FUDMA Journal of Sciences (FJS)
ISSN online: 2616-1370
ISSN print: 2645 - 2944
Vol. 10 No. 24, November, 2026, pp 57 – 64
DOI: https://doi.org/10.33003/fjs-2026-1024-6258

Design and Preliminary Performance Evaluation of a SIMON–LWE Hybrid Encryption Scheme for Cloud-Based IoT

[1]Alowolodu Olufunso Dayo, [2]Ibam Emmanuel Onwuka and [3]Jolayemi Olaoluwa Daniel

[1]Department of Cyber Security, Federal University of Technology, Akure, Nigeria.
[2]Department of Computer Science, Federal University of Technology, Akure, Nigeria.
[3]Department of Computer Science, McPherson University, Ogun State, Nigeria.

*Corresponding authors' email: jolayemiod@mcu.edu.ng
ORCID: https://orcid.org/0009-0003-1552-8502

Received: 17 Oct. 2026
Accepted: 05 Nov. 2026
Published: 07 Nov. 2026

ABSTRACT
Cloud-based Internet of Things (IoT) networks have transformed data collection, processing and communication across a wide variety of industries, including healthcare, agriculture, manufacturing, smart cities, transportation, and environmental monitoring. But, most of the resource constrained IoT devices have limited battery power, memory, storage and processing power, which make it hard to implement conventional cryptographic algorithms such as Advanced Encryption Standard (AES), Rivest–Shaumir–Adleman (RSA), and Elliptic Curve Cryptography (ECC) in them. Moreover, standard cryptographic systems are vulnerable to quantum computing attacks. In this work, we propose a resource-efficient encryption framework called SIMON-LBA, combining the SIMON block cipher with a key-generation scheme based on LWE lattice cryptography to achieve quantum resistance and compromise minimal resources. Numerical experimentation with the model was carried out in a simulated cloud-IoT environment using Python in a quantitative experimental approach. Over 100 iterations, the representative sensor data was assessed, such as PM2.5, temperature, and humidity data. Encryption and decryption times, throughput, energy usage, CPU usage and memory usage were measured and compared with 100 iterations for each of the following algorithms: AES, RSA, ECC, DES, ChaCha20, SIMON, SPECK, Attribute-Based Signcryption (ABSC) and Homomorphic Encryption. The results indicated that the time for encryption is 0.644 ms, the time for decryption is 0.589 ms, the throughput is 1,038.40 kbps, the CPU utilization is about 0.12%, the memory consumption is 0.48 MB and the energy consumption per operation is 0.009974 J. The SIMON-LBA shows a promising computational efficiency-potential postquantum security tradeoff. The study proposes a hybrid cryptographic approach that enhances lightweight encryption by incorporating lattice-based key generation to enable secure and efficient communication between cloud and IoT devices while preserving the need for lightweight cryptography.

Keywords: Internet of Things (IoT), Cloud Computing, Lightweight Cryptography, Lattice-Based Cryptography, SIMON Cipher, Data Encryption

INTRODUCTION

With the advent of the Internet of Things (IoT), physical devices are now collecting, sharing, and analyzing information in a myriad of application areas such as health care, industry automation, smart cities, intelligent transportation, agriculture, and environmental monitoring. It has been estimated that there will be tens of billions of IoT devices deployed globally in the next decade, consuming and producing enormous data flows of diverse types that will need constant processing, storage and secure delivery via cloud-based infrastructures (Myroshnyk et al., 2024; Thakor et al., 2021). IoT and cloud computing have thus become an important technology paradigm, allowing resource-limited devices to benefit from the unlimited computational power, scalability of storage and accessibility of cloud platforms. This has led to an increase in performance and efficient decision making in various applications, as well as a reduction in cost during deployment and operation (Suryateja & Rao, 2024; Ekwueme et al., 2024; Kyado et al., 2025).

Despite these advantages, there are a lot of security and privacy challenges in cloud computing based IoT environments. IoT nodes are resource-constrained compared to traditional computational devices in many ways, such as computing power, memory, communication capabilities and power consumption. The constraints involved make it very difficult to execute computationally complex cryptographic protocols and still be able to meet the efficiency of the system (Beaulieu et al., 2015). One of the biggest challenges in the security of IoT environments where there is an exchange of sensitive information between IoT nodes through communication channels that are publicly available (Abed et al., 2019) is: confidentiality, integrity, authentication and access control. This has turned the development of cryptographic schemes which can guarantee a high degree of security with low computational requirements into a highly investigated field.

Secure communication in distributed computing systems was traditionally ensured by cryptographic techniques like the Advanced Encryption Standard (AES), Rivest - Shamir - Adleman (RSA) and Elliptic Curve Cryptography (ECC). AES allows for a good encryption of data with confidentiality guarantees, whereas RSA and ECC are capable of ensuring the security of public-key infrastructures (Shor, 1994; Grover 1996). These encryption schemes have demonstrated a high

security degree in a classical computation environment, but when it comes to constrained IoT devices, implementing such algorithms becomes problematic. While AES is an algorithm requiring much computational effort for its recurrent applications, RSA and ECC have a very high computational complexity which causes a high execution time, high memory consumption and power requirements. Such characteristics render these cryptographic algorithms rather inefficient for situations when constrained hardware resources should be used continuously (Beaulieu et al., 2015; Kwala et al., 2024). The above problems can be solved by lightweight cryptography, which is a way of designing lightweight cryptographic algorithms that have been designed for use in limited conditions. Recently, the U.S. National Security Agency (NSA) has put forward the idea of lightweight block ciphers such as SIMON and SPECK, which try to strike the right balance between speed, efficiency, and robustness (Liu et al., 2024). There has been increased attention in the use of lightweight cryptography in wireless sensor network (WSN), RFID, embedded systems, and cloud based IoT applications, especially due to their small hardware implementation, low memory usage, and efficiency. Simon is one such algorithm that has proven to have excellent performance in terms of both software and hardware implementations owing to the simplicity of the Feistel network architecture (Figure 1), along with cheap logical operations, such as XOR, AND and Cyclic Shifts. As a result, SIMON is one of the most potential lightweight encryption algorithms for resource-limited environments.

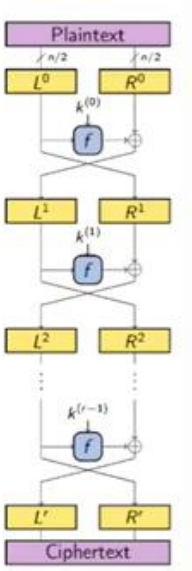


Figure 1: Feistel Cipher (Abed et al., 2019)

But computational efficiency wasn't enough to ensure security in the long term. The landscape of threats to modern cryptographic systems has changed significantly in recent advances in quantum computing. It has been shown theoretically that quantum algorithms can solve the integer factorization problem and the discrete logarithm problem in polynomial time that is exponentially faster than the classical counterpart, which would compromise the security bases of RSA, ECC, and many popular public-key cryptosystems (Dhanda et al., 2020). The symmetric encryption algorithms like AES are relatively better protected against quantum attacks but Grover's search algorithm brings the security margin down by around 50 % and it needs better key management procedures and larger key sizes to provide future security guarantees (Hatzivasilis et al., 2018). Securing cloud-based IoT infrastructures from classical and quantum threats is rapidly emerging as a key research challenge as practical quantum computers advance.

This is a new threat that has spurred research worldwide on Post-Quantum Cryptography (PQC) that aims to create cryptographic algorithms that are secure against both classical and quantum computers. For the families, Lattice-based cryptography is a popular option as the security of the systems is based on intractable mathematical problems, including the Learning With Errors (LWE) problem and the Shortest Vector Problem (SVP) (Radhakrishnan et al., 2024) which are considered intractable even with the known quantum algorithms. As a result, lattice-based schemes have been the subject of intensive study both in the academic community and in standardization bodies and have emerged as one of the most promising foundations for next generation secure communication systems.

However, embedding a lattice-based cryptography directly into IoT devices is still difficult. The majority of lattice-based algorithms have high dimensional matrix operations, a polynomial multiplication operation, and relatively large key sizes, which impose high computational, memory, and energy demands. However, due to these properties, they are not directly applicable to the constrained IoT devices, which have poor quantum resistance (Sutikno & Thalmann, 2022). Existing studies have thus identified a long-standing trade-off between the lightweight and the post-quantum security. Lightweight cryptography is usually not quantum resistant, but it is computationally efficient. On the other hand, post-quantum algorithms are highly future-proof but often are resource-intensive, which is a challenge for low-resource IoT platforms. A key open research issue in secure cloud based IoT systems is bridging this gap.

Furthermore, lightweight symmetric cryptography techniques can lower the expenses of data encryption, and lattice-based methods can be potential post-quantum key establishment methods. The combination of these elements, however, does not guarantee quantum resistance, but depends on how the device is actually built, which parameters are used, how it is implemented, and its security analysis. This study implements a preliminary prototype of SIMON-LWE and

present software-host performance measurements. It is not a validated post-quantum cryptosystem; its contribution will be an initial integration exploration and performance. The goal of this study is to describe the prototype and identify the evidence needed for reproducible and secure evaluation.

Literature Review

As the Internet of Things (IoT) enters the cloud, the increasing number of challenges to ensure data confidentiality, computational efficiency and scalability under strict resource limitations has inspired the development of cryptographic mechanisms in such environments. Initial research work was generally concerned with fine grained access control mechanisms for cloud computing, with the aim of decreasing the computational load of the data owner, and allowing secure cloud storage through the use of Attribute Based Encryption (ABE), proxy re-encryption and lazy re-encryption. These schemes provided greater flexibility and flexibility in access control and scalability, but relied on trusted cloud proxies which led to further security issues and increased complexity. These schemes offered more access control flexibility and scalability, but used trusted cloud proxies which caused further security issues and complexity.

The number of applications for the Internet of Things (IoT) grew at an incredibly fast pace, and as a result, the focus of the research was on a lightweight public-key cryptography system to overcome the computational constraints of embedded devices. An alternative public-key algorithm, Elliptic Curve Cryptography (ECC) has lower key sizes than traditional public-key algorithms, yet provides a similar level of security and is better suited for resource-constrained devices. Yet, when deploying a lot of thousands of connected devices in an IoT (Suryateja & Rao, 2024; Ekwueme et al., 2024), the key management difficulties and the increasing amount of computation became an issue for ECC schemes.

During the period from 2019 to 2020, much attention was paid to enhancing the performance of encryption, securing cloud access, and efficient ways of authentication. Comparative analysis indicated that AES was extremely efficient for cloud computing tasks, while lightweight cryptographic schemes were effective for IoT devices. Meanwhile, such approaches like adaptive encryption, outsourced ABE decryption, and hyper-elliptic curve signcryption became popular due to the reduced computational cost. These methods improved the encryption rates and the resistance to classic attacks, but had problems with scalability, communication burden, and complex key management in dynamic IoT networks (Beaulieu et al., 2015; Abed et al., 2019; Shor, 1994; Grover 1996).

Later studies focused on the concept of a holistic security architecture for covering the security of sensing, communication, and cloud layers. Multi-layered security frameworks and revocable ABE mechanisms to ensure better privacy preservation, traceability, and secure data exchange in cloud-IoT ecosystems, as well as data-sharing schemes supported by blockchain for improved traceability and secure data exchange. In particular, it was observed that the ABE with blockchain technology greatly enhanced trust management and forensic accountability and decreased reliance on centralized authorities. However, the integration with blockchain made it more expensive in terms of computation, communication delay and storage requirement, which made it impractical for deployments over battery powered IoT devices (Kwala et al., 2024; Liu et al., 2024; Almutairi & Sheldon, 2025; Dhanda et al., 2020).

Research in the last few years has gone beyond traditional encryption and incorporated more advanced techniques such as homomorphic encryption, DNA cryptography, blockchain, transformer-based intrusion detection, and PQC components into cloud-IoT security architectures. Fully Homomorphic Encryption (FHE) is an encryption method that allows privacy-preserving computation over encrypted data without any decryption required, but is still too time-intensive to be used on resource-constrained devices. Similarly, the DNA encryption showed great execution efficiency, but it was not random and was complicated to implement. In more recent times, lattice-based cryptography has been one of the most promising post-quantum cryptographic methods as its security is based on computationally hard problems like the Learning With Errors (LWE) and the Shortest Vector Problem (SVP). The lattice-based schemes are quantum resistant, however they usually involve high-dimensional matrix operations, larger key sizes and more memory usage, all of which hinder their use in lightweight IoT application settings (Hatzivasilis et al., 2018; Radhakrishnan et al., 2024; Sutikno & Thalmann, 2022).

Recent research (2024--2025) tends to combine elements of homomorphic encryption, blockchain, proxy re-encryption and lattice-based cryptography in a unified framework for healthcare IoT, smart cities, industrial IoT and cloud-edge computing. Experimental evaluations have demonstrated the improvement of privacy preservation, quantum resistance and secure distributed communication. However, researchers have repeatedly noted that there are still many bottlenecks such as energy inefficiency, memory usage, latency, high computational costs, scalability issues, interoperability, and difficulty in validating on large-scale IoT implementations. While the recent lattice-based quantum-resistant cryptography has shown improved resistance to quantum adversaries, there are still implementation challenges to address (Mohammed & Abdul-Wahab, 2024; Abualkas & Bhaskari, 2024; Kumar & Kumar, 2024).

MATERIALS AND METHODS

This research work uses a quantitative experimental research design to create and assess a lightweight post-quantum hybrid encryption scheme called SIMON-LBA for securing cloud-based Internet of Things (IoT) networks. The methodology consists of cryptographic system design, software implementation, and experimental performance assessment to study the effectiveness of using the SIMON lightweight block cipher together with a LWE-based key-generation mechanism (figure 2).

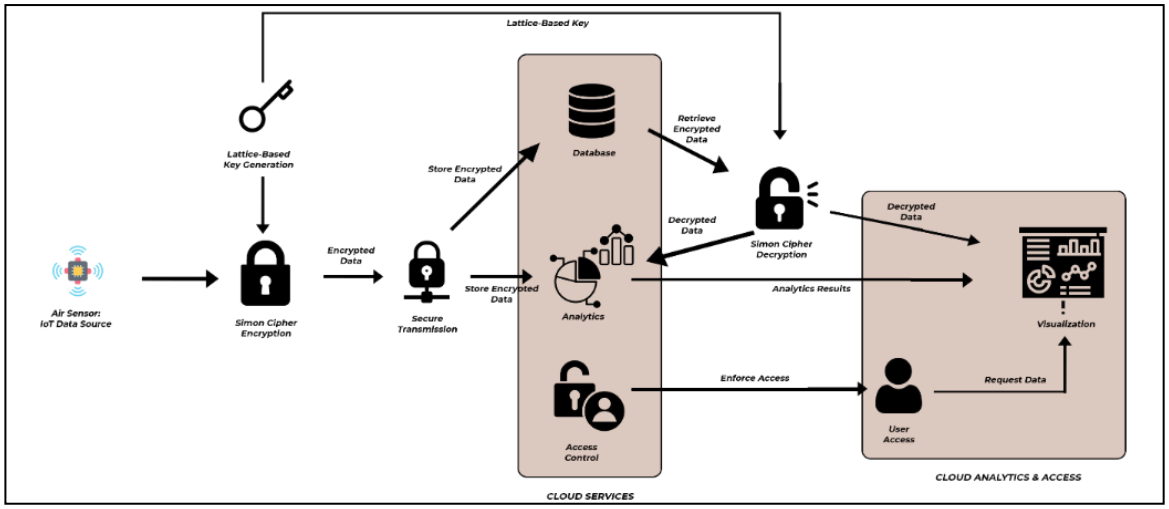


Figure 2: Conceptual Diagram of the SIMON-LBA

This is because it is necessary to develop schemes that satisfy multiple requirements, such as computational efficiency, lightweight implementation, and resistance to quantum attacks as the demands for encryption schemes are more and more increasing (Krishnan et al., 2024; Thakor et al., 2021; Suryateja & Rao, 2024; Ekwueme et al., 2024). The methodological framework involves four successive steps: Analysis of current cryptographic techniques, the design of the proposed hybrid architecture, implementation of the encryption model, and evaluation of the performance of the proposed model against the existing, current cryptographic techniques.

Mathematical Model Equation of SIMON-LBA

The proposed encryption framework fuses the simplicity of computation of the SIMON block cipher with the quantum-resistant properties of lattice-based cryptography (LBC). The symmetric encryption and decryption operations are carried out by SIMON due to its low computational complexity, small size of hardware, and its applicability to resource-limited devices (Krishnan et al., 2024; Beaulieu et al., 2015) in IoT. On the contrary, Learning With Errors (LWE) algorithm is used only for key generation and key management, and therefore ensures post-quantum security with minimum computational overhead that is normally required for lattice-based cryptography (Thakor et al., 2021; Suryateja & Rao, 2024; Ekwueme et al., 2024).

Let:

M = plaintext message block

C = ciphertext block

K = key material (generated/protected via lattice cryptography)

LWE(s, A, e) = Learning With Errors function with secret s, matrix *A*, and noise e

Simon(*M, K*) = output of Simon cipher encryption on *M* with key *K*

Then the combined model equation:

$$K = KeyGen_{Lattice}(s.A.e) \quad (1)$$

$$C = Simon(M, K) \quad (2)$$

Or expanded:

i. Key Generation using Lattice (LWE – Learning With Error method):

$$b = A.s + e \quad (3)$$

where s is a secret vector, A is a random public matrix, e is small noise, and b is public.

The derived key:

$$K = f_{(b)} \quad (4)$$

where f is a function mapping the lattice output to a usable symmetric key for Simon.

ii. Encryption using Simon cipher:

Simon uses round functions:

$$C = M \oplus ((M \lll \alpha) \wedge (M \lll \beta))(M \lll \gamma) \oplus K \quad (5)$$

where:

⋘α = left rotation by α\alphaα bits

∧ = bitwise AND

⊕ = XOR

K = round key derived from lattice

The Encryption formula

$$C = Simon(M, KeyGen_{Lattice}(s, A, e) \quad (6)$$

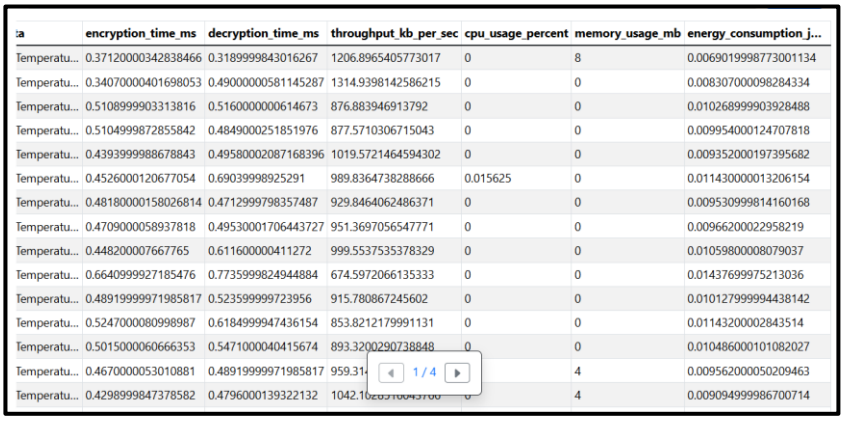
```
# --- LWE KEY GENERATION ---
q, n = 256, 16
A = np.random.randint(0, q, size=(n, n), dtype=np.uint8)
s = np.random.randint(0, q, size=(n, 1), dtype=np.uint8)
e = np.random.randint(-1, 2, size=(n, 1), dtype=np.int8)
b = (np.dot(A, s) + e) % q
key_bytes = b.flatten().tobytes()

# --- SIMON KEY SETUP ---
key_words = [int.from_bytes(key_bytes[i*4:(i+1)*4], 'little')
             for i in range(4)]


def rotl(x, r): return ((x << r) & MASK) | (x >> (WORD_SIZE - r))
def rotr(x, r): return (x >> r) | ((x << (WORD_SIZE - r)) & MASK)
```

Figure 3: LWE-Based Key Generation

The proposed architecture implementation has been done in the Visual Studio Code Integrated Development Environment (IDE) using Python 3 (figure 3). The experimental platform was a Windows 11 computer with 7th Generation Intel® Core™ i5 processor and 16 GB of RAM. To help with implementation, several python packages were added, such as NumPy for numerical computations, SQLite3 for database management, psutil for monitoring processor and memory usage, hashlib for hashing, and the time module for measuring the time taken for encryption and decryption (figure 4). Experimental data included representative data from IoT environment sensing applications including PM2.5, temperature, and relative humidity measurements, that represent typical cloud-enabled IoT applications. In every experiment, the sensor data was encrypted with the proposed SIMON-LBA algorithm and then decrypted to check the accuracy of the data. The entire encryption and decryption operation was performed a number of times for 100 iterations to enhance the statistical reliability and minimize variation in measurement to assess performance in comparison. The ciphertext, the decrypted text, the execution times, the energy consumption, the processor usage and the memory used, the throughput and the estimated energy consumption were automatically saved in an SQLite database for later evaluation.



:a	encryption_time_ms	decryption_time_ms	throughput_kb_per_sec	cpu_usage_percent	memory_usage_mb	energy_consumption_j...
Temperatu...	0.37120000342838466	0.3189999843016267	1206.8965405773017	0	8	0.0069019998773001134
Temperatu...	0.34070000401698053	0.49000000581145287	1314.9398142586215	0	0	0.008307000098284334
Temperatu...	0.5108999903313816	0.5160000000614673	876.883946913792	0	0	0.010268999903928488
Temperatu...	0.5104999872855842	0.4849000251851976	877.5710306715043	0	0	0.009954000124707818
Temperatu...	0.4393999988678843	0.49580002087168396	1019.5721464594302	0	0	0.009352000197395682
Temperatu...	0.4526000120677054	0.69039998925291	989.8364738288666	0.015625	0	0.011430000013206154
Temperatu...	0.48180000158026814	0.47129999798357487	929.8464062486371	0	0	0.009530999814160168
Temperatu...	0.4709000058937818	0.49530001706443727	951.3697056547771	0	0	0.00966200022958219
Temperatu...	0.448200007667765	0.611600000411272	999.5537535378329	0	0	0.01059800008079037
Temperatu...	0.6640999927185476	0.7735999824944884	674.5972066135333	0	0	0.01437699975213036
Temperatu...	0.48919999971985817	0.5235999999723956	915.780867245602	0	0	0.010127999994438142
Temperatu...	0.5247000080998987	0.6184999947436154	853.8212179991131	0	0	0.01143200002843514
Temperatu...	0.5015000060666353	0.5471000040415674	893.3200290738848	0	0	0.010486000101082027
Temperatu...	0.4670000053010881	0.48919999971985817	959.31	1 / 4	4	0.009562000050209463
Temperatu...	0.4298999847378582	0.4796000139322132	1042.10	0	4	0.009094999986700714

Figure 4: Sample Performance Metrics Data Collected

The evaluation of the performance concentrated on specific metrics important in the context of resource limited IoT application. These include encryption time, decryption time, throughput, CPU usage, memory usage, and power usage, which together give a wide array of metrics that can give an idea about computational efficiency and practical deployment (Beaulieu et al., 2015). The proposed encryption model was compared to general, lightweight and privacy-preserving cryptographic schemes: AES, RSA, ECC, DES, ChaCha20, SIMON, SPECK, Attribute-Based Signcryption (ABSC) and Homomorphic Encryption. The comparison of these algorithms allows an objective assessment of the proposed architecture in relation to security, performance, scalability, and applicability in cloud-based IoT applications.

In sum, the whole methodology is the combination of cryptography design, software engineering, and experiments that demonstrate the possibility of improved security of the proposed combination of lightweight symmetric encryption and lattice-based post-quantum key generation while maintaining computational efficiency of the next-generation cloud-based IoT systems. Furthermore, such experimental research provides an opportunity for repeated evaluation of lightweight quantum-resistant encryption schemes under realistic constrained conditions. (Thakor et al., 2021; Suryateja & Rao, 2024; Ekwueme et al., 2024; Beaulieu et al., 2015).

RESULTS AND DISCUSSION

The Python-based SIMON-LBA prototype was evaluated over 100 iterations, and its mean performance metrics were compared with those of nine benchmark encryption algorithms: AES, RSA, ECC, DES, ChaCha20, SIMON, SPECK, ABSC, and Homomorphic Encryption. An evaluation process has been carried out to verify the feasibility of the new design in resource constrained cloud-based IoT environments by determining encryption time, decryption time, throughput, CPU usage, memory usage, and energy consumption. Experimental results have shown that the SIMON light weight block cipher in conjunction with LWE key generation technique for lattice cryptography is a good combination.

The new SIMON-LBA architecture was designed to be highly efficient and secure, combining post-quantum cryptography and classical, high-speed computing. The extra overhead of generating the lattice-based key was only a marginal one, with an average encryption and decryption time of 0.644ms and 0.589ms, respectively as seen in Table 1.

Table 1: Raw Summary of Mean Performance Metrics for Encryption Algorithms

Encryption Technique	Encryption time (ms)	Decryption Time (ms)	Throughput (kbps)	CPU Usage (≈ %)	Memory Usage (MB)	Energy Consumption (J)
ABSC	0.004103	0.002501	145.49	70.96	18.74	0.00000660
AES	0.028755	0.017676	656.62	67.33	20.53	0.00002322
CHACHA20	0.069089	0.023727	1327.49	70.34	≈ 0.00	0.00666895
DES	0.049794	0.020511	2833.13	76.13	20942.20	0.00191913
ECC	0.442481	0.259042	32.21	≈0.00	5.82	0.00234375
Homomorphic	1365.23910	405.217335	15.88	1.34	0.70	87.13046875
RSA	1.678910	9.206913	157.56	66.89	0.43	0.48172292

Encryption Technique	Encryption time (ms)	Decryption Time (ms)	Throughput (kbps)	CPU Usage (≈ %)	Memory Usage (MB)	Energy Consumption (J)
Simon	0.167711	0.163708	845.79	≈0.00	0.82	0.00000000
Simon-LBA	0.644268	0.589178	1038.40	0.12	0.48	0.009974
Speck	0.077119	0.077989	1849.07	≈0.00	0.04	0.00000019

Discussion

These execution times (Figure 5) are still competitive for latency demanding IoT applications like smart healthcare, industrial automation, intelligent transportation, and environmental monitoring where fast encryption/decryption is crucial for real-time communication.

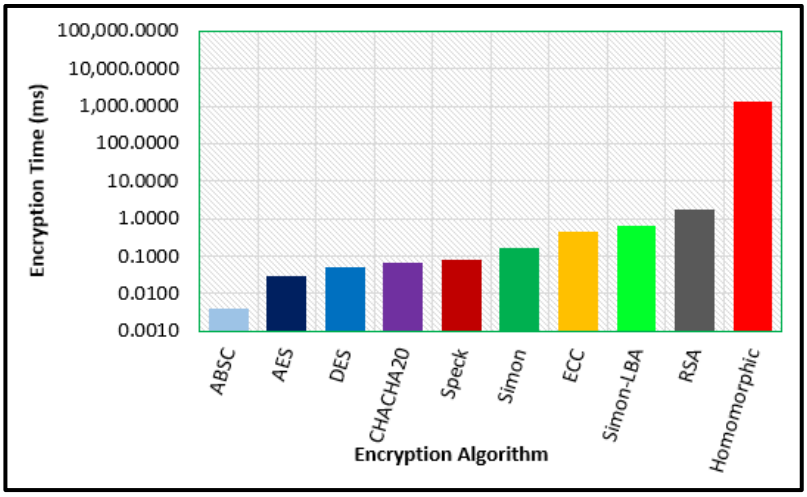


Figure 5: Encryption Time

Otherwise, the efficiency of the proposed architecture was also validated by conducting throughput evaluation (Figure 6). SIMON-LBA achieved a throughput of 1038.40 kbps, which is more than the standalone SIMON and AES. This higher throughput suggests that the proposed hybrid architecture will be able to encrypt more data in the same amount of time despite the use of lattice-based key generation. This observation supports the lightweight design of the SIMON cipher by showing that it is able to compensate for the computational complexity of post-quantum key management and keep data processing efficient for use in clouds for IoT applications.

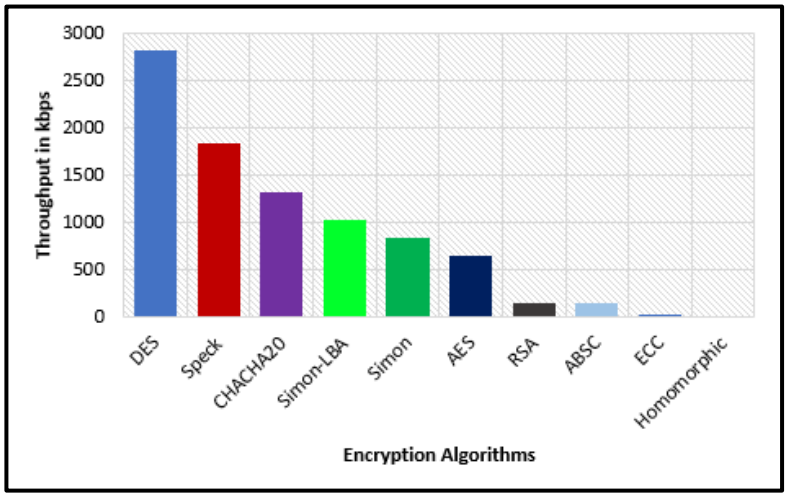


Figure 6: Throughput

The resource utilization results also showed how well the proposed architecture performs on resource-constrained devices. The overall CPU utilization was very low (around 0.12%), which shows that the encryption and decryption operations do not have a significant impact on the host processor. Likewise, the proposed architecture needed 0.48 MB of memory (Figure 7), considerably less than the stand-alone SIMON implementation (0.82 MB) and much less than conventional heavyweight algorithms, like DES. Lowering the processor and memory requirements allows IoT devices to devote increased computing resources to sensing, communication and application specific functions while ensuring secure data transfer.

The use of lattice-based cryptography did add to energy costs for key generation, but it was still manageable with battery-powered IoT devices. Computationally intensive encryption and decryption methods such as public-key and homomorphic encryption were far from the top of the list for SIMON-LBA, which used about 0.009974 J per cryptographic operation while also offering significantly

better security against attacks using quantum computers. The proposed architecture thus provides an adequate energy-efficiency/cryptographic resiliency tradeoff.

The proposed architecture has been further validated by comparing it with the already available lightweight and post-quantum encryption studies. SIMON-LBA outperformed the recent lightweight encryption, blockchain-assisted security, and lattice-based cryptographic frameworks in terms of execution time, throughput, CPU usage, memory usage, and practical energy consumption. Most of the currently known post-quantum schemes use large lattice dimensions, $n \geq 256$, and several layers of cryptographic operations, thereby requiring a significant number of computations and resources.

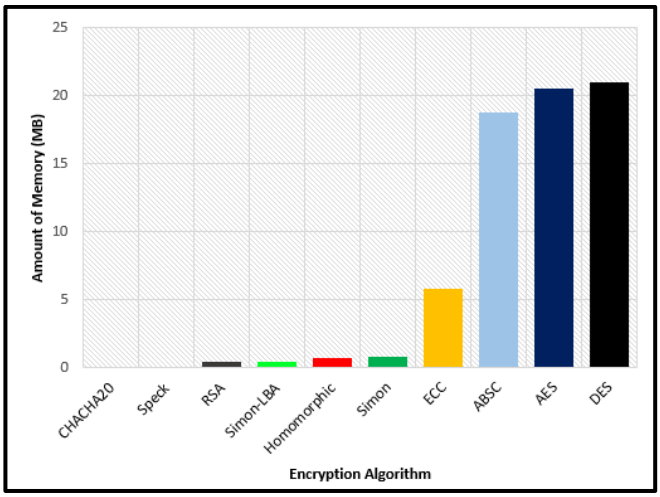


Figure 7: Amount of Memory

The proposed architecture, on the other hand, features a lightweight SIMON cipher with an optimized lattice-based key generation mechanism ($n = 16$), which ensures quantum-resistant security properties while allowing efficient deployment on resource-constrained IoT devices.

Conclusion

This study implemented and preliminarily evaluated SIMON-LBA, a software prototype combining SIMON symmetric encryption with an LWE-inspired key-generation component for a cloud-IoT use case. Across 100 reported iterations on a Windows 11 Core i5/16 GB host. The need for the proposed framework arises due to the growing restrictions of the conventional cryptographic algorithms, including AES, RSA, and ECC, when they are applied to resource-constrained devices, such as IoT devices, especially in the light of the potential threat of quantum computing. Experimental comparison was performed for SIMON-LBA with AES, RSA, ECC, ChaCha20, DES, Attribute-Based Signcryption (ABSC), Homomorphic Encryption, SIMON and SPECK with the same implementation settings and performance measurements. The evaluating parameters were encryption time, decryption time, throughput, CPU utilization, memory usage and energy consumption after one hundred experimental runs. The results show that lightweight symmetric encryption schemes are more appropriate for IoT applications in the cloud than more powerful traditional and privacy-preserving cryptographic schemes. Most significantly, the proposed SIMON-LBA architecture always provided an efficient trade-off between security and computational benefits by keeping the latency of the encryption function low, reducing the usage of processors and memory, increasing the throughput, and decreasing the energy consumption while providing quantum-resistant key generation by using lattice-based cryptography. The features of the framework make it a perfect solution for use on battery-powered sensors and embedded devices with limited computational resources as found in IoT. The results thus demonstrate empirically that the hybrid lightweight post-quantum cryptographic architectures could be efficient in terms of resource utilization and secure in terms of security in emerging cloud-edge IoT architectures.

REFERENCES

Abed, S., Jaffal, R., Mohd, B. J., & Alshayeji, M. (2019). FPGA Modeling and Optimization of a SIMON Lightweight Block Cipher. Sensors, 19(4), 913. https://doi.org/10.3390/s19040913.

Abualkas, Y. M. A., and Bhaskari, D. L. (2024). Hybrid Approach to Cloud Storage Security Using ECC-AES Encryption and Key Management Techniques. *International Journal of Engineering Trends and Technology*, 72(4): 92-100..

Almutairi, Y., & Sheldon, F. T. (2025). IoT-cloud integration security: A survey of challenges, solutions, and directions. Electronics, 14(7).

Beaulieu, R., Treatman-Clark, S., Shors, D., Weeks, B., Smith, J., & Winger, L. (2015). The SIMON and SPECK lightweight block ciphers. In Proceedings of the 52nd Design Automation Conference (DAC) (pp. 1–6).

Dhanda, S., Singh, B., & Jindal, P. (2020). Lightweight cryptography: A solution to secure IoT. *Wireless Personal Communications*, *112*(3), 1947-1980.

Ekwueme, C. P., Adam, I. H., & Dwivedi, A. (2024). Lightweight cryptography for Internet of Things: A review. *EAI Endorsed Transactions on Internet of Things, 10*(1).

Grover, L. K. (1996). A fast quantum mechanical algorithm for database search. *In Proceedings of the 28th Annual ACM Symposium on Theory of Computing* (pp. 212–219).

Hatzivasilis, G., Fysarakis, K., Papaefstathiou, I., & Manifavas, C. (2018). A review of lightweight block ciphers. *Journal of Cryptographic Engineering, 8*(2), 141–184.

Kumar, D., and Kumar, M. (2024). Hybrid Cryptographic Approach for Data Security Using Elliptic Curve Cryptography for IoT. International Journal of Computer Network and Information Security, 16(2): 42-54.

Kwala, A. K., Kant, S., & Mishra, A. (2024). Comparative analysis of lattice-based cryptographic schemes for secure IoT communications. *Discover Internet of Things, 4, Article 13.*

Kyado, D. J., Iliya, A. J., Mohammed, T., & Kenneth, S. N. (2025). IoT-Based Telemedicine System to Address Healthcare Access Challenges in Nigeria. FUDMA Journal of Sciences, 9(7), 142-150. https://doi.org/10.33003/fjs-2025-0907-3675

Liu, T., Ramachandran, G., & Jurdak, R. (2024). Post-quantum cryptography for Internet of Things: A survey on performance and optimization. *arXiv*. https://doi.org/10.48550/arXiv.2401.17538

Mohammed, M. A., & Abdul Wahab, H. B. (2024). Enhancing IoT data security with lightweight blockchain and Okamoto Uchiyama homomorphic encryption. *Computer Modeling in Engineering & Sciences, 138*(2), 1731–1748. https://doi.org/10.32604/cmes.2023.030528

Myroshnyk, Y., Krishnan, A., Taparia, A., Paraskevopoulos, D., Pasqua, E., Brügge, F., Fernandez, J., Sava, J.-A., Baviskar, K., Lueth, K. L., Kulezak, M., Hasan, M., Demir, O., Wegner, P., Kadian, R., Nair, R., Sinha, S., & Annaswamy, S. (2024). State of IoT summer 2024. *IoT Analytics*. https://iot-analytics.com/product/state-of-iot-summer-2024/

Radhakrishnan, I., Jadon, S., & Honnavalli, P. B. (2024). Efficiency and security evaluation of lightweight cryptographic algorithms for resource-constrained IoT devices. *Sensors, 24*(12), Article 4008. https://doi.org/10.3390/s24124008

Shor, P. W. (1994). Algorithms for quantum computation: Discrete logarithms and factoring. *In Proceedings of the 35th Annual Symposium on Foundations of Computer Science* (pp. 124–134). IEEE Computer Society Press. https://doi.org/10.1109/SFCS.1994.365700

Suryateja, P. S., & Rao, K. V. (2024). A survey on lightweight cryptographic algorithms in IoT. *Cybernetics and Information Technologies, 24*(1), 21–34. https://doi.org/10.2478/cait-2024-0002

Sutikno, T., & Thalmann, D. (2022). Insights on the internet of things: Past, present, and future directions. *TELKOMNIKA (Telecommunication Computing Electronics and Control), 20*(6), 1399–1420. https://doi.org/10.12928/telkomnika.v20i6.22028

Thakor, V. A., Razzaque, M. A., & Khandaker, M. R. A. (2021). Lightweight cryptography algorithms for resource-constrained IoT devices: A review, comparison and research opportunities. IEEE Access, 9, 28177-28193. https://doi.org/10.1109/ACCESS.2021.3052867

©2026 This is an Open Access article distributed under the terms of the Creative Commons Attribution 4.0 International license viewed via https://creativecommons.org/licenses/by/4.0/ which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is cited appropriately.