

ORIGINAL RESEARCH ARTICLE

A lightweight logisticsed chaotic S-box encryption for IoT enabled smart health care applications

Malathi Chakravarthula*, Venkata Krishna. P, Sandhya Rani. K

Department of Computer Science, Sri Padmavati Mahila Visvavidyalayam, Tirupati 517501, India

* Corresponding author: Malathi Chakravarthula, malathichakravarthula@gmail.com

ABSTRACT

The Internet of Things (IoT) acts as the major enabler for realizing more intelligent devices and establishes a new dimension of communication between humans and machines using the Internet. These intelligent devices find their role in numerous domains namely health care, automation, smart homes & other people-assisted applications. Although sensor-driven gadgets have significantly improved people's daily lives, the majority of IoT systems have been plagued by security backlogs, which results in privacy issues. Recently, Advanced Encryption Standard (AES) provides immense light of research in maintaining security and privacy among IoT health care devices. But encrypted data generated still needs to be improvised to defend against the various IoT attacks. The proposed scheme is implemented in the IoT infrastructure that consists of real-time health care sensors interfaced with the ESP8266. Extensive experimentation has been carried out to evaluate the proposed schemes and S-box tests are conducted and analyzed. Additionally, the efficacy of the suggested methods is evaluated with regard to of time and memory usage in comparison to the other encryption schemes already in use. Experimental findings demonstrate that the suggested L-DAL-SBoX has outperformed the other existing algorithms and finds its strong place in IoT security.

Keywords: IoT; AES; Fractional Multi-logistics; 3D-dimensional substitution box; NIST

ARTICLE INFO

Received: 17 October 2023
Accepted: 4 December 2023
Available online: 21 March 2024

COPYRIGHT

Copyright © 2024 by author(s).
Journal of Autonomous Intelligence is published by Frontier Scientific Publishing. This work is licensed under the Creative Commons Attribution-NonCommercial 4.0 International License (CC BY-NC 4.0).
<https://creativecommons.org/licenses/by-nc/4.0/>

1. Introduction

The IoT has been employed globally for numerous applications, including health care^[1], smart homes^[2], and automations^[3]. The objectives of IoT include comfort computations, effective communication and faster decision-making. Among the other domains, the role of IoT in health care applications is exponentially increasing day by day. The sensor-driven IoT technology is key in enabling the intelligent patient monitoring system that can sense, communicate and take appropriate

response actions by solving urgent medical issues^[4]. However, growing security issues include software bugs and hacking, may threat in utilizing IoT devices for health care applications. Attackers who get access to linked IoT devices, such as unauthorized users, may do so to misuse the network or the devices. The micro-shaped sensors and transceivers in IoT devices are used for collecting or sending medical data over a public network IP (Internet Protocol) channel that may expose hackers if data is not protected properly. Many lightweight encryption algorithms such as PRESENT^[5], CLEFIA^[6], KATAN^[7], SIMON/SPECK^[8], TSFS^[9], seeks to offer adequate security levels while making the best use of resources^[10-12] whereas standard encryption algorithms namely AES, RCA^[13],

elliptical curve cryptography, DES provides the strong defending characteristics to the data. Above mentioned algorithms encrypt the collected medical data and transmit it to the particular destination^[14].

Although the security of the current algorithms has been demonstrated, their key generation procedure can be compromised with the right key-breaking methods. Moreover, embedding the high security algorithms in IoT devices is complex and fails to consume less resources. Hence many researchers replaced the security operations of the encryption algorithms to ensure privacy with optimal consumption of resources^[15-17]. However, achieving the resource constraints data integrity remains to be a complex challenge for the researchers.

Motivated by the above drawback, this paper proposes the novel dynamic and lightweight S-Box L-DAL (Lightweight Dual Adaptive Logistics Maps) which incorporates the dual-level 3D logistics chaotic attractors with AES system to increase the defense effectiveness of the keys. In the approach, DNA operations have been adopted to ensure the data privacy and lightweight. According to the evaluation that was done, the suggested plan appears to have a positive conclusion to improve IoT healthcare security. The main contributions of the work are listed below:

- 1) The paper proposes the dynamic and lightweight 3D chaotic key generation process rather than conventional 2D S-Box. It is supported by 3D dual level Logistics Chaotic Maps to make it secure and lightweight.
- 2) The proposed system replaces the DNA computations in the place of conventional permutation and diffusion process. As a result, it becomes possible to preserve the integrity of IoT data for healthcare.
- 3) The proposed system is deployed on the Embedded Microcontrollers interfaced with medical sensors and ESP8266. To best of our knowledge, the hardware test bench created for experimentation is first of its kind and used to assess and contrast the effectiveness of the suggested plan with other similar methods.

The paper is mostly organized as follows:

The remainder of the essay is structured as follows: The background analysis of the AES & Multi-logistics Chaotic Attractor maps is illustrated in Section-II. The associated research on IoT security issues along with additional existing encryption techniques are presented in Section-III. The proposed IoT security scheme is provided in Section-IV. Section-V presents the experimental testbed, assessment criteria, and outcome analysis. In Section V, the paper is finished along with suggestions for improvement in the future.

2. Background

This section discusses about the IoT security challenges in health care environments and usage of AES for securing an IoT environment.

2.1. IoT security challenges in health care environment

Due to the development of medical technology, ensuring security in an IoT setting is a tough task. A device that offers more services is more likely to come under attack. Without an encryption mechanism in place, interactions between medical equipment in IoT contexts are vulnerable to numerous threats. In that situation, a hacker might access shared data and potentially alter it. In that situation, the intrusive party has access to shared data. Intruders can also study network traffic while collecting sensitive information (like login passwords) by having access to a communications channel. Without the target party's knowledge, the attacker has the ability to read, transmit, and alter data. Even if the information is encrypted, inadequate or poorly constructed encryption could still pose a major hazard. Additionally, important information stored on the machine needs to be protected by encryption. Lack of encryption while keeping API tokens or passwords in plain text on a device is a common issue. Other challenges include using subpar encryption technologies or accidentally using cryptographic methods. Sensitive data is frequently found on medical electronics.

Devices that can connect to a wireless network can save the password for it. In the space where they are installed, cameras have the ability to record both audio and video. If attackers are able to acquire this data, it would constitute a serious privacy violation. Sensitive data must be processed by IoT systems and related services precisely, securely, and only with the end-user's consent. This holds true for both the preparation and creation of sensitive data. There is no doubting the importance of security for IoT medical equipment. However, there is ongoing debate over the best way to include security into IoT-based medical devices. Among these countermeasures, cryptographic methods of encryption are particularly common. The cryptographic algorithms give IoT-based medical systems high-level robustness while being generic and device independent.

2.2. AES for medical data integrity

The commonly used cryptographic system AES uses a symmetric cipher to achieve the highest level of security. AES offers robust safety mechanisms and is easy to deploy (both in terms of software and hardware). AES^[18] has been a strong competitor for tackling the security issues with IoT-based medical equipment as a result of its effective implementations. The AES is one of the most widely used and consistently dependable encryption algorithms, despite being broken multiple times. As smart technology has developed, new and innovative modification strategies have been developed and are being employed to protect AES and enhance correctness. Intruders and their unauthorized access to information are increasingly a widespread occurrence. Chaos driven privacy has become a big issue in security research due to its unpredictable nature. Finding the right key may be challenging if the user is unfamiliar with the initial circumstance. The entire outcome can be altered by a small modification in text itself or a key. For instance, a change of one bit in text alone or a key alters the outcome by about 50%. Chaos driven cryptosystems are more flexible for massive amounts of data, including audio and video, than the previously mentioned cryptosystems. The current cryptosystems have been subject to several attempts to introduce chaos^[19,20]. While chaos deals with actual numbers^[21-24], other cryptographic techniques deal with the quantity of integers. Therefore, employing a chaos-based approach to key generation might make the design more secure.

2.3. Chaos based encryption schemes

The behavior of dynamic nonlinear systems that are very sensitive to the initial conditions is the main emphasis of chaos theory. As a result, a delta change in the beginning circumstances causes a substantial shift in the outputs^[25]. Lyapunov exponents are employed to evaluate the initial condition's sensitivity. This vital property adds more fuel of randomness in the outputs, that motivates many researchers to use the chaotic system in cryptographic encryptions^[26]. **Table 1** presents the list of chaotic maps used frequently for encryption.

Table 1. List of chaotic maps used for data encryption.

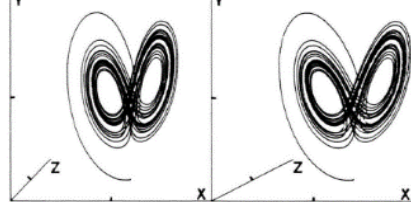
| | |
|---|--|
| Lorentz equation | $\dot{x} = x - xy - z$ $\dot{y} = x^2 - ay$ $z = bx - cz + d$ <p>where x, y is the double focus system. Z is the constant a and b is the bifurcation parameter</p> |
| <p>Lorentz-type chaos Parameter values assumed: $a = 0.1, b = 0.08, c = 0.38, d=0,$ Initial values: $x(0) = 10^{-6}, y(0) = 10^{-2}, z(0) = 10^{-6}, t = 0, \dots, 517,$ Axes: $-1.8, \dots, +1.8$ for x $0, \dots, 1.8$ for y $-0.18, \dots, +0.18$ for z</p> |  |

Table 1. (Continued).

Sandwich chaos

$a = 0.1, b = 0.07, c = 0.38, d = 0.0015$

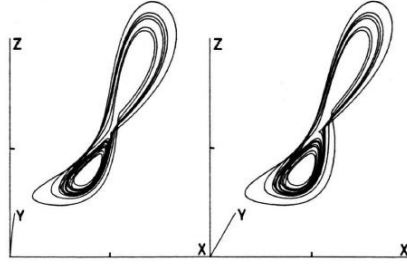
Initial values: $x(0) = 10^{-6}, y(0) = 10^{-2}, z(0) = 10^{-6}, t = 0, \dots, 517,$

Axes: $-1.2, \dots, +1.2$ for $x;$

$0, \dots, 1.4$ for $y;$

$-0.1, \dots, 0.1$ for z

$t = 0, \dots, 336.$

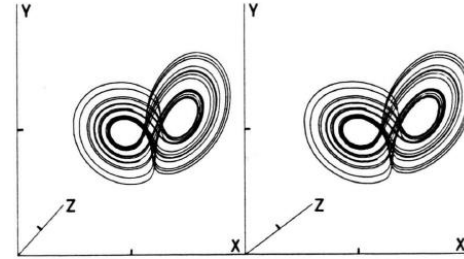


Double-horseshoe chaos

$a = 0.04, b = 0.06, c = 0.326, d = 0,$ initial values $x(0) = -0.066, y(0) = 0.8, z(0) = -0.066, t = 0, \dots, 451,$

Axes

$-1, \dots, +1$ for $x, 0, \dots, 2$ for $y, -0.1, \dots, 0.1$ for z

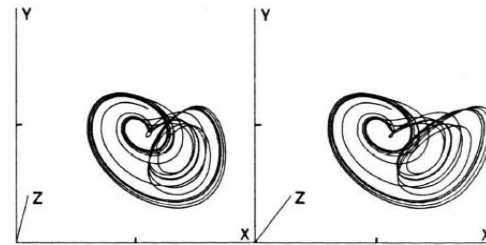


Screw type of chaos

$a = 0.55, b = 2, c = 4,$

initial values $x(0) = y(0) = z(0) = 1, t = 0, \dots, 94$

Axes: $-10, \dots, +10$ for x and $y, 0, \dots, 10$ for z



Besides the Lorenz maps, Logistic maps are predominantly used for the encryption to achieve the light weight and high secured data transmission.

3. Related works

A simple hierarchical attribute-based encryption system was presented by Ali et al.^[26] In this approach, user computing overhead is very little and the majority of user computation is handled by the cloud server. In order to enable scalable and adaptable key delegation as well as user revocation procedures, this architecture also employs a hierarchical paradigm. However, the secret keys of users are issued and revoked by a single authority. This architecture is not suitable for massive networks as a result^[26].

A lightweight Signcryption Protocol was proposed by Kim et al.^[27] to overcome authentication issues in contexts with limited resources. This framework used Elli for quick public-key cryptography and Keccak as the process hash function. Because of its reduced complexity, reduced energy use, and improved security, this framework is appropriate for IoT contexts. However, the time complexity for key encryption has been noted as the primary weakness in this approach^[27].

In order to create a high-performance key matrix for encryption, Gu et al.^[28] introduced a parallel chaotic system by integrating the piecewise linear chaotic map (PWLCM), skew tent map (STM), & bernoulli map. The cost-effectiveness and high level of security of this framework are its key benefits. However, the main limitation of this approach is that it becomes more computationally complex and its security performance degrades when dealing with massive datasets^[28].

In order to maintain data privacy in IoT applications, an efficient and practical identity-based public-key encryption method with revocation capabilities was presented by Sun et al.^[29] The ability for components like actuators and sensors to directly or indirectly communicate encrypted data over a cloud server is the fundamental benefit of this technology. The private key generator can alert the user if a private key is

compromised. However, this paradigm has a flaw in that it causes transmission delays as a result of few resources^[29].

Analyses for encrypted data from IoT devices that are secure even after a device’s key breach are required. Ramesh et al.^[30] presents an architecture termed proxy reciphering as a service. This structure’s key benefits include being safe, scalable, and simple to use for long-term calculations in the cloud that protect privacy for cloud-IoT applications. However, this framework’s noted disadvantage is that it is more costly and energy-intensive. In a real-time context, connection errors also happen more often^[30].

To improve the privacy of IoT networks, a powerful lightweight channel independent (LCI) physical layer encryption method based on optical OFDM was introduced by Al-Moliki et al.^[31] The findings show that the suggested strategy strengthens the VLC’s confidentiality defences against many types of attacks, including statistical assaults, known/selected plaintexts, and brute-force attacks. This framework’s key benefits include lowering the signal’s “peak to average power ratio”, improving “bit error rate efficiency”, and shortening communication latency. However, given huge datasets, this framework’s throughput starts to decline^[31].

A realistic implementation of the absolutely secure technique, the energy concealment (EC) encryption scheme developed by Kuldeep et al.^[32] does away with the need for a second safe channel. This system is resistant to a variety of cryptographic assaults. This framework’s key benefit is that it performs better with regards to code memory footprint & overall energy usage. However, when resisting additional cypher threats, this framework’s primary flaw is that it causes communication latency^[32].

MemEnc, a wholly hardware-based solution created by Gupta et al.^[33], processes memory requests transparently and conducts on-the-fly encryption without the need for OS intervention. A memory encryption engine and ARM TrustZone are integrated by this framework. This approach demonstrated that efficiency-security tradeoffs, both static and dynamic, are required in every situation. Less latency and low battery use make this framework ideal for IoT with limited resources. Less throughput and computational complexity are this framework’s biggest drawbacks, albeit^[33].

Durga et al.^[34] developed a chaotic encryption driven blockchain IoT design to protect the safety and confidentiality of data. IoT chaotic encrypted block chain architecture integration may improve defense against assaults. This framework’s key benefits are its high throughput and low energy usage. Large data sizes, however, cause performance issues and make it unsuitable for real-time settings^[34].

Marry et al.^[35] discussed how blockchain technology may be used in the healthcare business, such as allowing safe and anonymous exchange of health data for research reasons. The authors propose leveraging smart contracts to keep medical records in a unique, accessible, interoperable, and audible manner. This framework requires little time to encrypt but consumes a lot of energy^[35]. **Table 2** illustrates the review of related work for the proposed model.

Table 2. Side by Side review of above discussed related works.

| Author | Methodology proposed | Merits | Demerits |
|----------------------------|--|--|--|
| Ali et al. ^[26] | Lightweight revocable hierarchical attribute driven encryption | Flexible and scalable encryption key delegation | Users’ secret keys are issued and revoked by a single key authority. |
| Kim et al. ^[27] | Lightweight signcryption protocol | Less complexity, less energy consumption and enhanced security | Time complexity |
| Gu et al. ^[28] | Parallel chaotic system [“Piecewise Linear Chaotic Map+ Skew Tent Map+ Bernoulli map”] | Highly secured and cost efficient framework | Computational complexity |

Table 2. (Continued).

| Author | Methodology proposed | Merits | Demerits |
|----------------------------------|--|--|--|
| Sun et al. ^[29] | Identity based public key encryption scheme | Device components can communicate securely either directly or through a cloud server. | Transmission delay |
| Ramesh et al. ^[30] | Proxy reciphering scheme | long term foundation privacy preserving cloud computations are simple to implement, scalable, as well as safe. | Expensive, require more energy and connectivity failures |
| Al-Moliki et al. ^[31] | Lightweight channel, not dependent physical layer encryption | increases bit error rate efficiency & decreases communication latency | Low throughput |
| Kuldeep et al. ^[32] | Energy concealment encryption scheme | Less energy consumption | Communication overhead |
| Gupta et al. ^[33] | MemEnc | Less latency and low power consumption | Computational complexity |
| Durga et al. ^[34] | Chaotic encryption scheme | High throughput and less energy consumption | Not suitable for real time scenarios |
| Marry et al. ^[35] | Accessible, interoperable, and audible approach | Encryption time | High energy consumption |

4. Proposed framework

In traditional Advanced Encryption Standard (AES) systems, the Substitution-box (S-BOX) is employed to ensure effective data communication from sender to receiver. This is a critical component in maintaining data security and privacy, a requirement that is equally essential in the context of Internet of Things (IoT) security. However, several challenges persist in the IoT landscape. These include issues with power distribution uniformity, non-standardized user distribution, and the complexity of integrating sophisticated safety features within the IoT framework. When building the IoT security system, it is risky to assume all conventional cryptographic methods. As a result, algorithm is needed to disrupt the attacks and to withstand against the different category of the attacks.

To overcome this above drawback, novel lightweight and hybrid algorithm L-DAL has been proposed. The complete working architecture for the proposed L-DAL is presented in **Figure 1**. The proposed algorithm works on principle of hybrid chaotic maps which works on the principle of integration of different 3d logistics and DNA encoding technique. From the **Figure 1**, working mechanism of the proposed algorithm is of three different phases:

- 1) **IoT Data Collection:** This phase collects the information from the IoT devices using analog channels of the embedded CPU. The collected information is stored in the CPU's memory.
- 2) **Hybrid S-BOX:** The novel S-BOX is created using combination of the logistics and logistics maps in which the diffusion and permutation process has been replaced with the DNA coding to achieve the light weight, strong and deployable S-Box.
- 3) **Encryption Process:** Finally, the stored data are encrypted with the newly formed AES-S-box and transmitted to the cloud.

The working mechanism of the hybrid S-Box and its key generation has been explained in the subsequent sub sections.

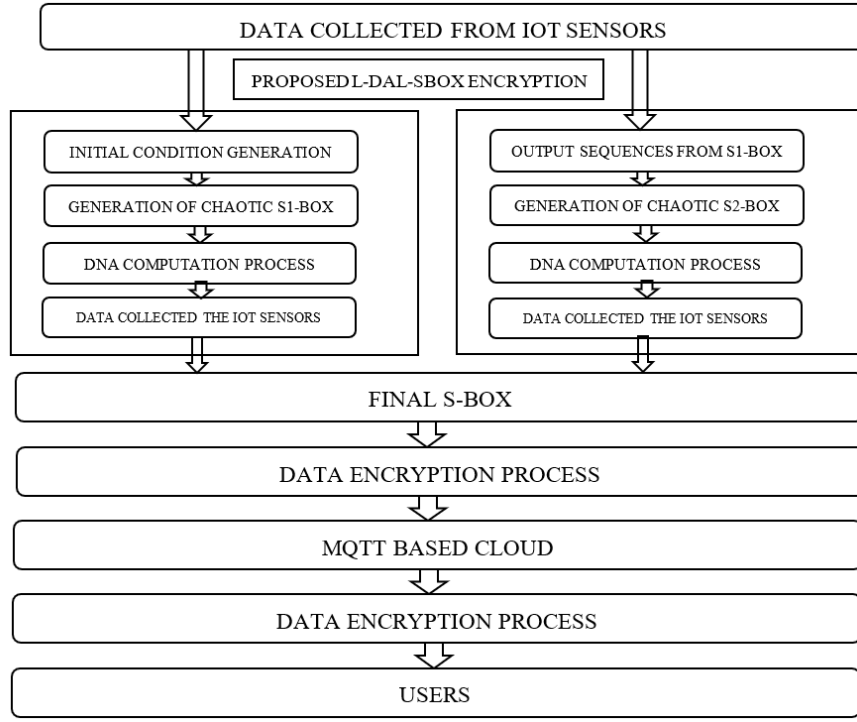


Figure 1. Proposed framework of the L-DAL S-box based Encryption.

4.1. 3D logistic chaotic maps

3D logistic chaotic maps exhibit greater chaotic properties than 1D chaotic maps, as discussed in the study of Beaulieu et al.^[36]. Given by are the mathematical formulae for 3D logistic maps.

$$P = \mu x(1 - x(j)) + \beta y'P + \alpha R \quad (1)$$

$$Q = \mu y(1 - y(j)) + \beta x'R + \alpha Q \quad (2)$$

$$R = \mu z(1 - z(j)) + \beta z'y + \alpha P \quad (3)$$

When the aforementioned equations $0.35 < \mu < 0.381$, $\beta < 0.0022$ & $\alpha = 0.0015$, the 3D logistic maps are displayed. **Figure 2** depicts the 3D chaotic systems' suggested Chaos phenomenon for the aforementioned values.

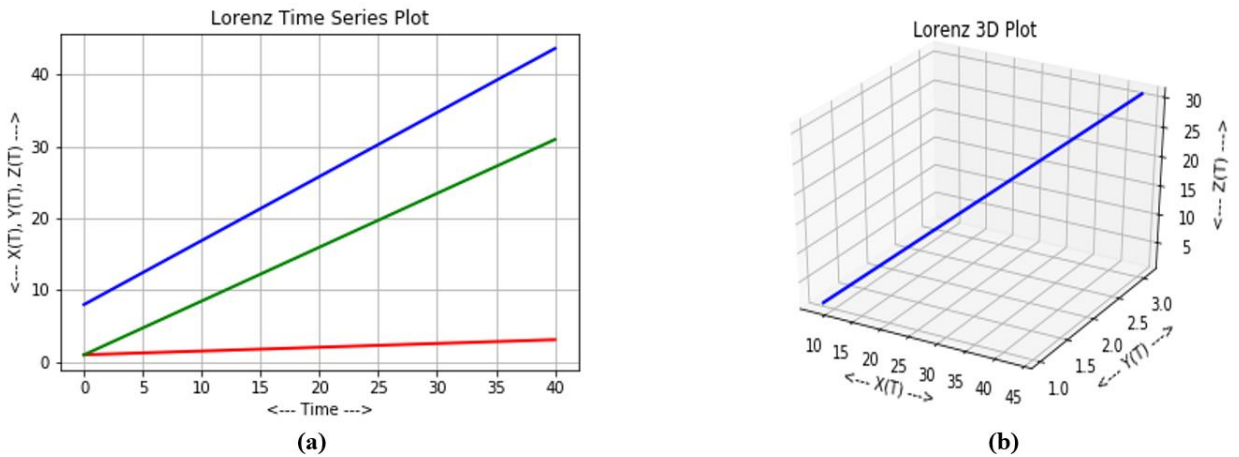


Figure 2. Chaos phenomenon (a) Lorenz time series plot; (b) Lorenz 3D Plot.

4.2. DNA computing process

DNA encoding has four “nucleotides” that are taken as “Adenine” (“A”), “Guanine” (“G”), “cytosine” (“C”), and “thymine” (“T”). Generally, the nucleotides ‘A’ sets with ‘T’ & nucleotides ‘G’ sets with ‘C’. The

intermediate results of S-box such as SDAC_I1, SDAC_I2 are encoded by applying the DNA pairing rule to generate DNA Sequence. The DNA sequence that performs algebraic measurements such as “DNA addition”, “DNA subtraction” & “DNA exclusive” [XOR] are employed from **Tables 3–5**.

The DNA pairing rule is applied as shown in **Table 3** to produce DNA Sequence. Then the DNA addition rule is applied to the DNA Sequence produced by the DNA pairing rule in **Table 4**. In this research, the intermediate S1-box and S2-box are formed using DNA addition process. Finally, the S-Box is formulated by encoding with DNA XOR rule shown in **Table 5**.

Table 3. DNA pairing rules^[37].

| | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
|---|----------|----------|----------|----------|----------|----------|----------|----------|
| A | 00 | 00 | 11 | 11 | 01 | 10 | 01 | 10 |
| T | 11 | 11 | 00 | 00 | 10 | 01 | 10 | 01 |
| C | 10 | 01 | 10 | 01 | 00 | 00 | 11 | 11 |
| G | 01 | 10 | 01 | 10 | 11 | 11 | 00 | 00 |

Table 4. Rules of DNA addition^[37].

| + | 1 | 2 | 3 | 4 |
|----------|----------|----------|----------|----------|
| A | A | T | G | C |
| T | T | C | G | A |
| C | G | A | C | T |
| G | C | G | T | A |

Table 5. Rules of DNA XOR^[37].

| | 1 | 2 | 3 | 4 |
|---|----------|----------|----------|----------|
| A | A | T | G | C |
| T | T | A | C | G |
| C | G | A | C | T |
| G | C | T | G | A |

4.3. Key generation process using proposed S-box

The proposal makes some adjustments to the original AES’s processes. DNA coding is introduced instead of tradition permutation and shifting process. This change aids in lowering the encryption/decryption time, still commands with the good defense characteristics. Fractional Dual level Logistic maps are used in construction of strong encryption. Initially, sensor data bytes are splitted into two different parts based on byte location. In the first level, 3d logistic maps are used to construct the S-box S1. Based on the first level outputs, initial conditions of second level 3d-Logistic maps are designed and used to generate the hybrid S-box (S2). The two S-boxes are encoded using DNA computation to form ensembled S-box (S3). Finally, the data is encrypted using the newly formed S-box (S3). All of these techniques strive for rendering AES lightweight by simultaneously cutting down on its encryption and decryption times while maintaining its resistance to IoT attacks.

To eradicate the complexity in employing the matrix in encryption technique, first bytes’ location of sensor inputs are taken into the consideration. Initially, logistic maps are generated randomly as mentioned in the study of Habeeb and Hassan^[38]. The generated logistic maps are used to form the intermediate S1 box. The intermediate S-box is formulated using the 3d logistic maps (I) and input data bytes (K). The DNA addition encoding is adopted in place of permutations and diffusions to yield high secured intermediate. S1-Box sequences. The formulation of S1 is depicted in Algorithm 1.

$$I = 3d \text{ logistic maps}(X, Y, Z) \text{ For } J = 1, 2, \dots, L \quad (4)$$

$$S1 = \text{mod}(\text{byte}\{ (I)DNA K(\text{input}), 16\}) \text{ For } i = 0, 1, 2, \dots, L \quad (5)$$

Algorithm 1 Formulation of Intermediate S1-Box

- 1: Input: Input Sequences of the 3D logistic Maps/Input sensor bytes K
 - 2: Output: S1-box with size (16×16)
 - 3: Start
 - 4: Generate the Random Sequences as initial conditions for 3d Logistic maps
 - 5: Generate the 3d Logistic maps using Equations 1–3
 - 6: Identify the missing values in K sensor bytes and replace it with zeros
 - 7: Rescale the maps and k-bytes to 16
 - 8: Formulate the intermediate S1-box using the equation
 - 9: End
-

In the next step, again 3d logistic maps are formulated, this time using the output sequences from the S1-box. The intermediate S2-box is generated using the last bytes of sensor inputs (O) and 3d logistic maps (M). In this formulation, all permutations are replaced with the DNA addition encoding to formulate the light weight and deployable, which gives better defensive characteristics. The formulation of S2 is depicted in Algorithm 2.

$$M = 3d \text{ logistic maps}(X, Y, Z) \text{ For } J = 1, 2, \dots, L \quad (6)$$

$$S1 = \text{mod}(\text{byte}\{ (M)DNA(O)(\text{input}), 16\}) \text{ For } i = 0, 1, 2, \dots, L \quad (7)$$

Algorithm 2 Formulation of S2 Intermediate Box

- 1: Input: Output Sequences from S1-box/Input Sensors bytes
 - 2: Output: Intermediate S2-box (16×16)
 - 3: Start
 - 4: Generate the Initial Conditions from the Output sequences of S1-box
 - 5: Generate the 3D logistic maps using the Equation 6
 - 6: Identify the missing values in O sensor bytes and replace it with zeros
 - 7: Rescale the maps and O-bytes to 16
 - 8: Formulate the intermediate S2-box using the Equation 7
 - 9: End
-

Finally, the intermediates are concatenated to formulate the new hybrid s-boxes. After continuing the several times, input data as well as the hybrid S-box keys are then put through with DNA XoR operation as mentioned in **Table 5**. As a result, it creates strong encrypted bytes that individually changes at each time. The complete encryption scheme using S-box is illustrated in Algorithm 3.

$$S = S1 \text{ DNA} - \text{XoR} - S2 \quad (8)$$

Algorithm 3 Complete Encryption Process

- 1: Input: Input Sensor Sequences stored in CPU
 - 2: Output: Encrypted data
 - 3: Start:
 - 4: Split the Data as K and O based on the byte locations.
 - 5: Generate the Random sequences for 3D logistic maps
-

Algorithm 3 (Continued)

- 6: Generate the 3D logistic maps using Equation
 - 7: Formulate the Intermediate S1-box -S1 -box
 - 8: Generate the 3D logistic maps using initial conditions from output sequences of S1-box
 - 9: Formulate the Intermediate S2-box
 - 10: S-box (keys) = S1 concatenates S2
 - 11: Encrypted Data = S-box (DNA) Input Sensor Sequences
 - 12: End
-

5. Experimental results

Figure 3 depicts the layout of a Smart Health care systems based on IoT. The suggested health care architecture includes five categories of entities, which are 1) Sensors; 2) Microcontrollers; 3) Gateways; 4) Cloud; 5) IoT transceivers. Ten medical sensors are interfaced with two Arduinos. The sensors used for interfacing with microcontroller are three lead ECG sensor, three axis accerolometer, pulse sensor, pulse oximeter, temperature sensor, BMI (Body Mass Index) Sensor and Blood Pressure Sensor (BP Sensor). ESP8266 is used to connect the board to cloud via WIFI gateways. Five analog sensors are interfaced in the Arduino -1 while five digital sensors are interfaced with Arduino-2. These boards are mounted on the human body and live sensor data are recorded in the cloud. The boards transmit the data over cloud using MQTT protocol. The complete experimental setup was allowed to run for a week and recorded data were taken as the inputs for the encryption. Using a PC workstations with the following characteristics, all results were obtained: Intel I7 CPU, 16GBRAM, Window11 Operating Systems with 3.2 GHZ. All the programming was implemented using Python 3.10 (S-box design) and Micro-python (Hardware deployment).

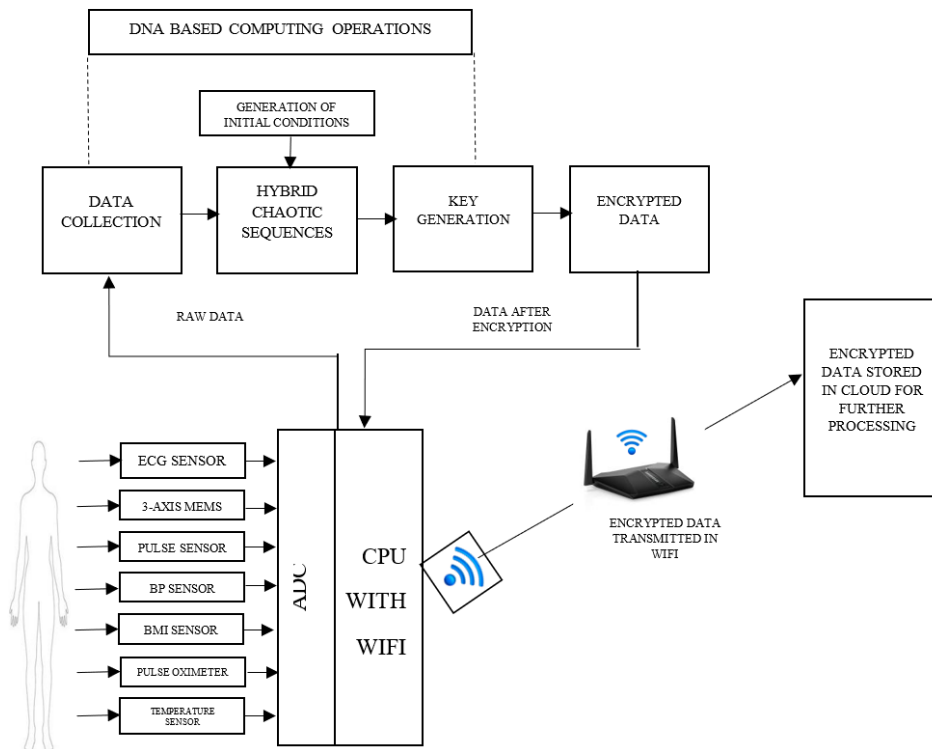


Figure 3. Experimental setup for the evaluating the proposed model in a smart IoT healthcare environment.

5.1. Evaluation metrics

In this study, a number of statistical tests and tests that are hardware-specific are run to evaluate the efficacy of the L-DAL algorithm's S-Box test criteria, such as balanced, completeness, avalanche, and strict avalanche, are used to evaluate the new S-Box. Moreover, encryption time and memory consumption of the proposed algorithm was also measured.

5.2. Analysis of results: Statistical analysis

5.2.1. Balanced Criteria (BC)

The distribution of the quantity of 0s and 1s that needs to be balanced in the output sequence is one of the fundamental requirements for S-Box tests^[39]. The suggested S-Box passes this test since it contains roughly equal quantities of 0s and 1s.

5.2.2. Completeness Criteria (CC)

Completeness Criteria is used to measure the dependency of output bits to the inputs. Since the designed S-box is based on the initial conditions of dual level chaotic maps, generated s-box will exhibit the high randomness bits as the initial conditions changes. It means the slight changes in the input results in significant modifications in the outcomes.

5.2.3. Avalanche Criteria (AC)

The avalanche effect, which describes the effects of minor changes in the bits that are inputted leading to huge changes in the outputs, is a crucial factor in block encryption. Strong cipher algorithms would benefit from having this condition. The avalanche value must fall between [0, 1]. In this research, optimal value is chosen as 0.5 which implies the S-box needs to satisfy the criteria for passing an avalanche test. The mathematical expression for calculating the avalanche test is given as

$$\text{Avalanche Criteria (AC)} = \frac{\text{No of Swap bits in Ciphers}}{\text{No of total bits in Ciphers}} \quad (9)$$

5.2.4. Complete Avalanche Criteria

If each bit in the S-Box's output is modified by a probability of a half when just a single bit of its generated outputs is complemented, the S-Box meets the rigorous avalanche condition. This criterion combines the avalanche and completion criteria. As a result, the SAC is met, and the suggested S-BOX meets this requirement. **Table 6** illustrates the complete avalanche test for the proposed model

Table 6. Avalanche criteria for the proposed model using the different sensor values (Modified by One Bit).

| Sensor type | Sensor data | ASCII value | Binary inputs | S-Box value | Binary value | CC value |
|----------------------------|-------------|-------------|---------------|-------------|--------------|-------------|
| ECG sensor | 45 | 45 | 01000101 | EA | 11101001 | 5/8 = 0.625 |
| | 67 | 67 | 01100111 | FE | 11111110 | 5/8 = 0.625 |
| | 12 | 12 | 00010010011 | A0 | 1001000 | 5/8 = 0.625 |
| 3-Axis MEMS Accerolometers | 78 | 78 | 01111000 | AF | 10011111 | 6/8 = 0.72 |
| | 89 | 8A | 10001001 | 34 | 00111000 | 6/8 = 0.72 |
| | 88 | 88 | 10001000 | 42 | 01000010 | 6/8 = 0.72 |
| Temperature Sensor | 40 | 40 | 0100000 | EF | 11101111 | 6/8 = 0.72 |
| BMI Sensor | 10 | 10 | 0001000 | EE | 11101110 | 6/8 = 0.72 |
| Pulse Oximeter | 95 | A5 | 10010101 | 4E | 01001110 | 5/8 = 0.625 |
| Pulse Sensor | 60 | 60 | 01100000 | EA | 11101001 | 5/8 = 0.625 |

5.3. Encryption time analysis

The amount of time needed to create the encrypted data for the suggested smart health care is analyzed and compared with the other existing algorithms. For a perfect evaluation of the proposed algorithm, different data sizes are employed for various sensors, and the time needed for the generation of encrypted data is calculated for the proposed algorithm along with the other existing. **Figures 4–7** presents the comparative analysis of generation time for the different algorithms with changes in the data sizes.

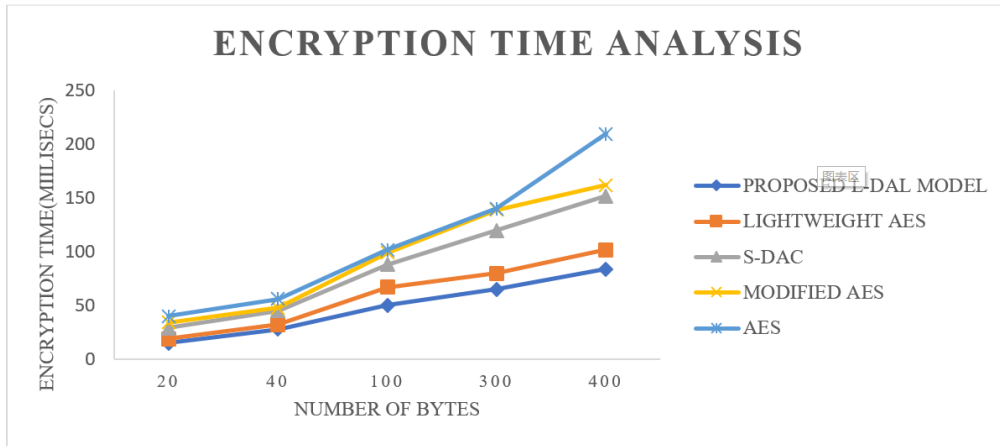


Figure 4. Encryption time analysis for encrypting ECG and Three Axis MEMS accelerometer data.

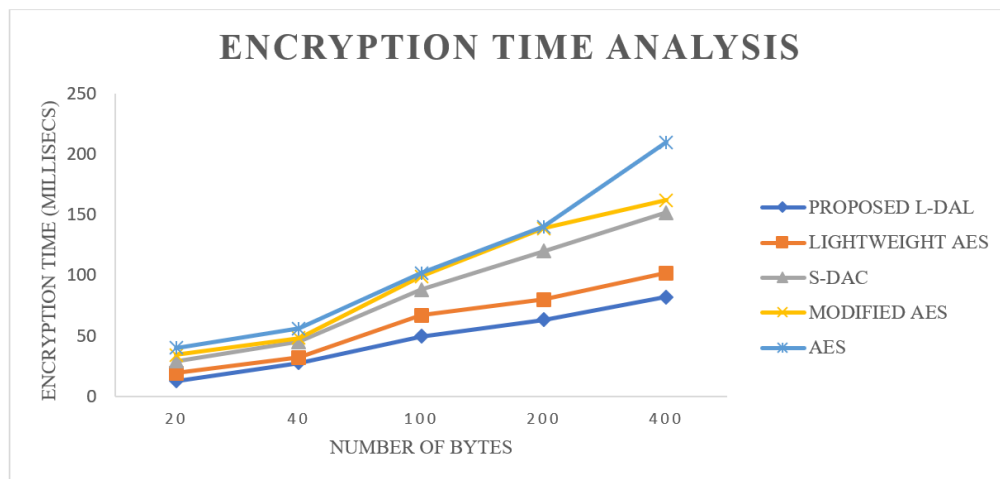


Figure 5. Encryption time analysis for encrypting BMI and blood pressure sensor data.

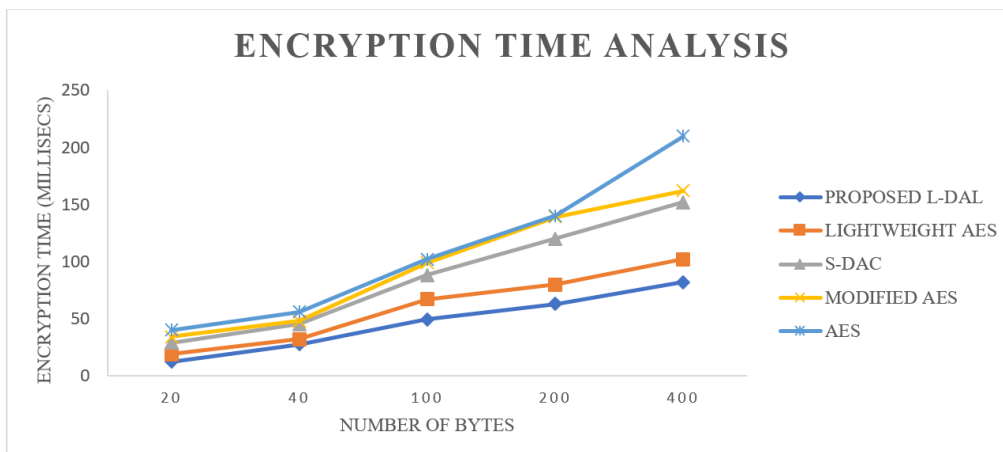


Figure 6. Encryption time analysis for encrypting pulse rate and temperature sensor.

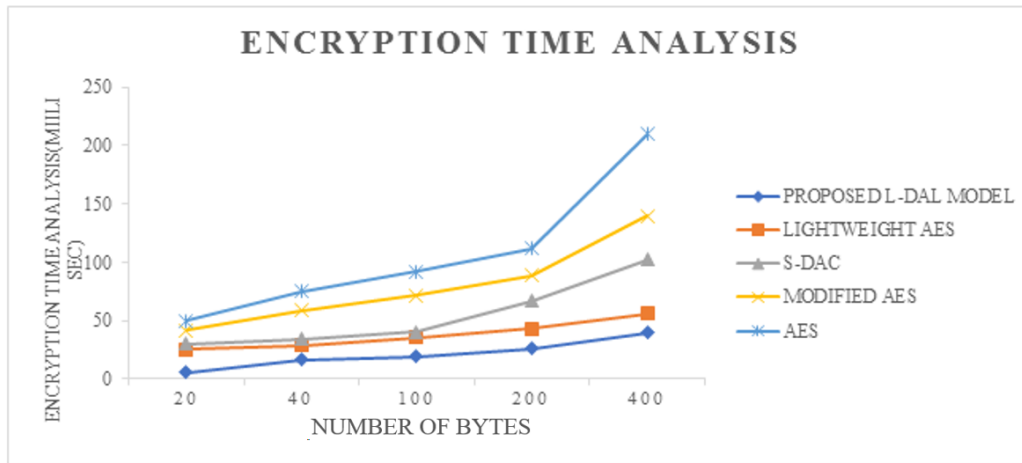


Figure 7. Encryption time Analysis for encrypting pulse oximeter data.

The suggested framework has been created and put into use for evaluating information security, credibility, non-tampering with confidentiality in IoT data communication. The proposed model which has been built on adaptive chaotic cryptographic technique has improved the internet security that has been illustrated in **Figures 4–7**. The keys generated using adaptive theory will be embedded as private key in each smart health care IoT devices. For the purpose of decoding medical information from the sender, hospitals and physicians employ the private key. However, if the encryption takes the lesser time, there is a chance of the intruder to hack the data. Hence the experimentation is carried out for measuring the encryption time of the suggested approach. To establish the supremacy of the suggested structure, existing algorithms such as lightweight AES^[40], S-DAC^[41], Modified AES^[42] and AES^[43] are considered. **Figures 4–7** show the comparative analysis of different algorithms in generating the encrypted data. **Figure 4** illustrates the encryption time comparison using MEMS accelerometer data. From **Figure 4** it is clear that when compared to other related works, the proposed framework shows extraordinary performance whereas other methods degrade in its performance when the number of bytes increased. It is clear that, AES has produced the longer time for the small size data which may increase the probability for intruder to tamper the medical data. Modified AES which works on the principle 3D dimensional logistic maps has shown considerable improvement over the traditional AES. Hence it is worthy to prove the integration of chaos has considerable effect on the performance of encryption time. But the keys generated are dependent on the inputs, hence the encryption time may little too long for the deploying in the embedded hardware. S-DAC and Light weight AES has produced considerable amount of time. In addition, they have increased the randomness and computational uncertainty in line with the suggested paradigm. But the S-DAC and Lightweight AES consumes more time, makes its unsuitable for deploying the Embedded CPU. In the same manner the **Figures 5–7** show the encryption time using pressure sensor data, pulse rate with temperature sensor data and pulse oximeter data respectively. For these sensors also the proposed methodology outperformed others in terms of encryption time. Hence, the results demonstrate the proposed model has provided more randomness and exhibits light weight behaviour (integration of dual adaptive chaos) that can be embedded in the CPU to ensure the high security and integrity in smart health care IoT systems.

6. Conclusion

In this research work, the lightweight, dynamic and high secured S-box AES has been proposed for IoT health care systems. The proposed work also introduces the DNA computation instead of traditional permutations and diffusion process which makes the data more random and security. The inclusion of DNA and adaptive logistic maps are shown the huge change in designing the S-Box. Furthermore, IoT based Smart Health care system has been designed to evaluate the proposed model whether it is secure from

vulnerabilities. The extensive experimentation has been carried out and S-box metrics are analysed and evaluated. The performance of designed S-Box has been compared with the other existing S-box deployed already for health care applications. The outcomes demonstrate that the suggested approach is quicker than the other current ones without pricing the data security and integrity. Besides, the proposed S-BoX passes the NIST statistical tests, that proves its high randomness behaviour which can defend against any attack. Hence the proposed L-DAL S-Box has a greater level of security and requires fewer calculations which makes its applicable to embed in IoT devices. As the future scope, the proposed S-BoX can further be enhanced by the reducing the computations so that it can be deployable in any IoT devices used for smart health care applications.

Author contributions

Conceptualization, CM and PVK; methodology, CM; software, CM; validation, CM, PVK and KSR; formal analysis, CM; writing—original draft preparation, CM; writing—review and editing, PVK and KSR; supervision, PVK and KSR. All authors have read and agreed to the published version of the manuscript.

Conflict of interest

The authors declare no conflict of interest.

References

1. Song T, Li R, Mei B, et al. A Privacy Preserving Communication Protocol for IoT Applications in Smart Homes. *IEEE Internet of Things Journal*. 2017, 4(6): 1844-1852. doi: 10.1109/jiot.2017.2707489
2. Moosavi SR, Gia TN, Nigussie E, et al. End-to-end security scheme for mobility enabled healthcare Internet of Things. *Future Generation Computer Systems*. 2016, 64: 108-124. doi: 10.1016/j.future.2016.02.020
3. Lee I, Lee K. The Internet of Things (IoT): Applications, investments, and challenges for enterprises. *Business Horizons*. 2015, 58(4): 431-440. doi: 10.1016/j.bushor.2015.03.008
4. Ion M, Zhang J, Schooler EM. Toward content-centric privacy in ICN. *Proceedings of the 3rd ACM SIGCOMM workshop on Information-centric networking*. Published online August 12, 2013. doi: 10.1145/2491224.2491237
5. Rahman Z, Yi X, Khalil I, et al. Chaos and Logistic Map Based Key Generation Technique for AES-Driven IoT Security. *Quality, Reliability, Security and Robustness in Heterogeneous Systems*. Published online 2021: 177-193. doi: 10.1007/978-3-030-91424-0_11
6. Rahaman Z, Corraya AD, Sumi MA, Bahar AN. A novel structure of advance encryption standard with 3-dimensional dynamic S-Box and key generation matrix. *arXiv 2020*, arXiv:2005.00157.
7. Ziv J, Lempel A. A universal algorithm for sequential data compression. *IEEE Transactions on Information Theory*. 1977, 23(3): 337-343. doi: 10.1109/tit.1977.1055714
8. Vashi S, Ram J, Modi J, et al. Internet of Things (IoT): A vision, architectural elements, and security issues. 2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC). Published online February 2017. doi: 10.1109/i-smac.2017.8058399
9. Farooq U, Aslam MF. Comparative analysis of different AES implementation techniques for efficient resource usage and better performance of an FPGA. *Journal of King Saud University - Computer and Information Sciences*. 2017, 29(3): 295-302. doi: 10.1016/j.jksuci.2016.01.004
10. Kocarev L. Chaos-based cryptography: a brief overview. *IEEE Circuits and Systems Magazine*. 2001, 1(3): 6-21. doi: 10.1109/7384.963463
11. Mukhopadhyay SC, ed. *Internet of Things*. Springer International Publishing, 2014. doi: 10.1007/978-3-319-04223-7
12. Towards Designing Efficient Lightweight Ciphers for Internet of Things. *KSII Transactions on Internet and Information Systems*. 2017, 11(8). doi: 10.3837/tiis.2017.08.014
13. Usman M, Ahmed I, Imran M, et al. SIT: A Lightweight Encryption Algorithm for Secure Internet of Things. *International Journal of Advanced Computer Science and Applications*. 2017, 8(1). doi: 10.14569/ijacsa.2017.080151
14. Kumar M, Kumar S, Budhiraja R, et al. Lightweight Data Security Model for IoT Applications: A Dynamic Key Approach. 2016 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData). Published online December 2016. doi: 10.1109/ithings-greencom-cpscom-smartdata.2016.100
15. Patil J, Bansod G, Kant KS. LiCi: A new ultra-lightweight block cipher. 2017 International Conference on Emerging Trends & Innovation in ICT (ICEI). Published online February 2017. doi: 10.1109/etiict.2017.7977007

16. Bapat C, Baleri G, Inamdar S, et al. Smart-Lock Security Re-engineered Using Cryptography and Steganography. Security in Computing and Communications. Published online 2017: 325-336. doi: 10.1007/978-981-10-6898-0_27
17. Indrayani R, Nugroho HA, Hidayat R, et al. Increasing the security of mp3 steganography using AES Encryption and MD5 hash function. 2016 2nd International Conference on Science and Technology-Computer (ICST). Published online October 2016. doi: 10.1109/icstc.2016.7877361
18. Aljawarneh S, Yassein MB, Talafha WA. A resource-efficient encryption algorithm for multimedia big data. Multimedia Tools and Applications. 2017, 76(21): 22703-22724. doi: 10.1007/s11042-016-4333-y
19. Schneier B. Applied Cryptography: Protocols, Algorithms, and Source Code in C. John Wiley & Sons; 2007.
20. Lian S, Sun J, Wang Z. A block cipher based on a suitable use of the chaotic standard map. Chaos, Solitons & Fractals. 2005, 26(1): 117-129. doi: 10.1016/j.chaos.2004.11.096
21. Rahulamathavan Y, Phan RCW, Rajarajan M, et al. Privacy-preserving blockchain based IoT ecosystem using attribute-based encryption. 2017 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS). Published online December 2017. doi: 10.1109/ants.2017.8384164
22. Yang J, He S, Lin Y, et al. Multimedia cloud transmission and storage system based on internet of things. Multimedia Tools and Applications. 2015, 76(17): 17735-17750. doi: 10.1007/s11042-015-2967-9
23. Rahman A, Islam MdJ, Rahman Z, et al. DistB-Condo: Distributed Blockchain-Based IoT-SDN Model for Smart Condominium. IEEE Access. 2020, 8: 209594-209609. doi: 10.1109/access.2020.3039113
24. Rahman A, Nasir MK, Rahman Z, et al. DistBlockBuilding: A Distributed Blockchain-Based SDN-IoT Network for Smart Building Management. IEEE Access. 2020, 8: 140008-140018. doi: 10.1109/access.2020.3012435
25. Rahman Z, Khalil I, Yi X, et al. Blockchain-Based Security Framework for a Critical Industry 4.0 Cyber-Physical System. IEEE Communications Magazine. 2021, 59(5): 128-134. doi: 10.1109/mcom.001.2000679
26. Ali M, Sadeghi MR, Liu X. Lightweight Revocable Hierarchical Attribute-Based Encryption for Internet of Things. IEEE Access. 2020, 8: 23951-23964. doi: 10.1109/access.2020.2969957
27. Kim TH, Kumar G, Saha R, et al. LiSP-XK: Extended Light-Weight Signcryption for IoT in Resource-Constrained Environments. IEEE Access. 2021, 9: 100972-100980. doi: 10.1109/access.2021.3097267
28. Gu Z, Li H, Khan S, et al. IEPSPB: A Cost-Efficient Image Encryption Algorithm Based on Parallel Chaotic System for Green IoT. IEEE Transactions on Green Communications and Networking. 2022, 6(1): 89-106. doi: 10.1109/tgcn.2021.3095707
29. Sun Y, Chatterjee P, Chen Y, et al. Efficient Identity-Based Encryption With Revocation for Data Privacy in Internet of Things. IEEE Internet of Things Journal. 2022, 9(4): 2734-2743. doi: 10.1109/jiot.2021.3109655
30. Ramesh S, Govindarasu M. An Efficient Framework for Privacy-Preserving Computations on Encrypted IoT Data. IEEE Internet of Things Journal. 2020, 7(9): 8700-8708. doi: 10.1109/jiot.2020.2998109
31. Al-Moliki YM, Alreshedi MT, Al-Harhi Y, et al. Robust Lightweight-Channel-Independent OFDM-Based Encryption Method for VLC-IoT Networks. IEEE Internet of Things Journal. 2022, 9(6): 4661-4676. doi: 10.1109/jiot.2021.3107395
32. Kuldeep G, Zhang Q. Design Prototype and Security Analysis of a Lightweight Joint Compression and Encryption Scheme for Resource-Constrained IoT Devices. IEEE Internet of Things Journal. 2022, 9(1): 165-181. doi: 10.1109/jiot.2021.3098859
33. Gupta N, Jati A, Chattopadhyay A. MemEnc: A Lightweight, Low-Power, and Transparent Memory Encryption Engine for IoT. IEEE Internet of Things Journal. 2021, 8(9): 7182-7191. doi: 10.1109/jiot.2020.3040846
34. Durga R, Poovammal E, Ramana K, et al. CES Blocks—A Novel Chaotic Encryption Schemes-Based Blockchain System for an IoT Environment. IEEE Access. 2022, 10: 11354-11371. doi: 10.1109/access.2022.3144681
35. Marry P, Yenumula K, Katakam A, et al. Blockchain based Smart Healthcare System. 2023 International Conference on Sustainable Computing and Smart Systems (ICSCSS). Published online June 14, 2023. doi: 10.1109/icscss57650.2023.10169704
36. Beaulieu R, Clark ST, Douglas S, et al. The SIMON and speck families of lightweight block ciphers. In: Proceedings of the 2015 52nd ACM/EDAC/IEEE Design Automation Conference (DAC); 8-12 June 2015; San Francisco, USA. pp. 1–6.
37. Salem Balobaid A, Alagrash YH, Hussein Fadel A, et al. Modeling of blockchain with encryption based secure education record management system. Egyptian Informatics Journal. 2023, 24(4): 100411. doi: 10.1016/j.eij.2023.100411
38. Habeeb S, Hassan RF. Sensors data encryption using TSFS Algorithm. Journal of Madent Alelem College. 2018, 10(1).
39. Naif JR, Majeed GA, Farhan AK. Secure IoT System Based on Chaos- Modified Lightweight AES. International Conference on Advanced Science and Engineering (ICOASE). 2019.
40. Saeed Al-Wattar AH. A Review of Block Ciphers S-Boxes Tests Criteria. Iraqi Journal of Statistical Science. 2019. 1-14.
41. Beaulieu R, Shors D, Smith J, et al. The SIMON and SPECK lightweight block ciphers. Proceedings of the 52nd Annual Design Automation Conference. Published online June 7, 2015. doi: 10.1145/2744769.2747946

42. Aruna S, Usha G. S-DAC: A Novel Dynamic Substitution boxes using hybrid chaotic system and Deoxyribonuceic Acid (DNA) coding for counterfeiting Side-Channel Attacks. *Personal and Ubiquitous Computing*. 2021, 27(3): 1321-1334. doi: 10.1007/s00779-021-01579-4
43. Rahman Z, Yi X, Billah M, et al. Enhancing AES Using Chaos and Logistic Map-Based Key Generation Technique for Securing IoT-Based Smart Home. *Electronics*. 2022, 11(7): 1083. doi: 10.3390/electronics11071083