ENHANCING SECURITY IN IOT DEVICES: A LIGHTWEIGHT HYBRID CRYPTOGRAPHIC SYSTEM (LCS) APPROACH

AMITA SHAH[1], SANJAY SHAH[2], DHAVAL PARIKH[3], NAMIT SHAH[4]

•

[1]Ph.D Scholar, Computer/IT Engineering, Gujarat Technological University, Gujarat, India
amitashah@ldce.ac.in
[2]Professor & Head, Computer Engineering Dept., Government Engineering College, Rajkot, Gujarat, India. sanjay_shah_r@yahoo.com
[3]Professor & Head, Computer Engineering Dept., Government Engineering College, G'nagar, Gujarat, India. daparikh@gecg28.ac.in
[4]Student, Computer Engineering Dept., L D College of Engineering, Ahmedabad, Gujarat, India. namitvshah@gmail.com

Abstract

The escalating connectivity of devices in the Internet of Things (IoT) era necessitates robust security measures while accommodating resource constraints. Lightweight cryptography addresses this need, focusing on algorithm development for devices with limited resources. This research proposes the Lightweight Crypto System (LCS) as a hybrid cryptosystem, integrating the Lightweight Symmetric Algorithm (LSA) and the Lightweight Hash Algorithm (LHA). LSA is a modified AES-128 variant, enhancing data confidentiality, while LHA, derived from SHA-256, verifies data integrity. The study evaluates the proposed LCS on criteria such as execution time, memory usage, avalanche effect, collision resistance, and entropy, emphasizing the optimal balance between performance and security achieved byLSA and LHA. The findings position LCS as a compelling solution for securing IoT devices without compromising on stringent security requirements.

Keywords: Internet of Things (IoT), Lightweight Cryptography, Hybrid Cryptosystems, LSA, LHA, Security.

1. Introduction

The Internet of Things (IoT) integration poses security challenges [1]. With threats like unauthorized access and data breaches, secure communication is vital. Our research introduces Lightweight Crypto System (LCS) as an adaptable solution [2], enhancing IoT security. It safeguards user privacy and ensures data integrity in the interconnected IoT landscape [3, 4].

The Lightweight Crypto System (LCS) is a breakthrough in IoT security, tailored for resource-constrained devices [5, 6, 7]. Comprising three key elements, it forms a comprehensive security framework. The Lightweight Symmetric Algorithm (LSA), a modified AES-128, ensures efficientsymmetric encryption for data confidentiality [8]. Elliptic Curve Cryptography (ECC) facilitates secure key exchange and authentication [9]. Additionally, the Lightweight Hash

Algorithm (LHA) enhances data integrity verification in the LCS system. Together, these components provide robust solutions for confidentiality, authenticity, access control, and data integrity in IoT communication.LCS's effectiveness stems from the collaboration of its three components: LSA ensures data confidentiality with a tailored version of AES-128 for IoT constraints, ECC facilitates secure key exchange, and the proposed LHA enhances data integrity verification. This integration positions LCS as a versatile solution addressing the complex security demands of the evolving IoT landscape.

1.1. Motivation and Contribution

This research is driven by the growing IoT landscape and the security challenges it poses. With the surge in connected devices, addressing security concerns becomes crucial. The motivation stems from the need to enhance IoT security infrastructure due to escalating concerns about data privacy and integrity. This research aims to provide innovative cryptographic solutions tailored for resource-constrained IoT devices, bridging the gap between security and performance. The major contribution is the exploration of a LCS ensuring efficient and secure communication in the interconnected IoT landscape.

- Lightweight Crypto System (LCS): Introduction of a specialized hybrid cryptosystem tailored for IoT environments, providing a comprehensive security solution for resource- constrained devices [11].
- Lightweight Symmetric Algorithm (LSA): Development and implementation of LSA, a modified AES-128 algorithm optimized for IoT devices, ensuring efficient and secure data confidentiality [8].
- Lightweight Hash Algorithm (LHA): Proposal and implementation of LHA, a novel lightweight hash algorithm designed for data integrity verification in resource-constrained IoT devices, striking a balance between security and performance [12].
- Performance and Security Parameter Analysis: Rigorous evaluation of LCS through performance metrics and key security parameters, including execution time, memory usage, avalanche effect, collision resistance, and entropy, offering insights into the system's robust- ness and efficiency.
- Real-world Testbed Implementation: Practical validation of LCS on an IoT testbed using ESP32 hardware, demonstrating its effectiveness in real-world IoT scenarios and providing a foundation for further optimization of cryptographic processes in IoT environments.

2. Related Work

IoT security literature investigates cryptographic methods due to the growing impact of IoT in daily life, especially in critical areas like smart homes and healthcare. The resource constraints of IoT devices necessitate lightweight and energy-efficient security solutions, posing a challenge to widespread adoption. Recent research explores the potential benefits of integrating lightweight blockchain technology, emphasizing the role of hashing in constructing a robust blockchain structure for enhanced IoT security [13]. This study evaluates various hash techniques on a Raspberry Pi device, providing quantitative insights into the performance of hash functions for lightweight blockchain-based IoT applications [13].

The IoT's growth introduces security challenges for embedded devices [14]. A solution proposes using MD5, a hashing algorithm, to enhance IoT security, fortifying embedded devices against internet-based attacks [14]. This approach seamlessly integrates with the IoT framework and is endorsed for securing embedded systems in IoT [14].

The study in [15] tackles the lack of reliable hybrid cryptosystems for securing critical IoT devices. It explores lightweight encryption algorithms such as TEA, XTEA, XXTEA, RSA, and ECC, aiming for optimal security in constrained environments. The proposed hybrid cryptosystem, incorporating chaotic theory for key generation, outperforms RSA and XXTEA by 40%, showcasing enhanced security and superior performance for safeguarding IoT devices [15].

In [16], the paper underscores the crucial role of cryptography in data security, introducing the Secure Hash Algorithm-3 (SHA-3) for data verification. Implementing a low-power technique, latch-based clock gating, enhances power efficiency in SHA-3 algorithm designs [16].

In [17], the paper recognizes the pivotal role of wireless sensor networks (WSNs) in collecting and transmitting sensitive information. It addresses challenges in WSN infrastructure design due to resource limitations and emphasizes the need for efficient authentication solutions. The proposed 2AMD-160, a Secure Hash Algorithm, outperforms MD5 and SHA1 in both execution time and security in comparative analysis [17].

The IoT’s global connectivity introduces security challenges, requiring energy-efficient solutions. Existing methods compromise between security and energy consumption [18] proposes a BLAKE2b-based authentication with modified ECDSA, demonstrating improved signature times on Raspberry Pi-3. The scheme exhibits resistance to attacks, suitable for resource-constrained IoT devices.

In [23], the paper shows how message-level security instead of transport level security is used to provide end-to-end secure communication between IoT devices and Gateway. Various symmetric and asymmetric security algorithms along with different data formats such as XML, JSON and EXI are executed and compared. Used Blowfish encryption algorithm for IoTSyS framework[23].

3. Proposed Methodology

In addressing the escalating security concerns associated with the ever-expanding Internet of Things (IoT) ecosystem, we introduce a comprehensive Lightweight Crypto System (LCS) that harmoniously integrates three key cryptographic components: “MyLightSymAlgo" (LSA), Elliptic Curve Cryptography (ECC), and the novel “MyLightHashAlgo" (LHA). This section gives detail description for each of the components. The architecture for proposed hybrid model (LCS) sender side and receiver side execution approach is presented in Figure 1 and 2, respectively.

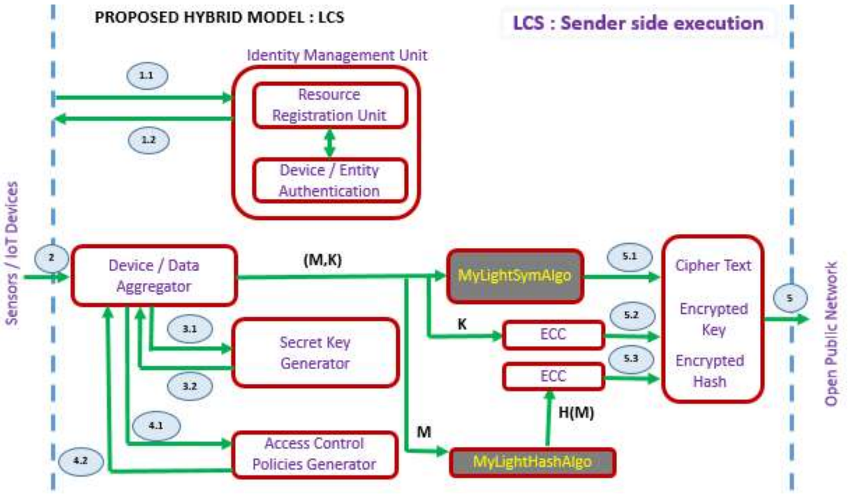

Figure 1: *Proposed Hybrid Model (LCS) (Sender Side Execution)*

The sequential execution flow of the proposed approach is illustrated in Figure 3. The detail explanation for each component for proposed hybrid model (LCS) is presented below.

3.1 MyLightSymAlgo (LSA): Lightweight Symmetric Encryption

LSA, a key element of the proposed LCS, is a tailored variant of AES-128, designed to address security requirements in resource-constrained IoT devices by introducing efficiency-enhancing modifications and replacements [8].

- Algorithmic Modifications: LSA undergoes meticulous changes within AES-128 to create a lightweight encryption process for IoT devices, considering constraints like limited processing power and memory.
- Enhanced Encryption/Decryption: The final LSA version shows notable improvements over AES-128, excelling in both encryption and decryption for faster data transformation, crucial for real-time processing in IoT.

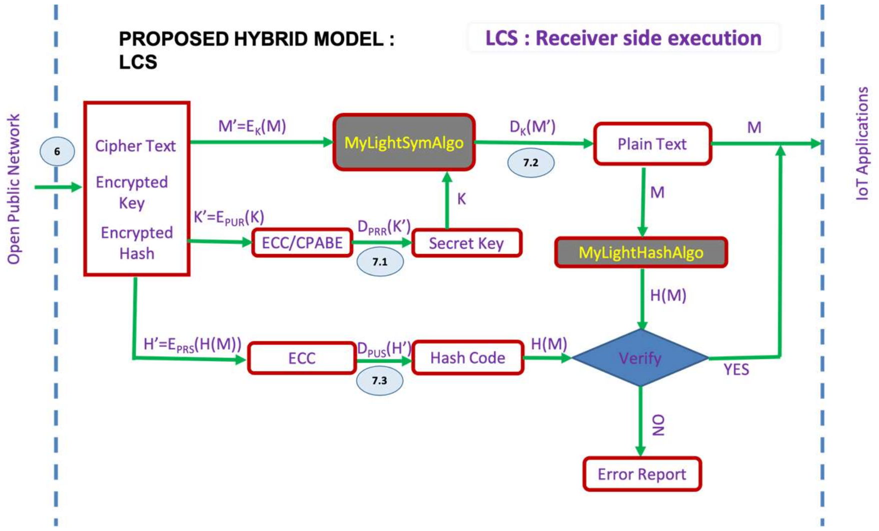

Figure 2: *Proposed Hybrid Model (LCS) (Receiver Side Execution)*

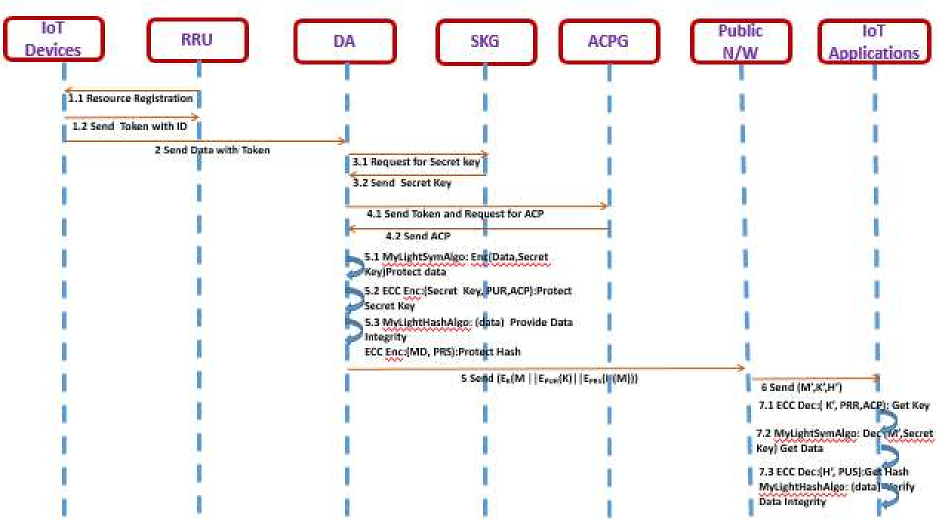
IoT Devices
RRU
DA
SKG
ACPG
Public N/W
IoT Applications
1.1 Resource Registration
1.2 Send Token with ID
2 Send Data with Token
3.1 Request for Secret key
3.2 Send Secret Key
4.1 Send Token and Request for ACP
4.2 Send ACP
5.1 MyLightSymAlgo: Enc(Data,Secret Key)Protect data
5.2 ECC Enc:(Secret Key, PUR,ACP):Protect Secret Key
5.3 MyLightHashAlgo: (data) Provide Data Integrity
ECC Enc:(MD, PRS):Protect Hash
5 Send (E_K(M | | E_PUR(K) | | E_PRS(H(M)))
6 Send (M',K',H')
7.1 ECC Dec:(K', PRR,ACP): Get Key
7.2 MyLightSymAlgo: Dec(M',Secret Key) Get Data
7.3 ECC Dec:(H', PUS):Get Hash
MyLightHashAlgo: (data) Verify Data Integrity

Figure 3: *Sequence of Execution*

- Security and Sensitivity: LSA aims for a highly secure encryption system with sensitivity to small input changes, enhancing overall security by producing significant output variations[8].
- IoT Data Security: LSA is designed to secure data from IoT sensors, suitable for resource-constrained devices where traditional cryptographic methods may be impractical.

As part of LCS, LSA ensures data confidentiality in IoT, protecting sensitive information while addressing IoT device limitations. The LSA diagram is depicted in Figure 4. The step-by-step operations of the LSA employed for secure data encryption is presented in Algorithm 1[8].

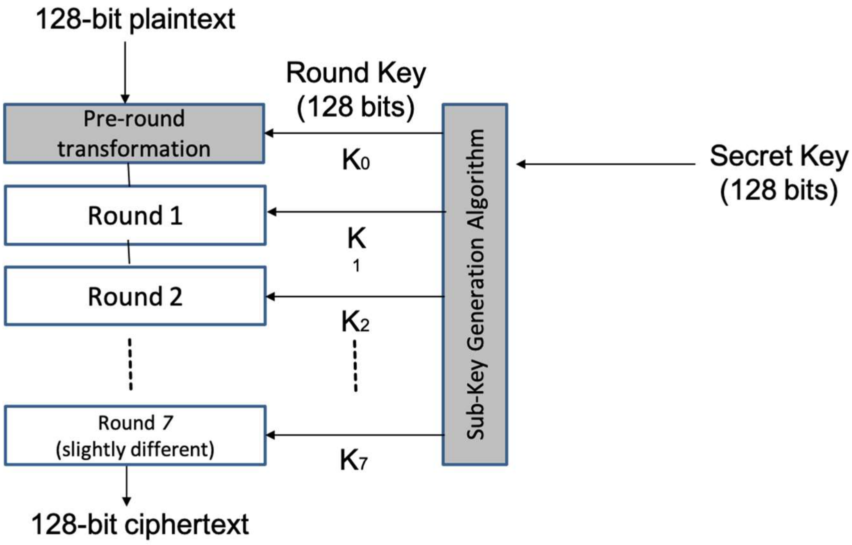

Figure 4: *LSA General Diagram*

Algorithm 1 Lightweight Symmetric Algorithm (LSA)

```
procedure LSA (Data Block, Round Keys)
        XOR Data Block with corresponding Pre Round Key
        Apply Parity Transformation
    for each byte in Data Block do
        Substitute byte using innovative SubBytes table
        Rearrange bytes using Junction Jumping strategy
        XOR with corresponding Round Key byte
    end for
        Substitute byte using innovative SubBytes table
        XOR Data Block with corresponding Round Key byte
    Output: Encrypted Data Block
end procedure
```

3.2 Elliptic Curve Cryptography (ECC): Asymmetric Encryption and Key Generation

Compared with other traditional public key encryption algorithm such as RSA algorithm, ECC algorithm can provide the same security with short key length. ECC operates on elliptic curves over finite fields so provide complexity [19]. The advantages of elliptic curves are: Encryption, Decryption and Signature Verification speed up, due to shorter key lengths, High safety performance, Small storage space, Fast processing speed, and Low bandwidth requirements [20, 21].

3.3 MyLightHashAlgo (LHA): Lightweight Hash Algorithm for Integrity

MyLightHashAlgo (LHA), a crucial element of Lightweight Crypto System (LCS) for resource-constrained IoT devices, improves data integrity using the optimal SHA256 variant, SHA256SUBPT. Proposed as the Lightweight Hash Algorithm (LHA), SHA256SUBPT achieves a balance between performance and security, with its architecture illustrated in Figure 5.

- LHA Architecture Block Wise: LHA processes data in 512-bit blocks, employing a block-wise approach for efficient handling, contributing to a 256-bit message digest. The block-wise architecture is illustrated in Figure 6.

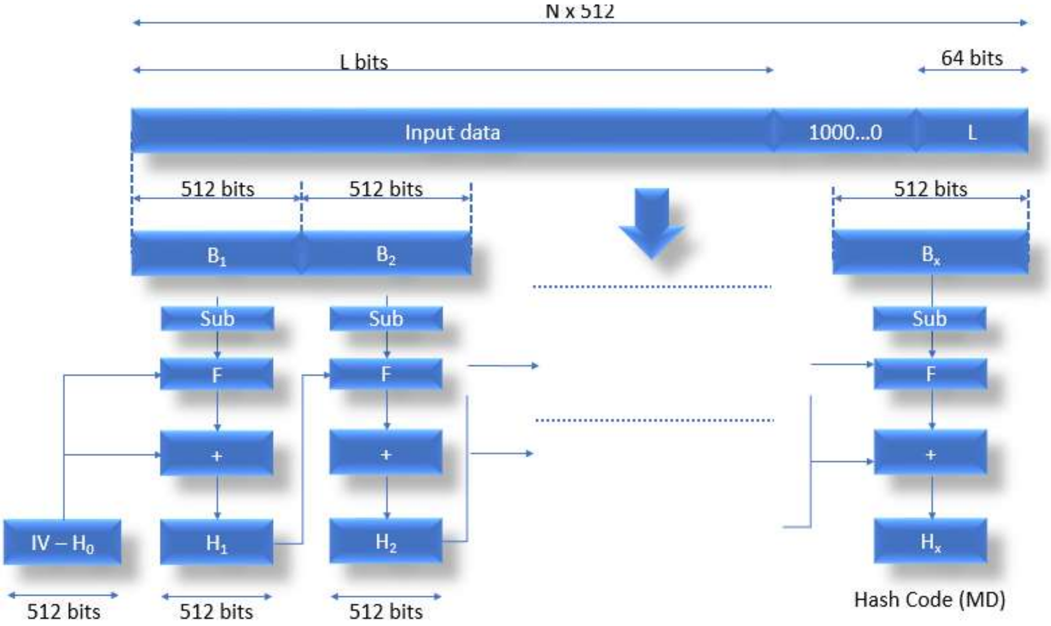

Figure 5: *LHA Architecture*

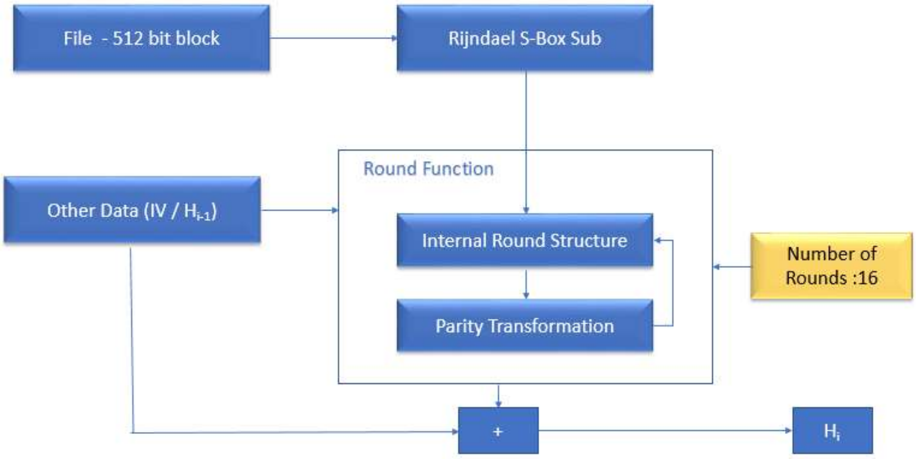

Figure 6: *LHA Architecture Block Wise*

- Hash Function of LHA: LHA's hash function, grounded in Merkle-damgard construction, executes multiple rounds of operations to generate a 256-bit message digest, ensuring data integrity. The graphical representation is illustrated in Figure 7.
- Each Round of Hash Function of LHA: In each round of the LHA hash function, crypto- graphic

operations like bitwise transformations and XOR summations are applied to input data, enhancing algorithm complexity. The iterative process ensures intricate manipulations, leading to the generation of a secure 256-bit hash digest, as depicted in Figure 8. LHA's hash function's round operation integrates key operations like Majority and Choose selections, XOR summations, and optimizations such as round reduction, Rijndael substitution, and Parity transformation which replace all state variables-64 bit, except A and E, with the 1's complements of their present values if their present values happen to be odd to enhance efficiency and security.

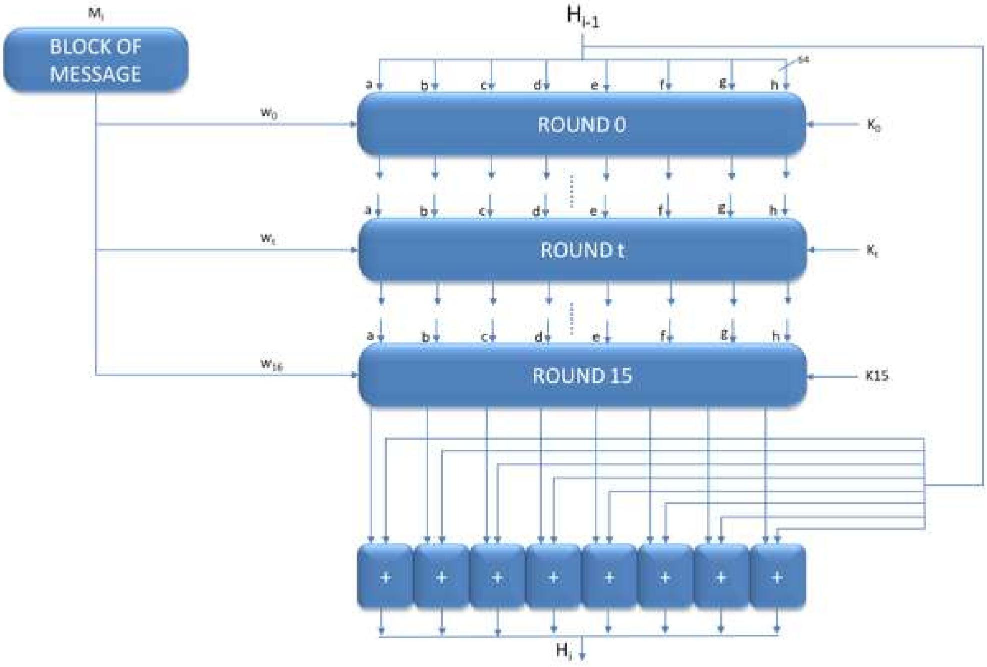

Figure 7: *Hash Function of LHA*

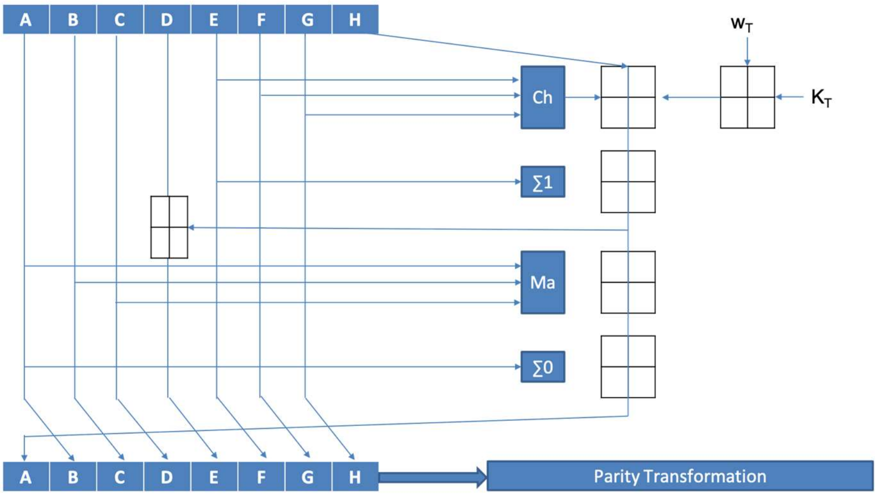

Figure 8: *Each Round of Hash function of LHA*

- **Ma:** Majority selects the next output in a bit-wise manner based on the majority bit forthe three input bytes.
- **Ch:** Choose selects the next output in a bit-wise manner based on the values in the 'x' variable; if $x[i] = 0$, $y[i]$ is selected, else $z[i]$ is selected.
- Σ0: Sigma A: XOR Summation on A.
- Σ1: Sigma E: XOR Summation on E.

- LHA - SECURITY PARAMETERS: To evaluate the security of the LHA algorithm, we consider Collision Resistance and Shannon Entropy as crucial security parameters.

Collision Resistance: This property in cryptographic hash functions ensures that it is challenging to find two inputs (a and b) such that they produce the same output (H(a) =H(b)), where *a* /= *b*.

Shannon Entropy: This parameter is employed to gauge Confusion, specifically the obfuscation of the Input-Output Relationship.

4. Experimental Result Analysis

The evaluation and results analysis were conducted to compare the performance of the Lightweight Symmetric Algorithm (LSA) against the Advanced Encryption Standard (AES) in terms of execution time and memory consumption. Security parameters such as avalanche effect, Hamming distance, and entropy were considered.

4.1 LSA vs AES Execution Time Comparison

We conducted a thorough evaluation of the execution time for the LSA compared to the Advanced Encryption Standard (AES). This analysis provides insights into the relative efficiency of LSA and AES in handling cryptographic operations, with implications for real-world applications and system performance. Figure 9 represents the LSA vs AES in terms of execution time.

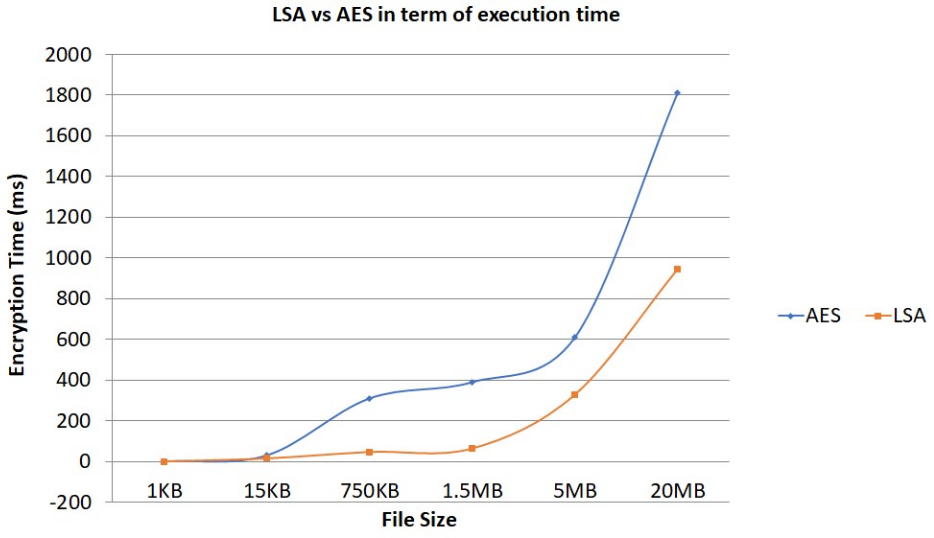

Figure 9: *LSA vs AES in term of Execution Time*

4.2 LSA vs AES Memory Consumption Comparison

Our study assessed the memory consumption of Lightweight Symmetric Algorithm (LSA) compared to Advanced Encryption Standard (AES), providing insights into their resource requirements for optimizing cryptographic algorithm performance. Figure 10 visually represents the LSA vs AES memory consumption dynamics.

4.3 Security Parameters Evaluation

The algorithm's security assessment centered on the avalanche effect, hamming distance, and entropy, evaluating diffusion, confusion, and bit changes. Parameters were derived from 10,000 randomly generated blocks to conduct a thorough security analysis.

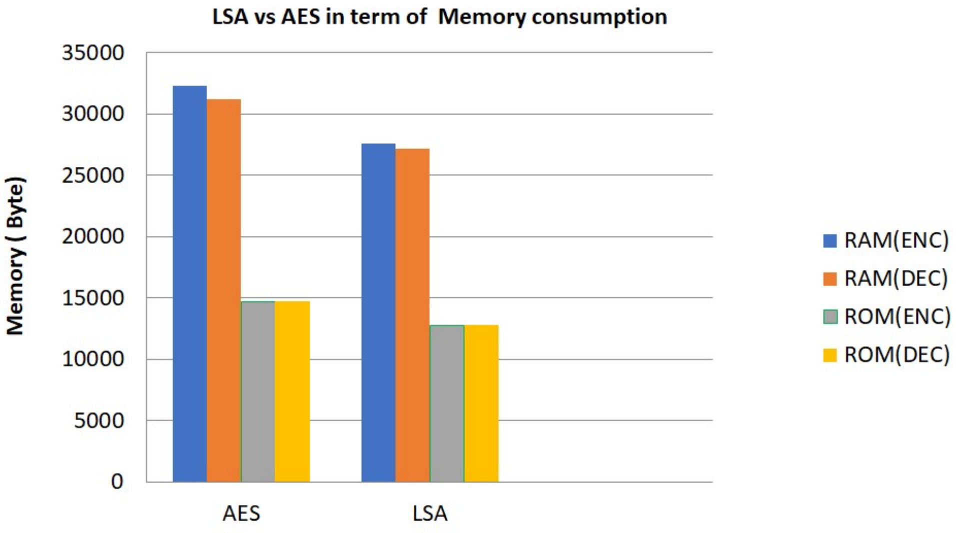

Figure 10: *LSA vs AES in term of Memory Consumption*

4.3.1 LSA Avalanche Criterion Evaluation

Our assessment of the Lightweight Symmetric Algorithm (LSA) scrutinizes its performance using the Avalanche Criterion (AC), considering first, second, and third-order criteria along with the average. This comprehensive analysis sheds light on LSA's efficacy in diffusing changes in input data, reflecting in output data, essential for robust cryptographic applications.

Table 1: *Performance of LSA in term of Avalanche Criterion*

	1st Order AC	2nd Order AC	3rd Order AC	Average AC
AES	49.00%	49.00%	49.00%	49.00%
LSA	49.00%	42.00%	49.00%	46.66%

Table 1 displays LSA's performance in Avalanche Criterion (AC) at various orders and the average AC, contrasting with AES's constant 49.00%. LSA shows variations, notably a 2nd Order AC drop to 42.00%, resulting in an average AC of 46.66%, indicating different levels of change propagation compared to AES. Figure 11 visually compares LSA and AES in terms of Avalanche Effect, offering insights into their respective responses to modifications in input data and highlighting their unique diffusion characteristics.

4.3.2 LSA Entropy Criteria

Table 2 reveals the performance of LSA and AES based on Entropy criteria, indicating a 50.00%

Hamming Distance for both and very close Shannon's Entropy values. LSA slightly edges higher at 3.612 compared to AES's 3.611, showcasing comparable security aspects related to confusion and the number of flipped bits after conversion.

Table 2: *Performance of LSA in term of Avalanche Criterion*

	Hamming Distance	Shannon's Entropy (Log2)
AES	50.00%	3.611
LSA	50.00%	3.612

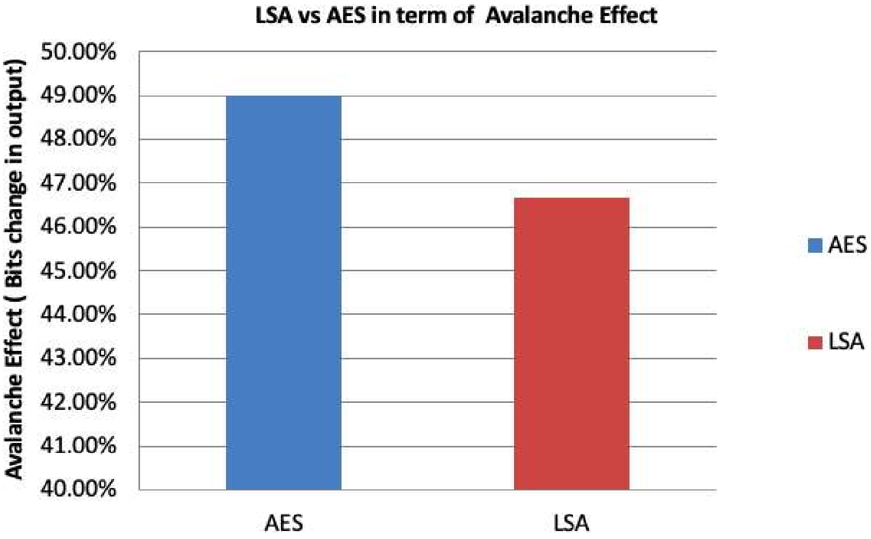

Figure 11: *LSA vs AES in Term of Avalanche Effect*

Figure 12 illustrates the evaluation of LSA versus AES based on Hamming Distance, showing an equivalent and favorable 50.00% for both algorithms. Hamming Distance, measuring bit differences between original and encrypted data, underscores their similar and consistent performance in this security parameter.

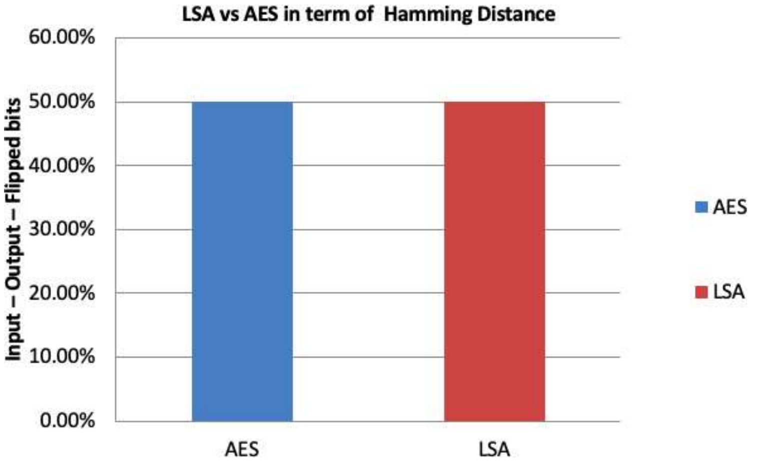

Figure 12: *LSA vs AES in Term of Hamming Distance*

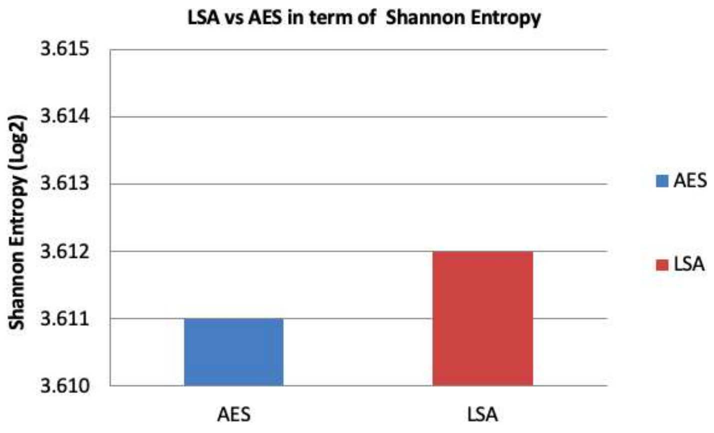

Figure 13: *LSA vs AES in term of Shannon Entropy*

In Figure 13, LSA and AES exhibit identical Shannon Entropy values of 3.612, emphasizing their equivalent performance in providing a high degree of confusion and obfuscation in the input-output relationship. These similar Shannon Entropy values highlight a strong level of security for both algorithms in this parameter.

4.1. Performance Analysis for SHA256 and LHA

4.4.1 Memory Consumption of SHA256 and LHA

Figure 14 presents the results of experiments evaluating the memory consumption of SHA256 and LHA, offering a comparison of their respective requirements under specified conditions. The analysis provides insights into the efficiency and resource utilization of SHA256 and LHA, highlighting their impacts on memory consumption in cryptographic operations.

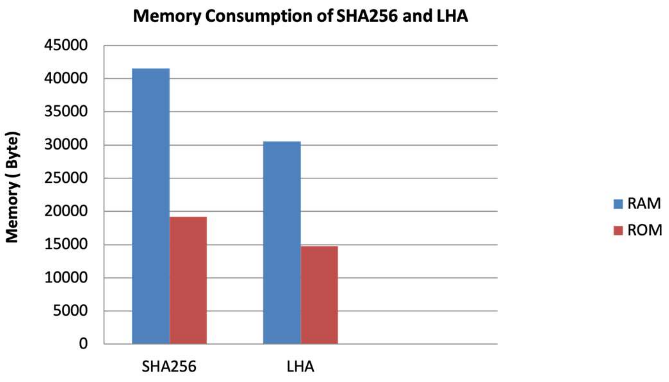

Figure 14: *Performance of SHA256 and LHA in Term of Memory Consumption*

4.4.2 Performance of SHA256 and LHA in Term of Execution time

Figure 15 illustrates the experimentally evaluated execution time performance of SHA256 and LHA, offering insights into the time efficiency of both algorithms, including processing time and overall execution speed.

4.4.3 Collision Count Analysis

The collision count analysis for SHA256 and LHA, considering different sizes of strings per hash, is presented in the Table 3. The collision count is an important metric to assess the robustness and security of hash functions.

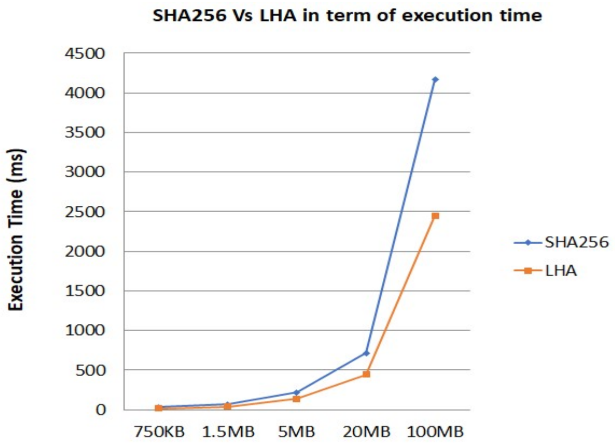

Figure 15: *Performance of SHA256 and LHA in Term of Execution time*

Table 3: *Collision Count Analysis for SHA256 and LHA*

Size of String per Hash	SHA256 Collision Count	LHA Collision Count
04 Hex	6.10621	6.10645
08 Hex	5.2e-05	3.25e-05
16 Hex	0	0
32 Hex	0	0
64 Hex (Full Hash code)	0	0

4.4.4 Shannon Entropy Analysis

The Shannon Entropy analysis for SHA256 and LHA, considering different sizes of strings per hash, is presented in the Table 4. Shannon Entropy is a measure of uncertainty or information content in a system.

Table 4: *Shannon Entropy Analysis for SHA256 and LHA*

Size of String per Hash	SHA256 Shannon Entropy	LHA Shannon Entropy
04 Hex	1.81759	1.81727
08 Hex	2.59429	2.59478
16 Hex	3.2089	3.20719
32 Hex	3.61134	3.61357
64 Hex (Full Hash code)	3.8196	3.82103

4.4.5 Performance Analysis of AES vs LSA and SHA vs LHA on ESP32 Platform

In this configuration, the ESP32-CAM acts as an access point with a WebSocket server and DHT11 sensor, transmitting encrypted data. The M5Stack ESP32 serves as a client, connecting to ESP32-CAM, triggering operations with three buttons, ensuring secure communication and decoding of encrypted data for display.

Table 5: *Comparison of LSA and AES Encryption/Decryption Performance for Text-Based Data*

Parameter	LSA (microseconds)	AES (microseconds)
Encryption Time	268	1680
Encryption Time per Block	48	384
Decryption Time	267	2060
Decryption Time per Block	48	464
Data Length	69 bytes	69 bytes

Table 6: *Comparison of LSA and AES Encryption/Decryption Performance for Image-Based Data*

Parameter	LSA (microseconds)	AES (microseconds)
Encryption Time	7205	61438
Encryption Time per Block	32	320
Decryption Time	3090	73251
Decryption Time per Block	32	368
Data Length	3056 bytes	3056 bytes

Table 7: *Comparison between the Performance of the LSA and AES For Image-based Data*

Algorithm	Operation	Time (µs)	Time per Block (µs)	Data Length (bytes)	Hash Function	Hash Time (µs)	Hash Time per Block (µs)
AES with SHA	Encrypt	69226	320	3440	SHA256	2037	9
AES with SHA	Decrypt	82459	368	3440	SHA256	2037	9
LSA with LHA	Encrypt	8108	32	3440	LHA256	1259	5
LSA with LHA	Decrypt	8059	32	3440	LHA256	1259	5

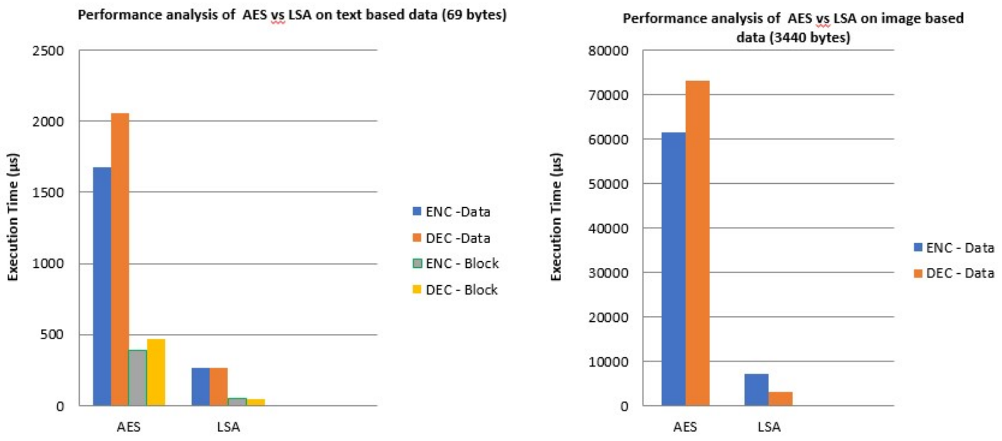

Figure 16: *Performance analysis of AES vs LSA on text/image based data on IoT Set up*

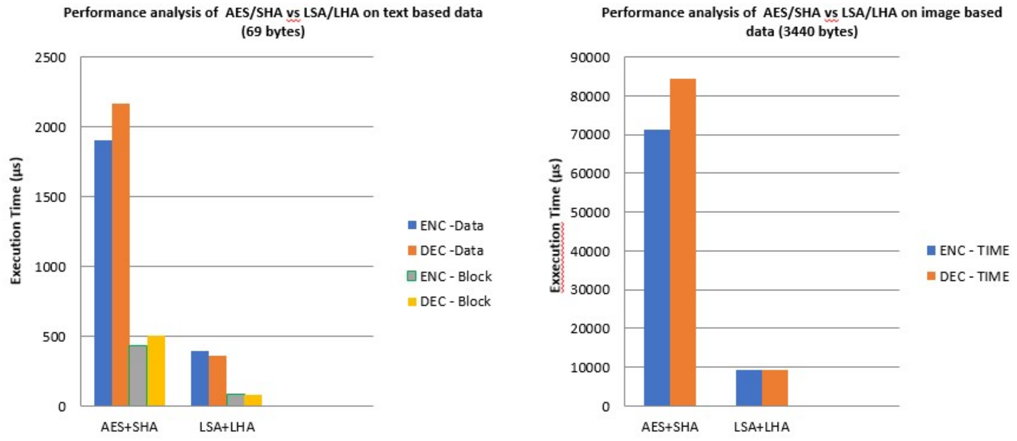

Figure 17: *Performance analysis of AES/SHA vs LSA/LHA on text/image based data on IoT Set up*

Tables 5 and 6 compare LSA and AES encryption/decryption performance for text-based and image-based data. Figure 16 illustrates the experimentally evaluated execution time performance of AES and LSA on IoT set up. Tables 7 and 8 compare performance of combination of LSA-LHA and AES-SHA encryption/decryption for text-based and image-based data. Figure 17 illustrates the experimentally evaluated execution time performance of AES-SHA and LSA-LHA on IoT setup.

Table 8: *Comparison between the Performance of the LSA and AES for Text based data*

Algorithm	Operation	Time (µs)	Time per Block (µs)	Data Length (bytes)	Hash Function	Hash Time (µs)	Hash Time per Block (µs)
AES with SHA	Encrypt	1755	400	69	SHA256	146	36
AES with SHA	Decrypt	2016	464	69	SHA256	146	36
LSA with LHA	Encrypt	311	64	69	LHA256	81	20
LSA with LHA	Decrypt	281	64	69	LHA256	81	20

Table 9 and 10 detail the throughput of AES and LSA for text-based and image-based data, respectively. Furthermore, Table 11 illustrates the throughput of AES and SHA for image data, while Table 12 showcases the throughput of LSA and LHA for image data.

Table 9: *Text-Based Data Throughput of LSA and AES*

Parameter	LSA Throughput (Mb/s)	AES Throughput (Mb/s)
Encryption Throughput	2.06	0.33
Decryption Throughput	2.07	0.27
Data Length	69 bytes	69 bytes

Table 10: *Image-Based Data Throughput LSA and AES*

Parameter	LSA Throughput (Mb/s)	AES Throughput (Mb/s)
Encryption Throughput	3.39	0.40
Decryption Throughput	3.41	0.33
Data Length	3056 bytes	3056 bytes

Table 11: *AES with SHA Throughput with Image Data*

Operation	Throughput (Mb/s)
AES Encryption	0.40
AES Decryption	0.33
SHA Hashing	13.51

Table 12: *LSA with LHA Throughput with Image Data*

Operation	Throughput (Mb/s)
LSA Encryption	3.39
LSA Decryption	3.415
LHA Hashing	21.86

The comparison tables show that LSA consistently outperforms AES in encryption and decryption performance for both text-based and image-based data, with lower times per block and higher throughput. When combined with LHA, LSA demonstrates remarkable efficiency, especially for image data, surpassing AES with SHA. These findings highlight LSA's potential for secure and efficient data transmission, particularly in applications like IoT and image processing.

5. Conclusion

Our Hybrid Lightweight Cryptographic System (LCS) is a significant advancement in IoT data security, employing LSA for encryption, ECC for key management, and LHA for integrity verification. Our LHA algorithm outperforms SHA-256, showcasing similar collision resistance in practical scenarios, ensuring enhanced performance without compromising security.Additionally, LSA with LHA exhibits notable performance improvements in comparison with AES128 with SHA256, particularly in real-time image-based data transmission on ESP32. When working with text data, there's an observed approximately 79.5% improvement in performance, and when working with image data, the improvement is approximately 86.8%. Such improvements have potential implications for real-time applications, particularly where latency is a concern. This study paves the way for future cryptographic optimizations in IoT. Identifying and addressing potential security vulnerabilities in these areas will be a key focus of our future research.

References

[1] Hernndez-Ramos, Jos© L., et al. "Protecting personal data in IoT platform scenarios through encryption-based selective disclosure." Computer Communications 130 (2018): 20-37.

[2] Yao, Xuanxia, Zhi Chen, and Ye Tian. "A lightweight attribute-based encryption scheme for the Internet of Things." Future Generation Computer Systems 49 (2015): 104-112.

[3] Goyal, Tarun Kumar, and Vineet Sahula. "Lightweight security algorithm for low power IoT devices." 2016 international conference on advances in computing, communications and informatics (ICACCI). IEEE, 2016.

[4] Singh, Saurabh, et al. "Advanced lightweight encryption algorithms for IoT devices: survey, challenges and solutions." Journal of Ambient Intelligence and Humanized Computing (2017): 1-18.

[5] Naru, Effy Raja, Hemraj Saini, and Mukesh Sharma. "A recent review on lightweight cryptography in IoT." 2017 international conference on I-SMAC (IoT in social, mobile, analytics and cloud)(I-SMAC). IEEE, 2017

[6] Dhanda, Sumit Singh, Brahmjit Singh, and Poonam Jindal. "Lightweight cryptography: a solution to secure IoT." Wireless Personal Communications 112 (2020): 1947-1980.

[7] Rana, Muhammad, Quazi Mamun, and Rafiqul Islam. "Lightweight cryptography in IoT networks: A survey." Future Generation Computer Systems 129 (2022): 77-89.

[8] Shah, Amita, et al. "LSA: A LIGHTWEIGHT SYMMETRIC ENCRYPTION ALGORITHM FOR RESOURCE-CONSTRAINED IOT SYSTEMS." Reliability: Theory & Applications 18.3 (74) (2023): 44-58.

[9] Bos, Joppe W., et al. "Elliptic curve cryptography in practice." Financial Cryptography andData Security: 18th International Conference, FC 2014, Christ Church, Barbados, March 3-7, 2014, Revised Selected Papers 18. Springer Berlin Heidelberg, 2014.

[10] Lara-Nino, Carlos Andres, Arturo Diaz-Perez, and Miguel Morales-Sandoval. "Lightweight elliptic curve cryptography accelerator for internet of things applications." Ad Hoc Networks 103 (2020): 102159.

[11] Yang, Xu, et al. "Blockchain-based secure and lightweight authentication for Internet of Things." IEEE Internet of Things Journal 9.5 (2021): 3321-3332.

[12] Mahlake, Ntebatseng, et al. "A Lightweight Encryption Algorithm to Enhance Wireless Sensor Network Security on the Internet of Things." J. Commun 18 (2023): 47-57.

[13] Alfrhan, Aishah, Tarek Moulahi, and Abdulatif Alabdulatif. "Comparative study on hash functions for lightweight blockchain in Internet of Things (IoT)." Blockchain: Research and Applications 2.4 (2021): 100036.

[14] Landge, Irfan A., and Hannan Satopay. "Secured IoT through hashing using MD5." 2018 fourth international conference on advances in electrical, electronics, information, communication and bio-informatics (AEEICB). IEEE, 2018.

[15] Ragab, Ahmed, et al. "Robust hybrid lightweight cryptosystem for protecting IoT smart devices." Security, Privacy, and Anonymity in Computation, Communication, and Storage: SpaCCS 2019 International Workshops, Atlanta, GA, USA, July 14“17, 2019, Proceedings 12.Springer International Publishing, 2019.

[16] Sharma, Jayanti, and Deepali Koppad. "Low power and pipelined secure hashing algorithm-3 (SHA-3)." 2016 IEEE Annual India Conference (INDICON). IEEE, 2016.

[17] Al-Mashhadi, Haider M., Hala B. Abdul-Wahab, and Rehab F. Hassan. "Secure and time

efficient hash-based message authentication algorithm for wireless sensor networks." 2014 Global Summit on Computer & Information Technology (GSCIT). IEEE, 2014.

[18] Rao, Vidya, and K. V. Prema. "Light-weight hashing method for user authentication in Internet-of-Things." Ad Hoc Networks 89 (2019): 97-106.

[19] Shah, Amita, et al. "LSA: A LIGHTWEIGHT SYMMETRIC ENCRYPTION ALGORITHM FOR RESOURCE-CONSTRAINED IOT SYSTEMS." Reliability: Theory & Applications 18.3 (74) (2023): 44-58.

[20] Zargar, Ansah Jeelani, Mehreen Manzoor, and Taha Mukhtar. "ENCRYPTION/DECRYPTION USING ELLIPTICAL CURVE CRYPTOGRAPHY." International journal of Advanced Re- search in computer science 8.7 (2017).

[21] Keerthi, K., and B. Surendiran. "Elliptic curve cryptography for secured text encryption." 2017 International Conference on Circuit, Power and Computing Technologies (ICCPCT). IEEE, 2017.

[22] Seok, Byoungjin, Jinseong Park, and Jong Hyuk Park. "A lightweight hash-based blockchain architecture for industrial IoT." Applied Sciences 9.18 (2019): 3740.

[23] Pandya, Hetal B., and Tushar A. Champaneria. "Enhancement of security in IoTSyS framework." Proceedings of International Conference on Communication and Networks: ComNet 2016. Springer Singapore, 2017.