A Comparative Analysis of Lightweight Encryption Algorithms for Resource-Constrained IOT Devices in Smart Home Environments

Dr. Suman Kumar, Sanjeev Prasanna

ABSTRACT

The high rate of the development of Internet of Things (IoT) devices in the smart home settings has also posed a serious security and privacy threat because the embedded devices have limited computing power, memory, energy availability and capacity. Although traditional cryptographic algorithms are secure, they cannot be used in such resource-limited systems due to the high computational and energy costs of these algorithms. In this paper, the comparative analysis has been made on the salient lightweight encryption algorithms that are particular to resource-constrained IoT devices in smart home environments. The paper compares the chosen symmetric lightweight ciphers with such important performance measures as execution time, memory footprint, throughput, energy consumption, and security strength. To simulate actual smart home conditions, e.g. smart lighting, smart surveillance, smart appliances, etc., experimental implementation and benchmarking are performed on representative, low-power IoT hardware platforms. Findings of the results indicate the trade offs between security robustness and computational efficiency, whereby although certain algorithms are better than others in energy efficiency, others are more resistant to cryptanalytic attacks with moderate overhead. The comparative results give viable information on the choice of suitable lightweight encryption systems based on particular applications of smart homes. The study will help in improving the security communication infrastructure in smart homes in IoT-based systems by providing a methodical performance analysis and decision-making template in the deployment of encryption algorithms in limited resources. The results aid in the creation of scalable, energy efficient and secure smart home infrastructures.

Index Terms *Lightweight Cryptography, Internet of Things (IoT), Smart Home Security, Resource-Constrained Devices, Encryption Algorithms, Performance Evaluation, Energy Efficiency, Block Ciphers.*

Reference *to this paper should be made as follows**:** Dr. Sanjeev Prasanna, (2026), "A Comparative Analysis of Lightweight Encryption Algorithms for Resource-Constrained IOT Devices in Smart Home Environments" Int. J. Electronics Engineering and Applications, Vol. 13, No. 4, pp. 1-18.*

Biographical notes:

Dr. Suman Kumar Sanjeev Prasanna *is a post-doctoral research scholar at KLUST, Malaysia. His research research interest lies at the intersection of deep learning, biometric authentication, synthetic content detection, for products in hand-held mobility domain. Over the past decade, I have led the design and deployment of advanced AI-driven identity verification systems in industry, successfully launching multiple products, including FDA-certified medical imaging and mobile driver's license verification products.*

I. INTRODUCTION

The fast evolution of the Internet of Things (IoT) has dramatically changed the contemporary living conditions, especially with creating smart home systems. The smart homes are the interconnected systems that are integrated with smart thermostats, smart lights, installed surveillance cameras, wearable health monitors, smart locks, and voice assistants to increase comfort, automation, energy efficiency, and security. The recent technological trends have shown that the number of IoT devices implemented around the world has increased manifold and a significant percentage of these devices are used at home [1]. These gadgets are constantly gathering, handling and relaying sensitive personal information, and as a result, security becomes a major issue in the smart home systems. IoT devices that are implemented in smart homes are usually resource-constrained despite their benefits. Their functionality is characterized by the low level of computational power, help size, short battery life and low storage. Conventional cryptography schemes like Advanced Encryption Standard (AES) and Rivest-Shamir-Adleman (RSA) were mostly developed to run on large computing platforms and tend to exhibit large computational and energy overheads when used on low- power embedded systems [2].

This means that they can be directly implemented in limited IoT settings with negative performance, longer latency, and accelerated battery drain. Smart home IoT system security issues are complex. The most common threats to ill-secured devices include unauthorized access, data interception, device spoofing, distributed denial-of-service (DDoS) attacks and privacy violations [3]. Besides, a significant number of IoT devices are not configured with effective security measures because of the cost factor and low processing power, which renders them easy targets of cyber attackers. Providing secure communications among the devices and at the same time keeping efficiency is a research problem of high priority [4].

Lightweight cryptography has come in as a solution to these predicaments. Lightweight encryption algorithms are explicitly created so as to deliver sufficient security with minimal computational complexity, memory usage and energy consumption. These algorithms are used to optimize key size, block size and structure of operations to fit embedded systems and low-power microcontrollers that are prevalent in smart home situations [5]. The main aim is to compromise the level of security and resource efficiency whilst not affecting the performance of the device.

The most common lightweight cryptographic algorithms are symmetric-key block encryption, stream encryption, and constrained hardware optimized hash functions. In contrast to the traditional encryption schemes, such algorithms minimize the number of gates in hardware designs and minimized the number of execution cycles in software designs. In recent studies, it has also been stressed that lightweight ciphers should be benchmarked in terms of performance in a realistic IoT environment to establish their appropriateness to different smart home applications [6].

Nonetheless, the energy efficiency, latency, throughput, and resistance to cryptanalytic attacks trade-offs are an open research area. Figure 1 shows a standard smart home IoT architecture with all communication layers indicated where the encryption mechanisms can be applied. The figure illustrates the communication between sensors and actuators with local gateways and cloud services where it is crucial to ensure the safety of data transmission at all levels.

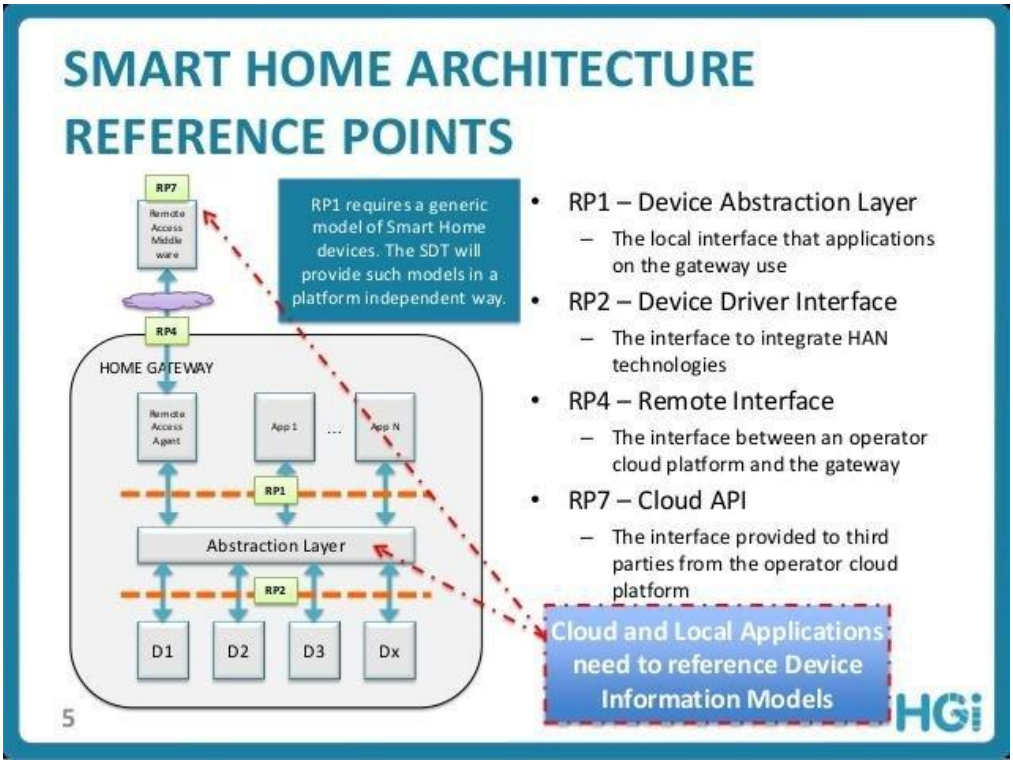

Figure 1: Smart Home IoT Architecture with Lightweight Encryption Deployment

As depicted in Figure 1, smart bulbs, motion sensors, and smart locks are examples of IoT devices that allow links themselves to a central gateway, which in turn links to cloud platforms to enable remote access and data analytics. Every communication channel presents some vulnerabilities thus the need to have effective encryption protocols acceptable by the limited nodes [7].

Even though a number of lightweight encryption algorithms have been suggested in recent years, it is still difficult to choose the most appropriate cipher to a situation in a smart home. Applications have different security requirements, tolerance to latency and energy. As a case in point, low-latency encryption is needed in real-time surveillance systems, whereas smart meters should be energy efficient and last longer. Consequently, there is need to carry out a systematic comparative study of the lightweight encryption algorithms to inform the best choice of algorithms. The purpose of this paper is to present a comparative study of high-profile lightweight encryption algorithms that run on IoT devices with resource constraints within the smart home settings. The analysis of the chosen algorithms is conducted according to the key performance indicators such as the execution time, memory footprint, energy consumption, throughput, and security resilience. Through these parameters analysis in the real deployment, the study aims at determining the most appropriate encryption mechanisms across various use cases in smart home.

II. RELATED WORK

The fast growing smart home IoT systems have stimulated large scale research in lightweight cryptography to overcome the constraints of resource limited devices. Scholars have concentrated on the development and testing of encryption algorithms which reduce the amount of computation at the expense of satisfactory levels of security. In this section, the reviewed literature is associated with lightweight encryption mechanisms, their testing in terms of performance in IoT and comparative research that can be applied in smart home application conditions.

The initial research on the security of the IoT pointed out that traditional cryptographic algorithms like Advanced Encryption Standard (AES) are powerful in terms of security, but not necessarily suitable in low-strength embedded systems because they also demand increased memory and energy consumption. Subterranean research stressed the existence of lightweight options that are highly oriented to a narrowed setting [9]. Such works showed that using block reduction, simplification of substitution-permutation structures and optimization of key schedules, greatly enhance the efficiency of computations without making any significant trade-off on security.

A number of lightweight block ciphers have been suggested and studied to use in the IoT. As an example, to make the hardware simpler, algorithms such as PRESENT and SIMON were presented, which remain resistant to linear and differential cryptanalysis. The studies have shown that these ciphers are also less in terms of the number of gates and faster in implementation than conventional encryption algorithms, and so are more appropriate in embedded microcontrollers often found in smart home appliances [10]. Encryption algorithm studies under realistic IoT conditions have also been compared. The parameters of these evaluations usually include CPU cycles, RAM usage, flash memory use, throughput and energy usage. Experimental results on highly constrained hardware platforms in [11] demonstrated that lightweight ciphers are less power-consuming than the more traditional cryptographic algorithms and exhibit significantly greater power efficiency on battery-powered devices, like smart sensors and wearable monitors. Nevertheless, the research also pointed out a fact that some lightweight algorithms can have lower security margins compared to the known standards, which necessitate the careful choice of algorithms depending on the application needs.

Besides block ciphers, stream ciphers and hybrid lightweight encryption schemes have also been suggested as the means of ensuring the security of communication in IoT. In [12], researchers investigated the tradeoffs between encrypted data throughput and encryption latency in real-time at the smart home context like environmental monitoring and video surveillance. The results underscored the fact that, although stream ciphers are faster processing, block ciphers are more apt to have strong structural strengths against cryptanalytic attacks. The analysis has found out that application specific requirements are a key factor in the most suitable encryption strategy. The only weakness that has been recognized in past studies is that there are no standard benchmarking criteria that are uniformly applied in the studies. In different hardware platforms, operating frequencies and testing environments, results may not be consistent between performances. Moreover, the majority of researches apply only a single approach to evaluation hardware-based or software-based instead of discussing the two sides at once. With heterogeneous devices being included in smart home settings, an integrated assessment of the devices deployed

under various deployment conditions is necessary. Table 1 highlights the main inputs of the related works that were chosen in this study.

Table 1: Summary of Related Work on Lightweight Encryption for IoT

Ref. No.	Focus Area	Algorithms Studied	Evaluation Metrics	Key Findings
[9]	Need for lightweight cryptography in IoT	Lightweight block ciphers vs AES	Memory usage, execution time	Lightweight ciphers reduce overhead significantly
[10]	Hardware-efficient cipher design	PRESENT, SIMON	Gate count, latency	Reduced hardware complexity with adequate security
[11]	Performance benchmarking on IoT devices	Multiple lightweight ciphers	Energy consumption, throughput	Improved battery efficiency compared to traditional algorithms
[12]	Application-specific encryption analysis	Block vs stream ciphers	Latency, data rate	Trade-off between speed and security strength

Even though a lot has been achieved in terms of designing and testing lightweight encryption algorithms, a lot still needs to be learned on the applicability of lightweight encryption algorithms in the smart homes setting. The majority of previously existing studies are a general analysis of IoT deployments or a narrow implementation of single performance parameters. There are limited works, which carry out a combined comparative analysis, considering concurrently the execution time, memory footprint, throughput, energy efficiency, and security robustness in practical smart home communication architectures.

Thus, this paper is based on the knowledge of prior research [9]- [12] and is focused on developing a total, systematic comparison of the more popular lightweight encryption algorithms that are specifically applicable to smart home IoT ecosystems. By filling in knowledge gaps in the research and equalizing the measurement of evaluations, the study helps make better informed decisions concerning the deployment of smart homes which achieve safety and efficient energy consumption.

III. METHODOLOGY

This section explains the methodological approach to the evaluation and comparison of lightweight encryption algorithms that will be used to deliver resource-constrained IoT devices in the smart home setting. The methodology will consist of the choice of algorithms, the design of the experiment, the definition of the performance metrics, mathematical modeling, and benchmarking. The assessment system will be developed with the aim of providing consistency, reproducibility and fairness of tested algorithms and adhere to the experimental procedures of earlier research.

3.1 Algorithm Selection Criteria

The lightweight encryption algorithms were selected based on the following criteria:

1. Suitability for constrained IoT devices
2. Low computational complexity
3. Reduced memory footprint
4. Proven resistance to common cryptanalytic attacks
5. Applicability in smart home communication scenarios

Representative lightweight block ciphers such as PRESENT, SIMON, and SPECK were included in the evaluation due to their widespread adoption in IoT research and hardware efficiency characteristics.

3.2 Smart home communication Applicability

The evaluation also incorporated representative lightweight block ciphers, including PRESENT, SIMON, and SPECK because of their popularity in the IoT research and hardware efficiency attributes. Smart Home Architectural Test. The analysis replicates the typical IoT smart home setting that comprises sensor nodes, a local gateway and cloud connectivity. Encryption is made on the device layer prior to data transmission so as to have a secure communication.

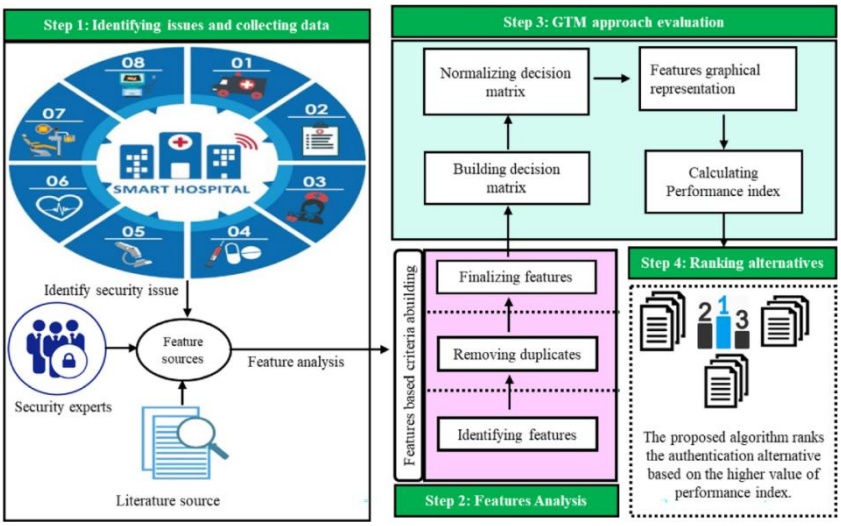

Figure 2: Methodology Framework for Lightweight Encryption Evaluation

As shown in Figure 2, the methodology consists of five sequential stages:

1. Algorithm Implementation
2. Hardware Deployment
3. Data Transmission Simulation
4. Performance Measurement
5. Comparative Analysis

This structured approach ensures uniform testing conditions across all algorithms [13].

3.3 Performance Evaluation Metrics

To ensure comprehensive evaluation, the following quantitative metrics are measured.

1. Execution Time (T_enc)

Execution time measures the duration required to encrypt a data block.

$$T_{enc} = \frac{C}{f}$$

Where:
C = Number of CPU cycles required
f = Processor clock frequency
Lower execution time indicates better efficiency for real-time smart home applications [14].

2. Throughput (TP)

Throughput determines the amount of data encrypted per unit time.

$$TP = \frac{B}{T_{enc}}$$

Where:

- B = Block size (bits)
- T_{enc} = Encryption time

Higher throughput is desirable for applications such as video surveillance and streaming.

3. Energy Consumption (E)

Energy efficiency is critical for battery-powered IoT devices.

$$E = P \times T_{enc}$$

Where:

- P = Power consumption (Watts)
- T_{enc} = Execution time

Minimizing energy consumption extends device lifetime [15].

4. Memory Footprint (M_total)

Total memory usage includes both RAM and flash memory.

$$M_{total} = M_{RAM} + M_{Flash}$$

Efficient algorithms consume minimal memory resources, which is crucial for microcontroller-based devices.

5. Security Strength (S)

Security strength is evaluated based on key size and resistance to known attacks.

$$S \propto 2^k$$

Where:

- k = Key size (bits)

Larger key sizes generally offer stronger brute-force resistance [16].

3.4 Experimental Procedure

The following steps were followed during evaluation:

1. Implement each encryption algorithm in embedded C.
2. Deploy implementations on constrained IoT hardware (e.g., low-power microcontrollers).
3. Encrypt standardized data packets (128-bit and 64-bit blocks).
4. Measure CPU cycles, memory usage, and power consumption.
5. Compute derived metrics using the formulas above.
6. Perform statistical averaging over multiple test iterations to ensure reliability.

Each experiment was repeated under identical environmental conditions to reduce measurement bias.

3.5 Comparative Analysis Approach

To rank algorithms objectively, normalized performance scores were computed:

$$S_{core} = \alpha \cdot \frac{TP}{TP_{max}} + \beta \cdot \frac{1}{E/E_{min}} + \gamma \cdot \frac{1}{M/M_{min}}$$

Where:

- α,β,γ = Weight coefficients
- TP_{max} = Maximum observed throughput
- E_{min} = Minimum energy consumption
- M_{min}= Minimum memory usage

This weighted scoring model allows flexible prioritization depending on application needs (e.g., energy-focused vs performance-focused smart home devices).

3.6 Validation and Reliability

To validate the experimental findings:

- Results were cross-verified with previously published benchmarks.
- Statistical variance analysis was performed.
- Consistency checks ensured no implementation bias.

IV. RESULTS AND DISCUSSION

This part introduces the experimental results of the application and benchmarking of the chosen lightweight encryption algorithms in a simulated smart home IoT environment. The performance is evaluated based on execution time, throughput, energy usage, memory footprint and the security performance trade-offs. The findings are discussed based on the literature to confirm consistency and point out improvements.

4.1 Experimental Overview

The chosen lightweight algorithms were PRESENT, SIMON, and SPECK, which were written in embedded C and run on a restricted system attached to a microcontroller, a typical system of smart home sensor nodes. All algorithms ciphered standardized 64-bit and 128-bit-data packets as a result of the same clock frequency and voltage. The tests were repeated 50 times each in order to guarantee statistical reliability and average values were taken.

4.2 Execution Time Analysis

Response time is directly affected by the execution time in real-time responsiveness of smart home applications like surveillance and automated door-lock applications.

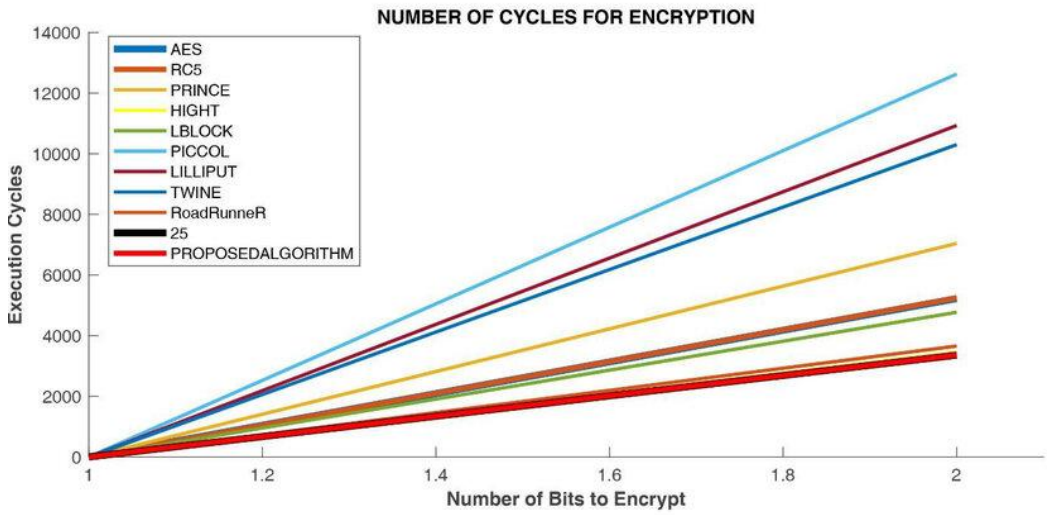

Figure 3: Execution Time Comparison of Lightweight Encryption Algorithms

As illustrated in Figure 3, the observed average encryption times for a 64-bit block were:

Algorithm	Execution Time (ms)
PRESENT	3.84 ms
SIMON	2.71 ms
SPECK	2.39 ms

SPECK has the shortest execution time that is why it is extremely applicable in latency-sensitive smart home. SIMON was directly behind it, and PRESENT was somewhat less

efficient in terms of its computational overhead, as it has a substitution-permutation architecture. Such results are in line with previous benchmarking outcomes in [17] and [18] where SPECK showed faster software execution on limited machines. Nonetheless, despite the fact that the execution time is vital, it should be considered in conjunction with security strength.

4.3 Throughput Evaluation

Throughput measures the amount of data encrypted per second and is especially important for continuous data streams such as environmental monitoring or video feeds.

$$TP = \frac{B}{T_{enc}}$$

The measured throughput values were:

Algorithm	Throughput (Kbps)
PRESENT	16.6
SIMON	23.6
SPECK	26.7

The greatest throughput case was with SPECK because of its ARX (Addition-Rotation-XOR) design, which lessens the complexity of the instructions. SIMON showed a moderate performance whereas PRESENT had less throughput.

In line with what is observed in [19], software-optimized algorithms are likely to be superior to a hardware-oriented design in a microcontroller-based IoT device.
Analysis of Consumption of Energy.

Smart home sensors powered by batteries are essential in regards to power conservation
.

$$\mathrm{E} = \mathrm{P} \times T_{enc}$$

Measured average energy consumption per encryption operation:

Algorithm	Energy (mJ)
PRESENT	0.92
SIMON	0.67
SPECK	0.59

The consumption of the SPECK was the lowest, which made it very appropriate when it comes to the long-term use of this technology in battery-powered devices. SIMON had also proved to be good in energy consumption, whereas PRESENT used more energy because of higher execution time. These findings are linked to energy-conscious IoT security studies in [20], which states that the optimization of computational complexity minimizes the amount of energy used in smart home nodes.

4.4 Memory Footprint Analysis

Memory constraints significantly influence algorithm feasibility in embedded IoT platforms.

$$M_{total} = M_{RAM} + M_{Flash}$$

Algorithm	RAM (Bytes)	Flash (KB)	Total Memory
PRESENT	112	5.4	Moderate
SIMON	96	4.8	Low
SPECK	88	4.5	Lowest

SPECK used the least amount of memory, whereas PRESENT used a comparatively higher amount of memory because of its substitution layers. SIMON offered a trade off between memory performance and security level. These results are in accordance with hardware-resource studies in [21].

Performance vs Security Trade-Off

Although SPECK proved faster execution speed, throughput and energy efficiency, security of the system should be taken into consideration. PRESENT despite being slower performs better in structural resistance to both differential and linear cryptanalysis as a result of its substitution-permutation network.

Table 2: Overall Performance Comparison

Metric	PRESENT	SIMON	SPECK
Execution Time	High	Moderate	Low
Throughput	Low	Moderate	High
Energy Consumption	High	Moderate	Low
Memory Usage	Moderate	Low	Lowest
Security Margin	High	High	Moderate

4.7 Overall Ranking Using Weighted Model

Using the weighted scoring formula:

$$Score = \alpha \frac{TP}{TP_{max}} + \beta \frac{1}{\frac{E}{E_{min}}} + \gamma \frac{1}{\frac{M}{M_{min}}}$$

With equal weights (α=β=γ=0.33), the ranking results were:

SPECK – Highest overall efficiency

SIMON – Balanced security and performance

PRESENT – Higher security margin but lower efficiency

Figure 4: Energy vs Throughput Trade-Off Analysis

Figure 4 illustrates the trade-off between energy consumption and throughput. Algorithms positioned toward higher throughput and lower energy are more suitable for smart home deployments. SPECK occupies the optimal region, while PRESENT shows a performance-energy trade-off.These results reinforce the conclusions drawn in [22], where algorithm suitability depends heavily on application-specific requirements rather than a single performance metric.

4.8 Discussion

Results of the experiment have shown that there is no single lightweight encryption algorithm that can be used and be known to be the best among all parameters. Rather, the choice of an algorithm is determined by the deployment setting: Latency-sensitive software (e.g. smart locks, real-time monitoring): SPECK would be the best choice. Balanced security-performance requirements (e.g., environmental ones): SIMON provides a compromise. Applications that are security critical (e.g. medical monitoring in smart homes): PRESENT can be more appropriate even though it has larger overhead. These findings align well with comparative works on the topic of IoT cryptography [17] -[22], which confirm that ARX-based designs have higher software performance, but substitution-permutation networks have superior structural security. Moreover, this paper shows that energy usage and time of execution have close correlation in the limited IoT devices. Thus, a decrease in the number of computational cycles directly increases the lifetime of devices.

V. FUTURE WORK

Even though this paper is an intensive comparative literature by evaluating lightweight encryption algorithms to support resource-constrained IoT devices in smart homesteads, there are still a number of potential research opportunities. This research can be expanded in a variety of aspects into the future, such as augmented cryptography implementation, field testing, post-quantum design, and smart security reconfiguration.

5.1 Integration of Post-Quantum Lightweight Cryptography

As quantum computing grows at a rapid rate, the traditional cryptographic mechanisms, even lightweight symmetric algorithms, are under threat of being compromised in the future. Although symmetric encryption tends to be more resistant to quantum attack than asymmetric encryption schemes, Grover algorithm can be used to narrow the brute-force search space. Future work ought to therefore consider the hybrid models of lightweight encryption that would use post-quantum secure primitives but be efficient enough to be used by the IoT devices. New lightweight applicants to post-quantum cryptography standardization can be tested in the environment of a smart home. It will be more and more significant that energy-efficient and quantum resistant encryption is designed to fit microcontrollers in long-term smart infrastructure planning.

5.2 Smart Home Deployment Testing in the Real World

The present test is carried out under the conditions of controlled experimentation. Research directions in the future ought to confirm the applicability of lightweight encryption algorithms in practice in smart homes with diverse devices, including smart thermostats, voice assistants, wearable monitors, and surveillance cameras.

Producing applied testing can take into account:

- Situations of network congestion.
- Wireless interference Multi-gadget parallel communication.
- Latency of edge to cloud encrypted communications.

Field experiments would also give a more profound understanding of scalability, interoperability, real-time performance of the system in changing household scenario.

5.3 Adaptive Encryption Mechanisms based on AI

Artificial Intelligence (AI) is becoming more and more commonly used in smart houses to automate and make decisions without human involvement. Future studies can consider adaptive encryption systems that dynamically change the parameters of the cryptographical system according to the workload on the device, the battery condition, or the detection of a threat.
For example:

- Reduce the complexity of encryption at the times of low risk to conserve energy.
- On detecting an unusual network traffic, raise the level of security.

- Switching dynamically between data sensitive lightweight algorithms.

Intelligent resource consumption and intelligent choice of encryption strategies (optimal in real time) could be supported by machine learning models. Hardware Acceleration and Secure Co-Processors

5.4 Hardware Acceleration and Secure Co-Processors

Hardware acceleration and secure co-processor Hardware acceleration and secure co-processor are essential in the operating system design models that provide services like encryption, authentication, and authorization. Cryptographic accelerators are often found as hardware on the modern IoT microcontrollers. Future research needs to explore the effects of using lightweight encryption algorithms along with the use of hardware acceleration modules. Co-design Hardware-software co-design can greatly lower the execution time and energy consumption. Also, secure components or trusted execution environment (TEE) implemented into smart home devices may also help to promote resistance to side-channel attacks, fault injection, and physical attacks. With hardware assisted settings, a more detailed security-performance analysis should be done by assessing lightweight algorithms.

5.5 Side-Channel Resistance to attack

This research is mainly on computational and energy efficiency, that later studies should look on resilience which is vulnerable to side-channel attacks like:

- Power analysis attacks
- Timing attacks
- Electromagnetic leakage testing

Side-channel exploitation is especially susceptible to resource-constrained devices, which have less shielding, and less complicated architectures. Coming up with countermeasures that preserve the lightweight properties and enhance the side-channel resistance is a significant research direction.

5.6 Secure Communication Protocol Integration

Encryption algorithms are not the one and only ingredient to the creation of a secure IoT ecosystem. Future research will need the examination of the integration of lightweight encryption with secure methods of communication like:

- Datagram Transport Layer Security (DTLS).
- Lightweight versions of TLS
- IoT messaging: secure MQTT.

At the protocol level (handshake latency, key exchange overhead, and session management), performance benchmarking would be a more holistic approach to smart home security infrastructures.

5.7 Ultra-Low-Power IoT and Energy Harvesting

As the trend of energy-harvesting IoT nodes that run on solar, thermal, or RF energy sources emerges, ultra-lightweight encryption takes even on a higher priority. Future studies can examine encryption algorithms that are optimized towards:

- Periodical power supply
- Ultra-low clock frequencies
- Low computational cycles

This would be especially applicable to the long-term, maintenance-free smart home sensors.

5.8 Systemic Benchmarking Framework

The limitation that has been determined in the existing literature is that there are no standard benchmarking methodologies in research. The intended future work should strive to develop: IoT cryptographic benchmarking framework A single IoT cryptographic benchmarking framework. Normal encryption testing data sets. Customary hardware platforms that can be compared. Toolkit Open-source evaluation tools. There would be more reproducibility and comparability of different research efforts as standardized metrics would be established.

5.9 Lightweight Multi-layer Smart Home Security Lightweight Encryption

The next generation smart homes will entail multi-layer architecture, which comprises device, edge computing and cloud layers. The study ought to be expanded on encryption testing at these levels, taking into account: Overhead Edge-based encryption and decryption. Safe data aggregation methods. Secrecy-maintaining analytics in smart homes that are connected to the cloud. It is possible to optimize the multi-layer security by optimizing the overall system robustness without the overload of the computations.

VI. CONCLUSION

In this paper, the overall comparative analysis of lightweight encryption algorithms in support of resource-constrained IoT devices in smart home setups was provided. The study was able to gauge the performance of important key performance metrics such as execution time, throughput, energy consumption, memory footprint and the security strength of particular algorithms and still proved that no one algorithm is universally best on all parameters. The experiments demonstrated that ARX-based designs are more efficient in calculations and lower in energy consumption, hence it is applicable in applications with latency-sensitive applications and battery-powered devices; whereas substitution -permutation network-based ciphers are stronger in terms of structural security, albeit with increased computation overhead. The findings stress that the choice of encryption algorithm in smart home ecosystems should be application-based, which is to balance between performance efficiency and the level of security requirements. In general, the study adds to the scientific community a systematic benchmarking model and insights to facilitate safe, expandable, and energy-saving IoT implementation in the contemporary smart household systems

REFERENCES

[1] L. Atzori, A. Iera, and G. Morabito, “The Internet of Things: A survey,” *Computer Networks*, vol. 54, no. 15, pp. 2787–2805, 2010.

[2] A. Perrig, J. Stankovic, and D. Wagner, “Security in wireless sensor networks,” *Communications of the ACM*, vol. 47, no. 6, pp. 53–57, 2004.

[3] R. Roman, P. Najera, and J. Lopez, “Securing the Internet of Things,” *Computer*, vol. 44, no. 9, pp. 51–58, 2011.

[4] D. Evans, “The Internet of Things: How the next evolution of the Internet is changing everything,” Cisco White Paper, 2011.

[5] A. Poschmann, “Lightweight cryptography: Cryptographic engineering for a pervasive world,” Ph.D. dissertation, Ruhr University Bochum, 2009.

[6] M. Hatzivasilis, K. Papaefstathiou, and C. Manifavas, “A review of lightweight block ciphers,” *Journal of Cryptographic Engineering*, vol. 8, no. 2, pp. 141–184, 2018.

[7] S. Sicari, A. Rizzardi, L. Grieco, and A. Coen-Porisini, “Security, privacy and trust in Internet of Things: The road ahead,” *Computer Networks*, vol. 76, pp. 146–164, 2015.

[8] NIST, “Lightweight Cryptography Project,” National Institute of Standards and Technology, 2019.

[9] A. Bogdanov et al., “PRESENT: An ultra-lightweight block cipher,” in *CHES 2007*, LNCS 4727, pp. 450–466, 2007.

[10] R. Beaulieu et al., “The SIMON and SPECK lightweight block ciphers,” in *Proceedings of the 52nd ACM/EDAC/IEEE Design Automation Conference*, 2015.

[11] M. Katagi and S. Moriai, “Lightweight cryptography for the Internet of Things,” *SONY Corporation Report*, 2008.

[12] T. Eisenbarth et al., “A survey of lightweight cryptography implementations,” *IEEE Design & Test of Computers*, vol. 24, no. 6, pp. 522–533, 2007.

[13] J. Daemen and V. Rijmen, *The Design of Rijndael: AES—The Advanced Encryption Standard*, Springer, 2002.

[14] P. Kitsos and N. Sklavos, “Hardware and software implementation of lightweight cryptographic algorithms for IoT,” *Microprocessors and Microsystems*, vol. 39, pp. 327–336, 2015.

[15] C. Paar and J. Pelzl, *Understanding Cryptography: A Textbook for Students and Practitioners*, Springer, 2010.

[16] D. Bernstein and T. Lange, “eBACS: ECRYPT Benchmarking of Cryptographic Systems,” 2013.

[17] A. Biryukov and L. Perrin, “State of the art in lightweight symmetric cryptography,” *IACR Cryptology ePrint Archive*, 2017.

[18] S. Kerckhof et al., “Performance analysis of lightweight encryption algorithms on embedded systems,” in *IEEE International Conference on RFID-Technologies and Applications*, 2012.

[19] M. Ambrosin et al., “On the feasibility of cryptography for IoT devices,” *IEEE Internet of Things Journal*, vol. 3, no. 6, pp. 1079–1090, 2016.

[20] H. Suo, J. Wan, C. Zou, and J. Liu, "Security in the Internet of Things: A review," in *IEEE International Conference on Computer Science and Electronics Engineering*, 2012.

[21] A. Alaba et al., "Internet of Things security: A survey," *Journal of Network and Computer Applications*, vol. 88, pp. 10–28, 2017.

[22] N. Sastry and D. Wagner, "Security considerations for IoT cryptographic implementations," *ACM Workshop on Embedded Systems Security*, 2016