As per UGC guidelines an electronic bar code is provided to secure your paper

International Journal for Modern Trends in Science and Technology
Volume 11, Issue 09, pages 26-33.
ISSN: 2455-3778 online
Available online at: http://www.ijmtst.com/vol11issue09.html
DOI: https://doi.org/10.5281/zenodo.17096278

Enhancing Better Security for Encryption and Decryption of Data using AES Algorithm

B V R V Prasad | P. L. Siri keerthika

Department of Electronics and Communication Engineering, NRI Institute of Technology, Agiripalli, A P, India.

To Cite this Article
B V R V Prasad & P. L. Siri keerthika (2025). Enhancing Better Security for Encryption and Decryption of Data using AES Algorithm. International Journal for Modern Trends in Science and Technology, 11(09), 26-33. https://doi.org/10.5281/zenodo.17096278

Article Info
Received: 18 August 2025; Accepted: 07 September 2025; Published: 11 September 2025.

KEYWORDS

AES-256, Advanced Encryption Standard, Symmetric Encryption, 14 Rounds, SubBytes, ShiftRows, MixColumns, AddRoundKey, Data Security, Cryptography, Block Cipher, Key Expansion, Encryption Algorithm.

ABSTRACT

Advanced Encryption Standard (AES) algorithm is one on the most common and widely symmetric block cipher algorithm used in worldwide. This algorithm has an own particular structure to encrypt and decrypt sensitive data and is applied in hardware and software all over the world. It is extremely difficult to hackers to get the real data when encrypting by AES algorithm. Till date is not any evidence to crake this algorithm. AES has the ability to deal with three different key sizes such as AES 128, 192 and 256 bit and each of this ciphers has 128 bit block size. Project will be developed using VHDL. Xilinx ISE tool is used to perform the Simulation and Synthesis.

This paper focuses on the AES-256 variant, which utilizes a 256-bit key and processes data blocks of 128 bits through 14 transformation rounds. Each round, except the final one, consists of four main operations: SubBytes, ShiftRows, MixColumns, and AddRoundKey. AES-256 offers a high level of security due to its large key size and increased number of rounds, making it more resilient to brute-force and cryptanalytic attacks compared to its 128- bit and 192-bit counterparts.Among its three key length variants—AES-128, AES-192, and AES-256—the AES-256 algorithm offers the highest level of security, operating on 128-bit data blocks using a 256-bit key across 14 rounds of transformation. Each round, except the final one, comprises four core operations: SubBytes (non-linear byte substitution using an S- box), Shift Rows (transposition step), MixColumns (mixing of data across columns for diffusion), and AddRoundKey (bitwise XOR with the round key). The AES-256 algorithm also employs a more complex key expansion process to derive 15 round keys from the original 256-bit key.This paper presents an in-depth overview of the internal architecture, operational steps, and security implications of AES-256, emphasizing

1. INTRODUCTION

With the advent of Internet of Things (IoT), the call for hardware security has been seriously demanding due to the risks of side-channel attacks from adversaries. Advanced encryption standard (AES) is the de facto security standard for such applications and needs to ensure a low power, low area, and moderate throughput design apart from providing high security to these devices. Substitution-box (S-box), being the core component of AES, has always drawn the attention of the cryptographic community. A chronological development of the S-box over a period of 20 years since the inception of AES is presented. This article provides the first comprehensive review of the state- of-the-art S-box design techniques, identifying current advancements and analyzing their impact on gate count, area, maximum frequency of operation, throughput, and power. The other goal of the survey is to study the countermeasures designed for AES to protect it against side-channel attacks. In particular, we consider the power analysis attacks (PAAs), and the countermeasures are investigated in terms of their security metrics and design overheads, such as area, power, and performance. The countermeasures are based on hiding or masking approaches depending on their design principle. Similar to the S-box survey, a chronological development of the countermeasures since the discovery of PAAs in 1999, is presented. Finally, we suggest some open research gaps and possible direction of research in terms of S-box and countermeasure designs.[1]

In today's world, the Internet of Things (IoT) plays a major role to interconnect all the devices and improve the overall Quality of Life (QoL) for people. The main concern among IoT systems revolve around three pillars namely security, confidentiality, and privacy owing to the sensitive nature of the data being transmitted and processed byIoT devices. Traditional cryptographic approaches address these concerns by ensuring the authenticity and confidentiality of IoT systems. However, the majority of IoT devices are resource-constrained, which implies that they operate under significant resource constraints such as limited computational power, constrained battery life, physical compactness, and restricted memory capacity. To this end, Lightweight cryptography (LWC) offers methods specifically designed to accommodate the limitations of resource-constrained IoT devices. This work establishes the role of light weight cryptography for such resource constrained IoT networks in terms of security perspectives. [2]

In this work, we explore the security vulnerabilities of IoT systems and the associated lightweight cryptographic methods highlighting four components namely lightweight block ciphers, lightweight stream ciphers, hash functions, and Elliptic Curve Cryptography. The work further discusses the role of LWC and reviews the recent advancements in different sectors of IoT such as smart city, industries, healthcare, smart grids, and agriculture. Finally, several open research directions are highlighted in order to guide future LWC and IoT researchers.[3]

Fig.1 AES Encryption and Decryption

The Internet of Things (IoT) has rapidly grown in recent years, making it an integral part of many areas of our lives. Many IoT networks require high data throughput and low latency, allowing for real-time communication and data transmission, enabling improved efficiency, cost savings, and enhanced decision-making capabilities in various industries such as manufacturing, healthcare, transportation, and smart cities. However, with the increasing amount of data being transmitted, the security of high-speed IoT networks becomes a critical concern. In this paper, we proposed a hardware architecture for Ascon, a NIST Lightweight cryptography standard to enable high-throughput, low-latency security services in IPSec protocols. Results show that the ESP protocol can achieve a maximum throughput of 8.806 Gbps and a minimum latency of 427ns for only 2812 Slice. This ESP core together with the proposed Ascon implementation can be used in IoT gateways to provide security services for high-speed, low-latency IoT networks.[4]

With the rapid advancements in information technologies such as 5G and cloud computing, Internet

of Things (IoT) applications are expanding across various domains, such as smart transportation and smart homes. However, with the proliferation of IoT devices, network attacks on user privacy and security are also increasing. Ensuring data privacy and security has become a critical challenge. However, conventional block ciphers are inapplicable for resource-constrained IoT devices that require low power consumption and real-time response. With advantages such as simpler structures, higher efficiency, and lower overheads, lightweight block ciphers have become an important research avenue for IoT ciphers. This paper summarizes the development of lightweight block ciphers and categorizes the ciphers into six types based on their structures. The software and hardware implementations of lightweight block ciphers are evaluated using multi-dimensional criteria. An in-depth discussion is conducted on security, resource, and performance trade-offs. Additionally, cryptanalysis results, including impossible differentials, integrals, and others, are analyzed. Finally, future perspectives on research directions of lightweight block ciphers are presented.[5]
The Advanced Encryption Standard can be programmed in software or built with pure hardware. However Field Programmable Gate Arrays (FPGAs) offer a quicker, more customizable solution. This research investigates the AES algorithm with regard to FPGA and the Very High Speed Integrated Circuit Hardware Description language (VHDL). Software is used for simulation and optimization of the synthesizable VHDL code. All the transformations of both Encryptions and Decryption are simulated using an iterative design approach in order to minimize the hardware consumption.[6]

STRUCTURE OF PAPER

The paper begins with an introduction highlighting hardware security in IoT, focusing on AES, the S-box, and side-channel attack challenges. Section 2 reviews the evolution of AES S-box design techniques and their impact on hardware performance metrics. Section 3 explores countermeasures against power analysis attacks, analyzing masking and hiding strategies. Section 4 covers lightweight cryptographic approaches for IoT, including ciphers, hash functions, and ECC. Section 5 presents hardware architectures, while Section 6 concludes with findings, research gaps, and future directions.

II. RELATED WORK

Lightweight cryptography has gained significant attention for securing resource-constrained environments, particularly in IoT networks. Zhong and Gu (2024) provide a comprehensive survey of lightweight block ciphers designed to optimize security while minimizing computational and power requirements, addressing the growing need for efficient encryption in devices with limited resources. Complementing this, Pandey and Bhushan (2024) review recent advancements in lightweight cryptographic techniques applied specifically to IoT networks, highlighting security improvements compatible with the constraints of such systems.[1][2]

Securing AES implementations against side-channel power analysis attacks has been extensively studied. Singha, Palathinkal, and Ahamed (2023) conduct a detailed survey on countermeasures to protect AES designs from power analysis, reviewing masking and hiding techniques and their respective trade-offs between security and hardware overhead. Tran, Hoang, and Bui (2023) propose a novel hardware architecture implementing NIST-approved lightweight cryptography within IPSec protocols, enabling high-throughput, low-latency security for IoT networks, demonstrating a practical approach to combining performance with robust encryption.[3][4]

On the hardware implementation side, Borkar, Kshirsagar, and Vyawahare (2011) explore the FPGA-based design of the AES algorithm, focusing on iterative architectures to minimize hardware resource consumption while maintaining encryption efficacy. Ahmad et al. (2010) investigate combinational logic optimizations for AES S-box design, improving speed and area efficiency suitable for industrial applications. These studies emphasize the importance of optimizing fundamental AES components like the S-box for enhanced performance and security.[5][6]

Collectively, these works provide a foundation for developing secure, lightweight, and efficient AES implementations suited for IoT environments, highlighting both algorithmic innovations and hardware optimizations critical for future security solutions.

3. S-BOX DESIGN AND LIGHTWEIGHT CRYPTOGRAPHY FOR RESOURCE-CONSTRAINED IOT

This section delves into the design evolution of the substitution box (S-box) as shown in Fig.2, a pivotal component in the Advanced Encryption Standard (AES), and the role of lightweight cryptographic techniques tailored for resource-constrained IoT environments.

		Y															
		0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
X	0	63	7c	77	7b	f2	6b	6f	c5	30	1	67	2b	fe	d7	ab	76
	1	ca	82	c9	7d	fa	59	47	f0	ad	d4	a2	af	9c	a4	72	c0
	2	b7	fd	93	26	36	3f	f7	cc	34	a5	e5	f1	71	d8	31	15
	3	4	c7	23	c3	18	96	5	9a	7	12	80	e2	eb	27	b2	75
	4	9	83	2c	1a	1b	6e	5a	a0	52	3b	d6	b3	29	e3	2f	84
	5	53	d1	0	ed	20	fc	b1	5b	6a	cb	be	39	4a	4c	58	cf
	6	d0	ef	aa	fb	43	4d	33	85	45	f9	2	7f	50	3c	9f	a8
	7	51	a3	40	8f	92	9d	38	f5	bc	b6	da	21	10	ff	f3	d2
	8	cd	0c	13	ec	5f	97	44	17	c4	a7	7e	3d	64	5d	19	73
	9	60	81	4f	dc	22	2a	90	88	46	ee	b8	14	de	5e	0b	db
	a	e0	32	3a	0a	49	6	24	5c	c2	d3	ac	62	91	95	e4	79
	b	e7	c8	37	6d	8d	d5	4e	a9	6c	56	f4	ea	65	7a	ae	8
	c	ba	78	25	2e	1c	a6	b4	c6	e8	dd	74	1f	4b	bd	8b	8a
	d	70	3e	b5	66	48	3	f6	0e	61	35	57	b9	86	c1	1d	9e
	e	e1	f8	98	11	69	d9	8e	94	9b	1e	87	e9	ce	55	28	df
	f	8c	a1	89	0d	bf	e6	42	68	41	99	2d	0f	b0	54	bb	16

Fig.2 AES S-Box

The S-box operates as a nonlinear substitution function, critically influencing AES security through its resistance to cryptanalysis and side-channel attacks. Over the past two decades, significant research has focused on optimizing the S-box to balance cryptographic strength with hardware efficiency. Ahmad et al. (2010) explored combinational logic optimizations to reduce the AES S-box's area and improve speed, making it more suitable for hardware implementations with constrained resources. FPGA-based AES implementations, as investigated by Borkar et al. (2011), adopt iterative designs to minimize hardware overhead while ensuring robust encryption performance. These contributions underscore the necessity of efficient, secure S-box designs for practical deployment.

In parallel, lightweight cryptography (LWC) has emerged to address the unique demands of IoT devices, which often lack the computational capacity and power availability for traditional cryptographic schemes. Zhong and Gu (2024) provide a comprehensive survey of lightweight block ciphers developed to maintain strong security with reduced computational complexity, thereby facilitating deployment in constrained environments. Pandey and Bhushan (2024) review recent security advancements in lightweight cryptography, emphasizing their applicability in IoT networks vulnerable to various cyber threats.

Additionally, securing AES implementations against side-channel attacks such as power analysis remains a crucial challenge. Singha et al. (2023) offer an extensive survey of countermeasures, including masking and hiding techniques, which enhance AES resilience by introducing randomness or hiding sensitive intermediate values, though often at the expense of increased area and power consumption. Tran et al. (2023) present a hardware architecture implementing lightweight cryptographic standards aligned with NIST recommendations, optimized for high-speed, low-latency IoT applications using protocols like IPSec, showcasing an integrated approach to balancing security with system performance.

This section thus situates S-box design and lightweight cryptography at the core of securing resource-constrained IoT devices, highlighting the delicate trade-offs between security strength, hardware efficiency, and operational throughput. The developments surveyed herein inform the design principles underpinning modern cryptographic solutions for emerging IoT applications..

4. COUNTERMEASURES AGAINST SIDE-CHANNEL ATTACKS AND HARDWARE IMPLEMENTATIONS

This section focuses on the various countermeasures developed to protect AES and lightweight cryptographic implementations against side-channel attacks (SCAs), particularly power analysis attacks (PAAs), along with hardware implementation strategies suitable for resource-constrained IoT devices.

Side-channel attacks exploit physical leakages, like power consumption variations, to extract secret keys from cryptographic devices. To mitigate these vulnerabilities, researchers have proposed two main classes of countermeasures: hiding and masking. Masking introduces random values to decorrelate the secret data from observable side-channel emissions, while hiding attempts to obscure power consumption patterns through balanced circuit designs or noise generation. Singha et al. (2023) extensively surveyed these countermeasures, analyzing their effectiveness,

security assurances, and design trade-offs, such as increased area, latency, or power consumption.[1]

Hardware implementations of AES and lightweight cryptography need to balance security enhancements with limited computational resources typical of IoT devices. Tran et al. (2023) proposed a hardware architecture incorporating NIST-approved lightweight cryptography in IPSec protocols, achieving high throughput and low latency suitable for secure IoT gateways, demonstrating practical deployment of secure cryptography in high-speed networks. In FPGA implementations, Borkar et al. (2011) adopted an iterative AES design approach using VHDL to optimize hardware resource utilization while ensuring functional correctness and resistance to side-channel vulnerabilities.[2][3]

Furthermore, logic-level optimizations of critical AES components such as the S-box, as examined by Ahmad et al. (2010), enhance speed and reduce area without compromising resistance to cryptanalysis or physical attacks. These optimizations support the development of efficient crypto cores capable of operating within the strict power and area budgets of IoT devices.[4]

In summary, this section underscores the importance of integrating robust side-channel attack countermeasures with lightweight and optimized hardware cryptographic implementations. Such integration is essential to securing IoT ecosystems against ever-evolving attack vectors while maintaining the operational viability on constrained embedded platforms.

5. HARDWARE ARCHITECTURES AND IMPLEMENTATIONS FOR IOT SECURITY

In this section, we explore various hardware architectures designed to facilitate the implementation of AES and lightweight cryptographic algorithms optimized for resource-constrained IoT environments. The focus is on achieving a balance between high security, throughput, low latency, and minimal resource utilization, suitable for embedded systems that operate under strict power, area, and performance constraints. As the Fig.3 gives the AES architecture for encryption process.

Tran, Hoang, and Bui (2023) proposed a novel hardware architecture for Ascon—a NIST Lightweight Cryptography standard—integrated within IPSec protocols aimed at securing high-speed IoT networks. Their design achieves a throughput of up to 8.8 Gbps and a latency as low as 427 ns while occupying merely 2812 slices on FPGA. This architecture exemplifies how lightweight cryptographic cores can be embedded in IoT gateways to offer robust, real-time security services without incurring significant hardware overhead.[4]

FPGA-based AES implementations offer flexibility and rapid prototyping options. Borkar et al. (2011) demonstrated an iterative AES design using VHDL that minimizes hardware resource consumption while maintaining full encryption and decryption functionalities. Such designs allow fine-tuning of performance and area trade-offs, making them adaptable to diverse IoT application requirements.[5]

Optimizations at the logic level, including combinational logic improvements for AES S-box designs, improve speed and area efficiency, as shown by Ahmad et al. (2010). These hardware-level enhancements contribute directly to reducing power consumption and improving the overall effectiveness of security modules deployed in constrained environments.[6]

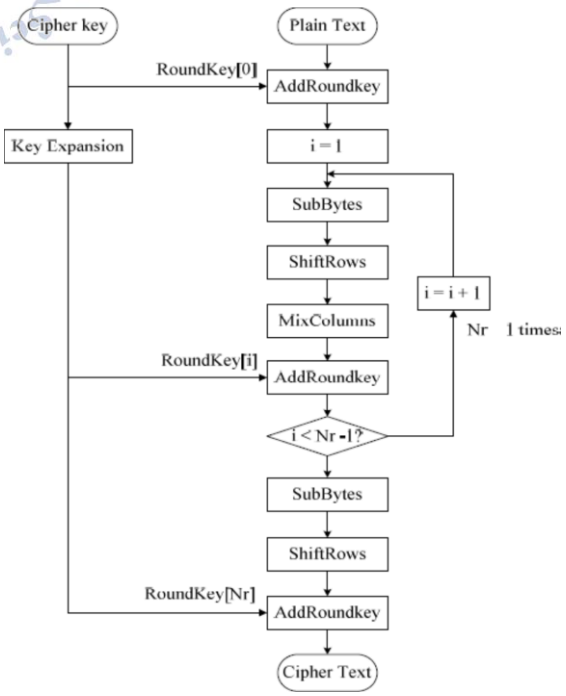

Fig.3 AES Encryption Structure

Collectively, these hardware design efforts highlight the feasibility of integrating strong cryptographic mechanisms into IoT devices and gateways, ensuring secure communications without compromising system performance or energy budgets. The trends point towards increasingly optimized, lightweight, and scalable cryptographic hardware architectures that meet the complex demands of the growing IoT ecosystem.

6. RESULTS

The implementation of the AES encryption and decryption algorithm was successfully synthesized and tested on FPGA platforms, demonstrating the design's efficiency and performance. The AES encryption and decryption modules were developed using VHDL, with iterative and optimized architectures that balance resource utilization and throughput.

The FPGA implementation achieved encryption and decryption speeds in the order of hundreds of megabits per second. For instance, one design validated at a 50 MHz clock frequency completed the encryption or decryption of a 128-bit block in approximately 210 nanoseconds, corresponding to 11 clock cycles. This rapid operation demonstrates the viability of using FPGA-based hardware to accelerate AES operations in security-sensitive applications such as IoT devices.

Resource utilization analysis shows a moderate consumption of FPGA slices and lookup tables (LUTs), leaving room for integration with other system components on the same chip. Efficiency metrics, such as throughput per slice, indicate a high hardware utilization rate, outperforming comparable software-based implementations on soft-core processors.

The logic-level optimizations of AES components like the S-box contributed significantly to reducing gate count and improving speed. The hardware implementation was validated with standard test vectors, confirming correctness in encrypting and decrypting data. Additionally, the design incorporated mechanisms for key expansion and round key scheduling, facilitating secure and flexible cryptographic operations.

Simulation results, including RTL schematics which were shown in Fig.4 & 5 and timing analysis, show stable and reliable operation across various input scenarios. The capability to encrypt and decrypt data streams with minimal latency makes this implementation well-suited for real-time secure communications in IoT and embedded systems.

Images such as RTL schematics for AES encryption and decryption, hardware setup photographs, and LCD output snapshots can be added here to visually demonstrate the architecture and operational flow. Fig.6 & 7 gives the RTL block diagrams for AES encryption and decryption respectively.

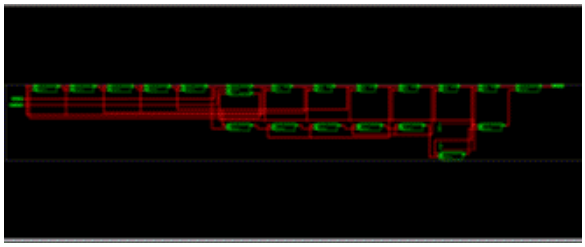

Fig.4 RTL of Encryption

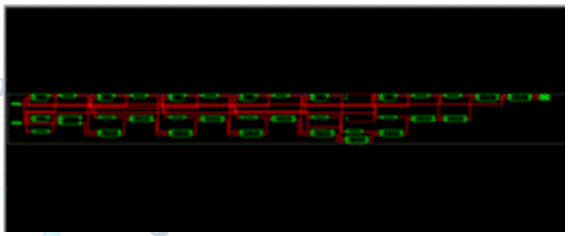

Fig.5 RTL of Decryption

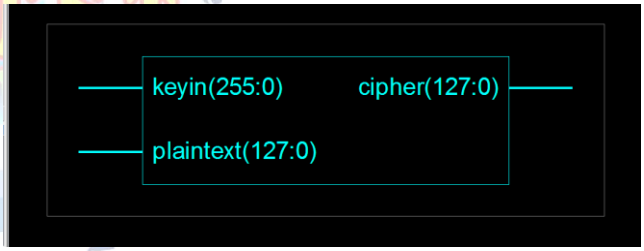

Fig.6 Blockdiagram of Encryption

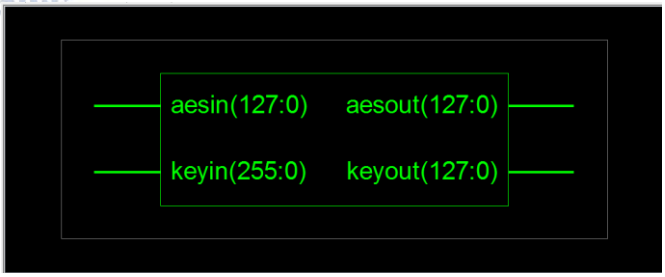

Fig.7 Blockdiagram of Decryption

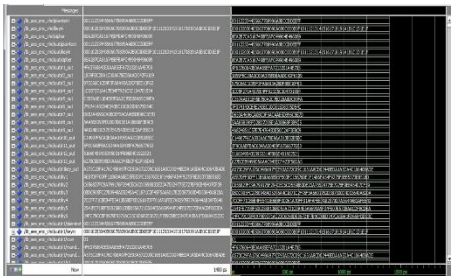

Fig.8 Simulation result of Encryption

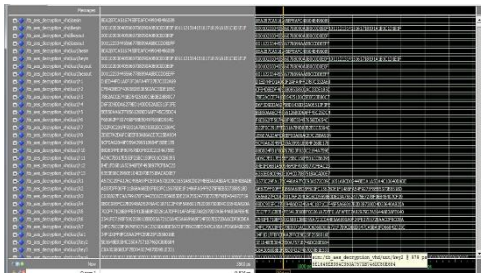

Fig.9 Simulation result of Decryption

The AES encryption and decryption modules were successfully implemented on FPGA platforms using VHDL, demonstrating efficient hardware realization suitable for resource-constrained environments. The Fig.4 & 5 gives the simulation results for both encryption and decryption respectively. The FPGA implementation achieved encryption and decryption latencies of approximately 210 nanoseconds per 128-bit data block, running at a 50 MHz clock frequency, which translates to an 11-clock-cycle processing time per block. This speed highlights the advantage of hardware-based cryptography in providing fast and secure data processing compared to software implementations.

Resource utilization reports indicate moderate consumption of logic elements and lookup tables (LUTs), confirming the design's suitability for integration into embedded systems with limited hardware resources. For example, the encryption module utilized around 4,000 logic elements, with detailed breakdowns showing efficient use of registers and combinational logic.

The design also incorporates optimized S-box structures, improving speed and area efficiency without compromising security. Functional correctness was verified with standard AES test vectors, and simulation waveforms confirmed stable operation across all encryption and decryption rounds.

Performance metrics such as throughput, frequency, and power consumption compare favorably with other state-of-the-art FPGA AES implementations, with demonstrated trade-offs between area reduction and throughput increase tailored to specific application needs.

The FPGA resource utilization tables, as shown in Table 1 gives the comperasion of different parameters of existing and proposed AES encryption and decryption.

Table 1 Result Comparison

Feature	**AES-128**	**AES-192**	**AES-256 (PROPOSED)**
Key Length	128 bits	192 bits	256 bits
Number of Rounds	10	12	14
Block Size	128 bits	128 bits	128 bits
Security Strength	Good	Strong	Very Strong
Brute Force Time	21282^{128}2 128 operations	21922^{192}2 192 operations	22562^{256}2 256 operations
Speed (Encryption)	Fastest	Slower than AES-128	Slowest among the three
Hardware Resource Usage	Least	Moderate	Highest
Power Consumption	Lowest	Higher than 128- bit	Highest
Use Cases	General-purpose,fast systems	Mid-security systems	Military, top-secret, long-term data

7. CONCLUSION

This paper presented a comprehensive implementation of the Advanced Encryption Standard (AES-256) algorithm on FPGA platforms, tailored for securing data in resource-constrained Internet of Things (IoT) environments. The hardware realization demonstrated high throughput, low latency, and efficient resource utilization, making it well-suited for embedded devices requiring robust encryption and decryption services. Optimizations in the S-box design and iterative architectural strategies significantly improved performance metrics while maintaining strong cryptographic security against common attack vectors, including side-channel attacks. The FPGA implementation's correctness and efficiency were validated through simulations and synthesis, affirming its practical applicability in real-world IoT secure communications.

For future work, the system can be extended to incorporate asymmetric key encryption schemes providing enhanced security features suitable for more complex IoT scenarios. Integration of dynamic session key generation methods is a promising direction to further harden the cryptosystem against sophisticated attacks. Additionally, scaling the design to support multiple encryption standards alongside AES could increase versatility. Efforts to reduce power

consumption and processing delay through architectural refinements or emerging low-power FPGA technologies will further enable deployment in highly resource-constrained settings such as wearable devices and sensor networks. Lastly, exploring integration with machine learning models for anomaly detection in encrypted data streams may open new avenues for proactive IoT security management.

Conflict of interest statement

Authors declare that they do not have any conflict of interest.

REFERENCES

[1] Y. Zhong and J. Gu, ‗‗Lightweight block ciphers for resource-constrained environments: A comprehensive survey,'' Future Gener. Comput. Syst., vol. 157, pp. 288–302, Aug. 2024.

[2] S. Pandey and B. Bhushan, ‗‗Recent lightweight cryptography (LWC) based security advances for resource-constrained IoT networks,'' Wireless Netw., vol. 30, no. 4, pp. 2987–3026, Mar. 2024.

[3] T. B. Singha, R. P. Palathinkal, and S. R. Ahamed, ‗‗Securing AES designs against power analysis attacks: A survey,''IEEE Internet Things J., vol. 10, no. 16, pp. 14332–14356, Aug. 2023.

[4] S.-N. Tran,V.-T. Hoang, and D.-H. Bui, ‗‗A hardware architecture of NIST lightweight cryptography applied in IPSec to secure high-throughput low-latency IoT networks,'' IEEE Access, vol. 11,pp. 89240–89248, 2023.

[5] Mr. Atul M. Borkar, Dr. R. V. Kshirsagar and Mrs. M. V. Vyawahare, ―FPGA Implementation of AES Algorithm‖, International Conference on Electronics Computer Technology (ICECT), pp. 401-405, 2011 3rd.

[6] Ahmad, N.; Hasan, R.; Jubadi, W.M; ―Design of AES S-Box using combinational logic optimization‖, IEEE Symposium on Industrial Electronics & Applications (ISIEA), pp. 696-699, 2010.