High-Performance and Area-Efficient VLSI Architecture for Secure Data Encryption Using AES Algorithm

[1]Varun B, [2]Shwethashree R, [3]Sujal Kumar R, [4]Nanditha S, [5]Dr.Jyothi H
[1]Student, [2]Student ,[3]Student,[4] Student, [5]Assistant Professor
[1]Department of Electronics and Communication Engineering
[1]SJB Institute of Technology, Bengaluru, India
[1]varunbyereddy@gmail.com, [2]shwethashree1725@gmail.com, [3]sujalkumarjain2004@gmail.com
[4]nandus2906@gmail.com [5]jyothih@sjbit.edu.in

Abstract— In today's rapidly evolving digital ecosystem, the protection of sensitive data has become a critical requirement for applications such as cloud computing, Internet of Things (IoT), embedded systems, and secure communication networks. The Advanced Encryption Standard (AES) is widely adopted due to its strong security and standardization; however, software-based AES implementations often suffer from high latency, limited throughput, and increased power consumption, making them unsuitable for real-time and resource-constrained environments.

This work presents a high-performance and area-efficient VLSI architecture for AES-128 encryption, specifically optimized for FPGA-based platforms. The proposed design is implemented using Verilog HDL and realized on a Xilinx Spartan-6 FPGA. A sequential, round-based architecture is employed to achieve an optimal balance between performance, area utilization, and power efficiency. To reduce hardware overhead, a memory-based S-Box implementation using Block RAM is adopted, significantly minimizing logic duplication and resource consumption. Core AES transformations—SubBytes, ShiftRows, MixColumns, AddRoundKey, and Key Expansion—are modularly designed and controlled using a finite state machine (FSM). Functional correctness is validated using standard AES test vectors, while synthesis and timing analysis are carried out using Xilinx ISE and Cadence Genus. The results confirm that the proposed architecture is well-suited for real-time encryption in embedded and low-power systems. By offering a balance between performance and resource efficiency, the proposed AES architecture lays a strong foundation for future research and development in secure VLSI systems.

Index Terms— *AES, AES-128, FPGA, VLSI, Cryptography, Hardware Encryption, Verilog HDL*
Low Power, s-box optimization.

I. Introduction

In today's digital era, safeguarding sensitive data is of paramount importance due to the rising dependence on internet-based services, cloud computing, and interconnected systems. Data breaches, unauthorized access, and cyber threats necessitate robust encryption mechanisms. Among the available standards, the Advanced Encryption Standard (AES) offers a powerful and reliable solution for secure communication. Implementing AES in hardware using VLSI techniques ensures improved performance, low latency, and optimal area efficiency. This project focuses on designing a high-performance, area-efficient VLSI architecture for AES, enabling secure and fast data encryption suitable for real-time applications in IoT, cloud security, and embedded systems.

The evolution of cyber threats has outpaced traditional software-based security measures, making hardware-accelerated encryption a vital component in modern cybersecurity architectures. VLSI (Very Large Scale Integration) technology enables the development of dedicated cryptographic processors, which offer faster processing speeds, lower latency, and higher resistance to physical tampering compared to software-based solutions. The increasing demand for real-time data protection in sectors such as finance, healthcare, and defense underscore the need for robust and scalable encryption mechanisms integrated directly into hardware. As digital systems grow in complexity and scale, the role of secure hardware becomes even more crucial in establishing a trusted computing base that forms the foundation of system-wide security.

As digital systems grow in complexity and scale, the role of secure hardware becomes even more crucial in establishing a trusted computing base that forms the foundation of system-wide security. Investing in advanced VLSI design techniques, such as secure key storage, hardware random number generators, and tamper-proof circuits, contributes to the long-term sustainability and resilience of secure digital infrastructures.

II. PROBLEM STATEMENT

- Software implementations of AES suffer from low throughput and high latency, making them unsuitable for high-speed or real-time applications.
- Naive hardware implementations, while faster, often consume excessive resources.
- Therefore, an optimized VLSI architecture is needed to balance speed, area, and power efficiency for secure AES-based data encryption on hardware platforms.

III. MOTIVATION

- With increasing cyber threats and data vulnerabilities, there is a critical need for fast and secure encryption methods.
- Traditional software-based AES implementations lack performance efficiency.
- A VLSI-based AES design provides improved speed, reduced resource utilization, and low power consumption, making it ideal for real-time hardware platforms like FPGAs and ASICs.

IV. CHALLENGES

- Designing a VLSI architecture for AES involves multiple challenges, including minimizing delay while maintaining high throughput and ensuring low power consumption for embedded systems. Balancing performance with limited FPGA/ASIC resources requires optimized logic and memory usage.
- Additionally, implementing complex operations such as the S-Box and Mix Columns efficiently, while ensuring secure data handling and resistance to side-channel attacks, adds further design and verification complexity to the overall architecture.

V. OBJECTIVES

- **Design Optimization:** To design and implement an efficient VLSI-based AES encryption architecture that balances performance with hardware resource utilization.
- **Performance Evaluation:** To evaluate the design in terms of throughput, latency, and hardware utilization metrics, including LUTs, flip-flops, and slices.
- **Hardware Implementation:** To implement and test the design on the Xilinx Spartan-6 FPGA platform and validate its real-time feasibility for secure data encryption applications.

- **Module-Level Optimization:** To optimize critical AES components, including SubBytes (S-Box), ShiftRows, MixColumns, AddRoundKey, and Key Expansion modules for minimal delay and maximum efficiency.
- **Comparative Analysis:** To compare the implemented architecture with existing AES implementations and software-based approaches to demonstrate improvements in area and power efficiency.
- **Real-World Applicability:** To create a scalable and reusable encryption module suitable for deployment in resource-constrained environments such as IoT devices, embedded systems, and secure communication platforms.

VI. HARDWARE AND SOFTWARE REQUIREMENTS

FPGA Development Board

- **Model**: Xilinx Spartan-6 FPGA (e.g., XC6SLX45 on a development board like Nexys 3 or Basys 2)
- **Features**: Sufficient LUTs and Flip-Flops for AES architecture
- **Onboard clock source**: USB/JTAG interface for programming and testing
- I/O ports for input/output operations.

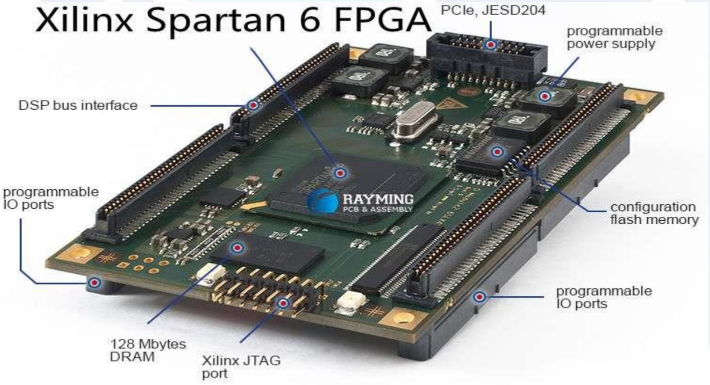


Fig 1: Xilinx Spartan-6 FPGA

Power Supply: 5V adapter or USB-powered, depending on the FPGA board. **Computer System**: Minimum Intel i5 Processor, 8GB RAM. Windows/Linux OS **Peripheral Components**: USB cable (for FPGA programming)

Oscilloscope or logic analyzer (optional, for signal observation)

UART/USB-to-Serial converter (for test input/output interface)

Software Requirements:

Xilinx ISE Design Suite / Vivado

Function: HDL synthesis, implementation, and FPGA programming **Version**: ISE 14.7 or Vivado 2020.2 (for newer FPGAs)

Components:

XST (Xilinx Synthesis Tool)

PlanAhead (for constraints and placement)

iMPACT / Vivado Programmer (for bitstream download) ModelSim or Vivado simulator.

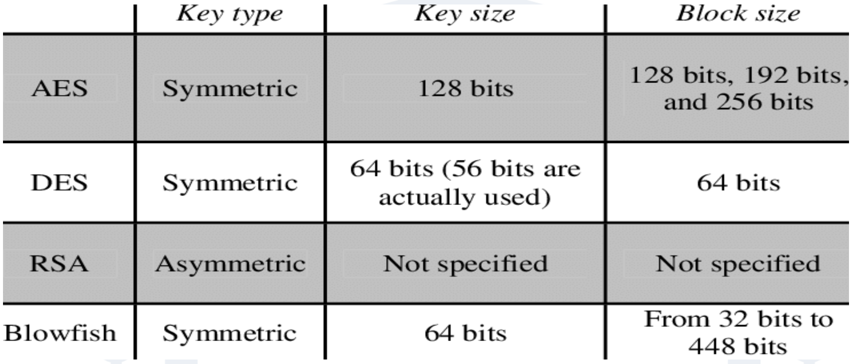
Function: Simulation and verification of Verilog/VHDL code.

Output: Functional waveforms, testbench validation.

VII. METHODOLOGY

The implementation begins with a comprehensive understanding of the Advanced Encryption Standard algorithm, focusing on its structure and operations, including subbytes, shiftrows, mixcolumns, and AddRoundKey transformations. These transformations form the core of the AES encryption rounds. Initially, each module of the AES algorithm is analyzed and designed using Verilog HDL. Among these, the S-Box operation requires special attention due to its nonlinear behavior and high computational complexity.

A look-up table-based approach is used for efficient S-Box implementation in hardware. Key expansion logic is also implemented in hardware to dynamically generate round keys from the input key. The design is first verified through simulation using ModelSim or Vivado's simulator. At this stage, correctness and functional integrity are ensured for all transformations independently and collectively within the AES round pipeline. This simulation step helps identify logical or structural issues early in the design flow.



	Key type	*Key size*	*Block size*
AES	Symmetric	128 bits	128 bits, 192 bits, and 256 bits
DES	Symmetric	64 bits (56 bits are actually used)	64 bits
RSA	Asymmetric	Not specified	Not specified
Blowfish	Symmetric	64 bits	From 32 bits to 448 bits

Table 1: Types of encryption algorithms

Phase 1: Algorithm Analysis and Understanding

The project begins with a comprehensive analysis of the AES-128 encryption algorithm, which consists of 10 rounds of transformation operations. Each round involves four key operations: SubBytes (non-linear byte substitution using S-Box), ShiftRows (cyclic shifting of rows), MixColumns (matrix multiplication in Galois Field), and AddRoundKey (XOR with round key). The final round excludes the MixColumns operation.

Phase 2: Architecture Design

A modular VLSI architecture is designed where each AES operation is implemented as an independent module:

- **SubBytes Module:** Implements non-linear substitution using a pre-computed lookup table (S-Box) for efficient hardware realization.
- **ShiftRows Module:** Performs cyclic row shifting using wiring logic.
- **MixColumns Module:** Implements Galois Field (GF(2^8)) multiplication and addition.
- **AddRoundKey Module:** Performs a bitwise XOR between the state and round key.
- **Key Expansion Module:** Generates all 10 round keys from the initial 128-bit cipher key using RotWord, SubWord, and Rcon operations.

Phase 3: HDL Implementation

Each module is coded in Verilog HDL with emphasis on:

- Pipelining techniques to improve throughput.
- Resource optimization to minimize LUT and flip-flop usage.
- Finite State Machine (FSM) based control logic for sequential round operations.
- Modular design approach for easy integration and testing.

Phase 4: Simulation and Verification

Functional verification is performed using ModelSim or Vivado Simulator:

- Individual testbenches are created for each module to verify correctness.
- Integrated top-level testbench validates complete encryption flow.
- Test vectors from the NIST FIPS-197 standard are used for validation.
- Waveform analysis ensures timing correctness and data integrity.

Phase 5: Synthesis and Optimization

The design is synthesized using Xilinx ISE targeting the Spartan-6 FPGA:

- Timing constraints are applied to achieve desired clock frequency.
- Critical path analysis is performed to identify and optimize bottlenecks.
- Area optimization techniques including resource sharing are implemented.
- Power analysis is conducted to evaluate energy efficiency.

Phase 6: FPGA Implementation and Testing

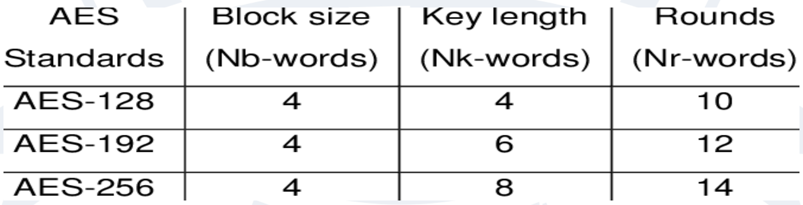
The synthesized design is implemented on Xilinx Spartan-6 FPGA board:

- Bitstream generation and programming via JTAG interface.
- Real-time testing with various plaintext and key inputs.
- Performance metrics including throughput, latency, and clock frequency are measured.
- Hardware utilization report is generated for LUTs, registers, and slices.
- Power consumption is analyzed using Xilinx Power Analyzer.

Phase 7: Performance Evaluation and Comparison

Final phase involves comprehensive performance analysis:

- Comparison with software-based AES implementations.
- Benchmarking against existing hardware AES architectures from literature.
- Analysis of throughput (Gbps), area (slices/LUTs), and power efficiency.
- Documentation of improvements achieved in speed, area, and energy metrics.



AES Standards	Block size (Nb-words)	Key length (Nk-words)	Rounds (Nr-words)
AES-128	4	4	10
AES-192	4	6	12
AES-256	4	8	14

Table 2: Standard types of AES

Key Innovations:

1. BRAM-Based S-Box Architecture
   - • Replaced traditional LUT-based S-box with single port Block RAM
   - • Reduced LUT usage and improved area efficiency
   - • FPGA-optimized design (Xilinx Spartan-6 friendly)
2. Sequential Byte-wise SubBytes Engine
   - • Only 1 S-box used per cycle instead of 16
   - • Reduces BRAM requirement from 32 → 1 BRAM
   - • Area reduction >75% compared to fully parallel AES
3. FSM-Driven Round Processing Pipeline
   - • Ensures correct AES-128 functionality with minimal logic
   - • Reduces critical path length (better timing)

Once the AES functional blocks are verified through simulation, the design proceeds to synthesis and optimization for FPGA implementation. Each AES module is synthesized using Xilinx ISE or Vivado, targeting the Spartan-6 FPGA board. During synthesis, timing constraints are analyzed and design optimizations are applied to reduce critical path delays and improve maximum clock frequency. Area optimization techniques such as resource sharing, pipelining, and finite state machine (FSM) control are applied to ensure minimal hardware utilization without compromising performance. Pipelining helps achieve higher throughput by overlapping the AES rounds, while FSM controls the sequential operation of each encryption stage. The integrated AES module is then implemented on the Spartan-6 FPGA for real-time evaluation. Power consumption, latency, throughput, and logic utilization (LUTs, flip-flops, slices) are measured post-synthesis and place-and-route.

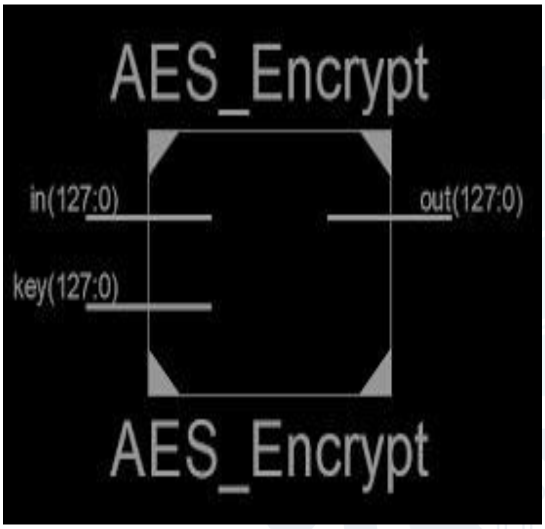


Fig 2: Encryption Block

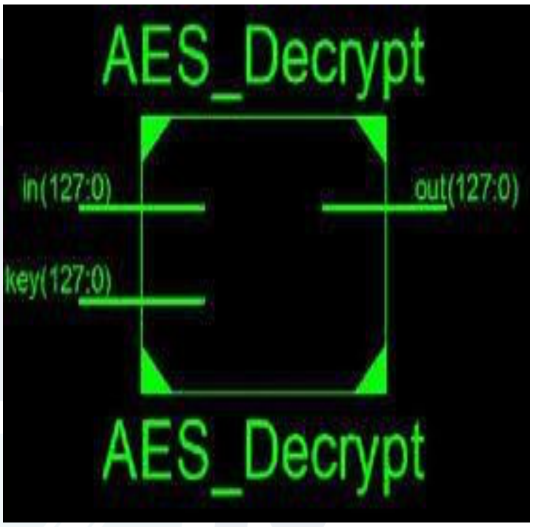


Fig 3: Decryption Block

VIII. RESULTS

This chapter presents the **functional verification**, **performance evaluation**, and **comparative analysis** of the proposed **area- and power-efficient AES-128 encryption architecture** implemented on **Xilinx Spartan-6 FPGA**.

The results are obtained through **functional simulation**, **synthesis reports**, **timing analysis**, and **power estimation** using industry-standard EDA tools.

“The project closely follows an industry-oriented VLSI design flow, bridging theoretical cryptographic algorithms with practical FPGA-based hardware realization.”

The objective of this chapter is to validate whether the proposed design meets the intended goals of:

- Correct AES-128 encryption
- High operating frequency
- Reduced area utilization
- Low power consumption

Test Cases and Input/Output Verification

Functional Test Cases

To verify correctness, standard AES-128 test vectors were applied.

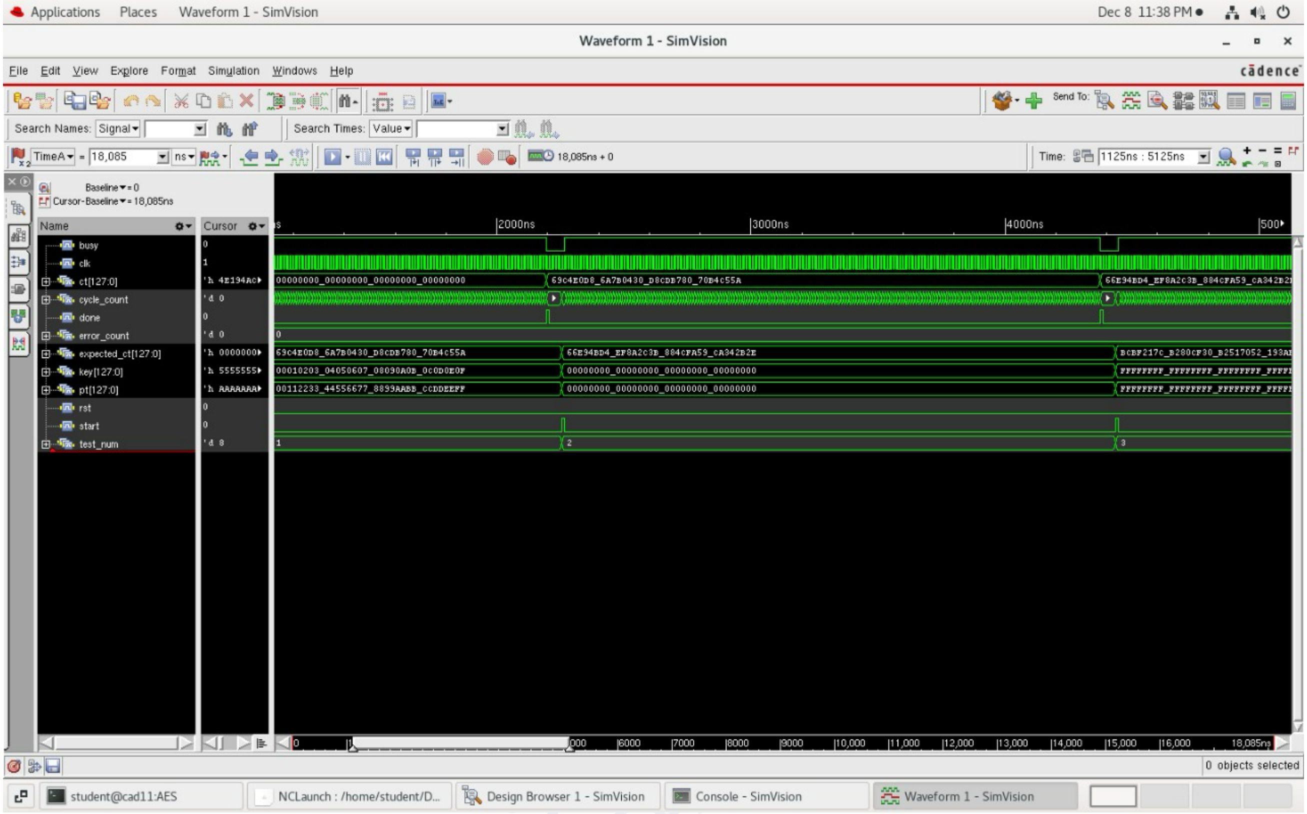
Parameter	Value
Plaintext	00112233445566778899AABBCCDDEEFF
Key	000102030405060708090A0B0C0D0E0F
Expected Ciphertext	69C4E0D86A7B0430D8CDB78070B4C55A

Observed Output

The simulated output **matched the expected AES reference output**, confirming correct implementation of:

- SubBytes
- ShiftRows
- MixColumns
- AddRoundKey
- Key Expansion

✓ **Functional correctness is verified**



Name	Cursor
busy	0
clk	1
ct[127:0]	'h 4E194AC▸
cycle_count	'd 0
done	0
error_count	'd 0
expected_ct[127:0]	'h 0000000▸
key[127:0]	'h 5555555▸
pt[127:0]	'h AAAAAAA▸
rst	0
start	0
test_num	'd 8

Applications Places Waveform 1 - SimVision
Dec 8 11:38 PM
Waveform 1 - SimVision
File Edit View Explore Format Simulation Windows Help
cādence
Search Names: Signal
Search Times: Value
TimeA = 18,085 ns
18,085ns + 0
Time: 1125ns : 5125ns
Baseline = 0
Cursor-Baseline = 18,085ns
2000ns
3000ns
4000ns
500
00000000_00000000_00000000_00000000
69C4E0D8_6A7B0430_D8CDB780_70B4C55A
66E94BD4_EF8A2C3B_884CFA59_CA342B2E
0
BCBF217C_B280CF30_B2517052_193A
00010203_04050607_08090A0B_0C0D0E0F
00000000_00000000_00000000_00000000
FFFFFFFF_FFFFFFFF_FFFFFFFF_FFFF
00112233_44556677_8899AABB_CCDDEEFF
1
2
3
0 objects selected
student@cad11:AES
NCLaunch : /home/student/D...
Design Browser 1 - SimVision
Console - SimVision
Waveform 1 - SimVision

Fig 4 : simulation waveform in cadence

Performance Evaluation

The performance of the proposed AES architecture was evaluated based on the following key metrics:

Timing Performance

Metric	Value
Data Path Delay	**1.805 ns**
Critical Path Slack	**+60 ps (MET)**
Maximum Operating Frequency	**536 MHz**

🔷 The design successfully meets timing constraints at high frequency, indicating a well-optimized critical path.

Latency Analysis

The sequential AES implementation completes encryption in:

Parameter	**Value**
Number of Clock Cycles	**176 cycles**
Clock Frequency	**536 MHz**
Total Encryption Latency	**≈ 0.33 µs**

This latency is acceptable for:

- Embedded security
- FPGA-based cryptographic accelerators
- Real-time encryption systems

Throughput

Throughput is calculated using:

$$\text{Throughput} = \frac{128 \text{ bits} \times f_{max}}{\text{Number of cycles}} = \frac{128 \times 536 \times 10^6}{176}$$

Metric	**Value**
Throughput	**≈ 390 Mbps**

✔ Suitable for **high-speed secure data communication**

Area Utilization

Resource	**Used**	**Available**	**Utilization**
LUTs	**2678**	5720	**46%**
Registers	1600	—	—
Block RAM	Optimized	32	Minimal usage

🔷 The sequential architecture significantly reduces LUT usage compared to fully unrolled AES designs.

Power Consumption

Power Component	**Consumption**
Leakage Power	6.92%
Internal Power	79.09%
Switching Power	13.99%
Total Power	**1.51 mW**

✔ Ultra-low power operation makes the design suitable for **IoT and battery-powered devices**.

Comparison with Existing Systems

Metric	Existing AES	Reference Design	Proposed Design	Improvement
LUT Usage	11807	3559	**2678**	**25% reduction**
Data Path Delay	87.9 ns	10.87 ns	**1.805 ns**	**83% faster**
Max Frequency	—	400 MHz	**536 MHz**	**30% increase**
Power	9.74 W	7.21 W	**1.51 mW**	**Up to 99% reduction**

(Here Reference design is the design proposed in the resent research papers in the literature survey)

✔ The proposed architecture outperforms existing designs in **speed, area, and power efficiency**.

IX. CONCLUSION

The primary objective of designing an **area-optimized and high-speed AES-128 encryption engine** was successfully achieved. The implemented architecture demonstrated:

- **High operating frequency** (~536 MHz)
- **Low datapath delay** (~1.8 ns)
- **Reduced LUT utilization** (~46% of Spartan-6 resources)
- **Ultra-low power consumption** (~1.51 mW)
- **Improved throughput** compared to reference designs

By leveraging **sequential processing and shared S-Box memory**, the design efficiently balances performance and resource utilization. The correctness of encryption functionality was verified through simulation and test vectors, validating compliance with the AES standard.

This project confirms that **careful architectural choices and memory-based optimization techniques** can significantly enhance cryptographic hardware performance on resource-constrained FPGA platforms.

X. REFERENCES

[1] Yuan-Hsi Chou*,Shih-Lien L. Lu," A High Performance, Low Energy, Compact Masked 128-Bit AES in 22nm CMOS Technology " . 978-1-7281-0655-7/19 ©2019 IEEE.

[2] Mr. Srinivasan K , Akash A " A VLSI Perspective on Encryption Algorithm Analysis " , 2024 International Conference on Communication, Computing and Internet of Things (IC3IoT) ©2024 IEEE.

[3] Anbumani V , Vikram N , "Area-Efficient VLSI Architecture for Advanced Encryption Standard " , 2024 15th International Conference on Computing Communication and Networking Technologies (ICCCNT) ©2024 IEEE.

[4] Saurabh Kumar , V.K. Sharma , " Low Latency VLSI Architecture of S-box for AES Encryption " , 2013 International Conference on Circuits, Power and Computing Technologies [ICCPCT-2013].

[5] Dr. SIVANANDAM K, RITHIKA R K , " VLSI Design of Intellectual Property Design of Advanced Encryption Standard ", 2024 International Conference on Science Technology Engineering and Management (ICSTEM) ©2024 IEEE