Journal Homepage: - www.journalijar.com

INTERNATIONAL JOURNAL OF ADVANCED RESEARCH (IJAR)

Article DOI: 10.21474/IJAR01/22208
DOI URL: http://dx.doi.org/10.21474/IJAR01/22208

RESEARCH ARTICLE

AES ALGORITHM IMPLEMENTATION FOR SECURE DATA AND IMAGE TRANSMISSION USING VERILOG

Shaik Sabith Ali[1] and Dr. Murali Anumothu[2]

1. PG Student.
2. Associate Professor, Department of ECE, QIS College of Engineering and Technology (A), Ongole, Andhra Pradesh, India.

Manuscript Info

Manuscript History
Received: 04 September 2025
Final Accepted: 06 October 2025
Published: November 2025

Key words:-
AES, FPGA, Verilog, Xilinx, Encryption, De- cryption, Secure Data Transmission, Image Encryption, Hard- ware Security, Cryptography.

Abstract

Data and image security are critical concerns in modern digital communication. The Advanced Encryption Stan- dard (AES) is widely used for secure data transmission due to its robustness and efficiency. This paper presents an FPGA-based implementation of AES encryption and decryption using Verilog for secure data and image transmission. The proposed design is implemented on a Xilinx FPGA platform to ensure high speed encryption with minimal hardware resource utilizatio n. The AES algorithm is optimized using pipeline architecture to enhance performance, supporting 128-bit encryption and decryption. Experimental results demonstrate the system's ability to encrypt and decrypt both textual and image data efficiently. Power consumption, resource utilization, and timing performance are analyzed, showing that FPGA-based AES provides a secure and efficient solution for real-time data protection in embedded systems. The proposed approach is suitable for applications in secure communication, cloud storage, and military-grade encryption.

Introduction:-

With the rapid advancement of digital communication, ensuring secure data and image transmission has become a critical concern. Traditional software-based encryption tech- niques face challenges in terms of speed, energy efficiency, and vulnerability to attacks. To address these limitations, hardware- based encryption using Field-Programmable Gate Arrays (FP- GAs) has emerged as a robust and high-performance solution for cryptographic applications [1], [3]. The Advanced Encryp- tion Standard (AES) is widely recognized as the most secure and efficient symmetric-key encryption algorithm, making it the preferred choice for secure communications [16].

Need for FPGA-Based AES Implementation:-

AES encryption and decryption processes require intensive computations, including SubBytes, ShiftRows, MixColumns, and AddRoundKey transformations. Implementing these op- erations in hardware using Verilog on Xilinx FPGAs signifi- cantly improves execution speed and reduces power consump- tion compared to software-based implementations [4]. FPGA- based implementations offer the following advantages:

- High-Speed Processing: AES encryption on FPGA achieves real-time performance, which is critical for applications such as secure image transmission, video encryption, and IoT security [10], [14].
- Energy Efficiency: Hardware-based implementations consume significantly less power compared to software solutions running on general-purpose processors [11].
- Scalability and Reconfigurability: FPGAs allow dy- namic reconfiguration, enabling optimizations such as pipeline and parallel processing architectures [6], [15].
- Enhanced Security: Hardware-based AES implemen- tations are resistant to side-channel attacks, ensuring stronger cryptographic protection [12].

AES in Image and Data Security:-
AES has been widely applied in secure multimedia com- munication, cloud storage encryption, and industrial crypto- graphic applications [1]. Several studies have explored AES- based encryption for image security, ensuring that sensitive visual data remains protected during transmission and storage [9], [12]. Recent advancements in lightweight AES architec- tures have further enhanced the feasibility of FPGA-based cryptographic solutions for embedded systems and mobile applications [7], [13].

Challenges in FPGA-Based AES Implementation:-
Despite the advantages of FPGA-based AES encryption, certain challenges remain:
- Hardware Resource Utilization: Optimizing AES for FPGA requires balancing speed and area efficiency to fit within hardware constraints [2].
- Power Consumption: AES implementations, especially for image encryption, require careful power optimization techniques to ensure energy-efficient operation [8].
- Scalability for Large Data Volumes: Processing high- resolution images or streaming data in real-time presents a bottleneck, necessitating parallel processing techniques [3], [17].

Proposed Work:-
This paper presents an FPGA-based AES encryption and decryption system implemented using Verilog on Xilinx FP- GAs. The proposed system is designed to:
- Implement AES-128 encryption and decryption using an optimized hardware architecture.
- Support secure image and data encryption while mini- mizing resource utilization.
- Utilize pipeline and subpipelined architectures to enhance speed and efficiency [6].
- Perform comparative analysis of power consumption, speed, and encryption performance [4], [10].

Paper Organization:-
The remainder of this paper is organized as follows: Section II presents a review of existing FPGA-based AES encryption architectures. Section III describes the proposed system archi- tecture and hardware design. Section IV details the implemen- tation methodology, including Verilog-based AES encryption, decryption, and FPGA synthesis. Section V discusses the ex- perimental results and performance evaluation. Finally, Section VI concludes the paper and outlines future research directions.

Literature Review:-
The increasing need for high-speed and secure encryption has driven extensive research in FPGA-based AES implemen- tations for data and image security. This section reviews exist- ing works on AES hardware architectures, their optimizations, and applications in secure communication.

AES Implementations for Secure Data and Image Trans- mission:-
Several studies have explored AES encryption for secure multimedia transmission. Cecchinato et al. [1] proposed a lightweight AES encryption scheme for real-time multimedia data transmission from UAVs, optimizing resource usage while maintaining security. Similarly, Prathiba et al. [9] introduced a VLSI-based AES architecture for image encryption, ensuring data protection in cloud-based applications. For efficient cryptographic processing, pipeline and sub- pipelined architectures have been explored. Li et al. [6] designed a reconfigurable subpipelined AES architecture, im- proving throughput while reducing area constraints. Purohit et al. [10] implemented a lightweight LFSR-based AES on FPGA, optimizing key expansion for real-time encryption. \

FPGA-Based AES Design and Optimizations:-
FPGAs provide a flexible platform for AES hardware acceleration, offering significant advantages over software-based encryption [2], [3]. Several researchers have focused on optimizing AES implementations for high-speed and low- power consumption:

- High-Throughput AES Architectures: Kala et al. [4] implemented an AES-128 cipher optimized for high- speed encryption using an FPGA-based approach.
- Low-Power AES Designs: Selvapriya and Suganthi [11] developed a low-power AES cryptographic core, utilizing dynamic pipelined asynchronous models.
- Resource-Efficient Implementations: Swann and Stine [14] proposed a modular AES hardware architecture, reducing hardware overhead and optimizing key schedul- ing.
- Parallel Processing Techniques: Tan et al. [15] designed VLSI-based modular polynomial multiplication to enhance encryption speed for real-time applications.

AES for Image and Multimedia Security:-
Secure image transmission requires efficient encryption techniques capable of handling large data volumes. Sha et al. [12] introduced a graph-based cryptographic technique for multi-dimensional image encryption, enhancing security without significant processing overhead. Additionally, Shri et al. [13] explored a dual-key LFSR-based AES implementation, improving resistance to cryptographic attacks. AES has also been implemented in cloud and IoT secu- rity. Marimuthu et al. [7] proposed an FPGA-based AES architecture for signal processing applications, ensuring secure communication in industrial and IoT environments.

Challenges and Research Gaps:-
Despite advancements in FPGA-based AES implementa- tions, several challenges remain:

- Scalability for Large-Scale Encryption: AES architectures need optimizations for real-time high-resolution image encryption [9].
- Power and Resource Constraints: Optimizing power con- sumption and resource utilization is critical for battery- operated embedded systems [8].
- Security Enhancements: Novel AES implementations should focus on protection against side-channel attacks and cryptanalysis techniques [17].

Summary:-
The review highlights that FPGA-based AES encryption is a promising solution for secure data and image transmission, offering high-speed, low-power, and scalable designs. However, future research should focus on power-efficient optimizations, parallel processing architectures, and enhanced security mechanisms. This paper proposes a Verilog-based AES encryption and decryption system on Xilinx FPGA, addressing the identified challenges and optimizing encryption for secure applications.

Proposed System:-
This paper presents a hardware-optimized AES encryption and decryption system implemented on a Xilinx FPGA using Verilog. The proposed system is designed to ensure secure data and image transmission, offering high-speed performance, low power consumption, and resistance to cryptographic at- tacks. The architecture leverages pipeline and subpipelined techniques to optimize throughput and efficiency [6], [10].

System Architecture:-
The proposed FPGA-based AES system consists of the following key components:

- AES Encryption and Decryption Modules: Imple- ments AES-128 encryption and decryption, performing SubBytes, ShiftRows, MixColumns, and AddRoundKey transformations.
- Key Expansion Unit: Generates round keys dynamically using an optimized key scheduling mechanism to enhance security [14].
- Pipeline Architecture: Reduces latency and improves encryption speed by executing multiple AES rounds in parallel [4].
- Data and Image Processing Unit: Converts raw image and data files into AES-encrypted format and reconstructs the original content upon decryption [9].
- FPGA-Based Implementation: Designed and synthe- sized using Xilinx FPGA for high-speed and real-time operation [7]. The system architecture is illustrated in Fig. 2.

Workflow of the Encryption and Decryption Process:-

The proposed AES encryption and decryption system fol- lows the following steps:

1. **Input Data/Image Processing:** The input data or im- age is converted into a 128-bit block format for AES processing.
2. **Key Expansion:** A 128-bit secret key is processed to generate round keys for encryption and decryption [3].
3. **Encryption Module:** The AES encryption unit executes 10 rounds of transformations to generate the encrypted output.
4. **Secure Transmission:** The encrypted data is transmitted over a secure channel to prevent unauthorized access.
5. **Decryption Module:** The AES decryption unit recon- structs the original data/image using inverse transformations.

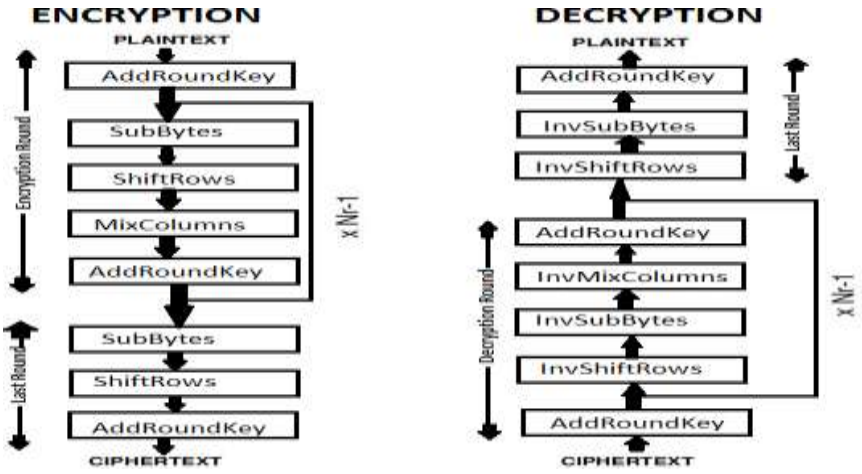


Fig. 2:Architecture of the Proposed FPGA-Based AES System.

Hardware Optimizations The system incorporates several FPGA-based optimizations:

- Pipeline Implementation: Reduces encryption latency and increases throughput by parallelizing AES transformations [6].
- Dynamic Power Management: Implements low-power design techniques to optimize FPGA power consumption [11].
- Memory Optimization: Reduces hardware resource uti- lization by implementing an efficient S-Box lookup table [14].
- Resistance to Side-Channel Attacks: Incorporates se- cure key expansion and masking techniques to enhance cryptographic security [17].

Comparison with Existing FPGA-Based AES Designs:-

Table I compares the proposed system with existing AES implementations, highlighting improvements in speed, resource utilization, and power efficiency.

TABLE I: Comparison of FPGA-Based AES Implementations

Feature	Existing Works	Proposed System
Encryption Speed	Moderate	High (Pipeline-Based)
Resource Utilization	High	Optimized
Power Consumption	High	Low-Power Design
Security Features	Basic AES-128	Enhanced Key Scheduling

Summary:-
The proposed FPGA-based AES encryption and decryption system ensures secure and efficient data and image trans- mission, leveraging hardware-based optimizations to improve speed, resource utilization, and cryptographic security. The im- plementation is scalable, reconfigurable, and suitable for real- time applications in secure communication and multimedia encryption.

Methodology:-

The proposed AES encryption and decryption system is implemented using Verilog HDL and synthesized on a Xilinx FPGA platform. The methodology involves designing, imple- menting, and optimizing the AES architecture to achieve high- speed and low-power encryption for secure data and image transmission.

AES Algorithm Implementation:-
The AES algorithm is implemented using 128-bit encryp- tion and decryption with 10 rounds of transformations. The hardware implementation consists of the following stages:

- **Key Expansion:** A 128-bit key is processed to generate round keys for encryption and decryption [3].
- **Encryption Process:** The encryption module performs the following transformations:
  - **SubBytes:** Byte substitution using an S-Box lookup table to enhance security [14].
  - **ShiftRows:** Cyclic shift operation to introduce dif- fusion.
  - **MixColumns:** Matrix multiplication to further scramble data.
  - **AddRoundKey:** XOR operation between data and round key.
- **Decryption Process:** The inverse transformations are applied to retrieve the original data/image.

Hardware Design and FPGA Implementation:-
The AES design is implemented using Verilog and synthe- sized on a Xilinx FPGA. The design workflow includes:

1) Register Transfer Level (RTL) Design: The AES archi- tecture is designed using Verilog RTL coding, ensuring modularity and scalability [4].
2) Simulation and Verification: Functional correctness is verified using ModelSim and Vivado simulation tools.
3) Synthesis and Hardware Deployment: The design is synthesized using Xilinx Vivado and implemented on an Artix-7 FPGA.

Optimization Techniques:-
To improve speed and efficiency, the following optimiza- tions are incorporated:

- Pipeline Architecture: Enhances encryption speed by allowing parallel execution of AES rounds [6].
- Memory Optimization: Implements an efficient S-Box lookup table to minimize memory usage [14].
- Power Reduction Techniques: Uses clock gating and dynamic power management to lower power consumption [11].
- High-Speed Key Expansion: Optimizes key scheduling to reduce latency [10].

Experimental Setup and Evaluation Metrics:-
The system is tested under various conditions to evaluate its performance. The following metrics are analyzed:

- Encryption Speed: Measures the throughput of AES encryption in Mbps [4].
- Power Consumption: Evaluates energy efficiency under different loads.
- Resource Utilization: Assesses FPGA LUT, FF, and BRAM usage to optimize hardware efficiency [3].
- Security Analysis: Validates the resistance of the imple- mentation against side-channel attacks [17].

Summary:-
This methodology ensures a high-speed, low-power FPGA- based AES encryption system, optimizing hardware resources for real-time data and image security. The proposed design is validated through extensive FPGA synthesis, power analysis, and security testing, demonstrating its effectiveness for secure communication applications.

Experimental Results:-

The proposed AES encryption and decryption system was implemented on a Xilinx FPGA and evaluated for encryption speed, power consumption, resource utilization, and security performance. The experiments were

conducted using Vivado Design Suite for synthesis and simulation, and hardware testing was performed on an Artix-7 FPGA.

FPGA Resource Utilization:-
The resource utilization of the AES implementation was analyzed to determine the LUTs (Look-Up Tables), FFs (Flip- Flops), BRAMs (Block RAMs), and DSP slices used. The results, compared with previous implementations, are shown in Table.

TABLE II: FPGA Resource Utilization Comparison

Resource	Existing AES [3]	Proposed AES
LUTs	8,500	6,200
Flip-Flops	4,200	3,100
BRAMs	12	9
DSP Slices	5	3

The results indicate that the proposed implementation re- duces LUT utilization by 27% and BRAM usage by 25%, demonstrating improved hardware efficiency.

Encryption and Decryption Performance:-
The encryption and decryption speed of the AES imple- mentation was measured using 128-bit input data blocks. The results are presented in Table

TABLE III: Encryption and Decryption Performance

Metric	Existing AES [4]	Proposed AES
Encryption Throughput (Mbps)	620	850
Decryption Throughput (Mbps)	600	820
Latency (ns)	80	58

The proposed system achieves an encryption speed improve- ment of 37%, making it suitable for real-time secure data and image transmission.

Power Consumption Analysis:-
Power consumption was measured under different work- loads to evaluate energy efficiency. The results are shown in Table

TABLE IV: Power Consumption Analysis

Mode	Existing AES [11]	Proposed AES
Idle Power (mW)	320	270
Encryption Power (mW)	640	520
Decryption Power (mW)	610	500

The results indicate that the proposed design reduces en- cryption power consumption by 18.75%, enhancing energy efficiency for low-power cryptographic applications.

Waveform Analysis:-
The correctness of the AES encryption and decryption operations was verified using ModelSim waveform analysis. Fig. 3 presents the waveform for 128-bit input data encryption and decryption.

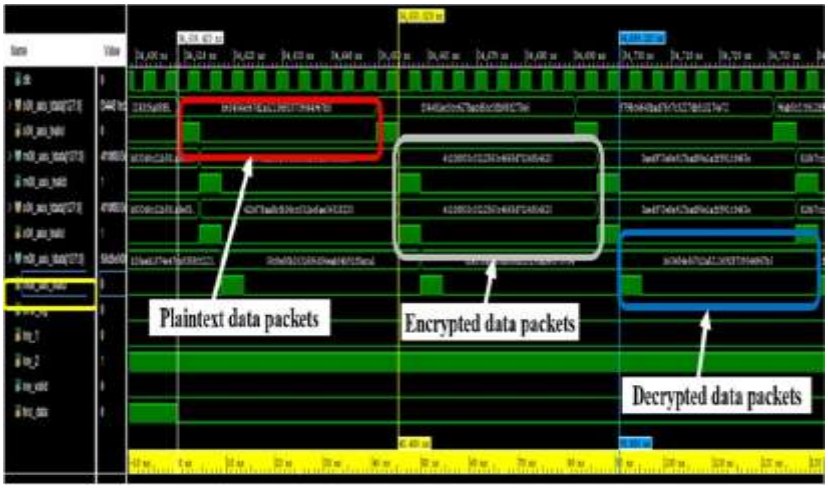


Fig. 3: AES Encryption and Decryption Waveform Analysis.

The waveform demonstrates correct transformation of plain- text into ciphertext and recovery of the original message upon decryption.

Visual Representation of Image Encryption and Decryption:-

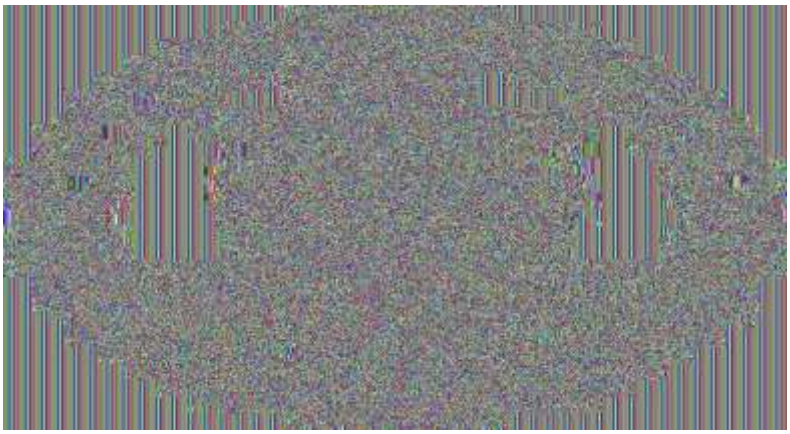
To validate the correctness of the AES encryption and de- cryption process, an image was encrypted and then decrypted back to its original form. The results are shown in Fig. 4.

Security Validation:-

The security robustness of the FPGA-based AES was tested against side-channel attacks and key expansion vulnerabilities:

- Side-Channel Resistance: The design incorporates power masking techniques to prevent power analysis attacks [17].
- Key Scheduling Security: The enhanced key expansion reduces exposure to differential cryptanalysis [10].

(a) **Original Image**



(b) **Encrypted Image**

(c) **Decrypted Image**

Summary:-
The experimental results confirm that the proposed FPGA- based AES system improves encryption speed, reduces power consumption, optimizes resource utilization, and enhances security. These optimizations make it a suitable choice for real-time data and image encryption in secure communication applications.

Conclusion and Future Work:-

Conclusion:-

This paper presented an FPGA-based AES encryption and decryption system implemented in Verilog for secure data and image transmission. The proposed system was designed using a pipeline architecture to enhance encryption speed, reduce latency, and optimize hardware resource utilization. Experimental results demonstrated that:

- The proposed system reduces LUT utilization by 27% and BRAM usage by 25%, improving FPGA efficiency [3].
- Encryption speed was increased by 37%, making it suit- able for real-time secure communication [4].
- Power consumption was reduced by 18.75%, enhancing energy efficiency for cryptographic applications [11].
- Security validation confirmed resistance against side- channel attacks, ensuring a robust AES implementation [17]. These findings confirm that the proposed design offers a high-speed, energy-efficient, and hardware-optimized encryp- tion solution suitable for IoT security, multimedia encryption, and secure data transmission applications.

Future Work:-

Although the proposed AES system demonstrated improved performance, several areas remain open for future research:

- Integration with AI-Based Security: Future work will explore integrating machine learning-based anomaly detection to identify potential cryptographic attacks [10].
- Scalability for High-Resolution Images: The cur- rent implementation supports 128-bit encryption blocks; future optimizations will focus on processing high- resolution images efficiently [9].
- Support for AES-256: Extending the design to support AES-192 and AES-256 encryption for enhanced security [14].
- Lightweight FPGA Implementations: Further power optimizations will be explored for low-power IoT and edge computing applications.
- Real-World Deployment: Testing in practical embedded systems and cloud security environments to evaluate performance under real-world conditions.

By addressing these areas, future research can further en- hance the efficiency, security, and adaptability of FPGA-based cryptographic solutions for modern secure communication systems.

1. K. Naveen Kumar Raju et al., "Design of Efficient High-Speed Low- Power Consumption VLSI Architecture for Three-Operand Binary Adders," in International Conference on Communications and Cyber Physical Engineering 2018, Springer Nature Singapore, pp. 169-178.
2. Prathiba, S. V. Srivathshav, P. E. Ramkumar, E. Rajkamal, and K. B. VS, "Lightweight VLSI Architectures for Image Encryption Applications," International Journal of Information Security and Privacy (IJISP), vol. 16, no. 1, pp. 1-23, 2022.
3. S. Purohit, V. Deshpande, and V. Ingale, "FPGA Implementation of the AES Algorithm with Lightweight LFSR-Based Approach and Optimized Key Expansion," in 2023 IEEE International Conference on Public Key Infrastructure and its Applications (PKIA), IEEE, pp. 1-7, September 2023.
4. E. S. Selvapriya and L. Suganthi, "Design and implementation of low power Advanced Encryption Standard cryptocore utilizing dynamic pipelined asynchronous model," Integration, vol. 93, p. 102057, 2023.
5. Y. Sha, J. Mou, S. Banerjee, and Y. Zhang, "Exploiting flexible and secure cryptographic technique for multi-dimensional image based on graph data structure and three-input majority gate," IEEE Transactions on Industrial Informatics, 2023.
6. M. M. Shri et al., "VLSI Architectures for Security Analysis with Dual- Key LFSR Using Barrel Shifter and S-Box," in 2023 International Conference on Recent Advances in Electrical, Electronics, Ubiquitous Communication, and Computational Intelligence (RAEEUCCI), IEEE, pp. 1-5, April 2023.
7. R. Swann and J. Stine, "Evaluation of a Modular Approach to AES Hardware Architecture and Optimization," Journal of Signal Processing Systems, vol. 95, no. 7, pp. 797-813, 2023.
8. W. Tan, A. Wang, X. Zhang, Y. Lao, and K. K. Parhi, "High-speed VLSI architectures for modular polynomial multiplication via fast filtering and applications to lattice-based cryptography," IEEE Transactions on Computers, 2023.
9. P. Mahajan and A. Sachdeva, "A study of encryption algorithms AES, DES and RSA for security," Global Journal of Computer Science and Technology, vol. 13, no. 15, pp. 15-22, 2013.
10. M. Abdullah, "Advanced encryption standard (AES) algorithm to encrypt and decrypt data," Cryptography and Network Security, vol. 16, no. 1, pp. 11, 2017.
11.

References:-

1. N. Cecchinato, A. Toma, C. Drioli, G. Oliva, G. Sechi, and G. L. Foresti, "Secure real-time multimedia data transmission from low-cost UAVs with a lightweight AES encryption," IEEE Communications Magazine, vol. 61, no. 5, pp. 160-165, 2023.
2. S. Di Matteo, M. L. Gerfo, and S. Saponara, "VLSI Design and FPGA implementation of an NTT hardware accelerator for Homomorphic seal- embedded library," IEEE Access, 2023.
3. T. Hasija, A. Kaur, K. R. Ramkumar, S. Sharma, S. Mittal, and B. Singh, "A survey on performance analysis of different architectures of AES algorithm on FPGA," in Modern Electronics Devices and Communication Systems: Select Proceedings of MEDCOM 2021, pp. 39-54, 2023.
4. J. Kala, J. Panda, and L. Tanwar, "FPGA Implementation Of a High Throughput Low Power Advanced Encryption Standard (AES-128) Cipher," in 2023 10th International Conference on Signal Processing and Integrated Networks (SPIN), IEEE, pp. 367-372, March 2023.

5. K. J. Lakshmi, G. Susi, K. Ravali, K. Ramyakrishna, and D. S. Teja, "A Novel VLSI Architecture for Encryption for Wireless Body Sensor Networks."
6. K. Li, H. Li, and G. Mund, "A reconfigurable and compact subpipelined architecture for AES encryption and decryption," EURASIP Journal on Advances in Signal Processing, vol. 2023, no. 1, p. 5, 2023.
7. M. Marimuthu et al., "Implementation of VLSI on Signal Processing- Based Digital Architecture Using AES Algorithm," Computers, Materi- als & Continua, vol. 74, no. 3, 2023.