iJRASET
International Journal For Research in
Applied Science and Engineering Technology

Volume: 12 Issue: X Month of publication: October 2024

DOI: https://doi.org/10.22214/ijraset.2024.64519

Enhancing IOT Security: Investigating Lightweight Encryption Algorithms for Resource-Constrained Devices

DR. Diwakar Ramanuj Tripathi[1], Huzaifa Naz Nasim Akhtar[2], Rohit Rajendra Bhandarkar[3]
[1]HOD, PG Department Of Computer Science, [2, 3]Research Scholars, S.S. Maniar College Of Computer & Management, Nagpur

Abstract: In this work, we examine three LWCs: namely AES-128, SPECK, and ASCON, considering their presentation on resource-constrained IoT devices. With the large-scale deployment of IoT in all areas of industry, ensuring the security and efficiency of cryptographic implementations has become highly critical because typical IoT devices are usually characterized by limited memory, processing power, and energy resources. The study ascertains the memory usage, throughput, energy efficiency, and strength of security in the chosen algorithms by highly popular resource-constrained boards such as Arduino Nano and Arduino Micro. The benchmarks have shown that SPECK has the highest throughput, which is much efficient for constrained environments. One of the significant features of ASCON is that it has minimized memory usage and high energy efficiency. Therefore, it suits for long-term usage in IoT. AES-128 is secure but resource-intensive, so its usage may be irrelevant in very constrained environments. The results are of great value for IoT developers as a contribution to the selection of cryptographic algorithms based on the conditions and resource restrictions of the IoT devices involved so that optimized security solutions are achieved.

Keywords: Lightweight Cryptographic Algorithms, IoT, Resource-Constrained Devices, Encryption, Cryptographic Security.

I. INTRODUCTION

An iconic concept in Internet annals, the "Internet of Things" (IoT) refers to a system of interconnected, miniature devices that, with the use of the IPV6(6LoWPAN) protocol, can link millions of objects on different platforms. Radio frequency identification (RFID) and wireless sensor networks (WSNs) constitute the backbone of the Internet of Things (IoT) and find extensive use in fields as diverse as environmental monitoring, traffic management, and home automation. New estimates from CISCO put the number of Internet-connected devices at around 50 billion by 2020. Instead of connecting individuals, it appears that technology in the coming years will connect devices. It follows that our physical interactions with the world will be transformed by the ubiquitous presence of sensors, actuators, smart items, and RFID tags. This growth poses serious threats to the privacy and security of IoT systems.

The storage, processing power, and gate count of IoT devices are kept to a minimum, and there is a restricted number of security gates as well. The primary objective of developing a lightweight cypher is to increase security with little resource consumption. Given the limited resources of these devices, traditional cryptographic algorithms are ill-suited for secure data transmission. Internet Security Protocols generally use one such state-of-the-art method, "Lightweight cryptography (LWC)," to provide enough protection. Stream, block, hash, and authenticated cyphers are the four main categories of lightweight symmetric cryptographic methods. Since they are more practical and easier to use than other cyphers, block cyphers are considered workhorses. Block cyphers aim to offer security, integrity, and authenticity as their key purposes. A lot of people in the research, academic, and consulting communities have been discussing about the lightweight block cypher design recently. In contrast to previous cryptographic cyphers, this paper gives a high-level overview of the software and hardware components used to create new, lightweight block cyphers.

A. IoT and Lightweight Cryptography

In lightweight symmetric algorithms, block cyphers often take the place of academic designers. Based on their structural anatomy, symmetric block cyphers are either SPN or Feistel networks. SPNs use a structure that is straightforward to analyse and take blocks of plaintext and keys. By reversing the key schedule, FN achieves the same encryption and decryption as before. A number of algorithms have been developed to deal with lightweight design constraints. In certain cases, block cyphers are to blame for these patterns. The emphasis is on crucial scheduling and nonlinear procedures.

1) *Nonlinear Methods:* There is no linearity in the cryptography algorithm. S-Boxes and non-linear mathematics make this quality accessible. S-Box algorithms can be categorised into two classes. In the first group, LUTs are used, whereas in the second, bit-slices are employed. When performing mathematical operations, the ARX primitives exclusively take modular additions into account. In LUT algorithms, S-Boxes and look-up tables are used. While S-Boxes are used by bit cut based algorithms also, table look-ups are excessive for the S-Box layer in these cases. S-Box calculations can be parallelised with the use of bitwise operations such as AND and XOR on words. When it comes to microcontroller cyphers, Felics framework recommends ARX-based algorithms.
2) *Key Schedule:* To simplify, lightweight encryption methods use key scheduling based on round functions and Even-Mansour architecture. The Even-Mansour method uses round constants and bits of the master key picked every round to generate subkeys without complex logic or hardware-intensive key state modifications. The method that relies on round functions refreshes the key state by reusing parts of the round function or the entire thing. An increase in mode flexibility is achieved by a "tweak" with the key, a public variable, in some new lightweight algorithms. This modification introduces unpredictability without influencing crucial timetables.

II. LITERATURE REVIEW

Sheena, N. (2024) created ways of lightweight cryptography for Internet of Things devices with limited resources. The IoT seamlessly connects the physical and digital realms. In order for heterogeneous IoT devices with limited resources to exchange data, communication protocols are essential. Security breaches are more likely to occur in systems with massive data flows. Encryption is the sole method that can guarantee the safety of data. Traditional encryption methods are inapplicable to IoT devices because of their limited computing capacity, communication capabilities, energy efficiency, and memory. The goal of developing lightweight protocols is to provide cost-effective security and performance. There are various lightweight cryptographic methods available, including normal, ultra, hybrid, and multilevel. Threats and lightweight methods to prevent critical assaults are also covered. This chapter provides solutions to problems and suggests a cryptographic system for transporting data at the application layer of the Internet of Things (IoT).

Alluhaidan, A. S. D. (2023) included symmetrical encryption, a modified Feistel architecture, and a specialist proxy network (SP). Regardless of the capabilities of individual networks or resources, the IoT will link a large number of networked devices. User privacy, security, and communication are paramount in the development of the IoT. Particularly when working with limited hardware, many applications necessitate encrypted connections. More and more devices are connecting to the internet, which means that low-power, networked computers are need. These gadgets have a vast amount of control and monitoring data to analyses, yet they have limited resources. Protect sensitive devices with encryption. Computationally costly and memory intensive encryption algorithms, such as RSA or AES, impact device performance. It is possible to hack simple encryption. An encryption solution that is both secure and lightweight for computing devices is used to overcome these difficulties. Tests have shown that the protocol is both secure and energy efficient. To encrypt symmetric keys, evolutionary algorithms and Feistel cypher sequences produce rounds and sub-keys. Processing cycles are minimized and security is assured.

Khan, M. N. (2020) built the Internet of Things (IoT) architecture, compute capacities of end, fog, cloud, and edge devices, and lightweight cryptographic protocols. One emerging technology that bridges the gap between the digital and physical realms is the IoT. Homes, hospitals, water and sanitation systems, transportation, and environmental monitoring all make use of the Internet of Things. IoT smart gadgets offer limitless potential, but they also present serious security vulnerabilities due to their limited computing, communication, storage, and energy capabilities. There are a number of computationally lightweight cryptography methods that can be used by IoT smart devices that have limited resources. Because nodes in resource-rich IoT systems (such as those operating in cloud, fog, or edge modes) can execute computationally expensive cryptographic protocols and operate in more hostile situations, lightweight solutions leave these systems vulnerable. The disequilibrium in computing power among nodes means that Internet of Things security protocols need to be flexible. It is clear that elastic cryptographic protocols are required to accommodate the asymmetric capabilities of IoT nodes after comparing the benefits, drawbacks, and vulnerabilities of various lightweight cryptographic solutions.

Meng, T. X., & Buchanan, W. (2020) examined future developments in lightweight algorithms and provided research on Internet of Things (IoT) architectures that can replace traditional cyphers. Ensuring the security, privacy, and integrity of sensitive information is of the utmost importance, especially when it comes to transmission, storage, and access. Systems with sufficient processing power and memory are ideal for using traditional cryptography methods such as AES, SHA 2 hashing, RSA, and Diffie Hellman for message authentication and identification.

These are not well-suited for use in embedded systems or sensor networks because of their diminutive size and low price. Lightweight cryptographic solutions address many traditional cryptography concerns, making them suitable for devices with limited resources. This include constraints on manufacturing cost, processing power, memory, and physical size. In order to test whether an embedded device is compatible, performance metrics are chosen with care. This study compares symmetric block cyphers, especially lightweight ones, against stream cyphers and public key techniques on flexible systems, and discovers performance characteristics for each. An efficient LW cypher will be tested against a variety of block cyphers on an Intel-core MacBook Pro and an ARM-processor-limited Raspberry Pi.

Labbi, M. Z. (2020) provided an outline of the essential building blocks for LWC in the IoT and laid out LWC algorithms according to important dimensions, block sizes, topologies, and rounds. An emerging network and computing paradigm, the Internet of Things (IoT) connects physical objects electronically. By linking up various gadgets, such as RFID tags, NFC tags, sensors, and more, they are able to converse online. The proliferation of interconnected goods is causing IoT devices to transmit and receive vast quantities of data. Despite dealing with critical data, the majority of IoT devices are underpowered. For this reason, conventional cryptographic methods fail to meet the necessary standards for safety because of limitations in available computing power, memory, energy, and performance. This led to the introduction of lightweight cryptographic primitives, or LWC. The hunt for an algorithm that meets the requirements of IoT applications is a hotly debated topic. Additionally, we look into security in the limited IoT setting, with an emphasis on research challenges, difficulties, and potential solutions. Finally, we resolved outstanding concerns and proposed a secure method to enhance the limited IoT environment.

III. RESEARCH METHODOLOGY

A. Research Method

This work assesses current LWC algorithms on Internet of Things (IoT) boards with limited resources. Memory usage, processing speed, data throughput, power consumption, and scalability will all be factors in the assessment. The assessment includes setting up a test bed with sample IoT devices and running tests using the suggested LWC algorithms. For this research, we chose three LWC algorithms that are used in Internet of Things applications and have been authorised by NIST: AES-128, SPECK, and ASCON. To evaluate these algorithms' efficiency, speed, memory utilisation, and throughput, we run benchmarks. To ascertain their usefulness and acceptability for devices with limited resources, this research is crucial. In order to assist IoT developers in selecting the optimal algorithm for their applications with limited resources, the evaluation will highlight the advantages and disadvantages of each method.

B. Board Selection

This study begins by identifying boards that are used in Internet of Things applications and have limited resources. For Internet of Things (IoT) use cases across domains, these boards are ideal because they reduce power consumption, maintenance costs, and battery life. Many boards have trouble securely implementing cryptographic algorithms because of memory and CPU capacity limits. Throughout the program's deployment, energy usage must be monitored. Presented here are some of the most common Internet of Things (IoT) boards that have limited resources.

C. Algorithm Selection

This study selects and evaluates three lightweights cryptographic (LWC) algorithms for Internet of Things (IoT) devices with limited resources. Size of the key, attack resistance, efficiency, and performance trade-offs are all considered, in addition to security and compatibility with IoT devices. The following algorithms were selected:

1) The NIST-approved authenticated encryption method known as ASCON is both lightweight and secure.
2) SPECK—A simplified block cypher that, in some restricted contexts, has strong hardware performance.
3) Despite its origins being in lightweight cryptography, **AES-128** has become a popular encryption standard for Internet of Things devices.

Time to execution, memory consumption, and security robustness are all measured for these algorithms.

IV. DATA ANALYSIS

This part of the review dives into the assessment rules, readings, and finishes of the trial arrangement.

A. Evaluation Standards: Evaluation Performance Metrics

These metrics will be employed to assess the chosen LWC algorithms:

Utilization of memory: When dealing with limited resources, memory usage is a key factor in the algorithms' practicality and viability. The resting code size (ROM utilization) of the algorithm, which encompasses encryption, decryption, and RAM use, is represented by this indication. The algorithm's auxiliary functions and subroutines are also part of it. Measuring memory use is done in two sections:

1) IoT boards with limited resources often use flash memory, which can store both read-only data and programs, as well as configuration data and permanent states, in a non-volatile format. The size of the executable modified into the board's perused just memory (ROM) or blaze memory is known as code size or ROM usage.

2) Random Access Memory (RAM) utilization: the quantity of RAM consumed by the method while it is running, which shows how efficient it is with resources and where its performance might be limited. Energy usage is also assessed.

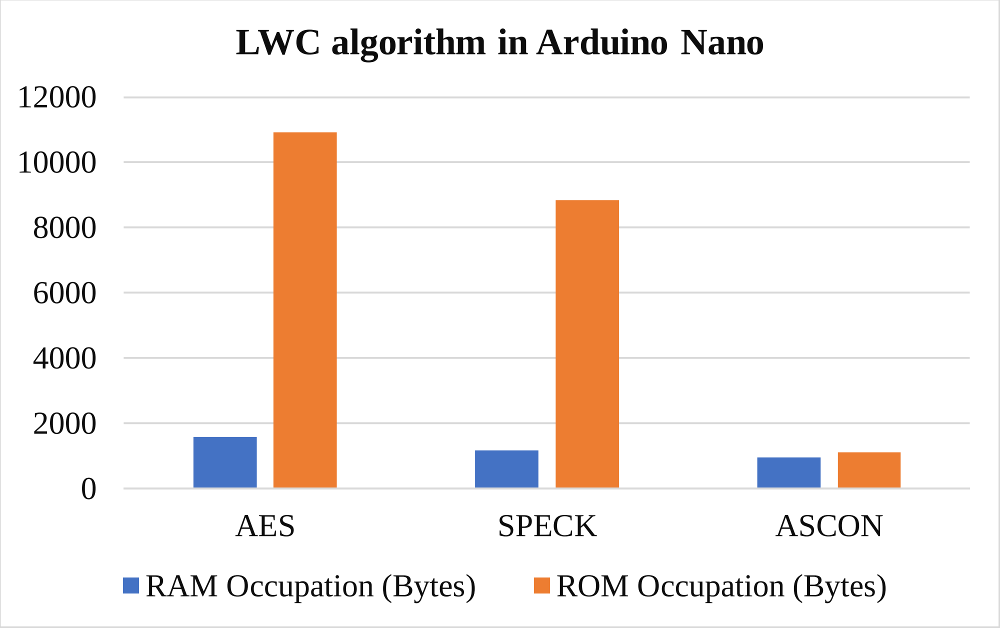
Assessment and observation of RAM/ROM occupations: Algorithm RAM and ROM utilization during execution is displayed in Tables 2 and 3, respectively.

Table 1: Memory control of LWC algorithm in Arduino Nano

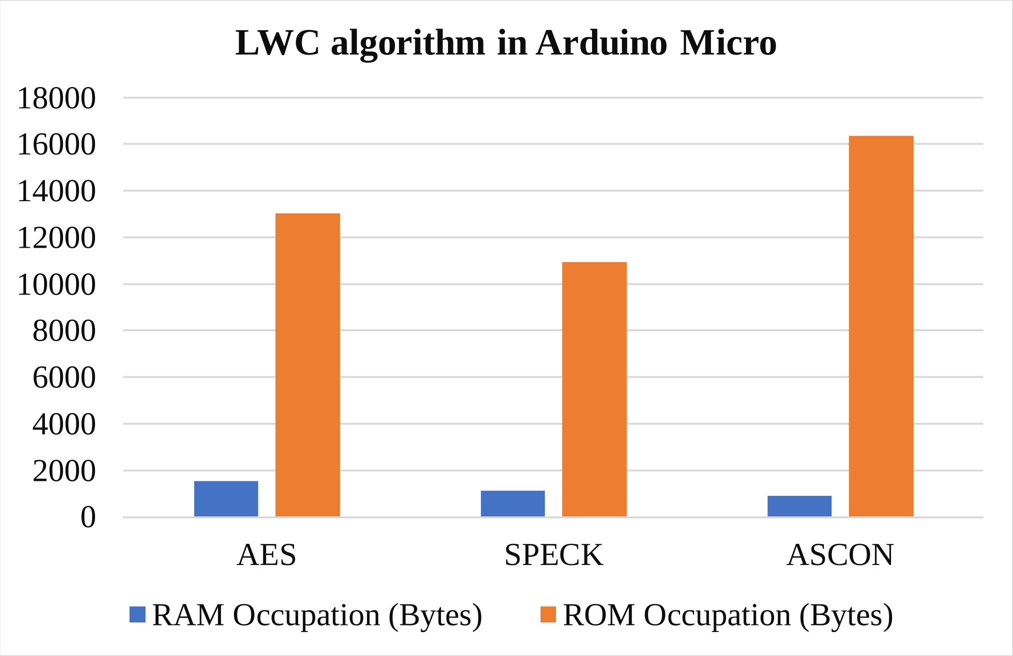
	RAM Occupation (Bytes)	**ROM Occupation (Bytes)**
AES	1568	10,930
SPECK	1167	8850
ASCON	938	1110

Table 2: Memory control of LWC algorithm in Arduino Miniature

	RAM Occupation (Bytes)	ROM Occupation (Bytes)
AES	1540	13,016
SPECK	1130	10,938
ASCON	907	16,357



(a)



(b)

Figure 1: (a) & (b) shows memory utilized in Arduino Nano and Miniature

SPECK's implementation is the lightest at run time compared to the other two algorithms, and ASCON's implementation is the lightest at rest due to its low RAM utilization.

3) Throughput: A cryptographic algorithm's throughput is a proportion of its proficiency not entirely set in stone by the quantity of encryption or unscrambling tasks performed per time unit. Software or equipment improvement methodologies, the intricacy of the algorithm, and the handling capacity of the equipment all assume a part in deciding the throughput of an encryption framework. One factor that can impact the throughput of cryptographic algorithms is key scheduling.

$Throughput=\alpha/t$ (2), where α = bit count and t = operation duration.

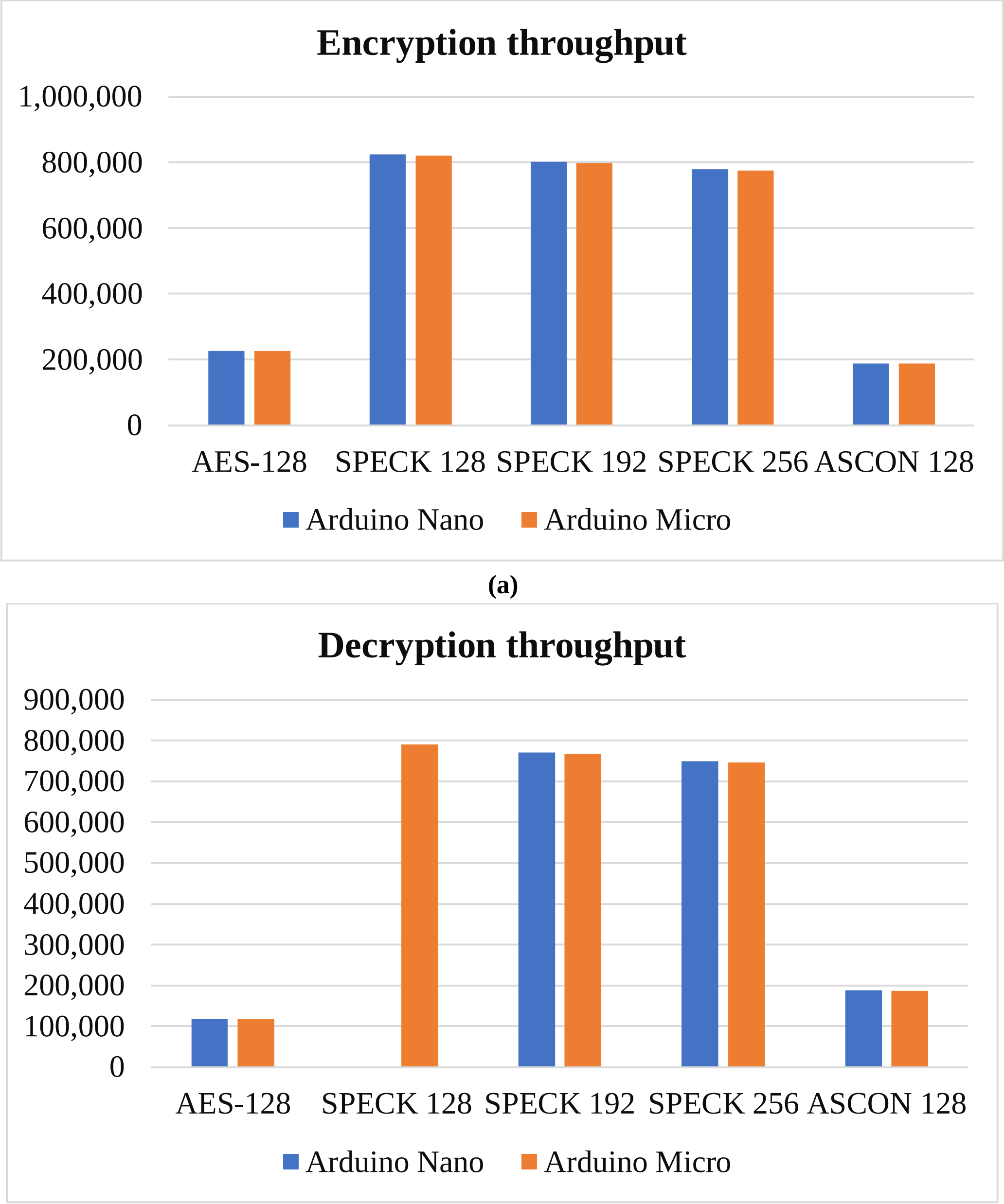
Analysis and measurement of throughput: During encryption and decryption, the throughput is monitored separately. Both Table 3 and Table 4 summaries the measured throughput. SPECK outperforms the other two algorithms in terms of throughput.

Table 3: Encryption throughput

	Arduino Nano	Arduino Micro
Encryption	Throughput (Bits/s)	Throughput (Bits/s)
AES-128	230,040	226,910
SPECK 128	826,040	818,275
SPECK 192	803,701	795,033
SPECK 256	780,658	778,067
ASCON 128	190,350	184,380

Table 4: Decryption throughput.

	Arduino Nano	Arduino Micro
Decryption	Throughput (Bits/s)	Throughput (Bits/s)
AES-128	120,602	118,999
SPECK 128	795,28	790,577
SPECK 192	768,698	769,138
SPECK 256	750,418	748,959
ASCON 128	189,520	184,557



(a)

(b)

Figure 2: (a) and (b) shows encryption and decryption throughput.

B. Security Analysis

The security analysis of AES-128, SPECK, and ASCON, which are designed for devices with limited resources, reveals trade-offs between security and efficiency. Multiple researchers have tested the algorithms' safety extensively. Analysis of comparative studies follows.

1) AES-128: This forms the basis of the encryption standard. As a symmetric encryption algorithm, NIST developed AES-128. It protects against cryptographic attacks, such as differential and linear cryptanalysis, and is a reliable security solution. In theory, symmetric-key algorithms are at risk from quantum computing. According to the study, the effective key size of AES-128 will be reduced to 2 by utilizing Grover's method to accelerate brute force searches.

2) One thing that stands out about the SPECK family of lightweight block cyphers is how flexible and simple they are. A lot of research has gone into SPECK's cryptographic protections. Even while there's some pushback, it's still not as secure as AES. Careful construction of the procedures is required to protect applications from side-channel attacks.

In settings with limited resources, the safety of ASCON has been thoroughly examined by numerous scholars. Secure and private information is provided by ASCON. It satisfies stringent security requirements while minimizing overhead, allowing devices to keep their performance and power consumption levels. The security and efficiency features of three algorithms for devices with limited resources are compared in Table 5.

Table 5: Security efficiency analysis

Algorithm	Security Strength	Efficiency	Suitability for IoT Devices
AES-128	High	Moderate (requires significant computational resources)	Secure, but not optimal for highly resource-constrained devices
SPECK	Moderate (subject to some security concerns)	High (tailored for lightweight operations)	Highly suitable for low-power, constrained devices
ASCON	High (excellent resistance against various attacks)	High (optimized for both speed and performance)	Very suitable for resource-limited IoT devices, with minimal overhead

Results from testing and comparing the lightweight cryptographic algorithms suggest that AES-128, SPECK, and ASCON meet the evolving resource constraints of IoT devices with promising performance. Results demonstrate that SPECK outperforms because to its reduced latency and faster throughput when speed latency readings are taken during encryption and decryption. However, when compared to the other algorithms, AES-128 seems to have better latency and key scheduling performance. Internet of Things (IoT) devices with limited resources that must balance the speed of encryption and decryption will find ASCON to be an excellent option due to its high energy economy, low memory usage, and good resilience to cryptographic attacks.

V. CONCLUSION

The performance of three LWC algorithms-AES-128, SPECK, and ASCON-will be successfully benchmarked on resource-constrained IoT boards in terms of memory consumption, throughput, energy efficiency, and security robustness. Among the three selected LWC algorithms, SPECK appears to be a promising candidate for high-throughput and low-latency applications, especially when the corresponding IoT appliances have constrained memory budgets as well as a strict energy budget. AES-128 provides better security but uses much more memory and higher computation, which may challenge its deployment to enough constrained devices. ASCON is the best balanced in regard to efficiency and security among them and is outstanding over other choices because of low memory size and high resistance to all kinds of cryptographic attacks, which perfectly fits the requirements proposed for IoT devices meant to have extended battery life. Comparing these cases already displays that the choice of cryptographic algorithms contingent upon the specific constraints and performance requirements of a device at hand can significantly improve IoT security.

REFERENCES

[1] Alluhaidan, A. S. D., & Prabu, P. (2023). End-to-end encryption in resource-constrained IoT device. IEEE Access, 11, 70040-70051.

[2] Khan, M. N., Rao, A., &Camtepe, S. (2020). Lightweight cryptographic protocols for IoT-constrained devices: A survey. IEEE Internet of Things Journal, 8(6), 4132-4156.

[3] Kuldeep, G., & Zhang, Q. (2021). Design prototype and security analysis of a lightweight joint compression and encryption scheme for resource-constrained IoT devices. IEEE Internet of Things Journal, 9(1), 165-181.

[4] Kumar, S., Kumar, D., Dangi, R., Choudhary, G., Dragoni, N., & You, I. (2024). A Review of Lightweight Security and Privacy for Resource-Constrained IoT Devices. Computers, Materials and Continua, 78(1), 31-63.

[5] Labbi, M. Z., Maarof, A., &Belkasmi, M. (2020). Lightweight cryptographic for securing constrained resource IoT devices. Int. J. Innov. Technol. Exploring Eng., 9, 8.

[6] Lara, E., Aguilar, L., García, J. A., & Sanchez, M. A. (2018). A lightweight cipher based on salsa20 for resource-constrained IoT devices. Sensors, 18(10), 3326.

[7] Mahlake, N., Mathonsi, T. E., Du Plessis, D., &Muchenje, T. (2023). A Lightweight Encryption Algorithm to Enhance Wireless Sensor Network Security on the Internet of Things. J. Commun., 18(1), 47-57.

[8] Mamvong, J. N., Goteng, G. L., Zhou, B., & Gao, Y. (2020). Efficient security algorithm for power-constrained IoT devices. IEEE Internet of Things Journal, 8(7), 5498-5509.

[9] Meng, T. X., & Buchanan, W. (2020). Lightweight cryptographic algorithms on resource-constrained devices.

[10] Noura, H., Couturier, R., Pham, C., & Chehab, A. (2019, October). Lightweight stream cipher scheme for resource-constrained IoT devices. In 2019 International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob) (pp. 1-8). IEEE.

[11] Radhakrishnan, I., Jadon, S., &Honnavalli, P. B. (2024). Efficiency and Security Evaluation of Lightweight Cryptographic Algorithms for Resource-Constrained IoT Devices. Sensors, 24(12), 4008.

[12] Sarker, V. K., Gia, T. N., Tenhunen, H., &Westerlund, T. (2020, June). Lightweight security algorithms for resource-constrained IoT-based sensor nodes. In ICC 2020-2020 IEEE International Conference on Communications (ICC) (pp. 1-7). IEEE.

[13] Sheena, N., Joseph, S., & Shailesh, S. (2024). Lightweight Encryption Algorithms for Resource-constrained Devices for Internet-of-Things Applications. In Emerging Trends for Securing Cyber Physical Systems and the Internet of Things (pp. 19-40). CRC Press.

[14] 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, 1-18.

[15] Thabit, F., Can, O., Aljahdali, A. O., Al-Gaphari, G. H., &Alkhzaimi, H. A. (2023). Cryptography algorithms for enhancing IoT security. Internet of Things, 22, 100759.