Lightweight Cryptographic Algorithms for Medical IoT Devices using Combined Transformation and Expansion (CTE) and Dynamic Chaotic System

Abdul Muhammed Rasheed, Retnaswami Mathusoothana Satheesh Kumar
Department of Information Technology, Noorul Islam Centre for Higher Education, Tamil Nadu, India

***Abstract*—IoT is growing in prominence as a result of its various applications across many industries. They gather information from the real world and send it over networks. The number of small computing devices, such as RFID tags, wireless sensors, embedded devices, and IoT devices, has increased significantly in the last few years. They are anticipated to produce enormous amounts of sensitive data for the purpose of controlling and monitoring. The security of those devices is crucial because they handle precious private data. An encryption algorithm is required to safeguard these delicate devices. The performance of devices is hampered by traditional encryption ciphers like RSA or AES, which are costly and easy to crack. In the realm of IoT security, lightweight image encryption is crucial. For image encryption, the majority of currently used lightweight techniques use separate pixel values and position modifications. These kinds of schemes are limited by their high vulnerability to cracking. This paper introduces a Lightweight cryptography (LWC) algorithm for medical IoT devices using Combined Transformation and Expansion (CTE) and Dynamic Chaos System. The suggested system is evaluated in terms of cross-entropy, UACI, and NPCR. As demonstrated by the experimental results, the suggested system is ideal for medical IoT systems and has very high encryption and decryption efficiency. The proposed system is characterized by its low memory usage and simplicity.**

Keywords*—Internet of Things (IoT); data transmission; data security; medical IoT devices; lightweight cryptography; encryption; decryption

I. Introduction

IoT is a network of integrated, sensing, and identifying devices that are accessible over the network and can communicate with each other. One of the new sensing application areas provided by IoT is smart environment monitoring systems. Other examples include smart homes, smart buildings, and smart transportation systems. The IoT is expected to grow rapidly by 2030, when 125 million smart devices will be merged to the Internet [1]. Smart things that can organize, configure, and reconfigure themselves constitute the IoT network. On the other hand, the implementation of these smart objects faces some difficulties [2].

With the advent of sensors, smart networking, RFID, and IoT, the world has become more networked in the last ten years in order to accomplish a wide range of tasks [3]. IoT is a modern technology used in smart objects. Tangible gadgets like laptops, refrigerators, phones, and cars are referred to as "smart objects." IoT refers to a network of smart objects that other networked devices can recognize, control, and access. They can compute and make decisions as well. IoT is a global network that uses common communication systems and has dynamic capabilities. It can work with both real and virtual objects. It can be used with intelligent platforms that are easily integrated into communication technologies [4].

The idea behind IoT is the integration of intelligent manufacturing equipment, advanced analytics, and automation driven by AI. It will make human life more economical and manageable. IoT may be a rapidly expanding field at the moment, bringing with it a variety of new problems such as short battery life, low memory, short device connection range, etc. [5]. Furthermore, it is evident that the current IoT is vulnerable in terms of energy and security, and its growth prevents it from concentrating on the security framework.

IoT provides an accurate and genuine picture of the challenges and solutions in the IoT framework today through the breakdown of existing devices with different spaces and advancements. Patients and specialists could only collaborate through in-person meetings and text and phone conversations before IoT. Devices enabled by IoT have made it possible to observe patients remotely in the medical field. The more comfortable and effective doctor-patient interactions have also led to a rise in patient engagement and satisfaction. In addition, the patient's condition has been tracked from a distance, which shortens the time spent in the clinic and avoids reaffirmations.

Instead of just creating stand-alone wearables, it is critical to design an entire ecosystem equipped with sensors and devices that will merge data to cloud services via the IoT framework [6–8]. The three primary layers of the design include the following components: the cloud, Internet-connected gateways, and edge devices; sensor-equipped body space networks; and the essential big data support layer. Security is always the primary concern when a new technology is introduced. It is extremely valid in the context of IoT, where devices are used to collect a lot of personal data. Desktop computers are giving way to resource-constrained, small-sized computing devices. The replacement of large amounts of data resulting from the interconnection of these small devices through the Internet and multiple networks poses an unprecedented challenge for the users in terms of data security [9], [10]. IoT devices interact quickly with the outside world to collect private information or control tangible environmental factors. Because of this, they become a desirable target for attackers [12] and are easily accessible, making them open to

different types of security breaches [11]. Cybersecurity is a major concern for IoT devices due to demands for secrecy, integrity of data, authorization and authentication, availability, privacy, and regulatory requirements, as well as frequent system upgrades [13]. In this situation, one of the best methods to ensure the data's secrecy, integrity, authentication, and authorization while it travels between IoT devices might be through cryptography. Data stored or transmitted over a network may be protected with the use of cryptography.

Conventional encryption algorithms provide high security, but they also consume a significant amount of memory, processing, and energy. Due to their limited resources, small devices are not an appropriate choice for traditional encryption. The advent of LWC is a new type of encryption that was made possible by advancements in processors, power consumption, and memory costs in traditional encryption. This encryption lowers memory costs and power consumption, making it appropriate for devices with constrained resources. The newest trend in encryption for devices with low resources is called LWC. This can be attributed to the utilization of basic mathematical operations, reduced memory expenses, and decreased power usage. LWC aims to reduce the overall costs associated with implementing traditional encryption by concentrating on a number of variables, including code size, memory cost, execution time, and energy consumption.

A safe and effective LWC algorithm for small IoT medical devices is suggested in this paper. The major contribution of the proposed work includes:

- Design and development of LWC algorithms applicable for IoT healthcare devices.
- Design and development of novel LWC algorithms based on Chaos theory to provide encryption with less computational complexity and more efficiency.
- Performance assessment of suggested LWC algorithms in terms of NPCR, UACI and Cross Entropy.

The remainder of the paper is organized as follows: A literature review is offered in Section II, highlighting areas necessitating further research. Section III elucidates the methodology in detail. Section IV delves into a comprehensive discussion of the outcomes resulting from the proposed approach. Lastly, in Section V, the paper concludes by summarizing the findings.

II. Literature Review

Fursan Thabit, Sharaf Alhomdy, Abdulrazzaq H.A. Al-Ahdal and Sudhir Jagtap [14] introduced a LWC algorithm for improving the data security. A 16-byte block cipher algorithm must be used to encrypt the data utilizing a 16-byte key. The complexity of the encryption is increased by drawing inspiration from Feistel and SP architectural techniques. According to the simulation results, the suggested algorithm has revealed a strong security level and a discernible enhancement in encryption and decryption, offering low computation costs and high security.

Mohammad Kamrul Hasan, Muhammad Shafiq, Shayla Islam, Bishwajeet Pandey, Yousef A. Baker El-Ebiary, Nazmus Shaker Nafi, R. Ciro Rodriguez and Doris Esenarro Vargas [15] carried out an investigation of cryptographic algorithms. It provides a thorough assessment of the timing complexity, size, encryption, and decryption performances of different algorithms. It has been tested to mitigate the assuming attack in complex real-time DL IoT applications. Using the simulation approach, an evaluation was carried out to test the encryption and decryption speeds of the preferred encryption algorithms. According to the simulation results, Blowfish performs better than the other widely used encryption algorithms.

An empirical investigation of the performance of 32 LWC algorithms that were deployed on three embedded platforms serving as IoT nodes was conducted by Fotovvat, A., Rahman, G. M., Vedaei, S. S., & Wahid, K. A [16]. The platforms selected for this work can be applied to different layers of the IoT ecosystem. Authenticated encryption algorithms such as AES-GCM, AES-CCM, and AES-OCB were compared with a range of test scenarios. The experiment results showed that other timing requirements are much more important than the encryption time of LWC algorithms.

A performance assessment of ten LWC algorithms was conducted by Panahi, P., Bayılmış, C., Çavuşoğlu, U., & Kaçar, S. [17]. These algorithms evaluate crucial aspects such as consumption of energy, throughput, memory usage, and execution time during cloud transmission. The most popular IoT devices used in the simulations are the Arduino Mega 2560 and Raspberry Pi 3.

Jadaun, A., Alaria, S. K., & Saini, Y [18] suggested the establishment of a symmetric key LWC algorithm for secure data transmission of text and images utilizing a reversible data hiding system and an image encryption system. A graphical user interface was utilized in the design of the suggested symmetric cryptographic key. A secure data transmission system was also intended to be used with the reversible data-hiding system. The simulation results revealed that the suggested algorithm yields the best results in terms of MSE and PSNR.

Toprak, S., Akbulut, A., Aydın, M. A., & Zaim, A. H. [19] introduced an energy-efficient LWC algorithm for IoT medical devices. A lightweight block cipher algorithm is proposed in order to have an encryption algorithm that is both secure enough to withstand primal cryptanalysis attacks and lightweight enough for constrained or limited hardware environments. Both the length of the key and the length of the blocks that need to be encrypted are 64 bits. It is intended for body sensor area devices and IoT systems with low-end microcontrollers. The well-known algorithms are employed for assessing the security and performance aspects of LWE. It was discovered that LWE can transmit raw data with a minimal amount of security without seriously taxing the network infrastructure. It can be claimed that the outcome is adequate and even outperforms other algorithms.

A novel ultra-LWC algorithm named SLIM was proposed by Aboushosha, B., Ramadan, R. A., Dwivedi, A. D., El-Sayed, A., & Dessouky, M. M [20] for RFID systems. The most popular type of cryptography, block ciphers, offer extremely strong security for IoT devices. SLIM is a 32-bit

block cipher that is built on the Feistel framework. Designing a lightweight block cipher that balances security, cost, and performance is a major challenge. The suggested algorithm is characterized by an appropriate cost/security for RFID framework, a small implementation area, excellent performance in both software and hardware platforms, and energy-efficient behaviour.

Kakali Chatterjee and Ravi Raushan Kumar Chaudhary [21] provided a lightweight block cipher method with a flexible structure. This aids in the creation of a flexible cryptosystem that can be implemented on a variety of IoT devices' hardware. The primary purpose of this framework is to support health monitoring systems, which are a component of electronic health care. The user can access the recorded data in this monitoring system only after completing the necessary authentication procedures. The data is encrypted using LWC. In addition, the system's performance is evaluated, and formal verification for high-level security is completed. The primary keys used in the LWC ciphering technique ranged from 128 to 256 bits. When compared to another current scheme, the computational cost of the suggested framework is low. So, it is appropriate for low-power and memory-intensive IoT devices.

Al-Husainy, M. A. F., Al-Shargabi, B., & Aljawarneh, S. [22] developed a lightweight, adaptable encryption system that includes transposition operations and strong, straightforward substitution in order to encrypt and decrypt data that is compatible with the limited processing power of IoT devices. By using a variable block size, the suggested framework was made more versatile so that it could be used on various IoT devices with different amounts of memory. Additionally, random encryption keys that are difficult for thieves to decipher are generated using the deoxyribonucleic acid sequence. When compared to well-known cryptographic systems, the experimental results of the suggested lightweight encryption system showed excellent outcomes for any IoT device in terms of memory size and encryption time.

Jabeen, T., Ashraf, H., Khatoon, A., Band, S. S., & Mosavi, A. [23] suggested a genetic-based encryption approach to secure the data in an unintelligible format. Security and confidentiality are additionally guaranteed by a lightweight telemetry transport protocol for encrypted data transmission across the network. The major aim of the suggested approach is to provide a bandwidth-efficient protocol with low battery power consumption. The suggested approach is evaluated in the MATLAB platform. The suggested encryption scheme is evaluated for efficacy in the WBAN sensor environment using a genetic-based encryption algorithm.

Atiewi, S., Al-Rahayfeh, A., Almiani, M., Yussof, S., Alfandi, O., Abugabah, A., & Jararweh, Y [24] proposed an IoT environment that is cloud-enabled and encouraged by multifactor authentication and LWC encryption techniques to secure big data systems. The goal of the suggested hybrid cloud platform is to offer extremely secure data protection for businesses. Private and public clouds are combined to create a hybrid cloud environment. Data from sensitive devices is split into two halves and encrypted with the Fiestel and RC6 algorithms. Through the use of a gateway device, these data are kept in a private cloud with maximum security. On the other hand, gateway devices are used to store non-sensitive device data in a public cloud after it has been encrypted using AES. The efficiency of the recommended strategy was evaluated. According to the simulation outcomes, the suggested approach outperforms existing encryption algorithms.

A safe, lightweight algorithmic encryption technique was presented by Hasan, M. K., Islam, S., Sulaiman, R., Khan, S., Hashim, A. H. A., Habib, S., & Hassan, M. A [25] to safeguard the privacy of patient medical images. Two permutation techniques are used in the suggested lightweight encryption method to protect medical images. The security and execution time of the suggested method are compared to those of conventionally encrypted methods after they have been examined and assessed. The effectiveness of the suggested algorithm was analyzed on a large number of test images. Extensive experiments revealed that the suggested algorithm for image cryptosystems provides higher efficiency compared to conventional techniques.

A lightweight, efficient healthcare monitoring system utilizing Radio Frequency Identification (RFID) tags and the IoT was proposed by Naresh, V. S., Reddi, S., & Murthy, N. V [26]. This work used a dual-band RFID protocol, wherein 2.45 GHz microwave bands are employed to monitor corporal information and 13.56 MHz high-frequency RFID is useful for identifying individuals. An RFID tag is utilized to identify the patient, and sensors are utilized to track and gather physiological data about them. According to the simulation results, the suggested protocol is more efficient than other currently used techniques.

An improved LWC algorithm was proposed by Jebri, S., Ben Amor, A., Abid, M., & Bouallegue, A. [27] to secure data transmission in IoT framework. The suggested solution ensures that most security flaws are addressed with regard to trust registration and anonymous mutual authentication. A lightweight, secure IoT system was ensured by employing elliptic curve cryptography, identity-based encryption, and pseudonym-based cryptography approaches. As per the evaluation results of the system with Raspberry cards and the MIRACL library, the system's execution time is adequate for the restricted number of IoT devices.

Chatterjee, K., Chaudhary, R. R. K., & Singh, A. [28] introduced an algorithm for LWC to assure the security of the electronic health care system. The addition substitution and XOR (LWARX) are the foundation of the suggested lightweight scheme. For secure communication within the healthcare system, an efficient authentication approach based on the LWARX approach is also suggested. The effectiveness of the suggested approach is evaluated using a variety of metrics, including throughput, latency, gate equivalent etc. The comparison outcomes show that the suggested ciphering technique has excellent performance, low power and energy consumption, and high throughput. The comparison of selected LWC algorithms is tabulated in Table I.

IoT-based smart environments are susceptible to privacy and data breaches. LWC solutions are crucial since IoT applications are implemented on devices with limited resources. The majority of these modern, LWC solutions rely on hashing techniques like message digests (MD5) or SHA

hash function variants. The device needs more resources to perform the intricate rotational and XOR operations of these current functions. Elliptic curve cryptography (ECC) is the foundation of many lightweight schemes. These ECC schemes generate signatures using single and static elliptic curve parameters. The embedded devices that store these elliptic curve parameters are susceptible to attacks involving node compromise. The publicly accessible Internet infrastructure on the Internet of Things allows devices to communicate with the server or with each other. It becomes a laborious task to issue certificates for every device on the Internet when thousands of devices are added and removed from the network on a regular basis. The key distribution center (KDC) must regularly distribute security keys for this kind of communication. Therefore, using standard KDC, or key management servers, is becoming more difficult as the number of IoT applications rises. Many cryptographic solutions based on ECDSA and ECIES use single or static elliptic curve parameters. Node compromise attacks can arise from ingesting cryptographic parameters or secret keys on the device. So, in order to overcome the above-mentioned limitations, a secure and effective LWC algorithm for small computing IoT healthcare devices was introduced in this work.

TABLE I. COMPARISON OF SELECTED LWC ALGORITHMS

Name	Block Size (bit)	Key Size (bit)	Structure
AES	128	128	SPN
PRESENT	64	128	SPN
MESA	128	256	Feistel
LEA	128	128	GFN
XTEA	64	128	Feistel
SIMON	64	128	Feistel
PRINCE	64	128	SPN
RECTANGLE	64	128	SPN

III. MATERIALS AND METHODS

In the field of IoT security, lightweight image encryption is crucial. Most existing Lightweight image encryption approaches adopt shuffling of pixel positions and modification of pixel values separately. So, in this paper, an LWC algorithm for medical IoT devices is developed using Combined Transformation and Expansion (CTE) and Dynamic Chaos System. The detailed block schematic of the suggested approach is visualized in Fig. 1.

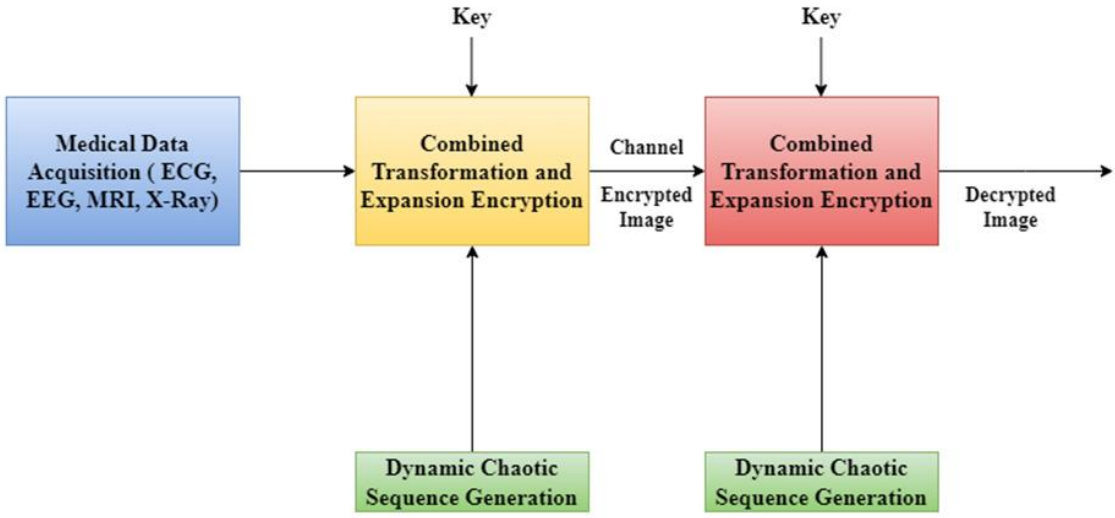

Fig. 1. Block diagram of proposed methodology.

A. Input Medical Images

The medical images were utilized as the input in the proposed work. The input medical images include ECG, EEG, MRI and X-Ray images. Fig. 2 displays the sample medical images.

B. Dynamic Chaotic System

Chaos is defined as "a state of disorder." Systems with dynamic behavior that are extremely sensitive to primary criterion are studied by chaos theory. A reaction that is occasionally indicated to as the "butterfly effect". For such dynamical systems, slight variations in the starting conditions result in widely divergent outcomes, making long-term prediction generally infeasible. This happens in spite of the fact that these systems are deterministic, implies that their future behavior is totally influenced by their primary criterion and that they do not contain any random elements.

Initially, a sequence is generated by means of a 4D dynamic chaos-based system with two positive Lyapunov exponents. The average exponential divergence rate of neighboring trajectories in phase space is represented numerically by the Lyapunov exponent. It is one of the characteristics that helps distinguish between various chaotic motion numerical values. It can be formulated as

$$\lambda = \lim_{n\to\infty} \frac{1}{n} \sum_{n=0}^{N-1} \ln \left| \frac{df(x_n,u)}{dx} \right| \quad (1)$$

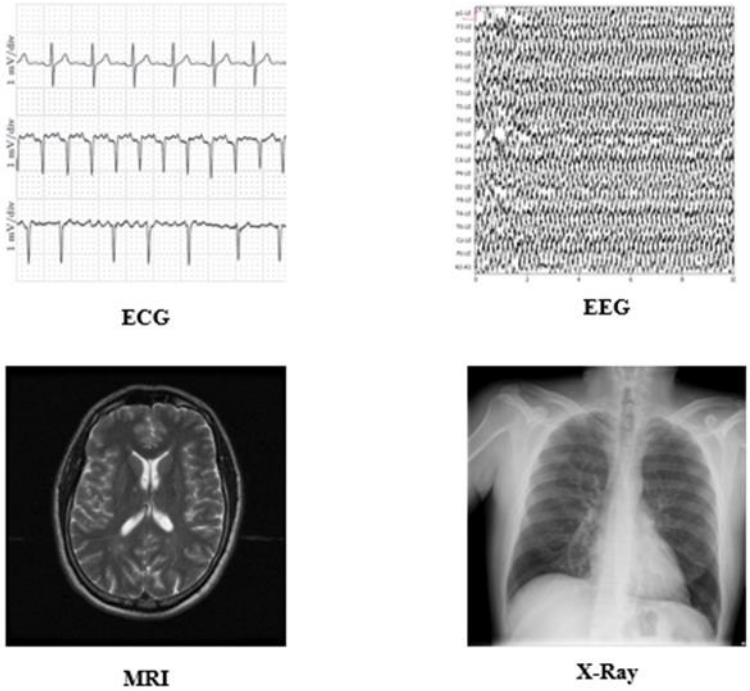

Fig. 2. Sample input medical image.

Fig. 3 depicts the dynamic chaotic system. The dynamic chaos system is initialized with the parameters of the medical image, in order to enhance security. The pixels in images are expanded and transformed using the dynamic chaos sequence. More precisely, the first index matrix establishes which pixels are going to be enlarged and altered. The expansion of the pixels is decided by the second mask matrix. The dynamic chaos sequence is responsible for producing these matrices. In this work, chaotic sequences for encryption were generated using a novel dynamic chaotic system. It can be formulated as

$$x = a(y - x) + w$$
$$y = bx - xz + w$$
$$z = xy - z - w$$
$$w = -c(x + y) \quad (2)$$

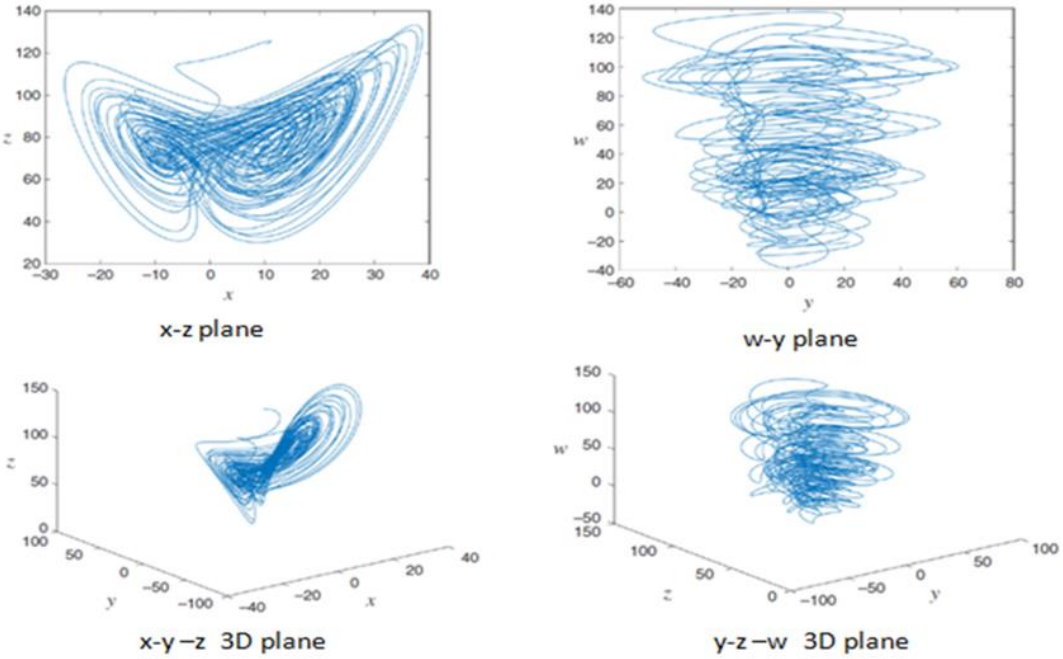

Fig. 3. Dynamic chaotic system.

where the state variables are x, y, z, and w, and the positive constants are a, b, and c. Divide the input image K into 32 blocks in order to generate the initial values for the dynamic chaotic system, which can be expressed as $K = \{k_1, k_2, k_3, \ldots, k_{32}\}$. The four intermediate parameters d_1, d_2, d_3 and d_4 can be calculated as

$$\begin{aligned} d_1 &= b_1 + \frac{1}{256}(k_1 \oplus k_2 \oplus \ldots\ldots \oplus k_8) \\ d_2 &= b_2 + \frac{1}{256}(k_9 \oplus k_{10} \oplus \ldots\ldots \oplus k_{16}) \\ d_3 &= b_3 + \frac{1}{256}(k_{17} \oplus k_{18} \oplus \ldots\ldots \oplus k_{24}) \\ d_4 &= b_4 + \frac{1}{256}(k_{25} \oplus k_{26} \oplus \ldots\ldots \oplus k_{32}) \end{aligned} \quad (3)$$

where, b_1, b_2, b_3 and b_4 are user-defined parameters that can be addressed as security keys.

The initial values x_0, y_0, z_0, and w_0, of the 4D dynamic chaotic system can be obtained from d_1, d_2, d_3 and d_4, which can be expressed as,

$$\begin{aligned} x_0 &= \frac{mod((d_1+d_2+d_3)\times 10^8,\ 256)}{255} \\ y_0 &= \frac{mod((d_2+d_3+d_4)\times 10^8,\ 256)}{255} \\ z_0 &= \frac{mod((d_1+d_2+d_3+d_4)\times 10^8,\ 256)}{255} \\ w_0 &= \frac{mod(mean(d_1+d_2+d_3+d_4)\times 10^8,\ 256)}{255} \end{aligned} \quad (4)$$

The 4D dynamic chaotic system uses the initial values (x_0, y_0, z_0 *and* w_0) to iterate to produce sequences long enough for the subsequent encryption operations. In the j^{th} iteration, it can obtain four state values described as,

$$S^j = \{x_j, y_j, z_j, w_j\} \quad (5)$$

After the iteration terminates, a dynamic chaotic sequence S can be obtained as

$$\begin{aligned} S &= \{s^1, s^2, s^3, \ldots . s^N\} = \{x_1, y_1, z_1, w_1, \ldots\ldots, x_N, y_N, z_N, w_N\} \\ &= \{s_1, s_2, s_3, s_4, \ldots\ldots, s_{4N-3}, s_{4N-2}, s_{4N-1}, s_{4N}\} \end{aligned} \quad (6)$$

C. Combined Transformation and Expansion (CTE)

Two types of auxiliary matrices are needed in the suggested approach. The schematic diagram of CTE is illustrated in Fig. 4. One matrix is used for expansion, and the other is used to identify which pixels need to be processed. Considering an image with dimensions h × w, where h and w stand for height and width, respectively. Two index matrices, I and T, are created for the first matrix using the four random sequences, r_1, r_2, r_3 and r_4, that we adopted from S. Fig. 5 and Fig. 6 show the visualization of the generation of various matrices, respectively.

$$\begin{aligned} I(i,j) &= si_1(mod(i + si_2(j) - 1, w) + 1) \\ T(i,j) &= si_3(mod(i + si_4(j) - 1, w) + 1) \end{aligned} \quad (7)$$

The mask matrix (M) for expansion is calculated using the below equation

$$M = reshape\big(mod\big((r_5 - \lfloor r_5 \rfloor) \times 2^{32}\big), 256\big), [h, w]) \quad (8)$$

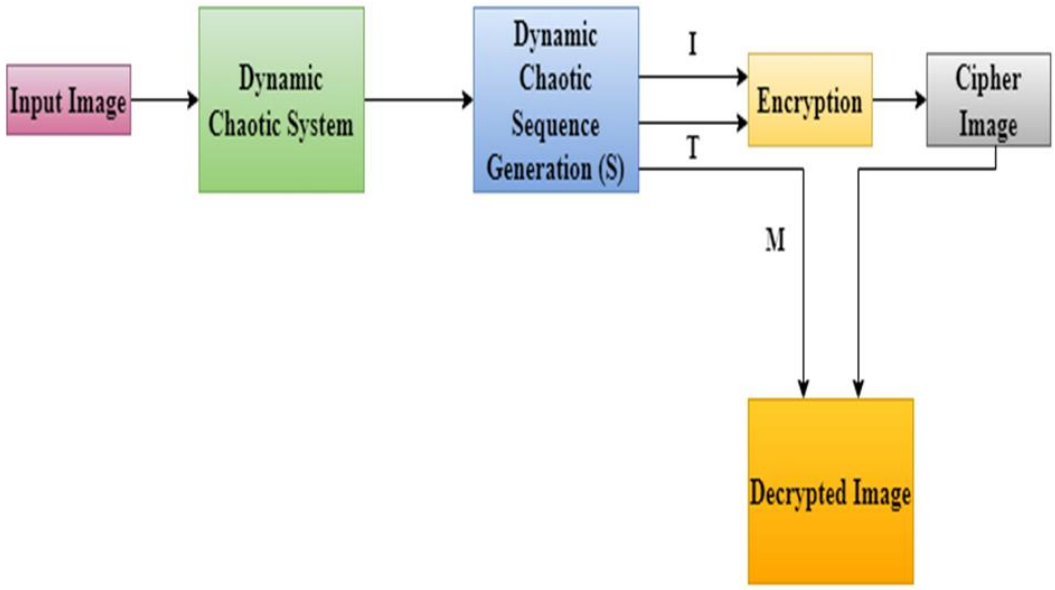

Fig. 4. Block diagram of combined transformation and expansion.

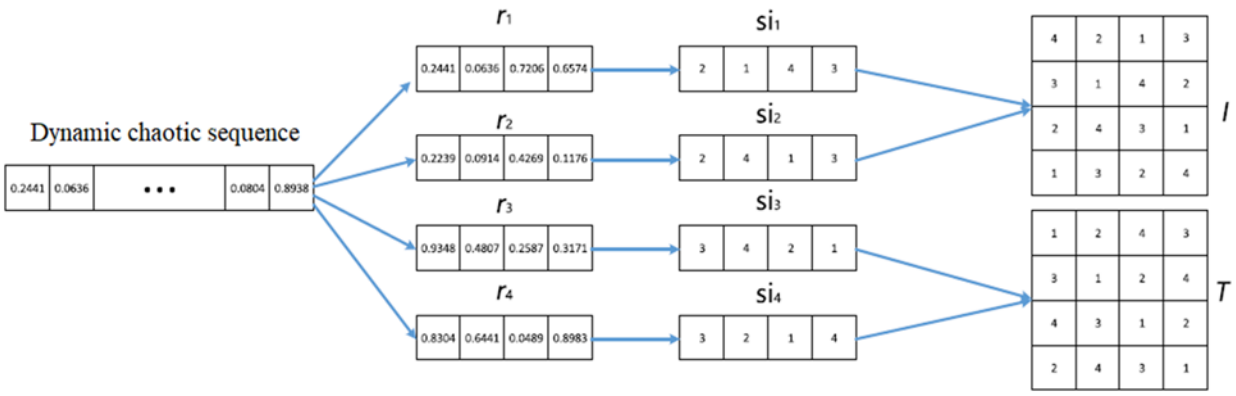

Fig. 5. Visualization of generation of I and T.

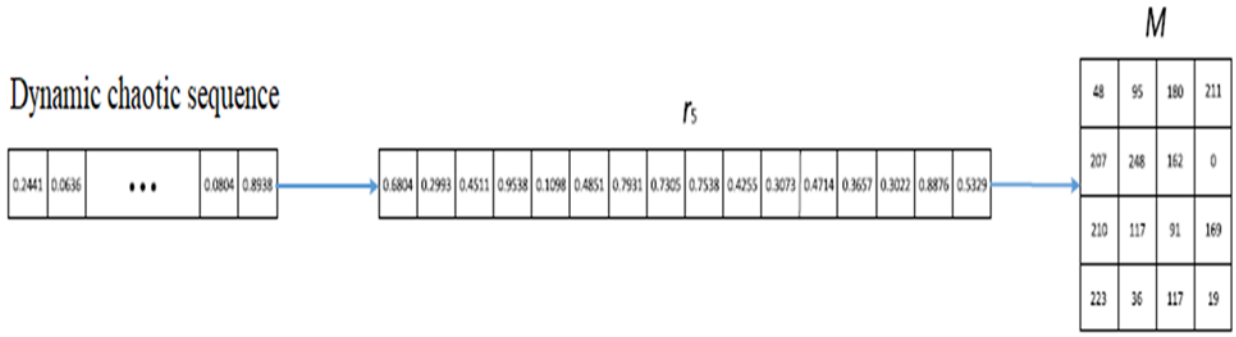

Fig. 6. Visualization of Generation of M.

The method of converting a plain image into a cipher image is known as encryption, and the method of converting a cipher image back into a plain image is known as decryption. Fig. 7 shows the encryption and decryption of the simple image. Data encryption and decryption using cryptographic algorithms typically require a set of characters known as a key. It is simple to encrypt or decrypt plain text into cipher text and back again with the use of a key or algorithm. The proposed CTE algorithm for image encryption and decryption is visualized in Fig. 8.

Considering the user-defined key F, the mask matrix M, the index matrices I and T, and a plain image with one channel P, the encrypted image or Cipher Image (C) can be described as

$$C_{I_{i,j},j} =$$

$$\begin{cases} mod\left(M_{i,j} \oplus P_{T_{j,I_{i,j}},I_{i,j}} + P_{I_{h,w},w}\right),F), & if\ i=1, j=1 \\ mod\left(M_{i,j} \oplus P_{T_{j,I_{i,j}},I_{i,j}} + C_{I_{i-1,w},w}\right),F), & if\ i\neq 1, j=1 \\ mod\left(M_{i,j} \oplus P_{T_{j,I_{i,j}},I_{i,j}} + C_{I_{i,j-1},j-1}\right),F), & if\ j\neq 1 \end{cases} \quad (9)$$

It is possible to obtain the decrypted image D from I, T, M, F, and C

$$D_{T_{j,I_{i,j}},I_{i,j}} =$$

$$\begin{cases} mod\left(M_{i,j} \oplus C_{I_{i,j},j} + C_{I_{h,w},w}\right),F), & if\ i=1, j=1 \\ mod\left(M_{i,j} \oplus C_{I_{i,j},j} + C_{I_{i-1,w},w}\right),F), & if\ i\neq 1, j=1 \\ mod\left(M_{i,j} \oplus C_{I_{i,j},j} + C_{I_{i,j-1},j-1}\right),F), & if\ j\neq 1 \end{cases} \quad (10)$$

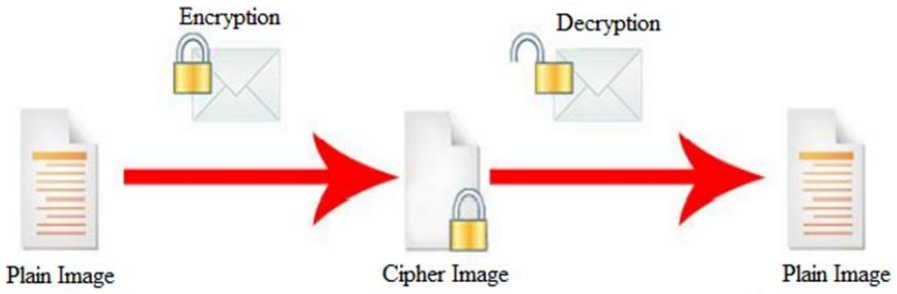

Fig. 7. General block diagram of image encryption and decryption.

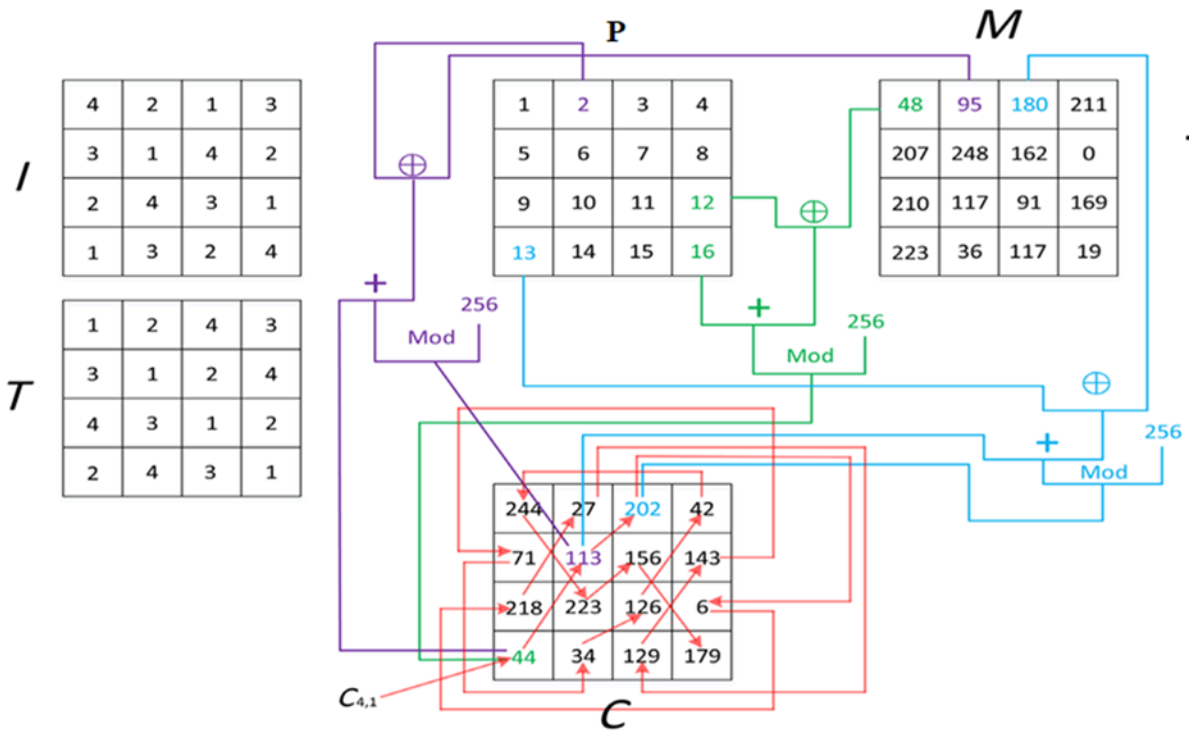

Fig. 8. Illustration of proposed CTE for encryption and decryption.

IV. Results and Discussion

Number of Pixel Changing Rate (NPCR), Unified Averaged Changed Intensity (UACI), and Cross Entropy were used to assess the performance of the suggested LWC algorithm. The strength of image encryption algorithms and ciphers is assessed using NPCR. Its purpose is to count the number of pixels that change between the real and encrypted images. NPCR can be mathematically expressed as,

$$D(i,j) = \begin{cases} 0, if\ C^1(i,j) = C^2(i,j) \\ 1, if\ C^1(i,j) \neq C^2(i,j) \end{cases}$$
$$NPCR: N(c^1, c^2) = \sum_{i,j} \frac{D(i,j)}{T} \times 100\% \quad (11)$$

The effectiveness of image encryption algorithms and ciphers is assessed using UACI. It calculates the average number of intensity changes between the original and encrypted images. It can be mathematically expressed as,

$$UACI: u(C^1, C^2) = \sum_{i,j} \frac{|C^1(i,j) - C^2(i,j)|}{F.T} \times 100\% \quad (12)$$

The cross-entropy between two images predicts the probability of divergence of encrypted pixels from the original image. Cross entropy is also considered as a loss function. The cross entropy can be expressed as

$$H(C^1, c^2) = -\sum_x C^1(x) log\ C^2(x) \quad (13)$$

The performance analysis of original image and encrypted image in terms of NPCR, UACI and cross entropy can be tabulated in Table II.

From Table II, it can be demonstrated that the NPCR and UACI value are high. The high NPCR value indicates that the input medical image and the encrypted medical image differ from each other. The input medical image and the encrypted medical image differ from one another, as indicated by the high UACI value. Cross-entropy has a finite value. This shows that the input medical image and the encrypted medical image have different structures. Table III tabulates the performance analysis of the original and decrypted images.

TABLE II. Original Vs Encrypted Image

Input Image	NPCR	UACI	Cross Entropy
ECG	99.62	47.16	0.1389
EEG	99.62	44.32	0.1103
MRI	99.61	39.67	0.1336
X-Ray	99.61	31.22	0.1318

TABLE III. Original Vs Decrypted Image

Input Image	NPCR	UACI	Cross Entropy
ECG	0	0	0
EEG	0	0	0
MRI	0	0	0
X-Ray	0	0	0

The value of NPCR, UACI and cross entropy are zero for all medical images. This shows that the decrypted image and the input medical image are identical. Fig. 9, 10, and 11 show the histograms for the MRI image channels, encrypted image channels, and decrypted image channels. Fig. 9, 10, and 11 depict histograms representing the distribution of pixel intensities within the MRI image channels, encrypted image channels, and decrypted image channels, respectively. The

MRI image channels histogram provides insight into the original image's intensity distribution, serving as a baseline. The encrypted image channels histogram illustrates the distribution after encryption, indicating potential alterations due to the encryption process. Finally, the decrypted image channels histogram reveals the distribution following decryption, ideally resembling the original MRI image channels histogram, affirming the fidelity of the decryption process in preserving the original intensity distribution. These histograms offer a visual comparison of intensity distributions across various stages of image processing, crucial for evaluating the efficacy and fidelity of encryption and decryption techniques applied to MRI images.

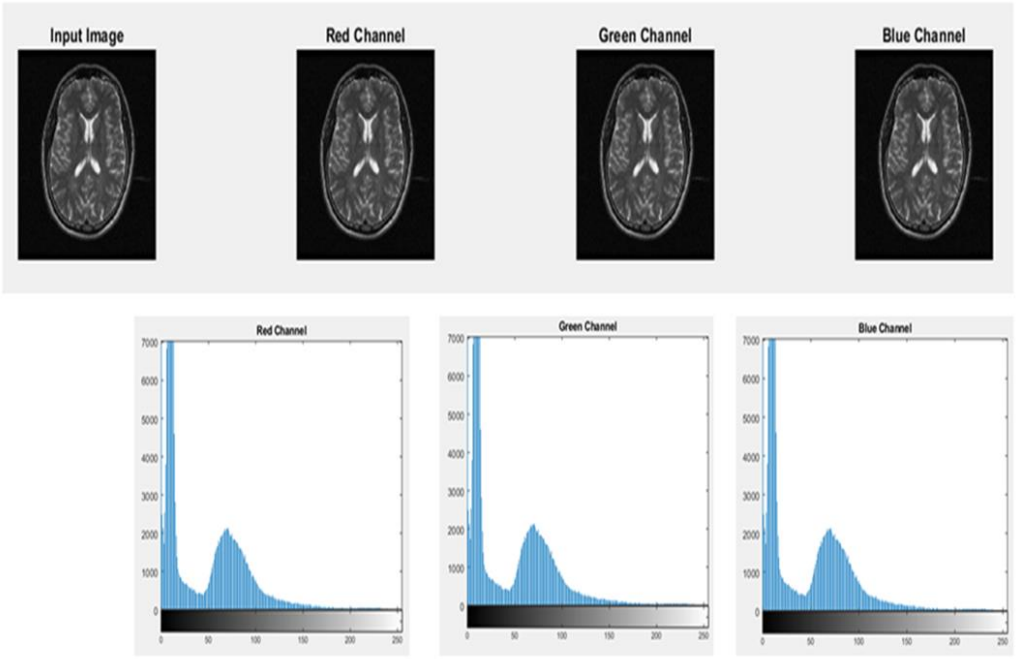

Fig. 9. Histogram of MRI image channels.

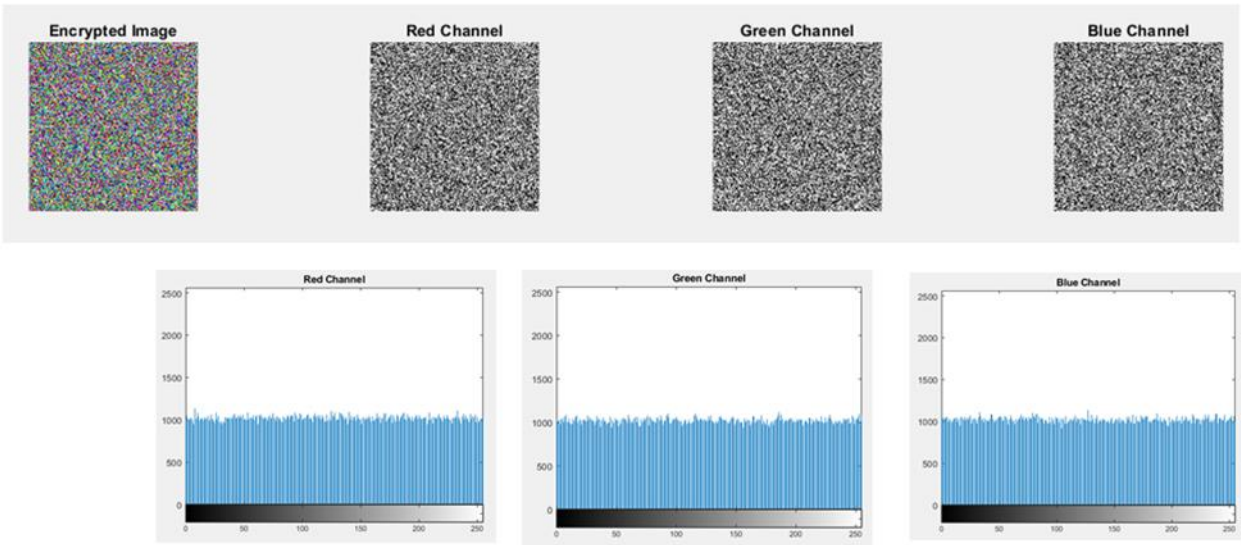

Fig. 10. Histogram of encrypted image channels.

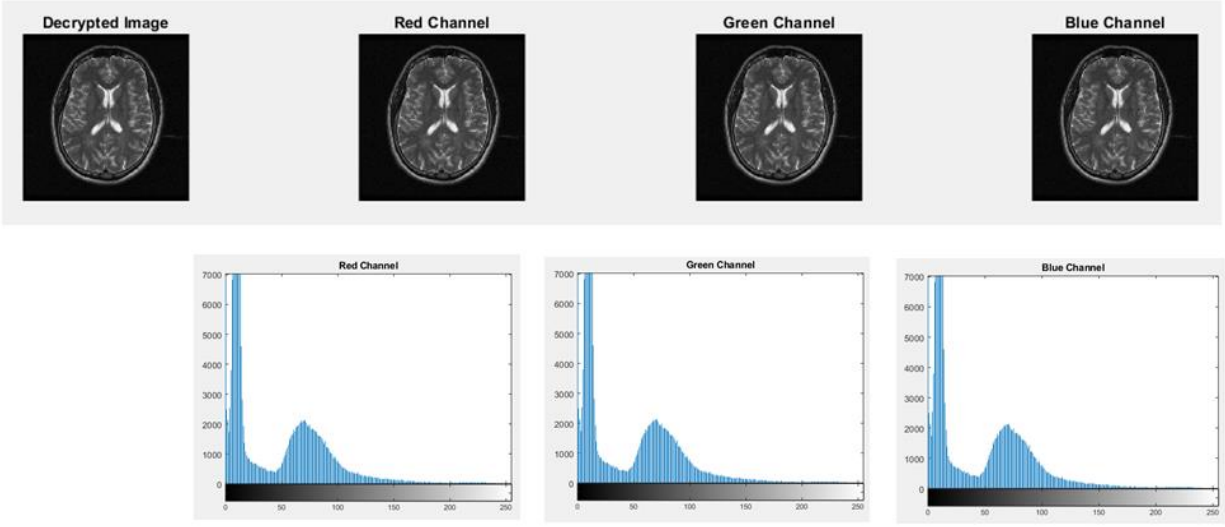

Fig. 11. Histogram of decrypted image channels.

V. CONCLUSION

The IoT is advancing every industry in our rapidly changing world. It facilitates communication between the real and virtual worlds, which will revolutionize operations very rapidly. Due to their limitations, data encryption algorithms must be included in IoT devices in order to increase security. IoT is a network of real, physical objects that have been equipped with RFID, sensors, smart networking, and other methodologies that support them to interchange data with other devices and systems. One important security tool that represents data security is cryptography. The advent of highly sophisticated technologies, coupled with the limitations of mathematical operations and practical applications in traditional cryptography—which also requires a significant amount of processing power and memory guided to the advancement of LWC, a novel approach to cryptography. In this paper, a lightweight cryptography algorithm utilizing the Dynamic Chaos System and Combined Transformation and Expansion (CTE) was proposed for medical IoT devices. The suggested system is assessed in terms of cross-entropy, UACI, and NPCR. The outcomes showed that the suggested method is very effective at both encryption and decryption. The system is less complex, and the memory usage is very low. This system is optimal for medical IoT systems

ACKNOWLEDGMENT

I would like to express my sincere gratitude to all those who contributed to the completion of this research paper. I extend my heartfelt thanks to my supervisor, my family, my colleagues and fellow researchers for their encouragement and understanding during the demanding phases of this work.

REFERENCES

[1] I. Markit, “The internet of things: a movement, not a market,” tech. rep., London, 2018. [Online]. Available: https://cdn.ihs.com/www/pdf/ IoT ebook.pdf. [Accessed on: 02-01-2020].

[2] Abbas, Z., & Yoon, W. (2015). A survey on energy conserving mechanisms for the internet of things: Wireless networking aspects. Sensors, 15(10), 24818-24847.

[3] N. M. McKay KA, Larry Bassham, and Meltem Sönmez Turan, ―NISTIR 8114 Report on Lightweight Cryptography, ‖2017.

[4] P. Nandhini, V.Vanitha, and P. Scholar, ―A Study of Lightweight Cryptographic Algorithms for IoT, ‖ Int.J. Innov.Adv.Comput.Sci. IJIACS ISSN, vol.6, no.1, pp. 2347–8616, 2017.

[5] Nižetić, S., Šolić, P., Gonzalez-De, D. L. D. I., & Patrono, L. (2020). Internet of Things (IoT): Opportunities, issues and challenges towards a smart and sustainable future. Journal of cleaner production, 274, 122877.

[6] “CASAGRAS an EU Framework 7 Project (Coordination and Support Action for Global RFID-related Activities and Standardisation),” [Online]. Available: http://grifsproject.uniweb.be/data/File/CASAGRAS%20FinalReport%20(2).pdf. [Accessed 15 April 2018].

[7] Posts capes, "Internet of Things Examples-Posts capes," [Online]. Available: http://postscapes.com/internet-of-things-examples/. [Accessed 17 April 2017].

[8] Bigbelly, “Big belly,” 2015. [Online]. Available: http://bigbelly.com/. [Accessed 4 May 2017].

[9] K. McKay, L. Bassham, M. S. Turan, and N. Mouha, ―Report on lightweight cryptography(nistir8114), ‖National Institute of Standards and Technology (NIST), 2017.

[10] B. J. Mohd and T. Hayajneh, ―Lightweight Block Ciphers for IoT: Energy Optimization and Survivability Techniques, ‖ IEEE Access, vol. 6, pp. 35966– 35978, 2018, doi: 10.1109/ACCESS.2018.2848586.

[11] S. Singh, P. K. Sharma, S. Y. Moon, and J. H. Park, ―Advanced lightweight encryption algorithms for IoT devices: survey, challenges and solutions, ‖ J. Ambient Intell. Humaniz. Comput., vol. 0, no. 0, pp. 1–18, 2017, doi: 10.1007/s12652-017-0494-4.

[12] W. Feng, Y. Qin, S. Zhao, and D. Feng, ―A AoT: Lightweight attestation and authentication of low-resource things in IoT and CPS, ‖ Comput. Networks, vol. 134, pp. 167–182, 2018, doi: 10.1016/j.comnet.2018.01.039.

[13] A. Banafa, ―Three major challenges facing IoT, ‖ IEEEIoTNewsletter,2017.

[14] Thabit, F., Alhomdy, S., Al-Ahdal, A. H., & Jagtap, S. (2021). A new lightweight cryptographic algorithm for enhancing data security in cloud computing. Global Transitions Proceedings, 2(1), 91-99.

[15] Hasan, M. K., Shafiq, M., Islam, S., Pandey, B., Baker El-Ebiary, Y. A., Nafi, N. S., ... & Vargas, D. E. (2021). Lightweight cryptographic algorithms for guessing attack protection in complex internet of things applications. Complexity, 2021, 1-13.

[16] Fotovvat, A., Rahman, G. M., Vedaei, S. S., & Wahid, K. A. (2020). Comparative performance analysis of lightweight cryptography algorithms for IoT sensor nodes. IEEE Internet of Things Journal, 8(10), 8279-8290.

[17] Panahi, P., Bayılmış, C., Çavuşoğlu, U., & Kaçar, S. (2021). Performance evaluation of lightweight encryption algorithms for IoT-based applications. Arabian Journal for Science and Engineering, 46, 4015-4037.

[18] Jadaun, A., Alaria, S. K., & Saini, Y. (2021). Comparative study and design light weight data security system for secure data transmission in internet of things. International Journal on Recent and Innovation Trends in Computing and Communication, 9(3), 28-32.

[19] Toprak, S., Akbulut, A., Aydın, M. A., & Zaim, A. H. (2020). LWE: An energy-efficient lightweight encryption algorithm for medical sensors and IoT devices.

[20] Aboushosha, B., Ramadan, R. A., Dwivedi, A. D., El-Sayed, A., & Dessouky, M. M. (2020). SLIM: A lightweight block cipher for internet of health things. IEEE Access, 8, 203747-203757.

[21] Chaudhary, R. R. K., & Chatterjee, K. (2022). A lightweight security framework for electronic healthcare system. International Journal of Information Technology, 14(6), 3109-3121.

[22] Al-Husainy, M. A. F., Al-Shargabi, B., & Aljawarneh, S. (2021). Lightweight cryptography system for IoT devices using DNA. Computers and Electrical Engineering, 95, 107418.

[23] Jabeen, T., Ashraf, H., Khatoon, A., Band, S. S., & Mosavi, A. (2020). A lightweight genetic based algorithm for data security in wireless body area networks. IEEE Access, 8, 183460-183469.

[24] Atiewi, S., Al-Rahayfeh, A., Almiani, M., Yussof, S., Alfandi, O., Abugabah, A., & Jararweh, Y. (2020). Scalable and secure big data IoT system based on multifactor authentication and lightweight cryptography. IEEE Access, 8, 113498-113511.

[25] Hasan, M. K., Islam, S., Sulaiman, R., Khan, S., Hashim, A. H. A., Habib, S., ... & Hassan, M. A. (2021). Lightweight encryption technique to enhance medical image security on internet of medical things applications. IEEE Access, 9, 47731-47742.

[26] Naresh, V. S., Reddi, S., & Murthy, N. V. (2020). Secure lightweight IoT integrated RFID mobile healthcare system. Wireless Communications and Mobile Computing, 2020, 1-13.

[27] Jebri, S., Ben Amor, A., Abid, M., & Bouallegue, A. (2021). Enhanced lightweight algorithm to secure data transmission in IOT systems. Wireless Personal Communications, 116, 2321-2344.

[28] Chatterjee, K., Chaudhary, R. R. K., & Singh, A. (2022). A lightweight block cipher technique for IoT based E-healthcare system security. Multimedia Tools and Applications, 81(30), 43551-43580.