International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 10 Issue: 10
Article Received: *25 July 2022* ***Revised:*** *12 September 2022* ***Accepted:*** *30 October 2022*

A Novel Lightweight Encryption Choatic Scheme for IOT based Healthcare Systems

J.Praveen kumar[1], M.Suresh Babu[2]
[1]Research Scholars in Department of Computer Science Bhartiar University Coimbatore.
[1]praveentkrecit@gmail.com
[2]Professor in Department of CSE, Teegala Krishna Reddy Engineering College Hyderabad
[2]surescse@tkrec.ac.in

Abstract: The Internet of Things (IoT) exhibits a crucial position in enabling smarter devices and establishing new communication channels between humans and machines via the Internet. Smart gadgets are widely used across sectors such as healthcare, automation, smart homes, and other user-assisted applications. While sensor-driven devices have significantly enhanced daily life, many IoT infrastructures suffer from security vulnerabilities that compromise privacy. Recently, the Advanced Encryption Standard (AES) has emerged as a promising area of research for securing IoT healthcare devices. However, encrypted data remains a target for various IoT attacks, necessitating further improvements in security measures. Motivated by these security concerns, this study proposes a novel lightweight encryption scheme called Biscroll maps. This scheme integrates dynamic dual logistic maps based on chaos theory into a three-dimensional substitution box (S-Box) to enhance data confidentiality, availability, and integrity. The proposed scheme has applicability of the DNA computing over the traditional S-Box operations such as permutations and shifting . The implemented system operates within an IoT infrastructure designed for real-time data collection from diverse sources. Rigorous experimentation has assessed the effectiveness of the proposed methodologies, including security evaluations such as NIST and S-box tests. Additionally, the performance of these methodologies has been benchmarked against existing encryption schemes in terms of time and memory usage. Results from the experiments indicate that the newly introduced L-DAL-SBoX algorithm surpasses other existing algorithms, establishing itself as a robust solution for IoT security.

Keywords: *Encryption, Choatic Scheme*

INTRODUCTION

The Internet of Things (IoT) has been applied to a number of industries, including automation, smart homes, and healthcare. The Internet of Things aims to facilitate comfortable computing, elevate collaboration, and expedite decision-making. The use of IoT in healthcare applications is growing daily, among other industries. Nonetheless, the usage of IoT devices in healthcare applications may be threatened by growing security risks like hackers and software flaws. Unauthorised users or other attackers may be able to access linked IoT devices and misuse the network or devices. When medical data is collected or transmitted via a public Internet Protocol (IP) channel using micro-format sensors and transceivers found in Internet of Things (IoT) devices, hackers may be exposed if the data is not well safeguarded. While many standard encryption algorithms, like Advanced Encryption Standard (AES), RCA, Elliptic Curve Encryption, and Digital Encryption Standard (DES), offer strong data protection features, numerous lightweight encryption algorithms, like PRESENT, CLEFIA, KATAN, SIMON/SPECK, and TSFS, aim to provide sufficient security through optimal resource utilisation. The aforementioned algorithms transfer the gathered medical data to a designated recipient while encrypting it.While the security of existing algorithms has been validated, an effective method for cracking keys could potentially undermine the process of generating keys. Furthermore, high security algorithm embedding is challenging and resource-intensive in IoT devices. As a result, numerous experts have upgraded encryption algorithms' security features to guarantee privacy while consuming the fewest resources possible. For the researchers, maintaining data integrity under resource limits continues to be a difficult task. Based on the aforementioned limitation, this study introduces novel dynamic and efficient Dual Adaptive Logistics Maps (DALMs), which integrate chaotic logistics attractors with AES systems to enhance critical Défense effectiveness DNA procedures have been incorporated into the plan to guarantee data privacy and portability. The recommended technique have a promising conclusion to elevate IoT healthcare security, according to the evaluation that was done.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 10 Issue: 10
***Article Received:** 25 July 2022 **Revised:** 12 September 2022 **Accepted:** 30 October 2022*

The primary significance of this study lies in the following aspects:

1. The dynamic and lightweight 3D chaotic key generation technique is proposed in the paper as an alternative to the traditional two-dimensional. Its lightweight and safe design is based on 3D dual level scroll Chaotic Maps architecture.
2. The proposed methodology takes the place of the traditional permutation and diffusion procedure in the DNA computations. This enhances the capability of preserving the accuracy of IoT data in healthcare.
3. The suggested system is employed within IoT testing environments and contrasted against other cutting-edge frameworks. Please provide references if available
4. The paper's framework unfolds as pursues: Section II presents an outline of the background research on AES and logistic chaotic attractor maps. Section III reviews existing literature on security vulnerabilities in IoT and other contemporary encryption algorithms. Section IV introduces a proposed scheme for enhancing IoT security. Section V covers the experimental setup, evaluation criteria, and analysis of results. At last, conclusions and avenues for future enhancements are addressed in Section VI

SECTION-II

2.BACKGROUND:

This segment explores the security hurdles of IoT in healthcare settings and the application of Advanced Encryption Standard (AES) to fortify IoT environments. Please provide any specific references for further clarification.

2.1 IoT Security Challenges in Health Care Environment:

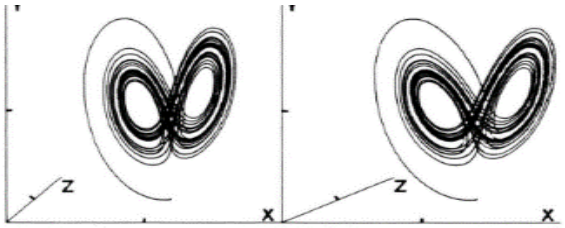
Health care advancements make it difficult to ensure security in an IoT context. Medical devices connected to the Internet of Things become more susceptible to attacks as they expand their range of services. When these devices communicate without encryption, they expose themselves to various vulnerabilities. Unauthorized individuals can access shared data and potentially alter it. Subsequently, hackers can intercept network traffic to obtain sensitive information such as login credentials. This breach allows attackers to access, intercept, and modify data without detection. Even when encryption is used, inadequate or poorly implemented encryption methods can still pose significant risks. Encryption should also safeguard highly confidential data stored on devices. Storing credentials or API tokens in plaintext without encryption is a common security risk. Additionally, improper application of cryptographic techniques or weak encryption methods further compound these challenges. Sensitive information is typically stored on medical electronic devices. Cameras installed in various locations have the capability to record both audio and video. Unauthorized access to this data by hackers would constitute a severe breach of privacy. This principle applies to both the generation and handling of sensitive data. Ensuring security in medical IoT devices is absolutely essential. However, there is ongoing discussion about the optimal methods for implementing security in IoT-based medical systems. Among the various measures, cryptographic encryption techniques are widely employed.

2.2 AES for Medical Data Integrity:

AES (Advanced Encryption Standard) utilizes a symmetric cipher to achieve robust security. AES is highly deployable across various hardware and software platforms and offers strong security features. AES remains utilized and reliable encryption algorithms, despite occasional breaches. Unauthorized access and breaches of privacy have been significant concerns in security research, especially regarding chaos-based encryption, which is known for its unpredictable nature. Chaos-based cryptosystems offer greater adaptability for handling large-scale data, including audio and video, compared to traditional cryptographic methods. Numerous researchers have explored integrating chaos into existing cryptosystems, leveraging chaos's inherent unpredictability to enhance security. When chaos-based approaches are used for key generation, the cryptographic design may achieve higher levels of security compared to integer-based methods.

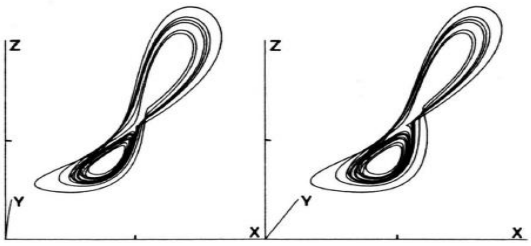
2.3 Chaos Based Encryption Schemes:

Chaos theory focuses on the characteristics of dynamic, nonlinear demonstrate exceptional sensitivity to minute changes represent a critical area of study to primary circumstances, causing outputs to diverge significantly in response to even small changes in starting parameters. Lyapunov exponents are utilized to measure this sensitivity to initial conditions, with positive Lyapunov exponents indicating chaotic behaviour. This crucial characteristic amplifies the unpredictability of outputs, prompting researchers to explore chaotic systems for cryptographic applications. However, this architecture may not be suitable for large-scale networks.

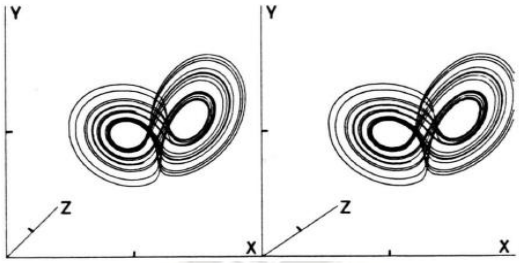


Lorenz-type chaos

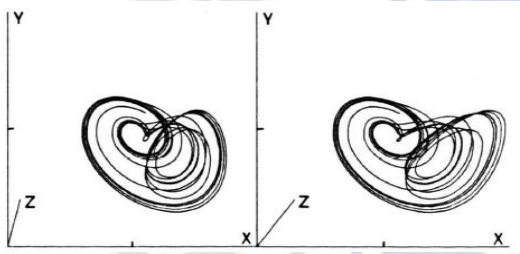
International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 10 Issue: 10
***Article Received:** 25 July 2022 **Revised:** 12 September 2022 **Accepted:** 30 October 2022*



Sandwich chaos



Double-horseshoe chaos



Screw type of chaos

3.RELATED WORKS:

M. Ali et al. prescribes a straightforward hierarchical attribute-based encryption (HABE) system. The computational load on the user's end is significantly minimized, with the cloud server handling most of the computational tasks. Moreover, this framework employs a hierarchical approach to facilitate user expulsion processes. However, the issuance and revocation of users' secret keys are centralized under a single authority.

T. H. Kim et al. introduced a streamlined Sign Encryption Protocol aimed at addressing authentication challenges in resource-constrained environments. Due to its simplified design, decreased energy consumption, and enhanced security features, this protocol is well-suited for IIoT scenarios. Critics have identified the time complexity associated with key encryption as its main drawback.

Z. Gu et al. developed a parallel chaotic system for encryption using a combination of the Piecewise Linear Chaotic Map (PWLCM), Skew Tent Map (STM), and Bernoulli Map. This framework is praised for its cost-effectiveness and robust security features. However, its primary drawback lies in its increased computational complexity and diminished security effectiveness when handling extensive datasets.

Y. Sun et al. introduced an practical identity-based encryption method with revocation features to safeguard data privacy in IoT applications. This technology enables actuators and sensors to securely transmit encrypted data through a cloud server, either directly or indirectly. One significant advantage is the private key generator's ability to notify users in case of compromised keys. Nonetheless, a drawback of this approach is the potential for transmission delays due to resource limitations.

Ramesh et al. introduce an architectural concept called "proxy reciphering as a service" to enable secure computation of encrypted IoT-device data. This framework offers significant advantages such as enhanced security, scalability, and user-friendliness for performing long-term computations in cloud environments while safeguarding privacy in cloud-IoT applications. However, a notable drawback of this approach is its higher cost and increased energy consumption. Additionally, in real-time scenarios, it is susceptible to frequent connection errors.

Y. M. Al-Moliki et al. introduced a robust lightweight channel-agnostic (LCI) physical-layer encryption method using optical OFDM to enhance IoT network privacy. Their research demonstrates that this approach enhances VLC's security against various attacks.

G. Kuldeep et al. eliminates the necessity for a secondary secure channel while providing robust resistance against numerous cryptographic attacks. A notable advantage of this system is its superior performance overall energy efficiency. However, a significant drawback of this framework is the introduction of communication latency when confronted with further cipher threats.

Gupta et al., seamlessly handles memory requests and performs real-time encryption without relying on OS intervention. This framework integrates a memory encryption engine with ARM Trust Zone, showcasing the necessity of balancing efficiency and security in all contexts, both static and dynamic. However, its main drawbacks lie in reduced throughput and increased computational complexity.

R. Durga et al. introduces a blockchain-IoT architecture enhanced by chaotic encryption to bolster data security and privacy. Integrating chaotic encryption with blockchain and IoT may enhance resistance against attacks. This architecture is noted for its capacity for high throughput and energy efficiency. However, it faces challenges in handling

large data volumes, which can lead to performance issues, thereby limiting its suitability for real-time applications.

U. Hijawi et al. introduced IoT devices with limited resources. This architecture enhanced wireless mesh network security and energy efficacy. However, the fundamental drawback of this architecture is that it makes the encryption process less energy-efficient and less available.

Table 1 presents a comparative analysis of the previously discussed related studies

Author	Methodology Proposed	Merits	Demerits
M. Ali et al.	Lightweight revocable hierarchical Attribute-based encryption	Versatile and expandable encryption key assignment.	A sole entity responsible for issuing and invalidating secret keys for users
T. H. Kim et al.	Light-weight Signcryption Protocol	Reduced complexity, lower energy consumption, and improved security	Time complexity
Z. Gu et al.	Parallel chaotic system (Piecewise Linear Chaotic Map+ Skew Tent Map+ Bernoulli map)	Prioritizes strong security measures and cost-effectiveness	Computational complexity
Y. Sun et al.	Identity-based public-key encryption scheme	Device elements can exchange encrypted data directly or via a cloud server	Transmission delay
S. Ramesh et al.	Proxy reciphering scheme	A framework that ensures security, scalability, and ease of adoption for conducting cloud computations while preserving privacy in the long term.	Costly, necessitating increased energy consumption and susceptibility to connectivity disruptions.
Y. M. Al-Moliki et al.	Lightweight channel-independent physical-layer encryption	Improves the efficiency of bit-error-rate performance, reduces communication latency.	Low throughput
G. Kuldeep et al.	Energy concealment encryption scheme	Less energy consumption	Communication overhead
N. Gupta et al.	MemEnc	Reducing latency and minimizing power usage	Computational complexity
R. Durga et al.	Chaotic encryption scheme	Achieving increased efficiency with minimal energy usage is crucial	Inappropriate for live situations
U. Hijawi et al.	Lighteweight Key-Policy Attribute Based Encryption	Scalability, and flexibility	Decrease the availability and consume more energy for the encryption process

4.PROPOSED FRAMEWORK:

S-BOX is used in the conventional AES to facilitate efficient data transfer from sender to recipient. The cornerstone of IoT security is data security with privacy. The other challenges that make integrating high-end security in an IoT context difficult include uneven user distribution, poor power distribution, and a lack of standardisation. When building the IoT security system, there is a risk associated with assuming that all existing cryptographic algorithms are risky. Consequently, an algorithm is required in order to thwart attacks and endure various types of attacks.

1) IoT Data Collection: This stage uses the integrated CPU's analogue channels to gather data from IoT devices. The memory of the CPU houses the gathered data.

2) Hybrid S-BOX: To develop a lightweight, robust, and deployable S-Box, a combination of scroll maps is used. 3) Encryption Process: Lastly, the data that has been stored is sent to the cloud encrypted using the recently created AES-S-box.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 10 Issue: 10
***Article Received:** 25 July 2022 **Revised:** 12 September 2022 **Accepted:** 30 October 2022*

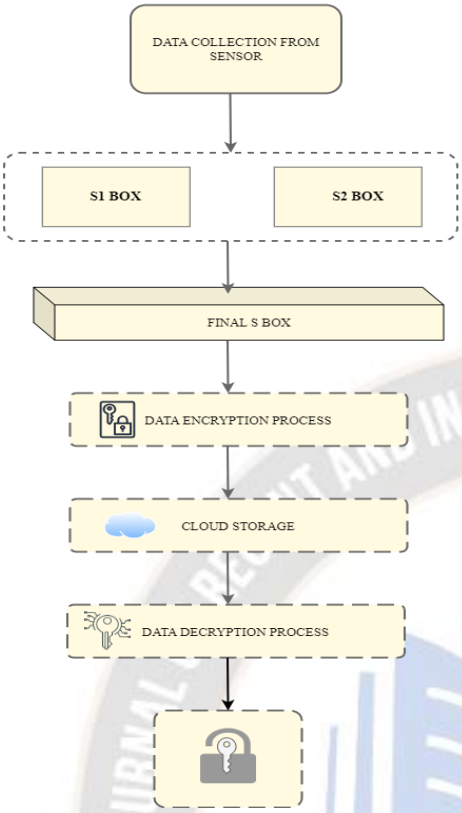


Fig 1:Iot based healthcare systems

As the proliferation of IoT devices connected to the internet escalates rapidly, so does the likelihood of vulnerabilities, rendering every unsecured device susceptible to potential cyber attacks. Consequently, ensuring security in these IoT devices is paramount, necessitating the development of a new IoT protocol to tackle these security challenges effectively and offer unparalleled authentication, message integrity, and confidentiality. The suggested custom aims to illustrate these security concerns comprehensively.

4.1 PRE-REQUISTIES:

This section discusses about the basic foundation for the Multi-scroll attractors and henon maps.

4.1.1 MULTI-SCROLL ATTRACTORS:

The state space illustration of a self-contained chaotic system is provided below

$$\dot{x}_1 = -ax_1 + bx_2x_3 \quad (1)$$
$$\dot{x}_2 = -cx_2^3 + dx_1x_3$$
(2)
$$\dot{x}_3 = ex_3 - fx_1x_2$$
(3)

The equation(1),(2),(3) can be altered by integrating the hyperbolic formula$p_1\ tanh(x_2 + g)$ which is given in eqn

$$\dot{x}_1 = -ax_1 + bx_2x_3 \quad (4)$$
$$\dot{x}_2 = -cx_2^3 + dx_1x_3$$
(5)$\dot{x}_3 = ex_3 - fx_1x_2 + p_1\ tanh(x_2 + g)$
(6)

Chaotic attractor is acquire when $a = 2$, $b = 6$, $c = 6$, $d = 3$, $e = 3$, $f = 1$, $p_1 = 1$, $g = 2$and the chosen primary conditions are $[x_1(0), x_2(0), x_3(0)] = [0.1, 0.1, 0.6]$.

In its early stages, the introduction of the hyperbolic function is characterized by a parameter g = -3. Under these conditions, starting from the initial states [0.1, -0.1, -0.6], a double scroll attractor is observed, as depicted in Figure 2. Transitioning to the subsequent phase, characterized by parameters p_1 = -1 and g = 3, and starting again from the initial conditions [0.1, -0.1, -0.6], a four-scroll pattern emerges, illustrated in Figure 3. Moving to the third phase with parameters p_1 = 1 and g = 3, and primary conditions [0.1, 0.1, 0.6], a single scroll behavior is displayed, as shown in Figure 4. These findings conclusively establish the system's multi-scroll characteristic.

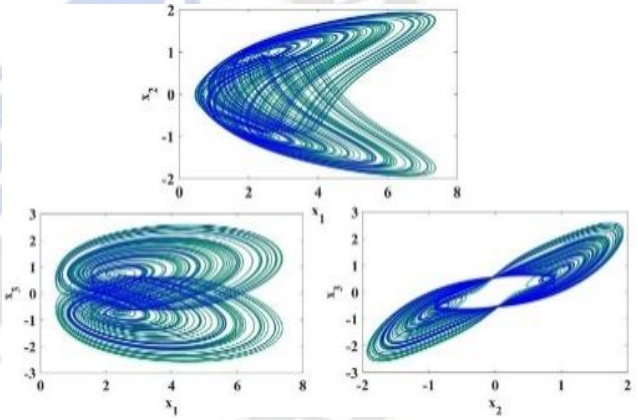


Figure 2. Phase portraits of cubic nonlinear system with $p_1\ tanh(x_2 + g)$ function in 1st state

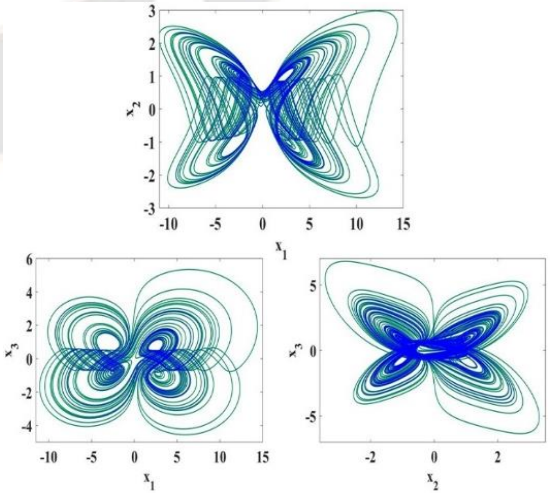


Figure 3. Phase portraits of cubic nonlinear system with $p_1\ tanh(x_2 + g)$ function in 2nd state

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 10 Issue: 10
Article Received: *25 July 2022* ***Revised:*** *12 September 2022* ***Accepted:*** *30 October 2022*

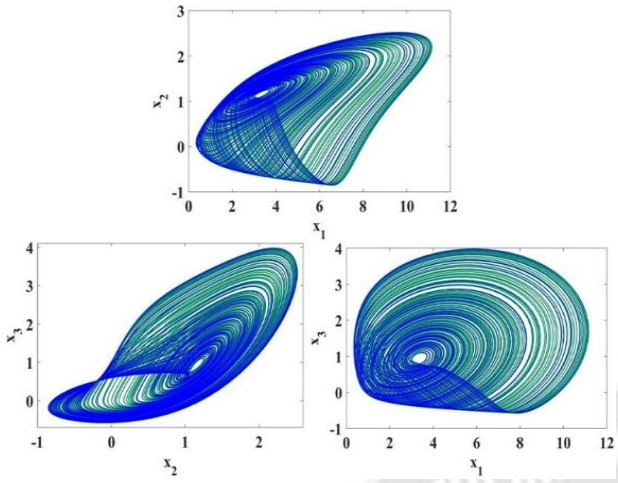


Figure 4. Phase portraits of cubic nonlinear system with $p_1\, tanh(\, x_2 + g)$ function in 3rd state

To develop Multi-scroll 3D chaotic systems with fractional or integer-order dynamics, the equations () were adjusted using derivative characteristics as detailed in [32]. The resultant chaotic system capable of displaying multi-scroll behaviors is provided as follows. Please ensure that references are included where applicable.

$$\frac{d^q x_1}{dt^q} = -ax_1 + bx_2x_3 \quad (7)$$

$$\frac{d^q x_2}{dt^q} = -cx_2^3 + dx_1x_3 \quad (8)$$

$$\frac{d^q x_3}{dt^q} = ex_3 - fx_1x_2 + p_1\, tanh(\, x_2 + g) \quad (9)$$

The bifurcation diagram for the recommendedmulti scroll integer order chaotic systems are shown in following fig 5.

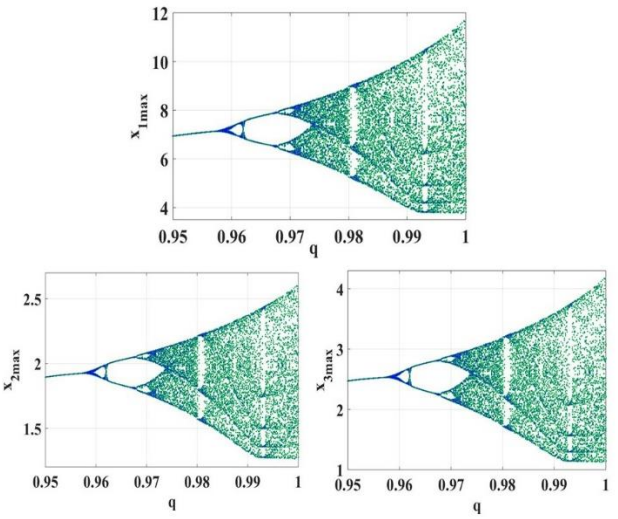


Fig 5 Fractional Bifurcation Diagrams for the Suggested Multi Scroll Chaotic Systems

4.1.2 ADVANTAGES OF MULTI-SCROLL ATTRACTORS:

The following advantages of the proposed scroll attractors used for encryption is mentioned below

1. This System needs less memory to generate the same number of scroll as it takes the less component for generation[32].
2. Random scroll can be generated on modifying any component of its any directions. This characteristics is much more different than the other chaotic systems.
3. Scroll maps are termed as the flexible maps in which the randomness doesn't depends in the scroll numbers, while that of other methods are closely related to the number of initial values.

4.1.3 DNA COMPUTING PROCESS:

DNA encodes information using four nucleotides: adenine (A), guanine (G), cytosine (C), and thymine (T). Typically, adenine pairs with thymine (A-T) and guanine pairs with cytosine (G-C). The intermediate outcomes of S-boxes, such as SDAC_I1 and SDAC_I2, are encoded through the application of pairing guidelines to produce DNA sequences. If there are any sources, please provide them for proper referencing. These sequences facilitate algebraic operations such as DNA addition, subtraction, and exclusive OR (XOR), as outlined in Table 1-3. If you have specific references or sources, please provide them for accuracy.

The DNA pairing rules, as illustrated in Table 4. Subsequently, the DNA addition rules are utilized to the resultant DNA sequence from the DNA pairing rules detailed in Table 4.

Table 2 DNA Pairing Rules

	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 3 Rules of DNA Addition

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

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 10 Issue: 10
***Article Received:** 25 July 2022 **Revised:** 12 September 2022 **Accepted:** 30 October 2022*

Table 4 Rules of DNA XOR

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

4.2 KEY GENERATION PROCESS USING PROPOSED S-BOX :

4.2.1 OVERVIEW :

The proposed method utilizes the core AES operations but incorporates DNA coding instead of traditional permutation and shifting techniques, aiming to streamline encryption/decryption times while maintaining robust defense capabilities. This modification integrates Fractional Dual-level Logistic maps to enhance encryption strength. At the outset, sensor data bytes are split into two distinct parts based on their byte location. In the first stage, 3D logistic maps construct the S-box S1. Data is encrypted using the newly formed S-box (S3). These processes collectively aim to optimize AES for lightweight performance by diminising encryption/decryption times while reinforcing resistance against IoT attacks.

4.2.2 KEY GENERATION PROCESS:

The complete key generation process is illustrated in Figure. To simplify the implementation of matrix encryption techniques, the initial step involves focusing on the first byte locations of sensor inputs. These logistic maps are then utilized to construct the intermediary S1 box. The moderate S-box is produced by integrating the 3D logistic maps (I) with input data bytes (K). Instead of using permutations and diffusions, DNA addition encoding is employed to enhance the security of the resulting S1-Box sequences.

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

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

Steps	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(16X16)
3	Start
4	Formulate the Random Sequences as initial conditions for 3d Logistic maps
5	Formulate the 3d Logistic maps using Equation(1)-(3)
6	Determine the missing values in K sensor bytes and replace it with zeros
7	Reconfigure the maps and k-bytes to 16
8	Construct the moderate S1-box using the equation
	End

The creation of S2 is detailed in Algorithm-2.

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

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

Steps	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	Formulate the starting states from the outcome sequences derived from the S1-box.
5	Formulate the 3D logistic maps using the Equation(6)
6	Determine the missing values in O sensor bytes and replace it with zeros
7	Reconfigure the maps and O-bytes to 16
8	Construct the moderate S2-box by utilizing the equation(7)
	End

4.2.3 ENCRYPTION PROCESS :

A comprehensive depiction of suggested S-DAC systems is provided below

Step 1 : The segmentation of images involves categorizing pixels into two types: inter-level pixels and intra-level pixels. Each category of pixel is denoted by matrices I1 and I2, respectively, each comprising pixels with a length of 128 units.

Step 2 : The separation of S-boxes into S1 and S2 boxes, each with a size of 256, involves decomposing the S-boxes. If there are existing references, could you please provide them?

Step 3 : The primary conditions for the 3D chaotic mappings have been produced. In this study, the research proposes employing stochastic computation of IoT network attributes. Attributeslike received signal strength (RSSI) and distance (D) were utilized to derive the initial states for 3D logistic mappings. The methodology for measuring RSSI and

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 10 Issue: 10
Article Received: *25 July 2022* ***Revised:*** *12 September 2022* ***Accepted:*** *30 October 2022*

distance is detailed in Section V. I(Chaotic maps) = IoT parameters(RSSI, Distance) (7)

Step 4 : The inter-bit pixels are subsequently encoded utilizing DNA computing, following the ruling pairs outlined in Table I. This process employs the previously generated 3D logistic maps to create new dynamic S1 boxes, which are then organized into an S1 matrix. Scaling is applied to adjust their length to 256.

$$\boldsymbol{S1(i) = mod(DNA\ (I1, SCROLL(X(i), Y(i), Z(i)) + r, 256\})} \textbf{(8)}$$

Step 5 : The primary parameters for the scroll maps is produced as described in Step 3. The content of these S2 compartments is denoted as the S2 Matrix. The mathematical expression for producing the S2 compartments is detailed below. If references are available, please provide them for verification.

$$\boldsymbol{S2(i) = mod(DNA\ (I1, SCROLL(X(i), Y(i), Z(i)) + r, 256\})} (9)$$

Step 6 : The DNA encoding is employed over the S1 and S2 matrix to form the keys through the S-box which is represented in the mathematical expression (10) and(11)

$$S1(i) = \left[S1^{1(i)x10^4}\right] mod\ 256 \qquad (10)$$

$$S2(i) = \left[S2^{2(i)x10^4}\right] mod\ 256 \qquad (11)$$

The DNA encoded S-Box is illustrated mathematically by

S(i) = DNA ENCODED(S1(i) , S2(i))mod 256 (12)

Step 7 : The DNA-XOR operation is executed again on the input images using the key derived in Step 6. This leads to the generation of new, intricately encrypted image data. The different types of S-boxes produced are depicted in Table 5, 6 and 7.

	0	1	2	3	4	6	6	7	8	9	10	11	12	13	14	15	16
0	25	FE	55	77	44	DA	01	21	E4	33	11	AA	23	DC	45	81	A1
1	124	EE	67	84	78	39	50	A7	179	185	105	79	91	18	AE	55	91
2	AE	102	46	96	120	89	34	45	68	73	82	91	133	150	170	181	46
3	79	90	45	89	A2	DE	135	157	AB	191	111	130	181	241	FE	BC	13
4	55	BE	91	191	79	68	24	101	240	168	154	AE	191	09	103	08	57
5	157	191	78	236	83	91	102	21	201	68	92	101	86	46	90	13	96
6	201	68	91	101	86	46	90	13	90	79	146	69	231	68	87	113	03
7	ED	101	125	103	96	232	122	30	03	04	122	AE	57	82	91	103	166
8	FE	99	168	240	68	91	91	57	25	FE	55	77	44	DA	99	11	74
9	91	79	146	69	231	68	87	113	124	EE	67	84	78	39	50	157	199
10	35	220	201	92	191	71	91	90	247	101	90	73	05	A5	CD	01	02
11	91	113	120	79	79	46	45	45	02	04	123	AE	57	82	91	103	11
12	03	04	122	AE	57	82	91	103	179	183	102	79	91	18	AE	55	91
13	35	101	141	AA	91	03	02	121	68	73	82	91	133	150	170	181	46
14	E0	124	111	BA	EE	81	06	BB	AB	191	111	130	181	241	FE	BC	13
15	46	57	256	68	79	101	201	24	240	168	154	AE	191	09	103	08	57
16	79	24	133	190	102	02	A0	90	42	211	103	E4	122	03	101	07	88

Table5 Formation of DNA Encoded Intermediate S1-Box using the 3D Logistic Chaotic Maps

	0	1	2	3	4	6	6	7	8	9	10	11	12	13	14	15	16
0	223	F3	56	78	45	DA	03	22	E4	34	12	AA	24	DC	46	82	A1
1	25	E1	68	85	79	40	51	A7	180	184	103	80	92	19	AE	56	92
2	47	13	47	97	121	90	35	46	69	74	83	92	135	151	171	182	47
3	92	82	46	90	A2	DE	136	158	AB	192	112	131	182	242	FE	BC	14
4	4	B1	92	192	80	69	25	102	241	169	155	AE	192	10	104	09	58
5	6	12	79	237	84	92	102	22	202	69	92	102	87	47	91	14	97
6	22	62	92	102	87	47	91	14	91	80	147	70	232	69	88	114	04
7	E6	104	126	104	97	233	123	91	04	05	123	AE	58	83	92	104	167
8	F5	95	169	241	69	92	92	58	26	FE	56	78	45	DA	101	12	75
9	86	82	147	70	232	69	88	114	125	EE	68	85	79	40	51	158	200
10	39	30	202	93	192	72	92	91	247	102	91	73	07	A5	CD	02	03
11	101	14	121	80	80	47	45	44	03	05	123	AE	58	83	92	104	12
12	03	25	123	AE	58	83	92	104	180	184	103	80	92	19	AE	56	92
13	33	12	142	AA	92	04	03	122	69	74	83	92	134	151	171	182	47
14	E0	185	112	BA	EE	82	07	BB	AB	192	112	131	182	242	FE	BC	14
15	44	194	257	69	80	102	202	25	241	169	155	AE	192	10	104	09	58
16	76	232	134	191	103	03	A0	91	43	212	104	E4	123	04	102	08	89

Table6 Formation of DNA Encoded Intermediate S2-Box using the 3D Henon Chaotic Maps

	0	1	2	3	4	6	6	7	8	9	10	11	12	13	14	15	16
0	247	FE	55	77	44	DA	02	21	E4	33	11	AA	23	DC	45	81	A1
1	125	EE	67	84	78	39	50	A7	179	183	102	79	91	18	AE	55	91
2	A3	102	46	96	120	89	34	45	68	73	82	91	133	150	170	181	46
3	79	90	45	89	A2	DE	135	157	AB	191	111	130	181	241	FE	BC	13
4	13	BE	91	191	79	68	24	101	240	168	154	AE	191	09	103	08	57
5	17	191	78	236	83	91	101	21	201	68	91	101	86	46	90	13	96
6	21	68	91	101	86	46	90	13	90	79	146	69	231	68	87	113	03
7	04	101	125	103	96	232	122	90	03	04	122	AE	57	82	91	103	166

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 10 Issue: 10
Article Received: *25 July 2022* ***Revised:*** *12 September 2022* ***Accepted:*** *30 October 2022*

8	05	99	168	240	68	91	91	57	25	FE	55	77	44	DA	100	11	74
9	92	79	146	69	231	68	87	113	124	EE	67	84	78	39	50	157	199
10	33	220	201	92	191	71	91	90	246	101	90	72	06	A5	CD	01	02
11	79	113	120	79	79	46	44	43	02	04	122	AE	57	82	91	103	11
12	06	04	122	AE	57	82	91	103	179	183	102	79	91	18	AE	55	91
13	07	101	141	AA	91	03	02	121	68	73	82	91	133	150	170	181	46
14	11	124	111	BA	EE	81	06	BB	AB	191	111	130	181	241	FE	BC	13
15	246	57	256	68	79	101	201	24	240	168	154	AE	191	09	103	08	57
16	125	24	133	190	102	02	A0	90	42	211	103	E4	122	03	101	07	88

Table 7 Formation of DNA Encoded Intermediate S--Box

5.EXPERIMENTAL RESULTS:

This section outlines the experimental configuration utilizing both hardware and software implementations. To measure the RSSI, we employed a Raspberry Pi 3 Model B+ integrated into an IoT network via Wi-Fi transceivers, preferably using hotspot gateways. Micro Python scripts were evolved based on AT commands to execute on the Raspberry Pi 3, enabling the measurement of various RSSI values for network connectivity. Additionally, the recommended algorithm was crafted using Python 3.7, leveraging numerous libraries.

5.1 NIST RANDOMNESS TEST:

To assess the ambiguity of the generated bits, the encryption scheme underwent statistical tests. The outcome of all tests met the NIST standards, demonstrating the algorithm's robust randomness, which is capable of withstanding various network attacks. Table 6 details the comprehensive performance outcome of the NIST tests for the suggested algorithm.

Table 6 NIST Standard Test Performance of the Proposed Algorithm

Sl.No	NIST Test Specification	Status of test
1	DFT Test	PASS
2	RunTest	PASS
3	Long Run Test	PASS
4	Frequency Test	PASS
5	Block Frequency Test	PASS
6	Frequency MonoTest	PASS
7	Overlapping Template of all One's test	PASS
8	Linear Complexity Test	PASS
9	Matrix Rank Test	PASS
10	Lempel-ZIV Compression Test	PASS
11	Random Excursion Test	PASS
12	Universal Statistical Test	PASS

In this assessment, the time required to generate encrypted information for the proposed smart healthcare system has been evaluated and juxtaposed with established algorithms. To ensure a thorough examination of the suggested approach, various data sizes from different sensors are used to calculate the encryption time. The performance of the suggested methodology is measured against other established models mentioned in the study. Figure 2-6 illustrates a examined analysis of the initial duration for various algorithms as the data sizes vary.

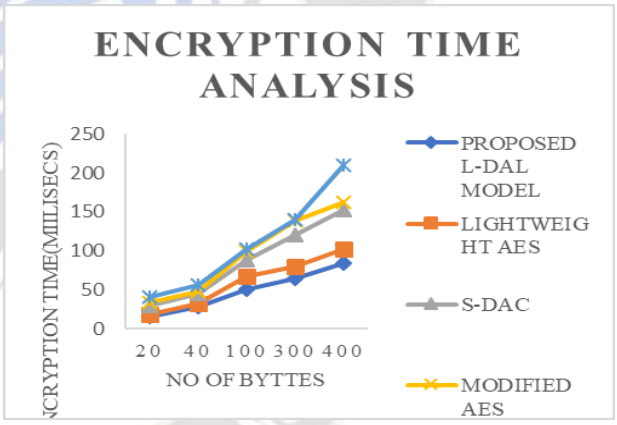


Figure 3 Encryption Time Analysis for encrypting ECG and Three Axis MEMS Accelerometer Data.

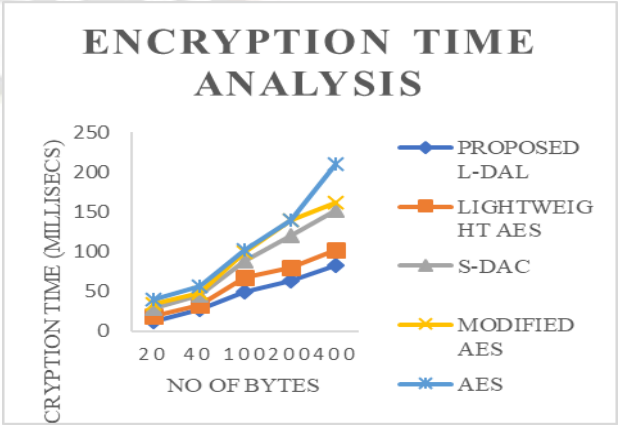


Figure 4 Encryption Time Analysis for encrypting BMI and Blood Pressure Sensor Data.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 10 Issue: 10
Article Received: *25 July 2022* ***Revised:*** *12 September 2022* ***Accepted:*** *30 October 2022*

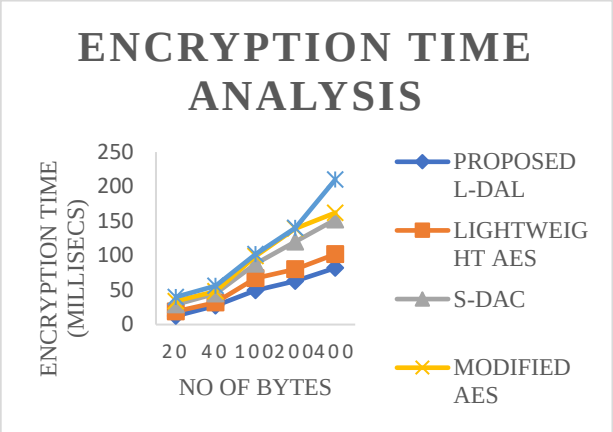


Figure 5 Encryption Time Analysis for encrypting Pulse Rate and Temperature Sensor

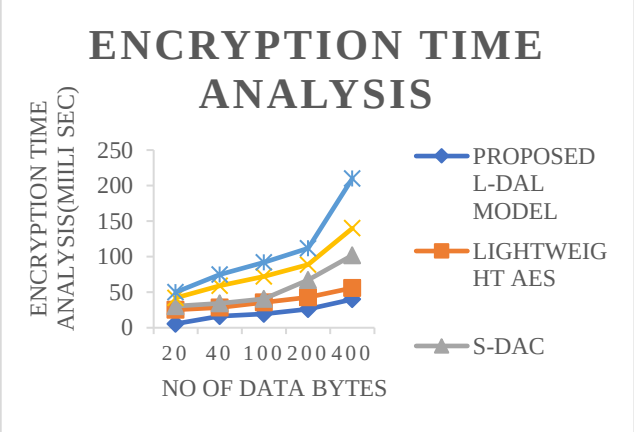


Figure6 Encryption Time Analysis for encrypting pulse oximeter data

The recommended approach, designed and executed to evaluate data security, integrity. This improvement is demonstrated in Figures 3-6. The keys developed by utilizing the adaptive theory are embedded as private keys in each smart healthcare IoT device. Hospitals and doctors utilize these private keys to decode medical data from the sender. Therefore, experiments were conducted to quantify the encryption time of the recommended approach. To illustrate the efficacy of the suggested framework, it was analysed with residing methodology such as AES, Modified AES[40], S-DAC[41], and Lightweight AES[42]. Figures 3-5 illustrate the examined analysis of these algorithms in producing encrypted data. Modified AES, based on 3D dimensional logistic maps, showed significant outcome over traditional AES, indicating the beneficial impact of chaotic integration on encryption performance. Nonetheless, the extended time required by S-DAC and Lightweight AES makes them less suitable for embedded CPU deployment. Therefore, the outcome depicts that the suggested model offers more randomness and lightweight characteristics (due to the integration of dual adaptive chaos), making it feasible for embedding in CPUs to establish robust security and maintain data integrity within smart healthcare IoT systems.

6. CONCLUSION

In this exploration, a lightweight, dynamic, and highly secure S-box AES is suggested for IoT healthcare systems. This innovative approach integrates DNA computation in place of traditional permutation and diffusion processes, enhancing data randomness and security. The introduction of DNA and adaptive logistic maps significantly alters the S-box design. Additionally, an IoT-based Smart Healthcare system has been developed to assess the security of the recommended model against potential vulnerabilities. Extensive experimentation has been conducted, and S-box metrics have been thoroughly analysed and examined. The performance of the designed S-box has been benchmarked against various residing S-boxes used in healthcare applications. The results indicate that the proposed model.

REFERENCES:

1. Song, T.; Li, R.; Mei, B.; Yu, J.; Xing, X.; Cheng, X. A privacy preserving communication protocol for IoT applications in smart homes. IEEE Internet Things J. 2017, 4, 1844–1852.
2. Moosavi, S.R.; Gia, T.N.; Nigussie, E.; Rahmani, A.M.; Virtanen, S.; Tenhunen, H.; Isoaho, J. End-to-end security scheme for mobility enabled healthcare Internet of Things. Future Gener. Comput. Syst. 2016, 64, 108–124.
3. Lee, I.; Lee, K. The Internet of Things (IoT): Applications, investments, and challenges for enterprises. Bus. Horizons 2015, 58, 431–440.
4. Ion, M.; Zhang, J.; Schooler, E.M. Toward content-centric privacy in ICN: Attribute-based encryption and routing. In Proceedings of the 3rd ACM SIGCOMM workshop on Information-Centric Networking, Hong Kong, China, 12 August 2013; pp. 39–40.
5. Rahman, Z.; Yi, X.; Khalil, I.; Sumi, M. Chaos and Logistic Map Based Key Generation Technique for AES-Driven IoT Security. In Proceedings of the International Conference on Heterogeneous Networking for Quality, Reliability, Security and Robustness, Online, 29–30 November 2021; pp. 177–193
6. Rahaman, Z.; Corraya, A.D.; Sumi, M.A.; Bahar, A.N. 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 Trans. Inf. Theory 1977, 23, 337–343.

8. Vashi, S.; Ram, J.; Modi, J.; Verma, S.; Prakash, C. Internet of Things (IoT): A vision, architectural elements, and security issues. In Proceedings of the 2017 international conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud), Tamil Nadu, India, 10–11 February 2017; pp. 492–496.
9. Farooq, U.; Aslam, M.F. Comparative analysis of different AES implementation techniques for efficient resource usage and better performance of an FPGA. J. King Saud Univ. Comput. Inf. Sci. 2017, 29, 295–302.
10. Kocarev, L. Chaos-based cryptography: A brief overview. IEEE Circuits Syst. Mag. 2001, 1, 6–21.
11. Mukhopadhyay, S.C.; Suryadevara, N.K. Internet of things: Challenges and opportunities. In Internet of Things; Springer: Berlin/Heidelberg, Germany, 2014; pp. 1–17.
12. Tausif, M.; Ferzund, J.; Jabbar, S.; Shahzadi, R. Towards designing efficient lightweight ciphers for internet of things. KSII Trans. Internet Inf. Syst. 2017, 11, 4006–4024.
13. Usman, M.; Ahmed, I.; Aslam, M.I.; Khan, S.; Shah, U.A. SIT: A lightweight encryption algorithm for secure internet of things. arXiv 2017, arXiv:1704.08688.
14. Kumar, M.; Kumar, S.; Budhiraja, R.; Das, M.; Singh, S. Lightweight data security model for IoTapplications: A dynamic key approach. In Proceedings of the 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), 2016; pp. 424–428.
15. Patil, J.; Bansod, G.; Kant, K.S. LiCi: A new ultra-lightweight block cipher. In Proceedings of the 2017 International Conference on Emerging Trends & Innovation in ICT (ICEI), Pune, India, 3–5 February 2017; pp. 40–45.
16. Bapat, C.; Baleri, G.; Inamdar, S.; Nimkar, A.V. Smart-lock security re-engineered using cryptography and steganography. In International Symposium on Security in Computing and Communication; Springer: Berlin, Germany, 2017; pp. 325–336.
17. Indrayani, R.; Nugroho, H.A.; Hidayat, R.; Pratama, I. Increasing the security of mp3 steganography using AES Encryption and MD5 hash function. In Proceedings of the 2016 2nd International Conference on Science and Technology-Computer (ICST), Yogyakarta, Indonesia, 27–28 October 2016; pp. 129–132.
18. Aljawarneh, S.; Yassein, M.B.; Talafha, W.A. A resource-efficient encryption algorithm for multimedia big data. Multimed. Tools Appl. 2017, 76, 22703–22724
19. Schneier, B. Applied Cryptography: Protocols, Algorithms, and Source Code in C; John Wiley & Sons: Hoboken, NJ, USA, 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, 117–129.
21. Rahulamathavan, Y.; Phan, R.C.W.; Rajarajan, M.; Misra, S.; Kondoz, A. Privacy-preserving blockchain based IoT ecosystem using attribute-based encryption. In Proceedings of the 2017 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS), Bhubaneswar, India, 17–20 December 2017; pp. 1–6
.22. Yang, J.; He, S.; Lin, Y.; Lv, Z. Multimedia cloud transmission and storage system based on internet of things. Multimed. Tools Appl. 2017, 76, 17735–17750.
23. Rahman, A.; Islam, M.J.; Rahman, Z.; Reza, M.M.; Anwar, A.; Mahmud, M.A.P.; Nasir, M.K.; Noor, R.M. DistBCondo: 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, M.K.; Rahman, Z.; Mosavi, A.; S., S.; Minaei-Bidgoli, B. 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.; Atiquzzaman, M. Blockchain-Based Security Framework for a Critical Industry 4.0 Cyber-Physical System. IEEE Commun. Mag. 2021, 59, 128–134. doi:10.1109/MCOM.001.2000679.
26. M. Ali, M. -R. Sadeghi and X. Liu, "Lightweight Revocable Hierarchical Attribute-Based Encryption for Internet of Things," in IEEE Access, vol. 8, pp. 23951-23964, 2020, doi: 10.1109/ACCESS.2020.2969957.
27. T. -H. Kim, G. Kumar, R. Saha, W. J. Buchanan, T. Devgun and R. Thomas, "LiSP-XK: Extended Light-Weight Signcryption for IoT in Resource-Constrained Environments," in IEEE Access, vol. 9, pp. 100972-100980, 2021, doi: 10.1109/ACCESS.2021.3097267.
28. Z. Gu et al., "IEPSBP: A Cost-Efficient Image Encryption Algorithm Based on Parallel Chaotic System for Green IoT," in IEEE Transactions on Green Communications and Networking, vol. 6, no. 1, pp. 89-106, March 2022, doi: 10.1109/TGCN.2021.3095707.
29. Y. Sun, P. Chatterjee, Y. Chen and Y. Zhang, "Efficient Identity-Based Encryption With Revocation for Data Privacy in Internet of Things," in IEEE Internet of Things Journal, vol. 9, no. 4, pp. 2734-2743, 15 Feb.15, 2022, doi: 10.1109/JIOT.2021.3109655.
30. S. Ramesh and M. Govindarasu, "An Efficient Framework for Privacy-Preserving Computations on

Encrypted IoT Data," in IEEE Internet of Things Journal, vol. 7, no. 9, pp. 8700-8708, Sept. 2020, doi: 10.1109/JIOT.2020.2998109.

31. Y. M. Al-Moliki, M. T. Alresheedi, Y. Al-Harthi and A. H. Alqahtani, "Robust Lightweight-Channel-Independent OFDM-Based Encryption Method for VLC-IoT Networks," in IEEE Internet of Things Journal, vol. 9, no. 6, pp. 4661-4676, 15 March15, 2022, doi: 10.1109/JIOT.2021.3107395.
32. G. Kuldeep and Q. Zhang, "Design Prototype and Security Analysis of a Lightweight Joint Compression and Encryption Scheme for Resource-Constrained IoT Devices," in IEEE Internet of Things Journal, vol. 9, no. 1, pp. 165-181, 1 Jan.1, 2022, doi: 10.1109/JIOT.2021.3098859.
33. N. Gupta, A. Jati and A. Chattopadhyay, "MemEnc: A Lightweight, Low-Power, and Transparent Memory Encryption Engine for IoT," in IEEE Internet of Things Journal, vol. 8, no. 9, pp. 7182-7191, 1 May1, 2021, doi: 10.1109/JIOT.2020.3040846.
34. R. Durga, E. Poovammal, K. Ramana, R. H. Jhaveri, S. Singh and B. Yoon, "CES Blocks—A Novel Chaotic Encryption Schemes-Based Blockchain System for an IoT Environment," in IEEE Access, vol. 10, pp. 11354-11371, 2022, doi: 10.1109/ACCESS.2022.3144681.
35. U. Hijawi, D. Unal, R. Hamila, A. Gastli and O. Ellabban, "Lightweight KPABE Architecture Enabled in Mesh Networked Resource-Constrained IoT Devices," in IEEE Access, vol. 9, pp. 5640-5650, 2021, doi: 10.1109/ACCESS.2020.3048192.
36. R. Beaulieu, S. T.Clark, S. Douglas, S. Weeks, B. Smith, and J. Wingers, "TheSIMON and speck families of lightweight block ciphers," in 52nd ACM/EDAC/IEEE Design Automation Conference (DAC), San Francisco, 2013, pp. 1–6.
37. S. Habeeb and R. F. Hassan, "Sensors data encryption using TSFS Algorithm," Journal of MadentAlelem College, Vol. 10, No. 1, 2018.
38. J. R. Naif, GH A. Majeed, and A. K. Farhan, "Secure IoT System Based on Chaos- Modified Lightweight AES," International Conference on Advanced Science and Engineering (ICOASE), 2019
39. A. H. Saeed Al-Wattar, "A Review of Block Ciphers S-Boxes Tests Criteria," Iraqi Journal of Statistical Science, pp.1-14, 2019.
40. Beaulieu, R.; Shors, D.; Smith, J.; Treatman-Clark, S.; Weeks, B.; Wingers, L. The SIMON and SPECK lightweight block ciphers. In Proceedings of the 52nd Annual Design Automation Conference, San Francisco, CA, USA, 7–10 June 2015; pp. 1–6.
41. S, A., G, U. S-DAC: A Novel Dynamic Substitution boxes using hybrid chaotic system and Deoxyribonuceic Acid(DNA) coding for counterfeiting Side-Channel Attacks. *Pers UbiquitComput* (2021). https://doi.org/10.1007/s00779-021-01579-4
42. Ziaur Rahman , Xun Yi , Mustain Billah , Mousumi Sumi and Adnan Anwar," Enhancing AES Using Chaos and Logistic Map-Based Key Generation Technique for Securing IoT-Based Smart Home", Mdpi/Electronics 0. https://doi.org/10.3390/electronics1010000