Iraqi Journal for Computers and Informatics
University of Information Technology and Communications
Vol. 51, No. 1, 2025, pp. 94-107
DOI: https://doi.org/10.25195/ijci.v51i1.559
Print ISSN: 2313-190X, Online ISSN: 2520-4912

Research Article

Data Security Model Using (AES-LEA) Algorithms for WoT Environment

[1]Zinah A. Al-jazaeri
Computer and Communication Department
Islamic University of Lebanon-IUL
Wardenieh, Lebanon
zzzrsaaa@gmail.com

[2] Joolan Rokan Naif
Informatic Institute for Postgraduate Studies, University of information Technology and Communications
Baghdad, Iraq
newjolan@gmail.com,
dr.jolan_alkhazraji@iips.edu.iq

[3] Ahmad Mohamad Ghandour
Computer and Communication Department
Islamic University of Lebanon-IUL
Wardenieh, Lebanon
ahmad.ghandour@iul.edu.lb

ARTICLE INFO
Article History
Received: 24/02/2025
Accepted: 02/04/2025
Published: 05/06/2025

ABSTRACT

The Web of Things WoT connects physical objects and displays them in the WWW. The growing number of Internet of Things IoT devices and data sharing has led to the attack on sensitive information and allowing unauthorized persons to access and manipulate it. Therefore, ensuring data privacy and protection is a major challenge for organizations and individuals. This paper presents a new hybrid method for the encryption of information to be more suitable for embedded devices in the WoT environment by modifying the Advanced Encryption Standard AES algorithm and hybridizing it with the Lightweight Encryption Algorithm LEA algorithm as well as the Secure Hash Algorithm version 3 SHA3-256 algorithm for integrity and using four dimensional-NSJR system for generation of chaos keys. The proposed method is designed to decrease encryption /decryption time for the information transmitted in the WoT environment and in areas such as government data that need protection against attacks. The proposed method comprises three sub-layers: Chaos Keys generation layer, Data encryption layer, and Authentication layer. The proposed method passed all 15 NIST (National Institute of Standards & Technology) tests. The amount of time needed to encrypt and decrypt the proposed method was compared with the original encryption methods for different data sizes and five sensitivity levels, and the proposed encryption method was found to be up to (150%) faster while maintaining security strength.

Keywords: Information Security; AES algorithm; PRESENT algorithm; LEA algorithm; Chaotic System.

1. INTRODUCTION

The IoT encompasses the network of physical devices, such as houses, vehicles, and buildings. These devices communicate through various application interfaces and can connect to the internet to transmit data. However, IoT limitations arise when devices are integrated into one application or system. To address this issue, the concept of WoT was introduced. The WoT involves the interconnection of devices (Things) that can collect, share, and act on data and their connection over a network. This means that WoT is designed to connect anything in the physical world and display it on the WWW, where users can communicate and share data. Furthermore, due to the growing number of devices, WoT uses existing web protocols like HTTP and HTTPS to connect, without necessitating the creation of new, intricate protocols [1, 2].

Because of the openness and sharing of resources in the WoT environment, users have expressed concerns about the future of information security, which is a major issue for the advancement of technology. This means that data and resources must be protected from malicious interference. Encryption techniques have been proposed to overcome privacy and security issues [3, 4]. Figure 1 [5] shows an overview of WoT, which aims to connect billions of devices and generate massive data.

Iraqi Journal for Computers and Informatics
University of Information Technology and Communications
Vol. 51, No. 1, 2025, pp. 94-107
DOI: https://doi.org/10.25195/ijci.v51i1.559
Print ISSN: 2313-190X, Online ISSN: 2520-4912

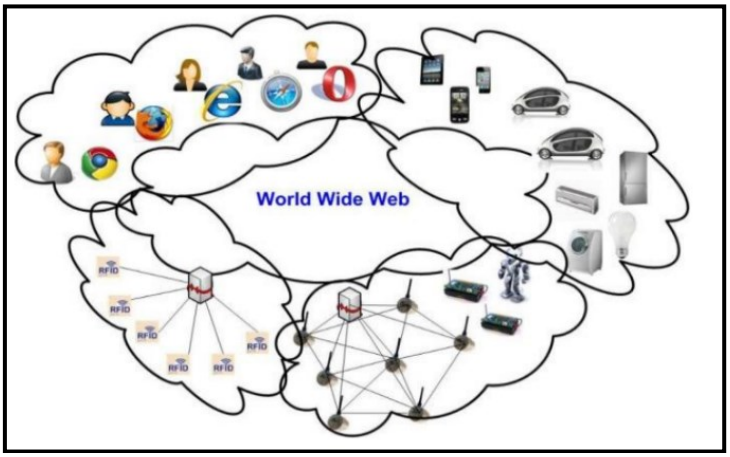


Fig. 1: Overview of Web of Things [5]

The primary goals that represent the heart of information security are called the CIA triad, which is used to protect organizational data. *Confidentiality*, encryption makes data inaccessible without authorization. *Integrity*, to ensure data integrity, you can use data validation, checksums, digital signatures, and regular backups. *Availability*, this ensures that information is available to authorized individuals whenever needed [11]. This paper aims to provide data security and integrity in the WoT environment by using encryption and authentication algorithms to protect data from unauthorized access.

The remainder of this paper is structured as follows: A brief overview of related works is presented in Section 2. The concept of lightweight cryptography algorithms is explained in Section 3. The concept of a chaotic system is explained in Section 4. The methodology of the presented algorithm is described in section 5. The results are presented in Section 6, and the paper is concluded in Section 7.

2. RELATED WORKS

Researchers have explored various cryptographic algorithms and techniques or developed a new hybrid cipher by combining two ciphers or more with the help of chaotic systems to optimize its performance.

- In (2018) Muhammad Asif Habib et al. suggested LEAIoT, an encryption algorithm that combines symmetric and asymmetric key methods using a single key. This approach aims to reduce key generation, encryption, and decryption times, particularly in IoT settings. [6].
- In (2020) Jolan Rokan Naif, et al. provided a security mechanism for the intelligent IoT data sensing cipher system that is lightweight. The PRESENT and SPECK algorithms were modified to create the hybrid HSPA algorithm. The encryption keys generate a new 5-D chaotic system. To ensure integrity, they employed SHA3-256. The encryption algorithm and generated keys pass all of the NIST tests. [7].
- In (2021) Haider K. Hoomod, et al. suggested a hybrid cryptography algorithm for WoT based on SPECK and GOST. It is intended to give users great flexibility and convenience in handling change operations, accelerating encryption processes, and verifying packet integrity messages as soon as they are received. With the highest level of randomness, the suggested algorithm completed all NIST standard tests. [8].
- In (2023) Somaiya, R., et al. proposed the EMAES hybrid encryption method in WoT to encrypt data. Combining the efficiency of MAES in data security with the security of ECC provides a robust public key algorithm that is nearly impossible to crack. This architecture offers several benefits in speed, accuracy, and security [9].
- In (2024) Smita Rath, et al. proposed a hybrid model for file encryption that modifies the traditional AES structure through dynamic rearrangement of operations. Additionally, it incorporates a masked key management mechanism using the RSA algorithm. This model offers a more secure method for protecting sensitive data [10].

3. LIGHTWEIGHT CRYPTOGRAPHY LWC

Many resource-constrained devices, like RFIDs and sensors, are compact; they generally have limited resources. LWC can help overcome the challenges faced by these devices. Designing LWC algorithms requires balancing security, cost, and performance [12]. LWC algorithms are categorized into two types based on key usage. Symmetric algorithms utilize the same key for both encryption and decryption, while asymmetric algorithms employ one key for encryption and a different key for decryption. Symmetric algorithms provide confidentiality, integrity, and

Iraqi Journal for Computers and Informatics
University of Information Technology and Communications
Vol. 51, No. 1, 2025, pp. 94-107
DOI: https://doi.org/10.25195/ijci.v51i1.559
Print ISSN: 2313-190X, Online ISSN: 2520-4912

authentication. Symmetric algorithms are classified into block ciphers and stream ciphers, depending on how they process plaintext. Additionally, hash functions fall into a different category within symmetric algorithms. Figure 2 shows the classification of LWC algorithms [13].

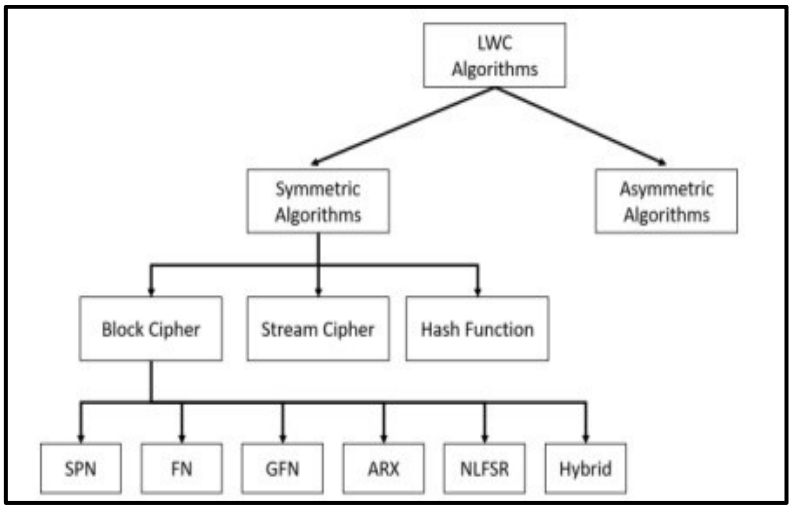


Fig. 2: Classification of LWC [13]

The primary objective of this paper is to develop a model to safeguard data. The hybrid of the AES and LEA forms the basis of this model to benefit from both of their features. The hybrid encryption algorithm is a high encryption security, and the P-layer of the PRESENT algorithm is used to enhance the AES algorithm to be suitable for the WoT environment.

❖ AES

AES is a symmetric block cipher chosen by NIST as a standard to replace the DES. The block size has been fixed at 128 bits with the key sizes 128 bits, 192 bits, and 256 bits. The number of rounds set with the respective key size is 10, 12, and 14 for the 128 bits, 192 bits, and 256 bits, respectively**.** This algorithm consists of the following operations in the encryption process [14]:

a) Key Expansion: This is an algorithm utilized for deriving the 128-bit round key for each round from the original 128-bit cipher key.
b) First Round: This initial round key addition (AddRoundKey) uses XOR with plaintext (state)**.**
c) Rounds: This is an internal structure of AES consisting of four basic transformations: *SubBytes, ShiftRows, MixColumns,* and *AddRoundKey***.**
d) Final round: The MixColumn step was not performed in this round but all other rounds are identical.

The decryption process is similar to the encryption process, but the steps are carried out differently [15].

❖ PRESENT

PRESENT is a symmetric block cipher introduced by A. Bogdanov et al. in 2007 for meeting the requirements of lightweight and ultra-lightweight cipher. It uses a 64-bit block length with a key length that supports two key lengths either 80 or 128-bit. It performs the input (plaintext) through 31 rounds; each round has one S-box layer, one P-Layer, and XORed with generated Keys. At the end of the algorithm operations, is XORed with the last generated key to produce the output (cipher text)**.** In 2017, the standardization of the PRESENT algorithm was noted at ISO/IEC 29192 [16].

❖ LEA

LEA is a symmetric block cipher designed by Deukjo Hong, et al**.** in Korea in 2013. LEA uses a block length of 128 bits, consisting of four 32-bit words. It employs only ARX operations (addition, rotation, and XOR). Key sizes are 128, 192, and 256 bits. The number of rounds is 24, 28, and 32 related to Key sizes [17] and its contains [18]:

A. ***Key Schedule***: Generates a sequence of 192-bit round keys at each round using *delta* several constant values defined in Table 1.
B. ***Round Function Computation***: Consists of:
- ***Initialization***: Intermediate variables are initialized with plaintext.

Iraqi Journal for Computers and Informatics
University of Information Technology and Communications
Vol. 51, No. 1, 2025, pp. 94-107
DOI: https://doi.org/10.25195/ijci.v51i1.559
Print ISSN: 2313-190X, Online ISSN: 2520-4912

- ***Iterating Rounds***: The number of iterations consisting of ARX operations is computed, and the final round function of LEA is identical to the other round functions**.**
- ***Finalization***: Producing the cipher text.

TABLE I. CONSISTENT KEY VALUES AND ROTATED CONSTANT KEY VALUES.

Constant Keys	Original value (δ)	Rotated value (δ^*)
δ [0]	0xc3efe9db	0xc3efe9db
δ [1]	0x44626b02	0x88c4d604
δ [2]	0x79e27c8a	0xe789f229
δ [3]	0x78df30ec	0xc6f98763
δ [4]	0x715ea49e	0x15ea49e7
δ [5]	0xc785da0a	0xf0bb4158
δ [6]	0xe04ef22a	0x13bc8ab8
δ [7]	0xe5c40957	0xe204abf2

Here, the original constant key values are represented by δ= (δ[0] to δ[7]; (each 32-bit), while the rotated constant key values are indicated by δ^*= (δ^*[0] to δ^*[7]; (each 32-bit), which minimizes the number of rotations during computation.

4. CHAOTIC SYSTEM

A complex, nonlinear dynamic system that is sensitive to its initial conditions is called a chaotic system. The theory of nonlinear systems has recently been applied to encryption to increase security. The chaotic system generates radically different keys when the initial states change slightly. Because of its intricate behavior, the chaotic system was attractive for use in cryptography systems and for the generation of pseudo-random keys [21]. Because chaotic systems are based on non-linear behavior, they are a strong contender for many encryption systems. Chaotic cryptography is a hybrid of chaos theory and cryptography. The dynamic role of chaos theory in enhancing cryptosystem security is demonstrated by the similarities between it and cryptographic techniques, and this includes their sensitivity to changes in parameters, long-term unpredictability, and random behavior [16].

5. THE PROPOSED METHOD

The proposed Hybrid Encryption method includes three phases: the Keys Generation phase, the Data Encryption phase, and the Integrity and Authentication Data phase.

A. The keys Generation stage

To provide high security, encryption now uses randomly generated keys. Consequently, many researchers incorporate chaotic systems into encryption processes for key generation. Therefore, many well-known chaotic systems, such as the logistic, Lorenz, Hanon, Chen, and Cat systems, are used. The 4D-NSJR chaotic system produced the keys used in the suggested hybrid encryption technique, which used mathematical analysis to design Four-dimensional 4D chaos equations. The four chaotic maps as followed in Equation (2.1) represents the chaotic system used in this study.

$$\begin{aligned} xt[i+1] &= xt[i]+yt[i]-b*(s*xt[i]*(1-s*yt[i]*(1-r*zt[i]*(xt[i]-u*kt[i])))) *dt \\ yt[i+1] &= yt[i]-u*xt[i]+(u*s*yt[i]*(1+u*xt[i]*(1-r*kt[i]*(1-s*zt[i])))) *dt \\ zt[i+1] &= zt[i]+(u*zt[i]*(1-u*kt[i]*(1-r*yt[i]*(1+s*xt[i])))) *dt \\ kt[i+1] &= kt[i]+u*kt[i]*(u*zt[i]*(1-u*xt[i]*(1-u*yt[i]))-r*(1+s*xt[i])) *dt \end{aligned} \quad \cdots (2.1)$$

B. Data Encryption stage

Many different modifications were made to the AES algorithm to get the optimal level of security for protecting sensor data in a WoT environment and avoiding different types of attacks. These modifications of AES are to increase the processing complexity of AES with decreased processing time. To improve the randomness of the encrypted results, the first change is to generate the keys using a chaotic key generator 4D-NSJR. To lessen the workload of the multiplications over finite fields GF when using MixColumns, the second change to the AES is to substitute a P-layer based on the P-layer of PRESENT using a chaotic key generator 4D-NSJR. This implies that there will be faster execution times. Using the chaos keys to strengthen the AES and thwart further attacks, this modification repeats three iterations of the original operations. Combining with LEA (with 5 rounds) is the

Iraqi Journal for Computers and Informatics
University of Information Technology and Communications
Vol. 51, No. 1, 2025, pp. 94-107
DOI: https://doi.org/10.25195/ijci.v51i1.559
Print ISSN: 2313-190X, Online ISSN: 2520-4912

third change to the AES (with 5 or 8 rounds). In the last two or five rounds of encryption using the AES algorithm, the LEA algorithm is introduced as the last layer. Initially, the AES algorithm provides the data (plaintext) as input to the LEA algorithm, which splits the plaintext into four segments that are changed every round. Using a chaotic key generator 4D-NSJR, this procedure in the LEA algorithm repeats five iterations in each of the final two or five rounds of the AES algorithm. This change aims to make the AES structure more complex to process, particularly in cases where key generation is chaotic. The total number of rounds for the proposed hybrid AESLEA algorithm is 5 or 8 rounds (but due to the LEA being 5 rounds get total actual rounds is 13 to 28), while the rounds iteration in the original AES is 10 and the rounds iteration in the original LEA is 24 rounds get total rounds is 240 rounds if its constraint as the proposed structure. Figure 3 and Figure 4 show the block diagram of the encryption/decryption of AESLEA Algorithm.

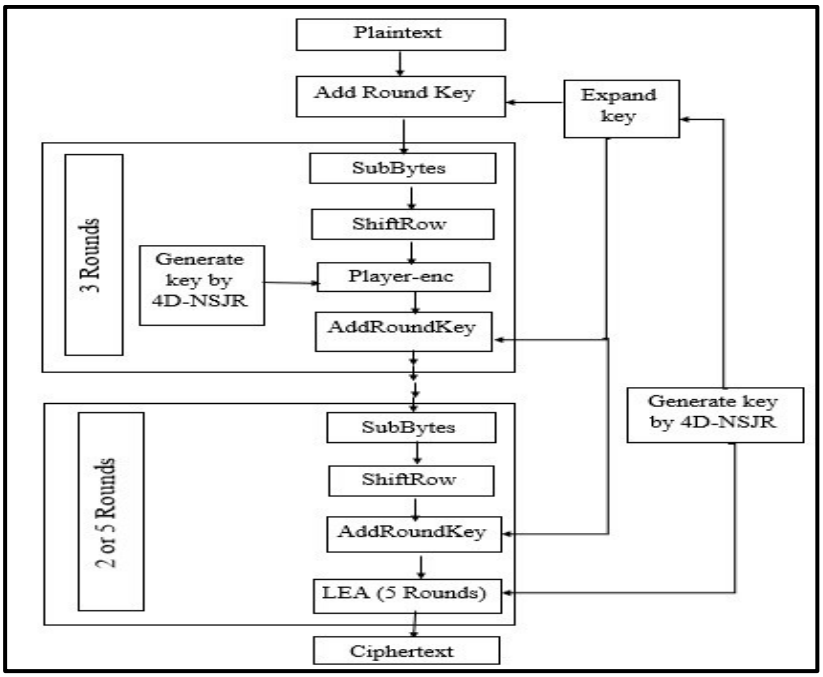


Fig. 3: The encryption of AESLEA Algorithm

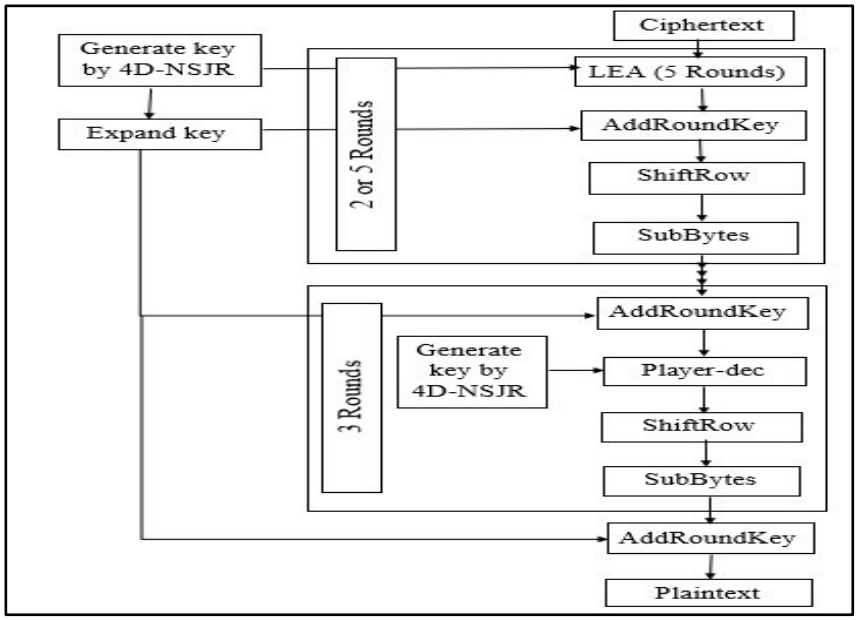


Fig. 4: The decryption of AESLEA Algorithm

Iraqi Journal for Computers and Informatics
University of Information Technology and Communications
Vol. 51, No. 1, 2025, pp. 94-107
DOI: https://doi.org/10.25195/ijci.v51i1.559
Print ISSN: 2313-190X, Online ISSN: 2520-4912

C. Integrity and Authentication Data stage

In this phase of the proposed method, the SHA3-256 algorithm is integrated with the hybrid AESLEA algorithm to form AESLEAH. The hybrid AESLEA algorithm is utilized for encryption and decryption. At the same time, SHA3-256 is employed to calculate the hash value of text files, ensuring the validation of information in the WoT environment. The proposed work AESLEAH is shown in Figure 5 at the sender site and Figure 6 at the receiver site.

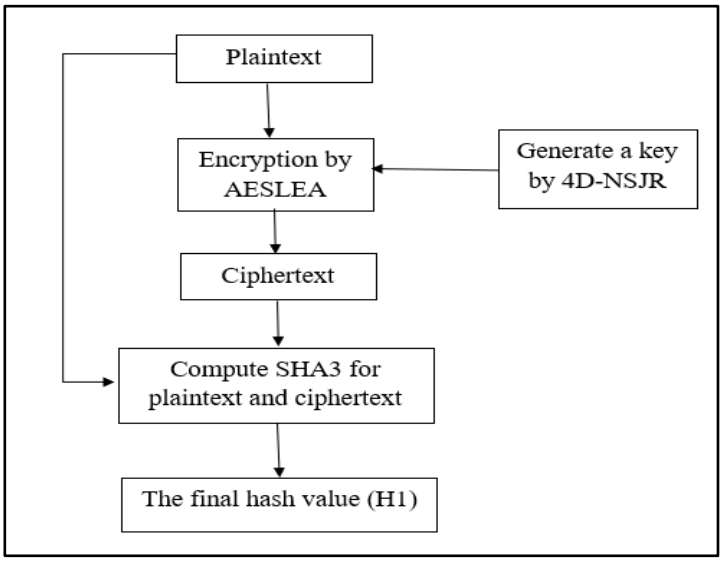


Fig. 5: Block diagram for computing (H1) at the sender's site

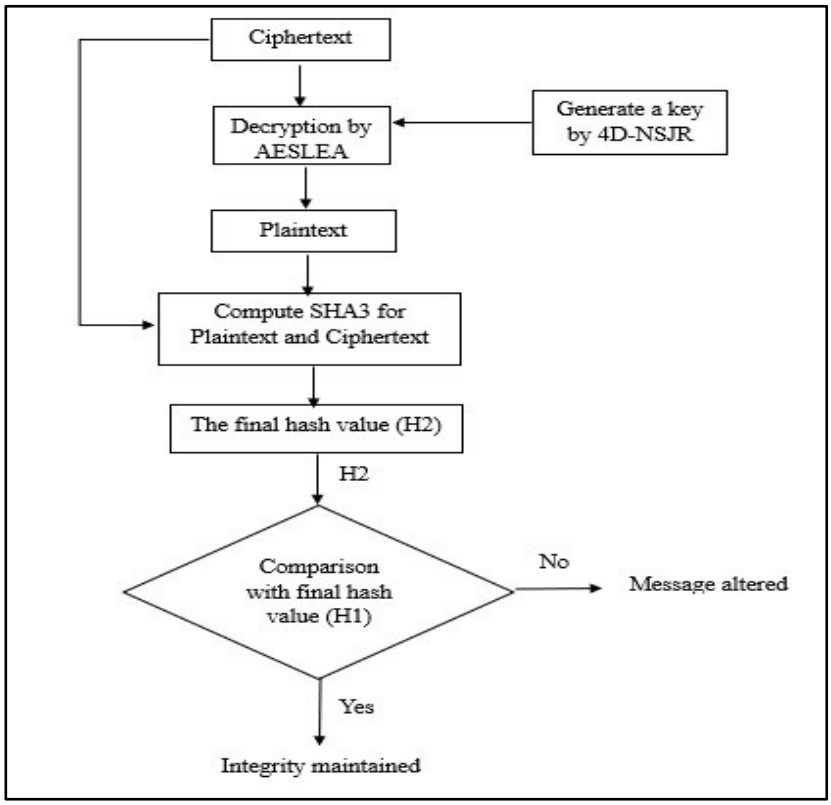


Fig. 6: Block diagram for computing (H2) at the receiver's site

6. IMPLEMENTATION AND RESULTS

Iraqi Journal for Computers and Informatics
University of Information Technology and Communications
Vol. 51, No. 1, 2025, pp. 94-107
DOI: https://doi.org/10.25195/ijci.v51i1.559
Print ISSN: 2313-190X, Online ISSN: 2520-4912

The evaluation criteria for comparing cryptographic algorithms in the WoT environment are thorough and well-defined. These standards address the key aspects of performance and security in cryptographic systems. Table 2 shows the results of AES, LEA, and the proposed new hybrid method based on multiple factors for data namely:

1. **Block Size**: Security is affected (larger blocks are generally more secure) as well as performance.
2. **Cipher Classification**: Ensures that the algorithm conforms to specific requirements and standards based on NIST's classification (e.g., block cipher, stream cipher).
3. **Computational Efficiency**: Measures the efficiency of each algorithm in environments with limited resources, especially in (WoT).
4. **Encryption Time**: Important to understand performance in real-world applications by analyzing the time required for encryption using each algorithm.
5. **Decryption Time**: Important to have timely access to data in the WoT environment and to process it efficiently by assessing the time required for decryption.
6. **Memory Usage:** Evaluates the memory consumption of each algorithm to understand its resource requirements in the WoT environment.
7. **Avalanche Effect**: This is one of the desirable characteristics of any cryptographic algorithm. It explains that any slight change in key or plain text should result in a significant change in the cipher text. The effect ensures that an attacker cannot easily predict a plaintext through a statistical analysis.
8. **Entropy**: Measures the output of algorithms to ensure randomness and unpredictability, which are vital to security. Higher entropy values indicate a higher degree of randomness and unpredictability in encrypted data, which is generally desirable for cryptographic security.

TABLE II. COMPARISON BETWEEN ENCRYPTION ALGORITHMS BASED ON VARIOUS FACTORS USING DATA SIZE OF 1.5 MB.

Factors	The original AES	The original LEA	Hybrid Algorithm
Block Size	128 bits	128 bits	128 bits
Cipher Classification	Block cipher	Block cipher	Block cipher
Encryption time	431.235 msec	265.123 msec	255.275 msec
Decryption time	429.485 msec	281.23 msec	247.885 msec
Memory Used after encryption	1.525 KB	1000 B	1.1 KB
CPU Consumption during encryption	2%	1%	1%
CPU Consumption during decryption	2%	1%	1%
Avalanche Effect	52%	41%	59%
Entropy	7.845	7.275	7.989

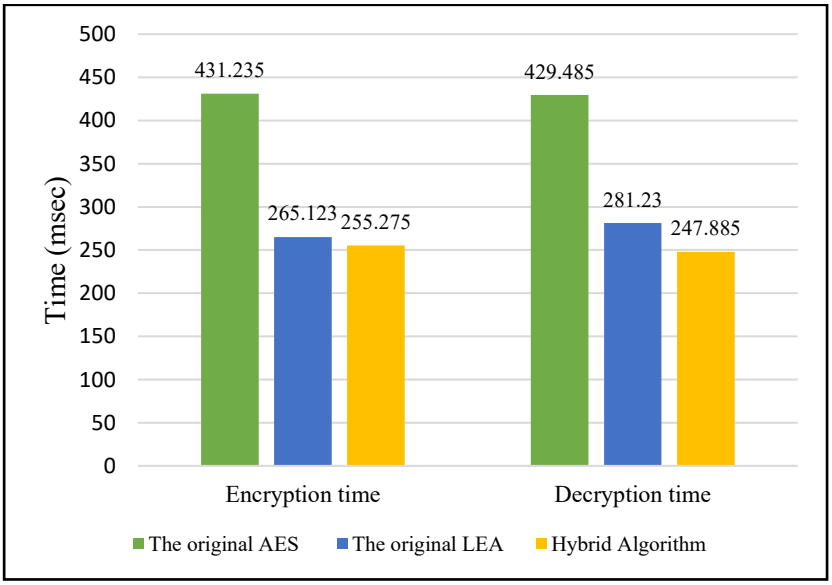


Fig. 7: The comparison of encryption-decryption time for data size 1.5 MB

According to Table 2 and Figure 7, the AESLEA algorithm requires less time for both encryption and decryption processes compared to the original AES and LEA algorithms when processing randomly generated data of 1.5

Iraqi Journal for Computers and Informatics
University of Information Technology and Communications
Vol. 51, No. 1, 2025, pp. 94-107
DOI: https://doi.org/10.25195/ijci.v51i1.559
Print ISSN: 2313-190X, Online ISSN: 2520-4912

megabytes. This indicates that AESLEA outperforms the original algorithms in terms of implementation speed, making it suitable for security operations in the WoT. Table 3 shows the comparison between the suggested method and previous studies for different data sizes for encryption-decryption time. The encryption and decryption times of the proposed method were found to be faster than the methods in previous studies.

TABLE III. COMPARISON BETWEEN THE PROPOSED METHOD AND PREVIOUS STUDIES

The proposed method			The Previous Studies				
Data Size	Encryption Time (msec)	Decryption Time (msec)	Title of Article	The technique Used	Data size	Encryption Time (msec)	Decryption Time (msec)
16 KB	2.895	2.134	[11]	Modified LEA	12.5 KB	210	210
			[18]	Hybrid (ECC, AES)	12.5 KB	510	510
112 KB	25.254	24.788	[11]	Modified LEA	125 KB	386	386
			[12]	Hybrid (AES, ECC)	100 KB	70.4	38.8
			[17]	Hybrid (AES, ElGamal)	465 KB	1525.2	1419.8
			[20]	Hybrid (AES, RSA)	176.25 KB	9621.16	13493.83
500 KB	89.127	87.548	----		----	----	----
1 MB	195.749	192.556	[18]	Hybrid (ECC, AES)	1 MB	1780	1860
1.5 MB	255.275	247.885	----	----	----	----	----

i. KEY SUITABILITY FOR WoT

The NSJR key map was selected because it is based on the Lorenz system. It features a large key space, providing strong protection against brute-force attacks. The NSJR sequence has high entropy, which ensures the generation of strong and unpredictable keys. Additionally, it possesses good statistical properties, making the keys closely resemble true randomness. The sequence is also sensitive to initial conditions, further enhancing key security.

ii. PERFORMANCE EVALUATION

Assessing the proposed encryption method is crucial as it improves resource management, lowers costs, and enhances performance in the WoT environment. Table 4 demonstrates the evaluation of the proposed method's performance for various data sizes and four sensitivity levels. The proposed method consumes a small size of memory and the CPU consumption is low. The larger the avalanche effect, the more likely it is that an attacker cannot easily predict the plaintext. Higher entropy values (the upper limit is 8) indicate a higher degree of randomness and unpredictability in the encrypted data, which is generally desirable for cryptographic security.

TABLE IV. ASSESSMENT OF THE PROPOSED METHOD'S PERFORMANCE ACROSS DIFFERENT DATA SIZES.

Data Size	Encryption Time (msec)	Decryption Time (msec)	Memory Usage (KB)	Consumption of CPU (%)	Avalanche Effect (%)	Entropy
16 KB	2.895	2.134	1.0	0.1	59	7.985
112 KB	25.254	24.788	1.0	0.91	58	7.988
500 KB	89.127	87.548	1.0	1.0	60	7.987
1 MB	195.749	192.556	1.1	1.0	61	7.989
1.5 MB	255.275	247.885	1.1	1.0	59	7.989

iii. CRYPTOGRAPHY ANALYSIS

Iraqi Journal for Computers and Informatics
University of Information Technology and Communications
Vol. 51, No. 1, 2025, pp. 94-107
DOI: https://doi.org/10.25195/ijci.v51i1.559
Print ISSN: 2313-190X, Online ISSN: 2520-4912

Various methods are used to evaluate the robustness of cryptographic algorithms, including correlation coefficient analysis CCA, Hamming distance analysis, entropy analysis, throughput analysis, mean absolute error MAE, and NIST randomness tests. The following sections will explain these methods with iteration rounds 8.

- **CORRELATION COEFFICIENT ANALYSIS**: The CCA measures the relationship between plain text and encrypted text., the encrypted text and plain text must be completely different. This analysis shows the extent to which the proposed encryption algorithm is resistant to statistical attacks. Table 5 and Figure 8 show a comparison of the correlation analysis for the encrypted text using the original AES algorithm, the original LEA algorithm, and the proposed method. It is obvious that the encrypted text using the proposed encryption method is highly uncorrelated (near to zero) and the proposed method is safe.

TABLE V. CCA OF ENCRYPTED TEXT FOR 8 ITERATION ROUNDS

Data Size (kB)	original AES	original LEA	Hybrid Algorithm
16	0.147	0.455	0.110
112	0.245	0.474	0.091
1552	0.401	0.444	0.090

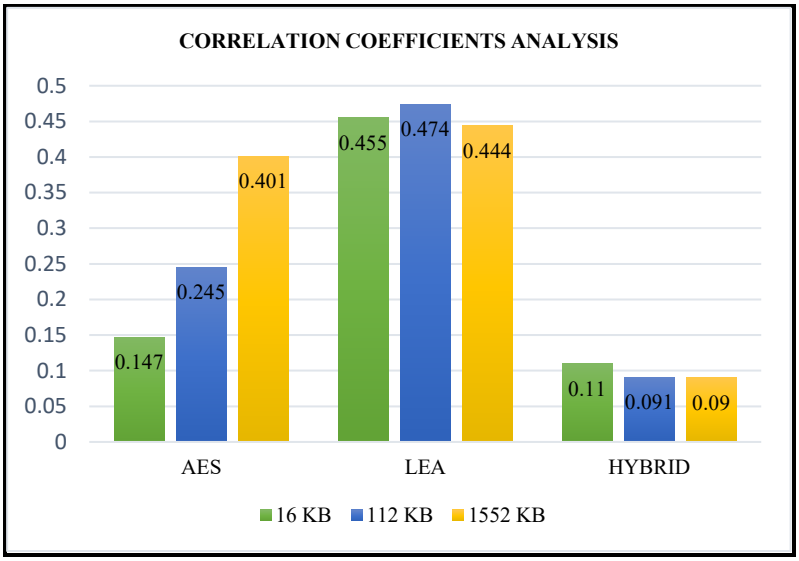


Fig. 8: The CCA results of the Proposed Hybrid Method

- **HAMMING DISTANCE ANALYSIS:** This test measures the difference between the plaintext and cipher text generated by the proposed method, to increase the sensitivity of cryptographic keys. A small Hamming distance value indicates a high degree of similarity, while a high value signifies low similarity. The results presented in Table 6 and Figure 9 demonstrate that the Hamming distance of the proposed algorithm is secure and effectively resists statistical attacks when the data size exceeds that of the original algorithms.

TABLE VI. HAMMING DISTANCE ANALYSIS RESULTS OF ENCRYPTED TEXT IN 8 ROUNDS

Data Size (KB)	original AES	original LEA	Hybrid Algorithm
16	51.11%	54.01%	40.45%
112	50.21%	53.74%	41.23%
1552	50.75%	52.79%	41.10%

Iraqi Journal for Computers and Informatics
University of Information Technology and Communications
Vol. 51, No. 1, 2025, pp. 94-107
DOI: https://doi.org/10.25195/ijci.v51i1.559
Print ISSN: 2313-190X, Online ISSN: 2520-4912

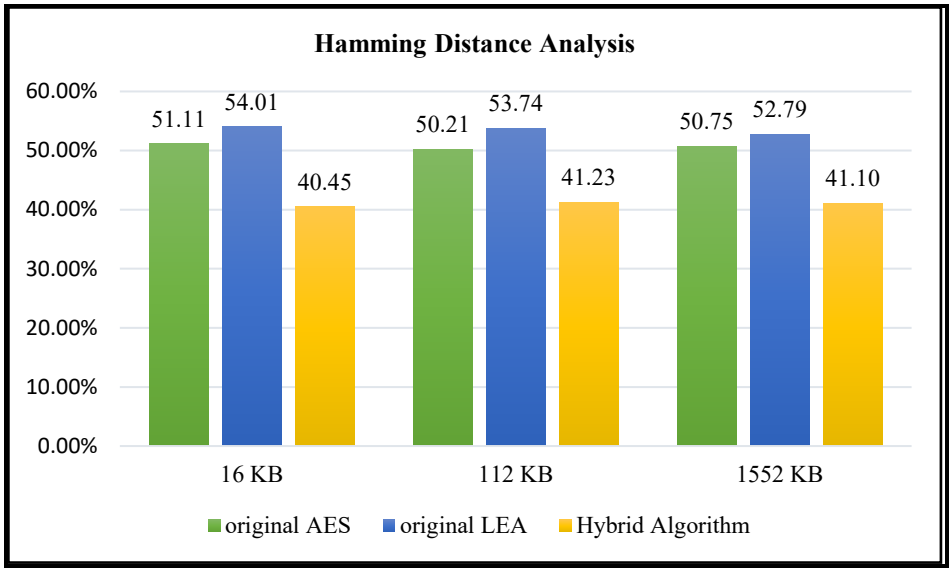
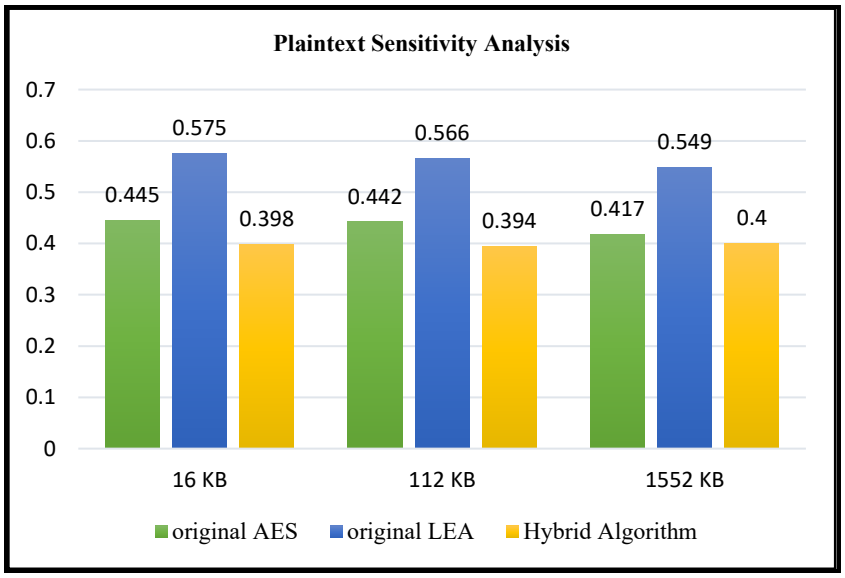


Fig. 9: Hamming distance analysis results of encrypted text

- **PLAINTEXT SENSITIVITY ANALYSIS:** This test can be used to prove the security of the suggested encryption algorithm. The level of sensitivity to changes is measured by a type of plaintext sensitivity analysis called the Mean Absolute Error MAE which calculates the average error per unit of change within a given data set. The higher the MAE, the more secure the text. Table 7 and Figure 10 show the MAE comparison among the original AES, the original LEA, and the proposed algorithm. The results of this analysis prove that the MAE of the suggested algorithm is less than the MAE of the original algorithm, which proves the proposed algorithms are better at security.

TABLE VII. MAE RESULTS OF PROPOSED ENCRYPTION ALGORITHM FOR 8 ROUNDS

Data Size (KB)	original AES	original LEA	Hybrid Algorithm
16	0.445	0.575	0.398
112	0.442	0.566	0.394
1552	0.417	0.549	0.400



Iraqi Journal for Computers and Informatics
University of Information Technology and Communications
Vol. 51, No. 1, 2025, pp. 94-107
DOI: https://doi.org/10.25195/ijci.v51i1.559
Print ISSN: 2313-190X, Online ISSN: 2520-4912

Fig. 10: The plaintext sensitivity Analysis Results of the Proposed method

- **ENTROPY ANALYSIS:** Utilizes entropy to generate random numbers that create security keys for safeguarding sensitive information. The effectiveness of the key's security relies on the quality of the random number generation. Table 9 and Figure 11 show the entropy comparison among the original AES, the original LEA, and the suggested algorithm. This concludes that the entropy of encoded text of the proposed encryption algorithm is nearer to the idyllic value, which is 8, and the suggested algorithm demonstrates a higher level of safety.

TABLE VIII. ENTROPY RESULTS OF ENCRYPTED TEXTS FOR 8 ROUNDS

Data Size (KB)	original AES	original LEA	Hybrid Algorithm
16	7.832	7.261	7.989
112	7.839	7.259	7.987
1552	7.845	7.275	7.988

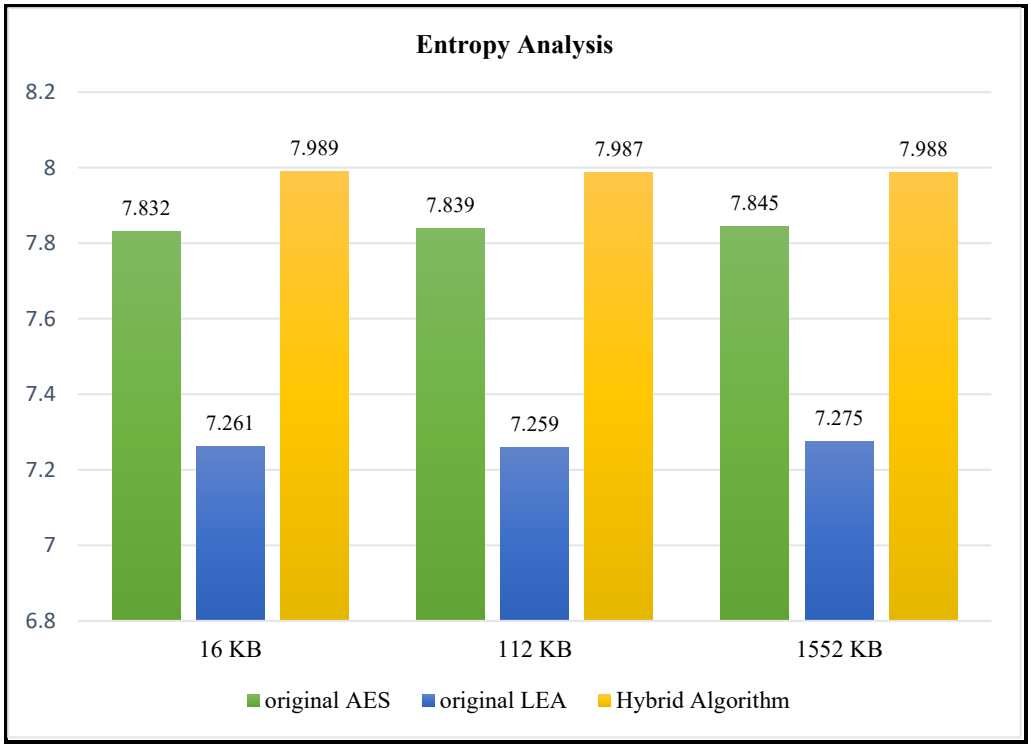


Fig. 11: The Entropy Analysis Results of the Proposed Method

- **Throughput Analysis:** Refers to the quantity of data that the encryption will handle. It is a critical element in determining the algorithm's performance in terms of execution time. It records the number of bytes per millisecond that the digital system executes. Table 10, and Figure 12 show the throughput comparison among the original AES, the original LEA, and the suggested algorithms. It concludes that the suggested encryption algorithm has a higher throughput than the original algorithms in different data sizes.

TABLE IX. THROUGHPUT RESULTS OF ENCRYPTED TEXTS FOR 8 ROUNDS

Data Size (KB)	Original AES KB/s	Original LEA KB/s	Hybrid Algorithm KB/s
16	5.8	6.45	7.85
112	4.01	4.41	4.95
1552	3.75	4.80	5.80

Iraqi Journal for Computers and Informatics
University of Information Technology and Communications
Vol. 51, No. 1, 2025, pp. 94-107
DOI: https://doi.org/10.25195/ijci.v51i1.559
Print ISSN: 2313-190X, Online ISSN: 2520-4912

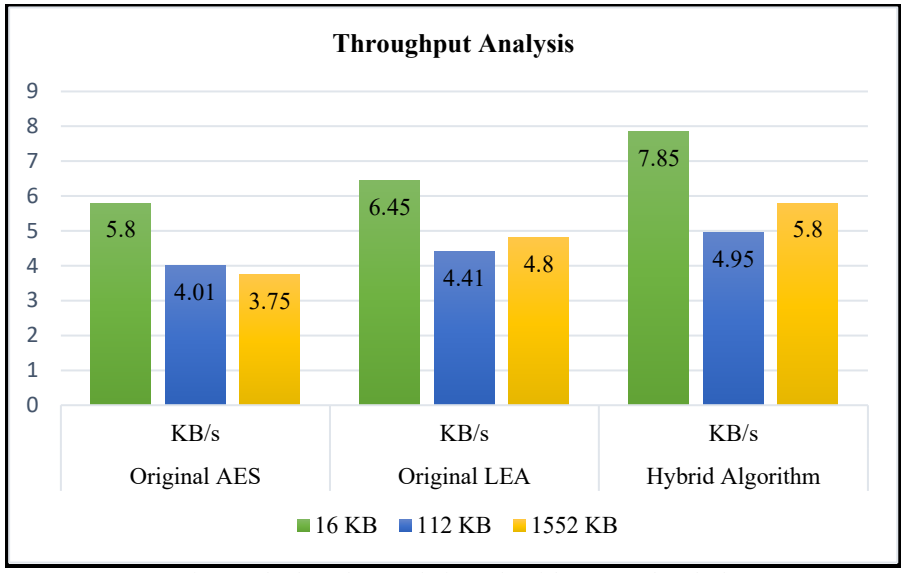


Fig. 12: The throughput analysis results of the proposed method

- **EVALUATION OF SECURITY:** To evaluate the randomness of an encryption algorithm's output, fifteen tests can be applied. This evaluation helps determine its suitability for providing secure and indistinguishable encryption. A P-value of 0.01 or higher indicates that the sequence can be considered random with a 99% confidence level. Conversely, if the P-value is less than 0.01, the sequence is not regarded as random, and the test fails. Due to modification in the AES algorithm structure, therefore AESLEA is passed in all NIST tests in 8 rounds using Chaos keys in each round. Table 11, displays the results of the NIST test.

TABLE X. NIST TEST RESULTS OF THE HYBRID AESLEA

Names of NIST Statistical Tests Results	Original AES	Original LEA	AESLEA (8 Rounds)
Frequency (Monobit) Test	0.2556	0.11280	0.54110
Frequency Within Block Test	0.2667	0.3089	0.4980
Runs Test	0.46517	0.46517	0.76640
Longest Run Ones in a Block Test	0.35531	0.1289	0.64059
Binary Matrix Rank Test	0.46737	0.3658	0.74432
Discrete Fourier Transform (DFT)Test	0.47681	0.2895	0.50899
Non-Overlapping Template Matching Test	0.43297	0.3332	0.55409
Overlapping Template Matching Test	0.76177	0.6590	0.89786
Maurer's Universal Test	0.461756	0.3876	0.96057
Linear Complexity Test	0.511297	0.2970	0.88870
Serial Test	0.366581	0.1109	0.74330
Approximate Entropy Test	0.16674	0.0765	0.43590
Cumulative Sums Test	0.11809	0.04556	0.38970
Random Excursion Test	0.59219	0.1775	0.97291
Random Excursion Variant Test	0.35055	0.0453	0.75983

Iraqi Journal for Computers and Informatics
University of Information Technology and Communications
Vol. 51, No. 1, 2025, pp. 94-107
DOI: https://doi.org/10.25195/ijci.v51i1.559
Print ISSN: 2313-190X, Online ISSN: 2520-4912

7. AUTHENTICATION

The WoT security method at this stage involves the hybrid AESLEAH algorithm. Therefore, after the data is encrypted using the AESLEA algorithm, the SHA3-256 algorithm is performed to produce the final hash to add more randomness while generating the final 256-bit hash. This means that if one character in the plaintext is changed, many or all characters in the cipher text will also be changed. The result of AESLEAH is shown in Table 12.

TABLE XI. COMPARATIVE AUTHENTICATION TIME

Data size (kB)	The original SHA3 time	The proposed AESLEAH time
16	0.451	0.375
112	1.702	1.046
1552	18.230	14.856

8. CONCLUSIONS

The proposed method demonstrated significantly faster encryption and decryption times compared to the traditional AES algorithm, as illustrated in Table 2, which is still strong in terms of security, and NIST tests prove this. Utilizing a chaotic system 4D-NSJR for key generation and in the P-layer generation resulted in enhanced randomness and unexpected outputs, which also boosted the robustness of the proposed method. After hybridization, the AES algorithm became more suitable for the WoT environment. The proposed authentication and integrity data mechanism (Hybrid SHA3-AESLEA) is designed to enhance the integrity of sensitive information during transmission over the network and to ensure that it is received from an authorized body .The encryption and decryption times of the proposed method were faster than those in previous studies, as illustrated in Table 3.

References

[1] Laaychi, A., Tanana, M., & Lazaar, S. (2022). Security issues of the Web of Things: challenges and solutions In *E3S Web of Conferences* (Vol. 351, p. 01013). EDP Sciences.

[2] Faheem, M.R., Anees,T., and Hussain, M. (2019). The web of things: findability taxonomy and challenges. *IEEE Access*, *7*, 185028-185041. Hassan, Baraa M. (2021) ، *Web of Things Data Security Based on Hybrid Gost-Speck Algorithms in Health Care*. Master Thesis, Informatics Institute for Postgraduate Studies \ Iraqi Commission for Computers and Informatics.

[3] Hoomod, H. K., Naif, J.R. & Ahmed, I. S. (2021), "A Hybrid Cryptography Algorithm for WoT based on Gost and Speck." *International Journal of Advances in Engineering and Management (IJAEM).*

[4] Sardar, R., & Anees, T. (2021). Web of things: security challenges and mechanisms. *IEEE Access*, *9*, 31695-31711.

[5] Habib, M. Asif, et al. (2018),"Speeding up the internet of things: Leaiot: A lightweight encryption algorithm toward low-latency communication for the internet of things." *IEEE Consumer Electronics Magazine* 7.6: 31-37.

[6] Hoomod, H. K.,Naif, J. R., & Ahmed, I. S. (2020). "A new intelligent hybrid encryption algorithm for IoT data based on modified PRESENT-SPECK and novel 5D chaotic system". *Periodicals of* Engineering and Natural Sciences, 8(4), 2333-2345.

[7] Hoomod, H. K., Naif, J.R. & Ahmed, I. S. (2021), "A Hybrid Cryptography Algorithm for WoT based on Gost and Speck." *International Journal of Advances in Engineering and Management (IJAEM).*

[8] Somaiya, R., Gonsai, A., & Tanna, R. (2023). Implementation and evaluation of EMAES–A hybrid encryption algorithm for sharing multimedia files with more security and speed. *International journal of electrical and computer engineering systems*, *14*(4), 401-409.

[9] Smita, R., Sushree, B. P., Deepak, K. P., Prabhat, K. S., Nibedita, J., Monalisa, P., Narayan, P., & Sipra, S.(2024). AES-RSA: An Innovative Hybrid Security Framework for File Authentication,

Iraqi Journal for Computers and Informatics
University of Information Technology and Communications
Vol. 51, No. 1, 2025, pp. 94-107
DOI: https://doi.org/10.25195/ijci.v51i1.559
Print ISSN: 2313-190X, Online ISSN: 2520-4912

Integrity, and Data Secrecy Model. INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING, (ijisae) 12(18s), 303–312.

[10] Death, D., (2023), *Information Security Handbook*, Packet Publishing Ltd, Birmingham.

[11] Thakor, V. A., Razzaque, M. A., & Khandaker, M. R. (2021). Lightweight cryptography algorithms for resource-constrained IoT devices: A review, comparison and research opportunities. IEEE Access, 9, 28177-28193.

[12] Suryateja, P. S., & Rao, K. V. (2024). A Survey on Lightweight Cryptographic Algorithms in IoT. Cybernetics and Information Technologies, 24(1).

[13] Su, N., Zhang, Y., & Li, M. (2019, March). Research on data encryption standard based on AES algorithm in internet of things environment. In *2019 IEEE 3rd Information Technology, Networking, Electronic and Automation Control Conference (ITNEC)* (pp. 2071-2075). IEEE.

[14] Wadday, G., et al. (2018), "Study of WiMAX based communication channel effects on the ciphered image using MAES algorithm." *International Journal of Applied Engineering Research* 13.8: 6009-6018.

[15] Naser, N. M., & Naif, J. R.(2022). NEW ULTRA-LIGHTWEIGHT IoT ENCRYPTION ALGORITHM USING NOVEL CHAOTIC SYSTEM. Int. J. Tech. Phys. Probl. Eng, 14(4), 253-259.

[16] Hong, Deukjo, et al. (2014), "LEA: A 128-bit block cipher for fast encryption on common processors."
Information Security Applications: 14th International Workshop, WISA 2013, Jeju Island, Korea, August 19-21, 2013, Revised Selected Papers 14. Springer International Publishing.

[17] Mishra, Zeesha, Pallab Kumar Nath, and Bibhudendra Acharya. (2020), "High throughput unified architecture of LEA algorithm for image encryption." *Microprocessors and Microsystems* 78: 103214.

[18] Kubba, Zaid M. Jawad, and Haider K. Hoomod. (2019), "A hybrid modified lightweight algorithm combined of two cryptography algorithms PRESENT and Salsa20 using chaotic system." *2019 First International Conference of Computer and Applied Sciences (CAS). IEEE.*