.98% improvement compared to LSEA. For message size 300, the proposed HELC algorithm exhibits a 12.77% improvement compared to OMKHE, a 9.74% improvement compared to SLER, and a 12.98% improvement compared to LSEA. For message size 400, the proposed HELC algorithm shows a 17.25% improvement compared to OMKHE, a 9.00% improvement compared to SLER, and an 11.07% improvement compared to LSEA. Table 5 compares the decryption time for various message sizes for various methods. Here, the proposed HELC resulted in reduced decryption time

Table 4. *Performance evaluation of encryption time for various message sizes.*

Message size	OMKHE [12]	SLER [15]	LSEA [17]	Proposed HELC
100	0.000951	0.000911	0.000925	0.000791
200	0.000860	0.000960	0.000910	0.000778
300	0.000906	0.000892	0.000897	0.000792
400	0.000942	0.000863	0.000897	0.000780

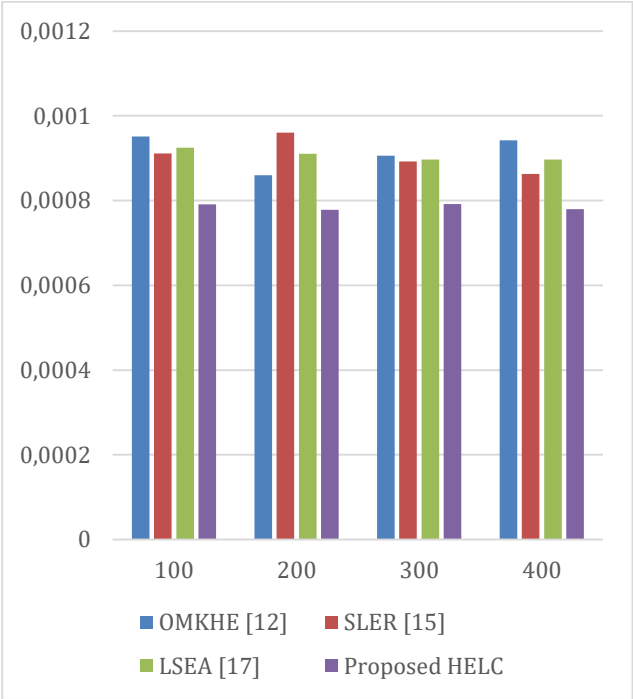

Figure 7. *Graphical representation of encryption time for various message sizes.*

as compared to existing OMKHE [12], SLER [15], and LSEA [17] methods. Figure 8 shows the graphical representation of decryption time for various message sizes. For message size 100, the proposed HELC algorithm shows a 17.14% improvement compared to OMKHE, a 23.15% improvement compared to SLER, and a 19.03% improvement compared to LSEA. For message size 200, the proposed HELC algorithm demonstrates a 14.69% improvement compared to OMKHE, a 9.07% improvement compared to SLER, and a 11.93% improvement compared to LSEA. For message size 300, the proposed HELC algorithm exhibits a 15.93% improvement compared to OMKHE, a 16.77% improvement compared to SLER, and a 19.31% improvement compared to LSEA. For message size 400, the proposed HELC algorithm shows a 10.39% improvement compared

to OMKHE, a 19.12% improvement compared to SLER, and a 13.17% improvement compared to LSEA.

Table 5. *Performance evaluation of decryption time for various message sizes.*

Message size	OMKHE [12]	SLER [15]	LSEA [17]	Proposed HELC
100	0.000875	0.000944	0.000889	0.000720
200	0.000911	0.000860	0.000882	0.000778
300	0.000918	0.000930	0.000957	0.000772
400	0.000869	0.000965	0.000896	0.000778

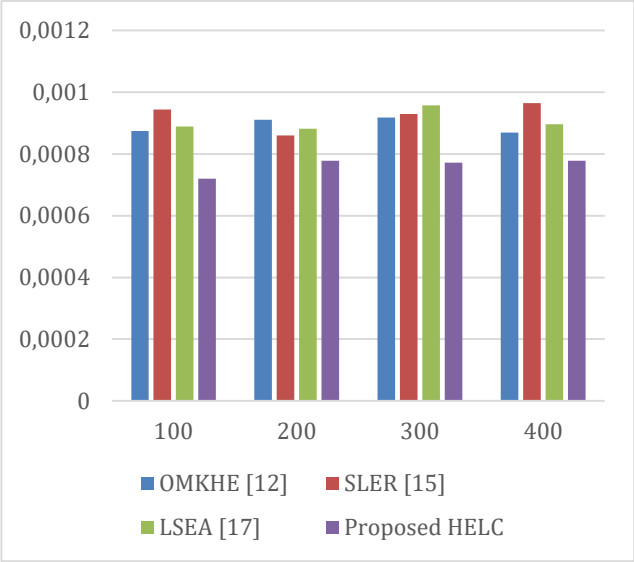

Figure 8. *Graphical representation of decryption time for various message sizes.*

4. Conclusions

This paper introduces an innovative cryptographic method by the name of HELC along with PRC6 and MFBC. The authors have found it to be the best available solution for data security within the complex IoMT landscape. When connected medical devices are proliferating rapidly in an age, and data related to patients is transferred, security and confidentiality of data are a high priority. The HELC incorporates the MFBC with the PRC6 encryption technique to offer comprehensive solutions to the security challenges inherent in the IoMT environment. Indeed, PRC6 encryption is a salient constituent of the HELC algorithm and ranks as one of the most powerful and secure forms of encryption. In this regard, it addresses an abstraction level and assures high-level data security. As a form of encryption, it ensures that medical confidential data be protected, with any form of unauthorized access or alterations thereof being militated against. However, the IoMT ecosystem also calls for more security layers in place, especially when transmitting and storing data. It is within this regard that MFBC fills the gap. Then, MFBC integrated with PRC6 within the HELC algorithm provides an essential strength of data security. Because it is a block cipher, MFBC enhances medical data security so that malicious intervention to intercept or tamper with it would be quite difficult while transferring or storing these data. The synergism of PRC6 with MFBC erects a multi-layered defense mechanism that can provide secrecy and security for such sensitive user data involved in all phases of handling IoMT data. Another notable feature of the HELC algorithm is that its performance is much better than the common encryption techniques in use nowadays in vast applications of IoMT. Research dictates that HELC outperforms the popular OMKHE encryption method by a substantial 13.33%. It further surpasses the SLER encryption approach by a notable 10.00% and the LSEA encryption method by a remarkable 15.71%. From these results, it can be observed that HELC carries huge potential and practicality in IoMT security applications. Future Avenues of Research: Several interesting avenues for future research and development exist in this area. It is an exciting idea for the study of advanced encryption methods and algorithms as it would further hone the level of security of the HELC system. Optimize the encryption and decryption processes, a step forward in that field; primarily cut down on computing overhead and enhance the overall system for greater efficiency. In so doing, it would lead to increased security efficiency and help in an easy integration of HELC into the IoMT devices and systems. Also, the HELC system can further be developed to include a much more robust authentication mechanism and access control protocols. This way only authorized medical professionals, or designated users could have access and decrypt the transmitted data. Such measures are critical to ensuring that the privacy and integrity of medical data are respected, thus making it an essential component in continued development and deployment of secure and efficient cryptographic systems in the ever-changing and emergent IoMT domain. IoT is important and it has been used in different works [41-48].

Author Statements:

- **Ethical approval:** The conducted research is not related to either human or animal use.
- **Conflict of interest:** The authors declare that they have no known competing financial interests

or personal relationships that could have appeared to influence the work reported in this paper

- **Acknowledgement:** The authors declare that they have nobody or no-company to acknowledge.
- **Author contributions:** The authors declare that they have equal right on this paper.
- **Funding information:** The authors declare that there is no funding to be acknowledged.

- **Data availability statement:** The data that support the findings of this study are available on request from the corresponding author. The data are not publicly available due to privacy or ethical restrictions.

References

[1] Koutras, D., Stergiopoulos, G., Dasaklis, T., Kotzanikolaou, P., Glynos, D., & Douligeris, C. (2019). Security in IoMT Communications: A Survey. *Sensors*. *20*(17); 4828. https://doi.org/10.3390/s20174828

[2] A. Ghubaish, T. Salman, M. Zolanvari, D. Unal, A. Al-Ali and R. Jain. (2021). Recent Advances in the Internet-of-Medical-Things (IoMT) Systems Security. *in IEEE Internet of Things Journal*. 8(11); 8707-8718, DOI: 10.1109/JIOT.2020.3045653.

[3] M. N. Hossen, V. Panneerselvam, D. Koundal, K. Ahmed, F. M. Bui and S. M. Ibrahim. (2023). Federated Machine Learning for Detection of Skin Diseases and Enhancement of Internet of Medical Things (IoMT) Security. *in IEEE Journal of Biomedical and Health Informatics*. 27(2); 835-841. DOI: 10.1109/JBHI.2022.3149288.

[4] Alsubaei, F., Abuhussein, A., Shandilya, V., & Shiva, S. (2019). IoMT-SAF: Internet of Medical Things Security Assessment Framework. *Internet of Things*, *8*; 100123. https://doi.org/10.1016/j.iot.2019.100123

[5] Yazid, Ahmed. (2023). Cybersecurity and Privacy Issues in the Internet of Medical Things (IoMT). *Eigenpub Review of Science and Technology* .7(1);1-21.

[6] Papaioannou, M., Karageorgou, M., Mantas, G., Sucasas, V., Essop, I., Rodriguez, J., & Lymberopoulos, D. (2022). A Survey on Security Threats and Countermeasures in Internet of Medical Things (IoMT). *Transactions on Emerging Telecommunications Technologies*, *33*(6), e4049. https://doi.org/10.1002/ett.4049

[7] Kumar, Randhir, and Rakesh Tripathi. (2021). Towards design and implementation of security and privacy framework for internet of medical things (iomt) by leveraging blockchain and ipfs technology. T*he Journal of Supercomputing*. 77, 7916–7955 (2021). https://doi.org/10.1007/s11227-020-03570-x

[8] Zachos, G., Papaioannou, M., De Ree, M., Ribeiro, J. C., Mantas, G., & Rodriguez, J. (2021). Blockchain-Based Security Mechanisms for IoMT Edge Networks in IoMT-Based Healthcare Monitoring Systems. *Sensors*. *22*(7); 2449. doi: 10.3390/s22072449.

[9] Vaiyapuri, Thavavel, Adel Binbusayyis, and Vijayakumar Varadarajan. (2021). Security, privacy and trust in IoMT enabled smart healthcare system: a systematic review of current and future trends. *International Journal of Advanced Computer Science and Applications.* 12(2). DOI:10.14569/IJACSA.2021.0120291

[10] Gopikrishnan, S., Priakanth, P., Srivastava, G., & Joe, C. V. (2023). SCHEISB: Design of a high efficiency IoMT security model based on sharded chains using bio-inspired optimizations. *Computers and Electrical Engineering*. 111;(108925). DOI:10.1016/j.compeleceng.2023.108925.

[11] Salim, M. M., Kim, I., Doniyor, U., Lee, C., & Park, J. H. (2020). Homomorphic Encryption Based Privacy-Preservation for IoMT. *Applied Sciences*. 11(18); 8757.

[12] Riya, K. S., Surendran, R., Tavera Romero, C. A., & Sendil, M. S. (2023). Encryption with User Authentication Model for Internet of Medical Things Environment. *Intelligent Automation & Soft Computing*. 35(1);507-520 DOI:10.32604/iasc.2023.027779

[13] Liu, Xiaoguang, Yingying Sun, and Hao Dong. (2023). A pairing-free certificateless searchable public key encryption scheme for IoMT. *Journal of Systems Architecture*. 139;102885. https://doi.org/10.1016/j.sysarc.2023.102885

[14] Ravi, Renjith V., S. B. Goyal, and Chawki Djeddi. (2022, December 17–18). A new medical image encryption algorithm for IoMT applications. *Pattern Recognition and Artificial Intelligence: 5th Mediterranean Conference, MedPRAI 2021 Istanbul-Turkey. Proceedings. Cham: Springer International Publishing*.

[15] Wei, Tiankuo, Sicong Liu, and Xiaojiang Du. (2022). Learning-based efficient sparse sensing and recovery for privacy-aware IoMT. *IEEE Internet of Things Journal*. 9(12); 9948-9959.

[16] Raj, Kamal, and Srinivasu Bodapati. (2022). FPGA Based Light Weight Encryption of Medical Data for IoMT Devices using ASCON Cipher. *2022 IEEE International Symposium on Smart Electronic Systems (iSES)*.

[17] Saif, Sohail, Priya Das, and Suparna Biswas. (2023). LSEA-IOMT: On the Implementation of Lightweight Symmetric Encryption Algorithm for Internet of Medical Things (IoMT). *Frontiers of ICT in Healthcare: Proceedings of EAIT 2022. Singapore: Springer Nature Singapore*. 565-575.

[18] Ravikumar, G., Venkatachalam, K., AlZain, M. A., Masud, M., & Abouhawwash, M. (2023). Neural cryptography with fog computing network for health monitoring using IoMT. *Computer Systems Science and Engineering*. *44*(1), 945-959. https://doi.org/10.32604/csse.2023.024605

[19] Wang, Haiyan. (2022). An Efficient Searchable Encryption Framework with Weighted Keywords for the Internet of Medical Things (IoMT). *TechRxiv. Preprint.*

[20] El-Shafai, W., Khallaf, F., El-Rabaie, ES.M. et al. (2024). Proposed 3D chaos-based medical image cryptosystem for secure cloud-IoMT eHealth

communication services. *J Ambient Intell Human Comput*. 15, 1–28 DOI: 10.1007/s12652-022-03832-x.

[21] Guitouni, Zied, Mohammed Ali Ghaieb, and Mohsen Machhout. (2023). Security Analysis of Medical Image Encryption using AES Modes for IoMT Systems. *International Journal of Computer Applications.* 14(2);975; 8887. DOI:10.5120/ijca2023922668

[22] Bhuvaneswari, S., and T. PramanandaPerumal. (2023). Secure Group Key Management for Group Communication in IoMT Environment with Dual Encryption Scheme. *Scandinavian Journal of Information Systems.* 35(1); 616-627.

[23] Bhushan, B., Kumar, A., Agarwal, A. K., Kumar, A., Bhattacharya, P., & Kumar, A. (2022). Towards a Secure and Sustainable Internet of Medical Things (IoMT): Requirements, Design Challenges, Security Techniques, and Future Trends. *Sustainability*. 15(7), 6177.

[24] M. Adil, M. K. Khan, M. M. Jadoon, M. Attique, H. Song and A. Farouk. (2023). An AI-Enabled Hybrid Lightweight Authentication Scheme for Intelligent IoMT Based Cyber-Physical Systems. *in IEEE Transactions on Network Science and Engineering*. 10(5); 2719-2730. DOI: 10.1109/TNSE.2022.3159526.

[25] Ravi, R. V., Goyal, S. B., Djeddi, C., & Kustov, V. (2022). Medical Image Transmission Using a Secure Cryptographic Approach for IoMT Applications. *In International Conference on Computing, Intelligence and Data Analytics*, *Cham: Springer International Publishing, pp. 27-38.*

[26] P. Singh, K. J. Devi, H. K. Thakkar and K. Kotecha. (2022). Region-Based Hybrid Medical Image Watermarking Scheme for Robust and Secured Transmission in IoMT. *in IEEE Access*. 10; 8974-8993. DOI: 10.1109/ACCESS.2022.3143801.

[27] Nie, X., Zhang, A., Chen, J., Qu, Y., & Yu, S. (2022). Blockchain-empowered secure and privacy-preserving health data sharing in edge-based IoMT. *Security and Communication Networks*. Article ID 8293716, 16 pages https://doi.org/10.1155/2022/8293716

[28] Sutradhar, S., Karforma, S., Bose, R., & Roy, S. (2023). A Dynamic Step-wise Tiny Encryption Algorithm with Fruit Fly Optimization for Quality of Service improvement in healthcare. *Healthcare Analytics*. *3*; 100177.

[29] Ktari, J., Frikha, T., Ben Amor, N., Louraidh, L., Elmannai, H., & Hamdi, M. (2021). IoMT-Based Platform for E-Health Monitoring Based on the Blockchain. *Electronics*. *11*(15); 2314.

[30] Karam, Asaad Ali. (2022). Investigating The Importance of Ethics And Security On Internet Of Medical Things (IoMT). *International Journal of Computations, Information and Manufacturing (IJCIM)*. 2(2). DOI:10.54489/ijcim.v2i2.114

[31] Hernandez-Jaimes, M. L., Martinez-Cruz, A., Ramírez-Gutiérrez, K. A., & Feregrino-Uribe, C. (2023). Artificial intelligence for IoMT security: A review of intrusion detection systems, attacks, datasets and Cloud–Fog–Edge architectures. *Internet of Things*. 23;(100887). https://doi.org/10.1016/j.iot.2023.100887

[32] Rajawat, A. S., Goyal, S. B., Bedi, P., Jan, T., Whaiduzzaman, M., & Prasad, M. (2023). Quantum Machine Learning for Security Assessment in the Internet of Medical Things (IoMT). *Future Internet*. 15(8);271.

[33] Ahmed, S. F., Alam, M. S. B., Afrin, S., Rafa, S. J., Rafa, N., & Gandomi, A. H. (2024). Insights into Internet of Medical Things (IoMT): Data fusion, security issues and potential solutions. *Information Fusion*. 102;102060. https://doi.org/10.1016/j.inffus.2023.102060

[34] Devi, S. S., Kuruba, C., Nam, Y., & Abouhawwash, M. (2023). Paillier Cryptography Based Message Authentication Code for IoMT Security. *Computer Systems Science & Engineering*. 44(3); 2209-2223. https://doi.org/10.32604/csse.2023.025514

[35] Wazid, Mohammad, and Prosanta Gope. (2023). BACKM-EHA: A novel blockchain-enabled security solution for IoMT-based e-healthcare applications. *ACM Transactions on Internet Technology*. 23(3); 1-28.

[36] Ribeiro, J. C., Mantas, G., Sakellari, G., & Gonzalez, J. (2023). Prototyping a Hyperledger Fabric-Based Security Architecture for IoMT-Based Health Monitoring Systems. *Future Internet*. 15(9); 308.

[37] Rani, S., Kataria, A., Kumar, S., & Tiwari, P. (2023). Federated learning for secure IoMT-applications in smart healthcare systems: A comprehensive review. *Knowledge-Based Systems*. 274;110658. https://doi.org/10.1016/j.knosys.2023.110658

[38] El-Banby, G. M., Elazm, L. A. A., El-Shafai, W., El-Bahnasawy, N. A., El-Samie, F. E. A., Elazm, A. A., & Siam, A. I. (2023). Security enhancement of the access control scheme in IoMT applications based on fuzzy logic processing and lightweight encryption. *Complex & Intelligent Systems*. 1-20(10); 435–454. https://doi.org/10.1007/s40747-023-01149-6

[39] Alsemmeari, R. A., Dahab, M. Y., Alsulami, A. A., Alturki, B., & Algarni, S. (2022). Resilient Security Framework Using TNN and Blockchain for IoMT. *Electronics*. 12(10); 2252.

[40] Singh, N., Das, A.K. (2024). TFAS: two factor authentication scheme for blockchain enabled IoMT using PUF and fuzzy extractor. *J Supercomput*. 80, 865–914. https://doi.org/10.1007/s11227-023-05507-6

[41] SOYSAL, E. N., GURKAN, H., & YAVSAN, E. (2023). IoT Band: A Wearable Sensor System to Track Vital Data and Location of Missing or Earthquake Victims. *International Journal of Computational and Experimental Science and Engineering*, 9(3), 213–218. Retrieved from https://ijcesen.com/index.php/ijcesen/article/view/257

[42] M, P., B, J., B, B., G, S., & S, P. (2024). Energy-efficient and location-aware IoT and WSN-based

precision agricultural frameworks. *International Journal of Computational and Experimental Science and Engineering*, 10(4);585-591. https://doi.org/10.22399/ijcesen.480

[43] Ponugoti Kalpana, L. Smitha, Dasari Madhavi, Shaik Abdul Nabi, G. Kalpana, & Kodati , S. (2024). A Smart Irrigation System Using the IoT and Advanced Machine Learning Model: A Systematic Literature Review. *International Journal of Computational and Experimental Science and Engineering*, 10(4);1158-1168. https://doi.org/10.22399/ijcesen.526

[44] M. Devika, & S. Maflin Shaby. (2024). Optimizing Wireless Sensor Networks: A Deep Reinforcement Learning-Assisted Butterfly Optimization Algorithm in MOD-LEACH Routing for Enhanced Energy Efficiency. *International Journal of Computational and Experimental Science and Engineering*, 10(4);1329-1336. https://doi.org/10.22399/ijcesen.708

[45] S, P. S., N. R., W. B., R, R. K., & S, K. (2024). Performance Evaluation of Predicting IoT Malicious Nodes Using Machine Learning Classification Algorithms. *International Journal of Computational and Experimental Science and Engineering*, 10(3);341-349. https://doi.org/10.22399/ijcesen.395

[46] Alkhatib, A., Albdor , L., Fayyad, S., & Ali, H. (2024). Blockchain-Enhanced Multi-Factor Authentication for Securing IoT Children's Toys: Securing IoT Children's Toys. *International Journal of Computational and Experimental Science and Engineering*, 10(4);1041-1049. https://doi.org/10.22399/ijcesen.417

[47] S, P., & A, P. (2024). Secured Fog-Body-Torrent : A Hybrid Symmetric Cryptography with Multi-layer Feed Forward Networks Tuned Chaotic Maps for Physiological Data Transmission in Fog-BAN Environment. *International Journal of Computational and Experimental Science and Engineering*, 10(4);671-681. https://doi.org/10.22399/ijcesen.490

[48] P. Jagdish Kumar, & S. Neduncheliyan. (2024). A novel optimized deep learning based intrusion detection framework for an IoT networks. *International Journal of Computational and Experimental Science and Engineering*, 10(4);1169-1180. https://doi.org/10.22399/ijcesen.597