International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347 - 6435 (Online) Volume 13, Issue 9, September 2024)

Review of Secure and Efficient Lightweight AES Algorithms for IoT Applications

[1]Praveen Kumar Bajpeyi, [2]Dr. Tarun Verma
[1]Research Scholar, [2]Professor
[1,2]Department of Electronics and Communication Engineering
[1,2]Lakshmi Narain College of Technology, Bhopal, India

***Abstract*— The rise of the Internet of Things (IoT) has introduced a new era of interconnected devices, enabling automation and real-time data exchange across various industries. However, these devices often operate under resource constraints, including limited power, memory, and processing capabilities. Ensuring secure communication between IoT devices while maintaining efficiency is a significant challenge. Advanced Encryption Standard (AES), a widely used cryptographic algorithm, offers robust security but can be computationally demanding for IoT applications. This paper reviews recent advancements in lightweight AES algorithms specifically designed for IoT environments. We explore how AES has been modified to meet the unique constraints of IoT devices, focusing on reducing power consumption, memory usage, and computational overhead without compromising security.**

***Keywords*— Image, Denoising, VLSI, Filter, Noise, FPGA.**

I. INTRODUCTION

The Internet of Things (IoT) is revolutionizing the way devices communicate and interact with each other. From smart homes and cities to industrial automation and healthcare, IoT devices have become an integral part of modern technology ecosystems. These devices collect, transmit, and process vast amounts of data, often in real-time, to support a wide range of applications. However, with the rapid proliferation of IoT devices comes the critical need to secure the data being transmitted between them. IoT devices are often deployed in environments where security breaches can have severe consequences, such as in healthcare systems, critical infrastructure, and industrial automation. Therefore, ensuring the confidentiality, integrity, and authenticity of data in IoT networks is paramount.

One of the most widely used cryptographic algorithms for securing data is the Advanced Encryption Standard (AES). Originally developed by the National Institute of Standards and Technology (NIST), AES has been the gold standard for encryption due to its strong security guarantees and widespread adoption. It is employed in a variety of applications, from securing online transactions to encrypting sensitive communications. However, AES was not originally designed with the unique constraints of IoT devices in mind. IoT devices often operate with limited computational power, memory, and battery life, making the implementation of standard AES algorithms a challenge.

Traditional AES algorithms are computationally intensive and consume significant power, which can drain the limited battery resources of IoT devices. Furthermore, IoT devices may lack the processing capabilities required to execute standard AES encryption and decryption operations in a timely manner. These constraints have driven the development of lightweight cryptographic algorithms that offer the same level of security as traditional AES but with reduced resource demands. Lightweight cryptography aims to tailor algorithms like AES to meet the needs of resource-constrained environments, making them suitable for IoT applications.

The concept of lightweight cryptography is not new, but its importance has grown in parallel with the expansion of the IoT landscape. A variety of lightweight AES implementations have been proposed, each with its own approach to reducing the resource footprint of the algorithm while maintaining its security properties. These implementations often focus on optimizing key operations within AES, such as substitution, permutation, and key expansion, to minimize power consumption, reduce memory usage, and lower computational overhead.

In this review, we aim to provide a comprehensive overview of the various lightweight AES algorithms designed for IoT applications. We will examine the trade-offs between security, efficiency, and resource consumption in these algorithms, highlighting the key techniques used to optimize AES for low-power, low-memory IoT devices. By reviewing both hardware and software-based approaches, this paper seeks to offer insights into the current state of lightweight AES implementations and their suitability for different IoT use cases.

We begin by discussing the fundamental challenges associated with implementing AES in IoT environments, followed by an exploration of the most prominent lightweight AES algorithms. The review will also analyze the impact of these algorithms on power consumption, memory efficiency, and computational performance. Finally, we will provide recommendations for future research directions and practical applications, emphasizing the need for continued innovation in lightweight cryptography to ensure the security and efficiency of IoT systems.

II. LITERATURE SURVEY

P. Y. Cheng et al.,[1] developed a new datapath for the advanced encryption standard (AES), which has been essentially improved with high efficiency of throughout-to-area for lightweight applications in Internet of Things (IoT) devices. Transmission of encrypted data is planned usage for this datapath. The proposed Advanced Encryption Standard (AES) architecture lets 32-bit blocks be concurrently encrypted, therefore enabling quick processing of 128-bit data while simultaneously reducing the need of hardware space. Using shift registers instead of standard registers allows optimization in the key expansion stages of the 32-bit AES operation as well as in MixColumns and ShiftRows.

Kumar et al.,[2] provided in this work a new block cipher: Simple Hybrid Cipher, SHC. Its key length is 128 bits while its block length is 64 bits. Its hardware implementation, which makes best use of little resources, qualifies it as a great candidate for use as an RFID tag or sensor in a wireless sensor network (WSN). S-Box-based composite field arithmetic technology is the fundamental ability of SHC. This technology is beneficial as, whilst at the same time providing sufficient security as a strong encryption technique, its implementation on hardware is somewhat affordable. The hardware implementation of SHC-64 requires 949 LUTs overall, which generates a maximum operational frequency of 515.995 MHz on the Artix-7 Field Programmable Gate Array (FPGA) development board run by Xilinx.

X. He et al., [3] Internet of Things (IoT) endpoint devices include many data or address ciphers meant to provide real-time memory protection. This is undertaken to stop certain side-channel assaults on memory. To provide memory address encryption with variable width adaptability, low latency, and low hardware overhead, this article offers a hardware engine of permutation-based address encryption (PAE). This work aims to meet real-time memory protection's demands more satisfactorially. With a gate count of 0.589 KGates, which is merely 0.37% of advanced encryption standard (AES) and 33.50% of address cipher Galois field encryption (GF-Enc), PAE offers lightweight qualities evaluated using TSMC's 40-nm standard CMOS technology. PAE counts 0.589 kg-gates.

R. Huang [4] Usually referred to as AES, the Advanced Encryption Standard is among the most often used cryptographic methods available to guarantee data security. Although they neglect the optimization of performance, most lightweight implementations of the method that have been described in the literature focus on maximizing the optimization of area and power. Within the framework of this work, a novel lightweight method to the AES algorithm is proposed and both encryption and decryption are taken under account. By 1.69 times in terms of performance per unit space and 1.27 times in terms of performance per unit power correspondingly, our 32-bit architecture surpasses the present state of the art. These advantages become significantly more important when larger data-path designs—such as 64-bit or 128-bit designs—are used.

J. Vimalkumar [5] Given the rapidly increasing use of Internet of Things devices, a suitable encryption technique is needed to guarantee the protection of data. Commonly used Advanced Encryption Standard (AES) approach is not best for Internet of

Things devices with low processing capacity because to computational complexity. With the aim of reducing the power and memory consumption, the proposed work generates ideal replacements for the phases of the 128-bit AES method. An Artix-7 Basys-3 FPGA board then housed a Modified Lightweight variant of AES built using Verilog HDL. The altered variety was shown to use 81.92% less chip power for encryption and 47.21% less for decoding. Decryption as well as encryption followed this pattern. With 76.84% for encryption and 53.53% for decryption, this technique lowers the number of LUTs required by a great degree, therefore it is fit for Internet of Things lightweight applications.

P. Satyanarayana [6] Applied on Internet of Things devices with low capability, the AES algorithm faced challenges in terms of the quantity of computational resources and energy usage. The change we have proposed uses lightweight cryptographic techniques to overcome these limitations, therefore enhancing the method for low-power microcontrollers, which are often used in Internet of Things devices. The revised AES algorithm shows a significant decrease in the computational accuracy it offers even if it maintains a high degree of security. The study seeks to use modified AES to the environment of the Internet of Things in order to improve the general security of Internet of Things networks and lower the danger of probable vulnerabilities. To confirm the efficacy of the proposed method, extensive simulations and practical studies were conducted on a broad range of Internet of Things devices under a variety of network environments.

GS Rajput et al., [7] It is evident that using cryptography in algorithms is secure and efficient. Though it is like other symmetric encryption systems, the secret key distribution is still seen as a fundamental challenge. One single block of data (128 bits) has to be encrypted or decrypted, which calls more computer activity and higher power consumption. Thanks to the Internet of Things (IoT), nearly everything on the planet is being connected to one another. This paper presents a 256-bit key, lightweight cryptography-based data security method used for an IOT use. We propose a new one-dimensional substitution box (S-box) instead of the conventional 2-D S-box and the previous 1-D S-box.

S. Purohit et al., [8] cryptography as a vital instrument. As a fundamental building component for safe systems, it performs two functions: safeguarding of private information and facilitation of honest communication and transactions. Hardware-based encryption allows one to reach the best degrees of security, performance, and compliance. The Advanced Encryption Standard encryption offers a good degree of cryptographic security by effectively scrambling the plain text, therefore providing a strong level of protection. The aim of this study is to provide a novel method for the challenge of attaining an efficient implementation of the Advanced Encryption Standard block cipher cryptographic algorithm on the Intel DE-10 Lite FPGA development board: Architectural enhancements for the forward and inverse AES SubBytes transformation (S-box and inverse S-box) are achieved by use of Linear Feedback Shift Registers. Furthermore included are computational enhancements meant to cut the memory storage used during round-wise key expansion.

Gong [9] presented and verify a lightweight digital true random number generator (DTRNG) circuit based on inverters on silicon. Silicon is used in construction of the circuit. Here is presentation of extraction and analysis of inverter jitter's entropy. Presenting a conventional digital cell library and a clock frequency of 8MHz, the DTRNG circuit is described. One may just transfer this circuit to other process platforms; Internet of Things devices with a limited size and low running frequency are ideal for it.

M. Nooruddin [10] use the features of ASCON, a lightweight cryptographic standard selected by the National Institute of Standards and Technology (NIST). Overcoming standard AES in Internet of Things applications, ASCON provides encryption and authentication within a single container that is memory-efficient. The system is built to be implemented utilizing a key exchange approach that makes use of pre-shared keys and a key exchange protocol thereby guaranteeing the safety of the negotiating of encryption keys between devices.

III. CHALLENGES

While lightweight AES algorithms provide an effective solution for securing IoT devices, their implementation presents several challenges that need to be addressed for widespread adoption. The nature of IoT environments, characterized by limited resources, varying device architectures, and diverse application requirements, complicates the task of designing cryptographic algorithms that are both secure and efficient. The key challenges in implementing lightweight AES for IoT applications are as follows:

1. Resource Constraints

One of the primary challenges in deploying AES in IoT devices is the severe limitation of computational resources. Most IoT devices operate with low-power processors, limited memory, and small battery capacities. Standard AES algorithms, while secure, are computationally expensive and memory-intensive, leading to high energy consumption. Lightweight AES implementations must, therefore, minimize these resource demands while maintaining the algorithm's cryptographic strength. Striking the right balance between security and efficiency in such constrained environments is a difficult task, as over-optimizing the algorithm for performance may lead to weaker security.

2. Power Consumption

IoT devices are often battery-powered and operate in environments where regular charging or battery replacement is impractical. Thus, power efficiency is crucial for extending the device's operational life. Traditional AES algorithms involve complex mathematical operations that require substantial energy. Lightweight cryptographic designs must reduce power consumption by simplifying operations, reducing the number of rounds, or optimizing hardware architecture. However, this can potentially weaken the algorithm's resilience against attacks, making power optimization a delicate challenge.

3. Security vs. Efficiency Trade-Off

A fundamental challenge in lightweight cryptography is the trade-off between security and efficiency. Reducing the computational and memory requirements of AES can expose the algorithm to new vulnerabilities. For example, using fewer rounds of encryption or simplifying key schedules might compromise the algorithm's resistance to certain attacks. Finding the optimal trade-off between reducing resource usage and maintaining robust security is an ongoing research challenge. IoT applications vary widely in their security requirements, which means that a one-size-fits-all solution is rarely feasible.

4. Vulnerability to Side-Channel Attacks

Lightweight AES implementations, particularly those optimized for hardware, are often more susceptible to side-channel attacks (SCAs), which exploit information leaked from the physical implementation of the algorithm. SCAs such as power analysis, electromagnetic analysis, or timing attacks can reveal critical information about the encryption process, potentially allowing attackers to break the cryptographic system. Securing lightweight AES against such attacks is a complex task, as adding countermeasures can increase the power consumption and computational complexity, counteracting the benefits of lightweight design.

5. Scalability Across Diverse IoT Devices

IoT networks are highly heterogeneous, consisting of devices with varying computational capabilities, memory capacities, and communication protocols. Designing a lightweight AES implementation that scales across such diverse environments is challenging. Some devices may have sufficient resources to run more complex encryption schemes, while others may be severely constrained. Additionally, IoT devices often communicate over wireless networks with low bandwidth, necessitating cryptographic protocols that are efficient in terms of both computation and communication overhead.

IV. CONCLUSION

In the growing landscape of IoT, ensuring secure communication while addressing the resource limitations of devices is critical. Lightweight AES algorithms offer a viable solution by optimizing the traditional AES for reduced power consumption, memory usage, and computational complexity. However, challenges such as the trade-off between security and efficiency, vulnerability to side-channel attacks, and the need for standardization remain significant hurdles. Continued research is necessary to refine these algorithms and develop more robust, scalable, and secure implementations. By addressing these challenges, lightweight AES can play a pivotal role in securing IoT ecosystems, ensuring that even resource-constrained devices can operate securely and efficiently. The future of lightweight cryptography lies in balancing performance with evolving security needs, particularly as threats become more sophisticated.

REFERENCES

1. P. Y. Cheng, Y. C. Su and P. C. P. Chao, "Novel High Throughput-to-Area Efficiency and Strong-Resilience Datapath of AES for Lightweight Implementation in IoT Devices," in IEEE Internet of Things Journal, vol. 11, no. 10, pp. 17678-17687, 15 May15, 2024, doi: 10.1109/JIOT.2024.3359714.

2. S. Kumar *et al.*, "SHC: 8-bit Compact and Efficient S-Box Structure for Lightweight Cryptography," in *IEEE Access*, vol. 12, pp. 39430-39449, 2024, doi: 10.1109/ACCESS.2024.3372388.

3. X. He, Y. Bai, Y. Liu, L. Du, Z. Wang and Y. Du, "Low-Latency PAE: Permutation-Based Address Encryption Hardware Engine for IoT Real-Time Memory Protection," in *IEEE Internet of Things Journal*, vol. 11, no. 7, pp. 12319-12330, 1 April1, 2024, doi: 10.1109/JIOT.2023.3333203.

4. R. Huang, A. Aljuffri, S. Hamdioui, K. Ma and M. Taouil, "Securing an Efficient Lightweight AES Accelerator," *2023 IEEE 22nd International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*, Exeter, United Kingdom, 2023, pp. 841-848, doi: 10.1109/TrustCom60117.2023.00121.

5. J. Vimalkumar, H. R. Babu and B. M, "FPGA Implementation of Modified Lightweight 128-Bit AES Algorithm for IoT Applications," *2023 IEEE International Symposium on Smart Electronic Systems (iSES)*, Ahmedabad, India, 2023, pp. 306-309, doi: 10.1109/iSES58672.2023.00069.

6. P. Satyanarayana, N. Sriramdas, B. Madhavi, A. M, N. V. Phani Sai Kumar and V. Gokula Krishnan, "Enhancement of Security in IoT Using Modified AES Algorithm for IoT Applications," *2023 International Conference on Sustainable Communication Networks and Application (ICSCNA)*, Theni, India, 2023, pp. 380-386, doi: 10.1109/ICSCNA58489.2023.10370606.

7. GS Rajput, R Thakur, R Tiwari "VLSI implementation of lightweight cryptography technique for FPGA-IOT application" Materials Today: Proceedings, 2023, ISSN 2214-7853, doi: 10.1016/j.matpr.2023.03.486.

8. S. Purohit, V. Deshpande and V. Ingale, "FPGA Implementation of the AES Algorithm with Lightweight LFSR-Based Approach and Optimized Key Expansion," *2023 IEEE International Conference on Public Key Infrastructure and its Applications (PKIA)*, Bangalore, India, 2023, pp. 1-7, doi: 10.1109/PKIA58446.2023.10262697.

9. M. Gong, Z. Zheng and H. Li, "An Inverter-based Lightweight Digital True Random Number Generator Circuit for IoT Device," *2022 10th International Symposium on Next-Generation Electronics (ISNE)*, Wuxi, China, 2023, pp. 1-3, doi: 10.1109/ISNE56211.2023.10221587.

10. M. Nooruddin and D. Valles, "An Advanced IoT Framework for Long Range Connectivity and Secure Data Transmission Leveraging LoRa and ASCON Encryption," *2023 IEEE World AI IoT Congress (AIIoT)*, Seattle, WA, USA, 2023, pp. 0583-0589, doi: 10.1109/AIIoT58121.2023.10174401.