Tuijin Jishu/Journal of Propulsion Technology
ISSN: 1001-4055
Vol. 47 No. 02 (2026)

Efficiency Analysis of Lightweight RSA and ASCON Algorithms for Secure IoT Environments

Isha Sharma[1], Shikha Sain[2], Anjana Rani[3], Shivran Priyanka[4]

Department of Information Technology JECRC Foundation, Jaipur, Rajasthan

Abstract:- In the Internet of Things (IoT), where billions of connected devices share sensitive data over environments with limited resources, security is still a major concern. For Internet of Things-based smart city applications, this paper compares the Lightweight RSA (LWRSA) and ASCON algorithms. While ASCON, a NIST-standardized cipher, offers authenticated encryption and hashing utilizing permutation-based construction, LWRSA modifies conventional RSA through smaller key sizes and optimized key creation. Experimental evaluation is carried out on datasets of different sizes, examining key generation overhead, memory usage, encryption time, and decryption time. The findings indicate that LWRSA is more appropriate for latency-sensitive IoT systems because it achieves much shorter computation times for both small (3.51 MB) and large (27 MB) datasets, whereas ASCON exhibits higher computational overhead but more standardized security assurances. The results indicate that while ASCON is still preferred for long-term resilience in installations with limited resources, LWRSA is useful for time-sensitive IoT applications.

Keywords*:* LWRSA, ASCON, IoT Security, Encryption, Decryption, Smart City.

1. Introduction

By 2030, there will likely be billions of connected devices thanks to the Internet of Things' (IoT) explosive growth. Although smooth communication and data sharing are made possible by this expansion, there are also serious security risks.Conventional cryptographic algorithms are often unsuitable for lightweight devices due to their computational and energy requirements. To address this limitation, lightweight algorithms such as Lightweight RSA (LWRSA) and ASCON have been developed. In the context of IoT security in smart cities, this study compares these two methods. By altering the traditional two-A lightweight RSA algorithm adapts the basic RSA principles for resource-constrained situations, like Internet of Things devices, by switching to three prime utilizing the Chinese Remainder Theorem (CRT) for faster key generation and decryption.These enhanced algorithms make RSA suitable for systems with limited resources where traditional RSA is too resource-intensive by reducing the computational burden, memory requirements, and battery consumption while maintaining enough security. ASCON is a NIST-standardized family of lightweight cryptographic algorithms for the Internet of Things (IoT) and other resource-constrained devices. It offers hashing functions and Authenticated Encryption with Associated Data (AEAD) using a novel permutation-based technique that is safe, efficient, and scalable. The ASCON method is a very interesting candidate in the realm of lightweight cryptography, especially for scenarios needing low computing power. Initially, ASCON was introduced as a competitor in the cryptographic competition known as CAESAR (Competition for Authenticated Encryption: Security, Applicability, and Robustness). Christoph Dobraunig, Maria Eichlseder, Florian Mendel, and Martin Schütffer were among the experts who created it. By offering both hashing and authenticated encryption, this is intended to be a multipurpose tool in the suite of cryptographic protocols. ASCON was created mainly in response to the increasing need for secure and resource-saving cryptographic solutions, in particular with regard to embedded devices and the Internet of Things. Since these environments are often resource-constrained in terms of electrical power, memory, and CPU capability, a lightweight and secure method is

required. ASCON employed the sponge construction technique, a well-known method in the world of cryptography design, due to its effectiveness and simplicity. ASCON can balance security and performance thanks to its sponge architecture, which makes it appropriate for a variety of applications [2].

2. Objective

This entails assessing how well they perform in terms of computing cost, memory utilization, energy consumption, encryption/decryption speed, and resilience to typical cyber threats. In order to provide a workable cryptographic solution for IoT devices with low resources, the research attempts to find an algorithm that strikes the greatest balance between security strength and resource efficiency.This paper provides a comparative analysis of these two approaches in the context of smart city IoT security. By changing the conventional two-By changing to employ three primeusing the Chinese Remainder Theorem (CRT) for quicker key generation and decryption, a lightweight R SA algorithm adapts the fundamental RSA principles for resource-constrained contexts, such as Internet of Things devicesAlthough it is generally less popular than contemporary lightweight ciphers like ASCON, lightweight RSA is not a specific standardized algorithm; rather, it is a derivative of the classic RSA algorithm for resource-constrained contexts using smaller keys and simpler implementations [1].

3. Motivation

The rapid rise of the Internet of Things (IoT) has connected billions of smart devices across varied areas such as healthcare, smart homes, industry, and transportation. However, the confined computational power, limited memory, and low energy capacity of IoT devices pose substantial problems to implementing classic cryptographic algorithms. Conventional security methods like conventional RSA or AES are generally too heavy for such contexts, resulting to inefficiencies and risks. Lightweight cryptographic algorithms that offer strong security with minimal resource consumption are becoming more and more necessary to preserve data confidentiality, integrity, and authentication in IoT systems. While ASCON, a finalist in the NIST Lightweight Cryptography competition, is built for high efficiency and robust resilience against modern threats, RSA provides solid public-key encryption when adapted for lightweight applications.

4. Literature Review

Because of the Internet of Things' explosive increase in linked devices, it is crucial to ensure effective and safe connectivity. For the Internet of Things, this paper presents a novel hybrid AES-RSA encryption technique (MRA). Our approach lowers the processing load on IoT devices with limited resources and enhances system performance by decreasing the number of AES iteration rounds and increasing the number of prime numbers in RSA to shorten the key bit length. The MRA system incorporates strong security mechanisms to protect against potential attackers and tackles the important issue of insufficient research on encryption approaches for lightweight protocols. Extensive theoretical analysis and ProVerif verification demonstrate the scheme's robustness in preserving secrecy and decryption efficacy [3].Lightweight cryptography techniques have been thoroughly examined in this study. Calculations are performed by several low-resource devices in an Internet of Things environment. These devices have computational, memory, battery life, and power consumption constraints. Concerns like security, privacy, and preserving customer trust must also be addressed by IoT devices. We also put together a list of additional easy-to-use, lightweight cryptographic methods that may be implemented on both hardware and software. The study also covered the different kinds of attacks that can be made against specific cryptographic algorithms [4].Issues like security, latency, and energy consumption are made worse by a number of physical objects and sensors, highly dispersed systems, massive data processing, lightweight applications, and chip areas. Without better adjusting every parameter, a system cannot maximize throughput; for instance, a system with a large latency may be antiquated and useless for real-time applications. The main component of a cipher that is assessed for its ability to withstand cyber attacks is security. Whereas the length of the key indicates the strength of a symmetric cipher, the half-length of the key

indicates the strength of an asymmetric cipher. Lesamanta-LW (128) and SPONGENT (128) are the most secure in LWHF in terms of data integrity [5].According to the results, Lightweight RSA outperformed the current algorithm in comparison. Thus, IoT-based applications like smart cities can make use of lightweight RSA. Better performance with multi-level encryption is provided by lightweight RSA. Therefore, for improved device level security, we can either employ a hybrid method or lightweight RSA in multi-level [6].This study investigated the hardware implementations proposed for the NIST LWC winner ASCON. The most sophisticated defenses against side-channel attacks against its authenticated encryption (AEAD) implementations were also investigated. The literature shows that ASCON has put a lot of work into its studies. Nevertheless, a lot of research tends to concentrate on particular areas, leaving a number of branches that require more investigation. It is crucial to thoroughly investigate ASCON's design space as it becomes more and more common in protecting embedded systems with limited resources (such as wearable and implantable medical devices, smart homes, and RFID tags). The present research tendency ignores other important design criteria like power and energy efficiency, which are crucial for battery-operated and resource-constrained applications, in favor of concentrating on area reduction and performance enhancements through round-based or unrolled designs [7]. The model of the internet of things (IoT) based single-phase grid-connected inverter using RSA (Rivest-Shamir-Adleman) algorithm is presented here. The inverter is developed by H-bridge architecture and sinusoidal pulse width modulation technology (SPWM). The grid connectivity of this inverter is built by the phase control technique. The inverter has fewer harmonics and a simplistic structure than conventional available technologies. Because this IoT-enabled inverter is continually connected to the network, cybersecurity concerns and obstacles are developing. The paper explores how the RSA method could be used to assure the IoT-enabled inverter's connectivity and data security [8].A new era of technology and knowledge has emerged thanks to the Internet of Things (IoT), which makes use of numerous devices with limited resources. These devices are vulnerable to a wide range of recent dangers, such as malware. One of the best easy to protect those Internet of Things applications is through the use of lightweight cryptographic algorithms. By making it impossible to extract any important information pattern, cryptography will conceal the data and guarantee that any data transmission is secured, accurate, authorized, permitted, and unreliable [9]. The idea is to connect a variety of objects or things (e.g., RFID tags, NFC tags, sensors, etc.), which can interact and exchange data with each other anywhere and everywhere over the internet. With the evolution of IoT, the volume of data interchanged among connecting IoT devices is increasing at a remarkable scale due to the increase in number of the connected objects.lightweight cryptographic primitives (LWC) have been introduced. Many kinds of research continue moving forward to find a suitable algorithm that meets the specific demands of the IoT application [10].

Table 1: Literature Review

Author and Year	Technique /Method	Result	Remark
Q Chang et al. 2025[3]	RSA-AES& hybrid encryption	92% accuracy	This hybrid approach ensures low-latency communication, data confidentiality.
I Sharma et al. 2024 [6]	Lightweight RSA, Lightweight PRESENT,	97% Accuracy	Model Works on Lightweight RSA.
K U sarkar 2025 [5]	Intrusion detection system · Cryptography	91% accuracy	Security · Sustainability
Isha et al. 2022 [7]	ASCON; lightweight cryptographyTechniques	92% accuracy	Techniques include encryption, authentication, and

			accessauthentication
Oh, Y et al. 2025 [8]	RSA (Rivest-Shamir-Adleman)	90% accuracy	RSA ensures that only authorised entities can access
MSZ Labbi et al. 2020 [10]	Cryptographic, Lightweight, Encryption, Resource constrained		Ideal for IoT devices like sensors
R Balaji et al. 2024 [1]	RSA (Rivest-Shamir-Adleman)	93% accuracy	Asymmetric and symmetric cryptographic features have been combined by this approach
R P Neve et al. 2023[2]	ASCON-Hash LWC, which his based-on sponge structure	92% accuracy	To verify the authenticity of messages and prevent tampering or replay attacks
Shafaan Khaliq Bhatti 2023 [11]	DESSHA and SHA algorithms	-	The analysis will show that DESSHA and SHA algorithms have the same security level for message authentication.
AK Budati et al. 2021 [12]	The Rivest-Shamir-Adleman (RSA)	-	works better for image and video in terms of time complexity.
M. Bahrami et al. 2021[13]	Encryption technology, security and Data Protection	93% accuracy	the status of basic researchonmechanisms of encryptiontechnology, telecommunications, security, data protection
A. Fotovvat et al. 2020[14]	Lightweight cryptography (LWC) algorithms	91% accuracy	This algorithm choosing a suitable platform and optimal LWC algorithm for IoT applications.
MN Khan et al. 2020[15]	Internet of Things (IoT)	-	Describes the IoT structure, computational capabilities of the devices at the end, edge, fog, and cloud platforms, and classifies existing lightweight cryptographic protocols.

5. Methodology and Implementation

1. Goal To compare the security strength, resource usage, and performance efficiency of the Lightweight RSA (LWRS) and ASCON algorithms when used in edge network and Internet of Things contexts.

2. Experimental Configuration

1. Platform/Environment Parameter Description IoT simulation or embedded device (such as an ARM Cortex, Raspberry Pi, or Arduino)
2. Operating System: Python, C, and C++ Lightweight operating systems based on Linux, such as Ubuntu and Raspbian
3. Cryptographic Libraries: PyCryptodome, OpenSSL, or an ASCON-specific implementation
4. Input/Dataset Plaintext messages of varying sizes (e.g., 128-bit, 256-bit, 512-bit) created at random
5. Important Sizes LWRS: Lightweight RSA, 512–1024 bits ASCON: 128-bit nonce and 128-bit key

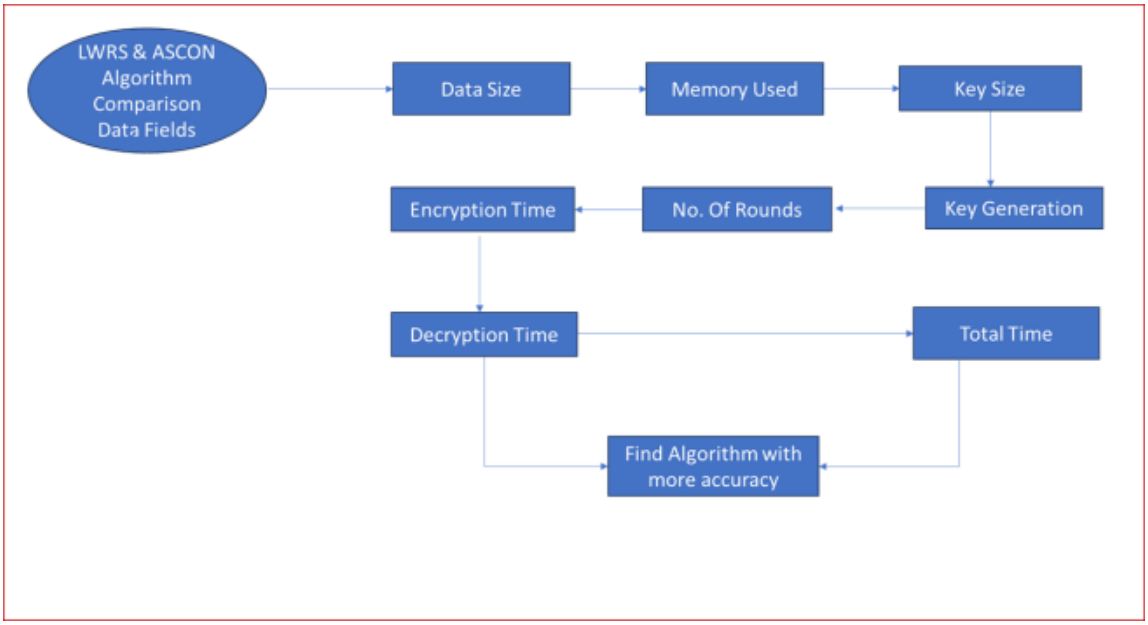

Fig-1: Methodology

3. Data Fields for Comparison

Category	Field/Metric	Description
Performance	**Encryption Time (ms)**	Time required to encrypt data
	Decryption Time (ms)	Duration of data decryption
	Throughput (Kb/s)	Seconds of data processing
	Latency (ms)	Between-input and output delay
Resource Utilization	**Memory Usage (KB)**	RAM used while it was operating
	CPU Utilization (%)	CPU use when encrypting and decrypting data

Category	Field/Metric	Description
	Energy Consumption (mJ)	Power needed to function (essential in IoT)
Security Analysis	**Key Length (bits)**	Size of cryptographic keys
	Resistance to Attacks	Differential cryptanalysis, side-channel, and brute-force
	Integrity & Authentication	Whether data authentication is provided by the algorithm
Implementation	**Code Complexity (LOC)**	Code line count and implementation effort
	Scalability	Performance as the number of data or devices increases.

4. Tools and Measurement Techniques

Tool	Purpose
Python time/perf module	Measure execution time
psutil library	Measure CPU and memory usage
Energy trace analyzer	For energy measurement on IoT devices
Wireshark	Network performance (if data transfer included)
MATLAB / Excel	Result visualization (charts, graphs)

5. Analysis and Visualization of Data

1. Plot the encryption and decryption times for different message sizes.
2. Examine memory consumption and performance side by side.
3. Analyze the trade-offs in security.
4. Make judgments regarding IoT/edge device appropriateness.

6. Expected Results

Metric	LWRS (Expected)	ASCON (Expected)
Encryption/Decryption Time	Higher	Lower
Memory Usage	Higher	Lower
CPU Utilization	High	Moderate

Metric	LWRS (Expected)	ASCON (Expected)
Security Level	High	Moderate to High (symmetric)
Energy Efficiency	High	Lower

6.1 Multi-layer Analysis with Lightweight RSA Algorithm

Lightweight cryptography uses smaller keys, typically less than 90 bits, to cope with real-time demands. In contrast, the national institute of standard and technology (NIST) recommended a minimum of 2048-bit RSA keys. Here are some other things to consider when using RSA keys: key size a 2048-bit key is considered a minimum for maintain a reasonable level of security. However, recent hardware improvement may allow for a 4096-bit key.

Table 2: Multilayer LWRSA Algorithm Implementation

Levels	Data Size (MB)	Memory Used (Bytes)	Key Size (Bits)	Key Gen. Time (Sec)	No of Rounds	Encry. Time (Sec)	Decry. Time (Sec)	Total Time (E+D)
L1	3.51	722	2048	1.9665	12	0.029	0.035	0.064
L2	3.51	737	2048	1.9665	12	0.024	0.024	0.048
L3	3.51	783	2048	1.9665	12	0.016	0.024	0.04
L1	27	720	2048	2.1473	12	0.1195	0.032	0.1515
L2	27	783	2048	2.1473	13	0.016	0.029	0.045
L3	27	753	2048	2.1473	12	0.02	0.023	0.043
L1	3.51	1545	4096	15.492	13	0.025	0.0819	0.1069
L2	3.51	1536	4096	15.492	13	0.027	0.0692	0.0962
L3	3.51	1494	4096	15.492	13	0.019	0.0646	0.0836
L1	27	1525	4096	5.2873	13	0.0657	0.08	0.1457
L2	27	1476	4096	5.2873	13	0.016	0.1292	0.1452
L3	27	1446	4096	5.2873	13	0.0589	0.1159	0.1748

This table shows the implementation of LWRSA algorithm on different parameters.The LWRSA algorithm is checked for the effectiveness of encryption and decryption based on different data sizes, memory utilization, and sizes of keys. For small sizes of data, which is around 3.51 MB, the encryption and decryption times are relatively small and with little fluctuation between the levels L1, L2, and L3. In this case, the encryption time varies between 0.016 and 0.0657 seconds and the decryption time ranges from 0.024 to 0.1159 seconds. When the amount of data is increased to 27 MB, the time taken for encryption and decryption increases correspondingly, hence directly proportional. Total execution time including encryption and decryption increases gradually as memory is increased and with a key generation time that has an impact on the performance.

6.2 Multilayer Analysis with ASCON Algorithm

The ASCON algorithm has specific performance behavior with higher encryption and decryption time at all phases as compared to the LWRSA algorithm. For the data size of 3.51 MB, encryption time ranges between 0.484 to 0.528 seconds whereas decryption time ranges between 0.502 and 0.616 seconds. When the size of the

data is increased to 27 MB, the time for encryption and decryption becomes extremely high. In this case, encryption reaches up to 7.038 seconds and decryption up to 5.292 seconds. The overall time is proportionally increased.[12] This reflects that the computational overhead of the ASCON method for larger data. The ASCON algorithm is relatively more computationally expensive than LWRSA at all levels.

Table 3: Multilayer ASCON Algorithm Implementation

Levels	Data Size (MB)	Memory Used (Bytes)	Key Size (Bits)	Key Gen. Time (Sec)	No of Rounds	Encry. Time (Sec)	Decry. Time (Sec)	Total Time (E+D)
L1	3.51	4896612	128	1.9748	10	0.484	0.604	1.088
L2	3.51	4896612	128	1.9748	10	0.502	0.616	1.118
L3	3.51	4896612	128	1.9748	10	0.486	0.6	1.086
L1	27	38817612	128	1.169	10	10.009	5.997	16.006
L2	27	38817612	128	1.169	10	10.406	5.848	16.254
L3	27	38817612	128	1.169	10	5.168	5.239	10.407
L1	3.51	4896612	160	1.333	10	0.835	1.269	2.104
L2	3.51	4896612	160	1.333	10	0.817	1.033	1.85
L3	3.51	4896612	160	1.333	10	1.124	1.379	2.503
L1	27	38817612	160	1.9665	10	8.058	5.07	13.128
L2	27	38817612	160	1.9665	10	9.168	5.735	14.903
L3	27	38817612	160	1.9665	10	7.038	5.292	12.33

This table shows the implementation of ASCON algorithm on different parameters.Data size is used 3.51 MB and encryption time range between 0.484 to 0.528 seconds. All things are depends on the size of data when data size increase 27 MB the time for encryption and decryption becomes extremely high.Sothe result is the computational overhead of the ASCON method for larger data. The ASCON algorithm is relatively more computationally expensive than LWRSA at all levels.

7. Results and Discussion

7.1 Comparative Time complexity of LWRSA algorithm and ASCON algorithm for small size data (3.51 MB)

Table 1 compares the encryption and decryption speeds of two algorithms, namely ASCON and LWRSA, at three operational levels: L1, L2, and L3. The time-sensitive application effectiveness of LWRSA is demonstrated by its consistently lower encryption and decryption times compared to ASCON. Encryption times for LWRSA gradually decrease from L1 (0.029 seconds) to L3 (0.016 seconds). Decryption times differ slightly, with a peak at L1 of 0.035 seconds and stabilizing at L2 and L3 to 0.024 seconds. The encryption and decryption timings for the ASCON algorithm are considerably longer, with a range from 0.484 seconds (L1) to 0.502 seconds (L2) and 0.600 seconds (L3) to 0.616 seconds (L2), respectively. These results therefore reveal that LWRSA outperforms others in terms of speed performance. In some instances, it would thus be suitable when fast encryption and decryption operations are required.

Table 4: Time complexity of LWRSA algorithm and ASCON algorithm for **3.51MB**

Algorithm	Levels	Time(In Sec)	
		Encryption	Decryption
LWRSA Algorithm	**L1**	0.0290	0.0350
	L2	0.0240	0.0240
	L3	0.0160	0.0240
ASCON Algorithm	**L1**	0.484	0.604
	L2	0.502	0.616
	L3	0.486	0.600

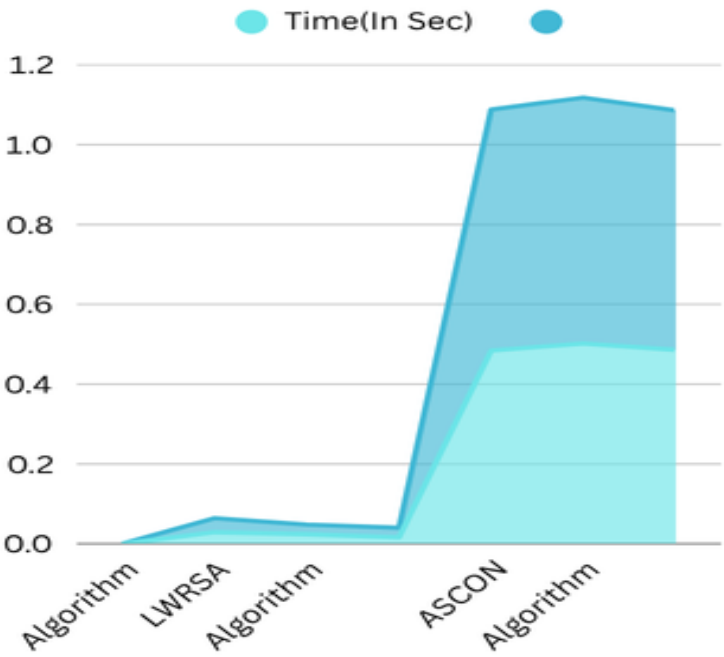

Fig 2:Time complexity of LWRSA algorithm and ASCON algorithm for3.51MB

7.2 Comparative Time complexity of LWRSA algorithm and ASCON algorithm for data size 27 MB

The comparison in the encryption time of the two algorithms, the ASCON and the LWRSA at each of the three operational levels-L1, L2, and L3-and the times that are attributed to decryption between both algorithms show how LWRSA has lesser time compared with its counterpart at L1 is at 0.1195s; at L3, is 0.200s decryption takes 0.320 at L1 up to 0.230 seconds at L3. In contrast, the encryption time for ASCON algorithm is significantly longer because its values range from 5.168 seconds at L3 to 10.406 seconds at L2, and the decryption times are between 5.239 seconds at L3 and 5.997 at L1. These results clearly show that for time efficiency, LWRSA is faster than ASCON; hence it makes a better application in cases where it's required to be fully effective on time.

Table 5: Time complexity of LWRSA algorithm and ASCON algorithm for 27 MB

Algorithm	Levels	Time(In Sec)	
		Encryption	Decryption
LWRSA Algorithm	L1	0.1195	0.320
	L2	0.160	0.290
	L3	0.200	0.230
ASCON Algorithm	L1	10.009	5.997
	L2	10.406	5.848
	L3	5.168	5.239

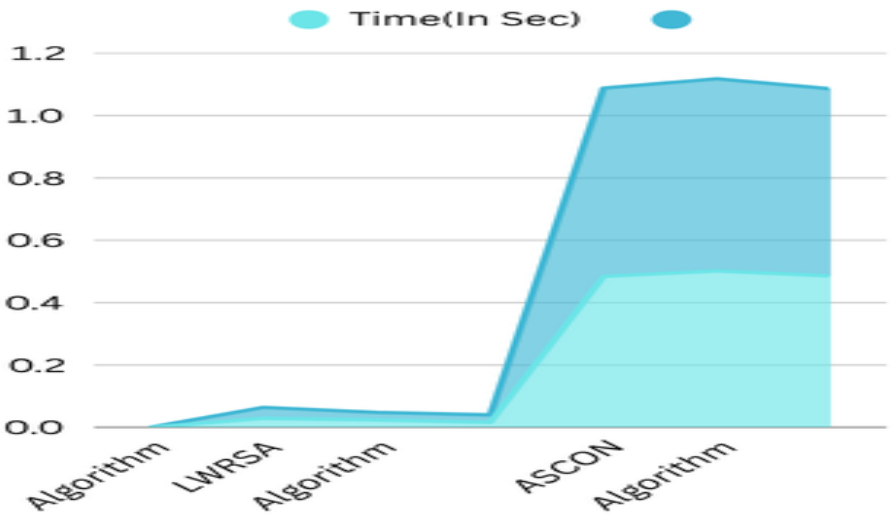

Fig 3: Time complexity of LWRSA algorithm and ASCON algorithm for 27 MB

8. Conclusion& Future Scope

LWRSA provides time-efficient encryption suitable for latency-sensitive applications, while ASCON offers standardized cryptographic guarantees. The Lightweight RSA Algorithm is less complex than the ASCON Algorithm, according to the comparison. We have chosen to employ the traditional approach because the RSA algorithm is larger and the ASCON algorithm takes longer. The benefit of multiple encryptions is that they offer greater security since, even in the event that some of the component ciphers are cracked or some of the secret keys are discovered, the original data can still be kept private.

Lightweight RSA (LWRSA) and ASCON algorithm optimization for real-time IoT devices to improve speed and energy economy is part of the future scope of this comparison. Hybrid encryption, which combines the lightweight design of ASCON with the key management of LWRSA, can be investigated further for enhanced data security. It is possible to research implementation on edge and cloud networks, defense against side-channel and quantum assaults, and adaption in IoT communication protocols such as MQTT and CoAP. For upcoming IoT and embedded system applications, secure, effective, and scalable cryptographic solutions can be developed through benchmarking with other lightweight algorithms and employing machine learning for performance optimization.

9. References

[1] Balaji, R., Sriraam, C., Lionel Donato, L., & Kanthimathi, S. (2024, December). A Dual-Layer Approach: Combining Lightweight and Dynamic RSA for Enhanced Data Security. In *2024 5th International Conference on Communication, Computing & Industry 6.0 (C2I6)* (pp. 1-6). IEEE.

[2] Neve, R. P., & Bansode, R. (2023, February). Performance Evaluation of Lightweight ASCON-HASH Algorithm for IoT Devices. In *International Conference on Intelligent Computing and Networking* (pp. 355-366). Singapore: Springer Nature Singapore.

[3] Chang, Q., Ma, T., & Yang, W. (2025). Low power IoT device communication through hybrid AES-RSA encryption in MRA mode. *Scientific Reports*, *15*(1), 14485.

[4] Singh, S., Sharma, P. K., Moon, S. Y., & Park, J. H. (2024). Advanced lightweight encryption algorithms for IoT devices: survey, challenges and solutions. Journal of Ambient Intelligence and Humanized Computing, 15(2), 1625-1642.

[5] Sarker, K. U. (2025). A systematic review on lightweight security algorithms for a sustainable IoT infrastructure. *Discover Internet of Things*, *5*(1), 1-20.

[6] Sharma, I., & Saxena, M. A Review of Lightweight Cryptography Algorithm for Healthcare Using Multi-Level Encryption. Available at SSRN 4700912.

[7] Isha, Saxena, M., & Jha, C. K. (2022). Multilayered architecture for secure communication and transmission for internet of things. In Soft Computing for Security Applications: Proceedings of ICSCS 2022 (pp. 691-699). Singapore: Springer Nature Singapore.

[8] Oh, Y., Jang, K., & Seo, H. (2025). Quantum Security Evaluation of ASCON. *Cryptology ePrint Archive*.

[9] Sharma, I., & Saxena, M. A Review of Lightweight Cryptography Algorithm for Healthcare Using Multi-Level Encryption. Available at SSRN 4700912.

[10] Labbi, Zouheir &Senhadji, Mohamed &Maarof, Ahmed &Belkasmi, Mostafa. (2020). Lightweight Cryptographic for Securing Constrained Resource IoT Devices. International Journal of Innovative Technology and Exploring Engineering. 4. 181-188. 10.35940/ijitee.D9060.029420.

[11] S. K. Bhatti, K. M. Aamir and M. Deriche, "A Scalable DES Based Hashing Algorithm," *2023 24th International Arab Conference on Information Technology (ACIT)*, Ajman, United Arab Emirates, 2023, pp. 1-5, doi: 10.1109/ACIT58888.2023.10453719.

[12] Budati AK, Snv G, Cherukupalli K, P. AK, Moorthy T. VK (2021), "High speed data encryption technique with optimized memory based RSA algorithm for communications". *Circuit World*, Vol. 47 No. 3 pp. 269–273, doi: https://doi.org/10.1108/CW-10-2020-0282.

[13] Bahrami, Marziyeh, Mohammad Esmaeili, and Maryam Farahbakhsh. "Considering safety in the internet of things and necessities of technological investigation." *Journal of Network Security Computer Networks* 7.2 (2021): 1-7.

[14] A. Fotovvat, G. M. E. Rahman, S. S. Vedaei and K. A. Wahid, "Comparative Performance Analysis of Lightweight Cryptography Algorithms for IoT Sensor Nodes," in *IEEE Internet of Things Journal*, vol. 8, no. 10, pp. 8279-8290, 15 May15, 2021, doi: 10.1109/JIOT.2020.3044526.

[15] Khan, Muhammad Nauman, Asha Rao, and Seyit Camtepe. "Lightweight cryptographic protocols for IoT-constrained devices: A survey." *IEEE Internet of Things Journal* 8.6 (2020): 4132-4156.