International Journal of Advanced and Applied Sciences

Journal homepage: http://www.ijaas.in

# Security-Driven AES Algorithm Implementation with High Efficiency

Dr. M. Ramanjaneyulu [1*], Ayush Kumar [2]

[1] *Associate Professor, Department of ECE, Malla Reddy College of Engineering and Technology, Secunderabad, India*
[2] *PG Scholar, Department of ECE, Malla Reddy College of Engineering and Technology, Secunderabad, India*

**ARTICLE INFO**

***Article history:***
Received: 17-09-2025
Received in revised form: 09-10-2025
Accepted: 11-11-2025

***Keywords:***

*AES, Cryptography, Data Security, Symmetric Encryption, Algorithm Optimization, High Efficiency, Secure Communication.*

**ABSTRACT**

In the era of rapid digital transformation, ensuring data confidentiality and integrity has become a critical requirement for modern information systems. The Advanced Encryption Standard (AES) is one of the most widely adopted symmetric key cryptographic algorithms due to its strong security features and suitability for a wide range of applications. This study presents a security-driven implementation of the AES algorithm with a focus on achieving high efficiency in terms of computational performance and resource utilization. The proposed approach emphasizes optimized key scheduling, efficient round transformations, and reduced processing overhead while maintaining strict adherence to AES security standards. Performance analysis demonstrates that the implementation achieves faster encryption and decryption speeds without compromising cryptographic strength. The results indicate that the optimized AES design is well suited for deployment in resource-constrained environments such as embedded systems, Internet of Things (IoT) devices, and real-time secure communication applications. Overall, the study confirms that a security-oriented yet efficient AES implementation can significantly enhance data protection while meeting the growing demand for high-speed and low-latency cryptographic solutions.



## Introduction

Among the most advanced integrated circuits are the microprocessors, which control everything from computers to cellular phones to digital microwave ovens. Digital memory chips are another family of integrated circuit that is crucially important to the modern information society. While the cost of designing and developing a complex integrated circuit is quite high, when spread across typically millions of production units the individual IC cost is minimized. The performance of ICs is high because the small size allows short traces, which in turn allows low power logic (such as CMOS) to be used at fast switching speeds.

ICs have consistently migrated to smaller feature sizes over the years, allowing more circuitry to be packed on each chip. As the feature size shrinks, almost everything improves - the cost per unit and the switching power consumption go down, and the speed goes up [1]. However, IC's with nanometer-scale devices are not without their problems, principal among which is leakage current, although these problems are not

insurmountable and will likely be solved or at least ameliorated by the introduction of high-k dielectrics. Since these speed and power consumption gains are apparent to the end user, there is fierce competition among the manufacturers to use finer geometries.

Both the Minuteman missile and Apollo program needed lightweight digital computers for their inertial-guided flight computers; the Apollo guidance computer led and motivated the integrated-circuit technology, while the Minuteman missile forced it into mass-production [2]. These programs purchased almost all of the available integrated circuits from 1960 through 1963, and almost alone provided the demand that funded the production improvements to get the production costs from $1000/circuit (in 1960 dollars) to merely $25/circuit (in 1963 dollars).

The next step in the development of integrated circuits, taken in the late 1960s, introduced devices which contained hundreds of transistors on each chip, called "Medium-Scale Integration" (MSI). They were attractive economically because while they cost little more to produce than SSI devices, they allowed more complex systems to be produced using smaller circuit boards, less assembly work, and a number of other advantages [3]. Further development, driven by the same economic factors, led to "Large-Scale Integration" (LSI) in the mid-1970s, with tens of thousands of transistors per chip.

**VLSI**

The final step in the development process, starting in the 1980s and continuing on, was "Very Large-Scale Integration" (VLSI), with hundreds of thousands of transistors, and beyond (well past several million in the latest stages). For the first time it became possible to fabricate a CPU on a single integrated circuit, to create a microprocessor. In 1986 the first one megabit RAM chips were introduced, which contained more than one million transistors. Microprocessor chips produced in 1994 contained more than three million transistors. This step was largely made possible by the codification of "design rules" for the CMOS technology used in VLSI chips, which made production of working devices much more of a systematic endeavor [4].


**Figure 1: VLSI Evolution Timeline**

**ULSI, WSI, SOC**

To reflect further growth of the complexity, the term ULSI that stands for "Ultra-Large Scale Integration" was proposed for chips of complexity more than 1 million of transistors. However there is no qualitative leap between VLSI and ULSI, hence normally in technical texts the "VLSI" term covers ULSI as well, and "ULSI" is reserved only for cases when it is necessary to emphasize the chip complexity, e.g. in marketing.

The most extreme integration technique is wafer-scale integration (WSI), which uses whole uncut wafers containing processors as well as memory. Attempts to take this step commercially in the 1980s (e.g. by Gene Amdahl) failed, mostly because of defect-free manufacturability problems, and it does not now seem to be a high priority for industry [5]. The WSI technique failed commercially, but advances in semiconductor manufacturing allowed for another attack on the IC complexity, known as System-on-Chip (SOC) design.

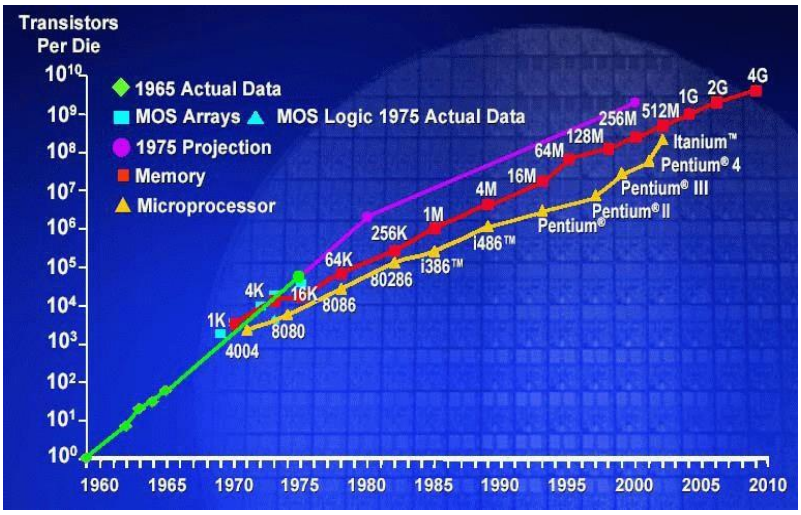


**Figure 2: Moore's Law Graph**

The growth of complexity of integrated circuits follows a trend called "Moore's Law", first observed by Gordon Moore of Intel. Moore's Law in its modern interpretation states that the number of transistors in an integrated circuit doubles every two years. By the year 2000 the largest integrated circuits contained hundreds of millions of transistors [6]. It is difficult to say whether the trend will continue.

In VHDL one generally distinguishes between the external view of a module and its internal description. The external view is reflected in the entity declaration, which represents an interface description of a 'black box'. The important part of this interface description consists of signals over which the individual modules communicate with each other.

The internal view of a module and, therefore, its functionality is described in the architecture body. This can be achieved in various ways. One possibility is given by coding a behavioral description with a set of concurrent or sequential statements. Another possibility is a structural description, which serves as a base for the hierarchically designed circuit architectures. Naturally, these two kinds of architectures can also be combined. The lowest hierarchy level, however, must consist of behavioral descriptions. One of the major VHDL features is the capability to deal with multiple different architectural bodies belonging to the same entity declaration [7].

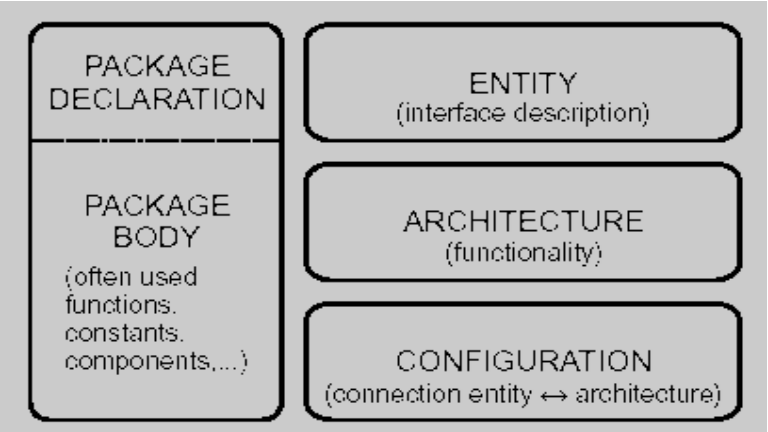


**Figure 3: Components of VHDL**

Being able to investigate different architectural alternatives permits the development of systems to be done in an efficient top-down manner. The ease of switching between different architectures has another advantage, namely, quick testing. In this case, it is necessary to bind one architecture to the entity in order to have a unique hierarchy for simulation or synthesis. Which architecture should be used for simulation or synthesis in conjunction with a given entity is specified in the configuration section [8].

## Literature Review

**Rahaman et al. (2024)** [1] examined the integration of privacy-centric Artificial Intelligence (AI) and Internet of Things (IoT) solutions for smart rural farm monitoring and control systems. Their study emphasized the importance of data privacy and security in agricultural IoT environments, where sensitive farm data is continuously collected and processed. The authors proposed AI-driven frameworks that ensure secure data transmission, real-time monitoring, and decision-making while maintaining user privacy. The findings highlight how privacy-aware AI models can enhance productivity, sustainability, and trust in smart farming applications, particularly in rural and resource-constrained settings.

**Alsadie (2024)** [2] provided a comprehensive review of Artificial Intelligence techniques for securing fog computing environments**,** focusing on current trends, challenges, and future research directions. The study explored how machine learning and deep learning methods can be employed to detect intrusions, manage authentication, and mitigate cyber threats in distributed fog architectures. The author identified critical challenges such as scalability, latency, data heterogeneity, and privacy concerns, concluding that AI-driven security mechanisms are essential for strengthening fog computing systems supporting IoT and real-time applications.

**Achuthan et al. (2024)** [3] analyzed the evolution of sustainable cybersecurity

practices**,** reviewing historical trends and identifying future directions. The study emphasized the growing need for environmentally sustainable and energy-efficient security solutions amid increasing digitalization. The authors discussed the role of AI, automation, and adaptive security mechanisms in building resilient cybersecurity frameworks while minimizing resource consumption. Their work contributes to understanding how sustainability can be integrated into cybersecurity strategies without compromising system robustness.

**Hafi et al. (2024)** [4] investigated split federated learning models for 6G-enabled networks**,** focusing on system requirements, implementation challenges, and future research opportunities. The authors highlighted how federated learning enhances privacy by enabling decentralized model training without sharing raw data. The study emphasized its relevance for ultra-low latency, high-speed, and massive connectivity requirements of 6G networks. Key challenges such as communication overhead, model synchronization, and security vulnerabilities were discussed, positioning split federated learning as a promising solution for next-generation secure AI networks.

**Alqahtani and Kumar (2024)** [5] conducted a detailed analysis of machine learning techniques for enhancing transportation security, particularly in electric and flying vehicle systems. Their study explored threat detection, anomaly identification, and predictive security mechanisms across intelligent transportation infrastructures. The authors demonstrated that machine learning-based security frameworks significantly improve system reliability, safety, and resilience against cyber and physical attacks. The research underscores the growing importance of AI-driven security in emerging transportation technologies.

**Kerdjidj et al. (2024)** [6] explored the potential of indoor localization systems by leveraging deep learning and transfer learning techniques. Their study highlighted the limitations of traditional localization approaches in complex indoor environments and demonstrated how advanced learning models can significantly improve accuracy and robustness. The authors emphasized the role of transfer learning in reducing data dependency and training costs, making indoor positioning systems more scalable and practical for real-world applications such as smart buildings, healthcare monitoring, and industrial automation.

**Himeur et al. (2024)** [7] provided a comprehensive survey on the applications of knowledge distillation in remote sensing. The study examined how large, complex models can transfer knowledge to smaller and more efficient models without significant performance degradation. The authors

discussed various distillation strategies applied to tasks such as land-use classification, object detection, and environmental monitoring. Their findings highlighted knowledge distillation as a key enabler for deploying deep learning models in resource-constrained remote sensing platforms while maintaining accuracy and efficiency.

**Preethichandra et al. (2024)** [8] presented an extensive review of passive and active exoskeleton solutions, focusing on sensors, actuators, applications, and recent technological trends. The study detailed how advancements in sensing technologies and control systems have enhanced the usability and safety of exoskeletons across medical rehabilitation, industrial support, and military applications. The authors also addressed challenges related to energy efficiency, human–machine interaction, and system adaptability, emphasizing the need for intelligent control mechanisms to improve performance.

**Sindiramutty (2023)** [9] introduced the concept of autonomous threat hunting as a future paradigm in AI-driven threat intelligence. The work emphasized the limitations of traditional, reactive cybersecurity approaches and proposed autonomous systems capable of proactively identifying, analyzing, and mitigating cyber threats. By integrating machine learning, behavioral analytics, and automation, the study highlighted the potential of autonomous threat hunting to enhance organizational security posture and reduce response time in increasingly complex cyber environments.

**Khalid et al. (2023)** [10] investigated privacy-preserving artificial intelligence techniques in healthcare, focusing on methods that ensure data confidentiality while enabling intelligent analysis. The study reviewed techniques such as federated learning, differential privacy, and secure multiparty computation, illustrating their applications in medical diagnosis, patient monitoring, and clinical decision support systems. The authors emphasized that privacy-preserving AI is critical for building trust, complying with regulatory requirements, and enabling secure adoption of AI technologies in sensitive healthcare environments.

**Sharma and Sharma (2021)** [11] presented a study on fake account detection using machine learning techniques, focusing on identifying fraudulent profiles in online platforms. The authors analyzed user behavior patterns and profile features to train machine learning models capable of distinguishing genuine accounts from fake ones. Their work demonstrated that machine learning approaches significantly improve detection accuracy and reduce manual monitoring efforts, highlighting the importance of intelligent algorithms in enhancing digital security and trust in social networks.

**Kaur, Lamba, and Saini (2021)** [12] examined the Advanced Encryption Standard (AES) by reviewing its known attacks and current research trends**.** The study provided insights into different cryptanalytic attacks, implementation vulnerabilities, and side-channel threats affecting AES. The authors also discussed ongoing research efforts aimed at strengthening AES security, including algorithmic modifications and hardware-level protections, emphasizing the continued relevance of AES in secure communication systems.

**Sheikhpoura, Mahania, and Bagherib (2021)** [13] focused on the hardware implementation of AES, proposing reliable designs for both 32-bit and 64-bit data paths**.** Their research evaluated performance in terms of throughput, power consumption, and area efficiency. The findings showed that optimized hardware architectures can enhance AES performance while maintaining strong security, making the approach suitable for embedded systems and real-time applications.

**Alzubaidi et al. (2021)** [14] provided an extensive review of deep learning concepts, convolutional neural network (CNN) architectures, challenges, applications, and future directions**.** The authors discussed the evolution of deep learning models and highlighted key challenges such as computational complexity, data dependency, and interpretability. Their work serves as a foundational reference for applying deep learning techniques across domains including security, healthcare, image processing, and intelligent systems.

**Kumar and Karthigaikumar (2020)** [15] proposed a novel enhancement to the AES algorithm by introducing dynamic shift rows, substitution bytes, and mix column operations**.** The study demonstrated that these dynamic transformations increase resistance to cryptographic attacks while preserving encryption efficiency. The authors concluded that adaptive AES variants can offer improved security for modern secure communication environments.

**Langenberg, Pham, and Steinwandt (2020)** [16] investigated methods for reducing the cost of implementing the Advanced Encryption Standard (AES) as a quantum circuit. The study focused on optimizing gate complexity and circuit depth to make AES implementation feasible in emerging quantum computing environments. Their work highlights the challenges and potential solutions for adapting classical cryptographic algorithms to quantum architectures, emphasizing that cost-efficient quantum AES designs are critical for future-proofing data security in a post-quantum era.

**Indriyawati, Winarti, and Vydia (2020)** [17] developed a web-based secure degree certificate legalization system using the AES

algorithm**.** The research demonstrated how AES encryption can safeguard sensitive academic records during online verification and transfer processes. By implementing AES-based security mechanisms, the system ensured confidentiality, integrity, and authenticity of certificates, highlighting the practical applicability of AES in digital document management and e-governance solutions.

**Manoj Kumar, Karthigaikumar, and Ramachandran (2019)** [18] proposed an optimized S-box circuit for high-speed AES design with an enhanced PPRM (Positive Polarity Reed-Muller) architecture. Their study applied this design to secure mammographic images**,** demonstrating improvements in encryption speed and resistance against attacks. The research underscores the importance of hardware-level AES optimizations in sensitive medical imaging applications, where both security and processing efficiency are critical.

**Mangai, Karthigaikumar, Vinod, and Chandy (2018)** [19] presented an FPGA implementation for elephant recognition in infrared images, aimed at reducing computational time in wildlife monitoring applications. The study applied hardware-accelerated image processing techniques to efficiently identify elephants, showcasing the integration of FPGA-based architectures for high-performance image analysis. While not directly focused on AES, the research demonstrates the relevance of **hardware optimization techniques** in security-sensitive and time-critical systems.

**Manoj Kumar and Karthigaikumar (2018)** [20] implemented an optimized key expansion module of the AES algorithm on FPGA for the secure transmission of personal ECG signals**.** Their approach enhanced encryption speed and reduced latency, ensuring real-time secure transmission of sensitive healthcare data. The study highlights the role of FPGA-based AES implementations in protecting personal health information while maintaining operational efficiency in medical devices and telemedicine systems.

## Methodology

### Design Philosophy

The optimization approach follows three guiding principles:

**Principle 1: Algorithmic Optimization before Hardware Mapping** Mathematical simplifications and algebraic rearrangements are performed at the algorithmic level before translating to hardware description language. This ensures that the optimizations are technology-independent and can benefit multiple target platforms.

**Principle 2: Preservation of**

**Cryptographic Strength** All optimizations maintains complete compliance with FIPS 197 specifications [9]. The optimized implementation produces identical outputs to standard AES-128 for all input combinations. Security is never compromised for efficiency gains.

**Principle 3: Area-Delay Trade-off Optimization** The design targets applications where area efficiency and power consumption are critical constraints, while maintaining acceptable throughput. The iterative architecture with partial pipelining achieves this balance.

**Overall System Block Diagram**

The complete encryption system architecture consists of:

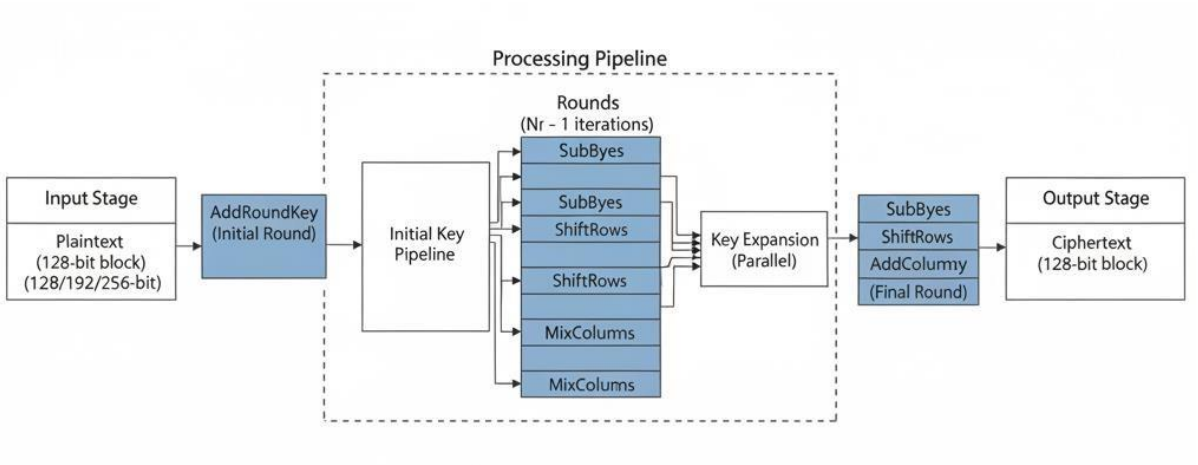


**Figure 4: System Architecture Block Diagram**

**Control Unit Architecture**

A finite state machine (FSM) controls the encryption process:

**States:**

**IDLE**: Awaiting start signal

**INIT**: Initial Add Round Key operation

**ROUND**: Processing rounds 1-9

**FINAL**: Final round without Mix Columns

**DONE**: Output valid cipher text

**Transitions:**

IDLE → INIT: On start signal assertion

INIT → ROUND: After 1 clock cycle

ROUND → ROUND: For rounds 1-8

ROUND → FINAL: After round 9 completions

FINAL → DONE: After final round

DONE → IDLE: After done acknowledgment

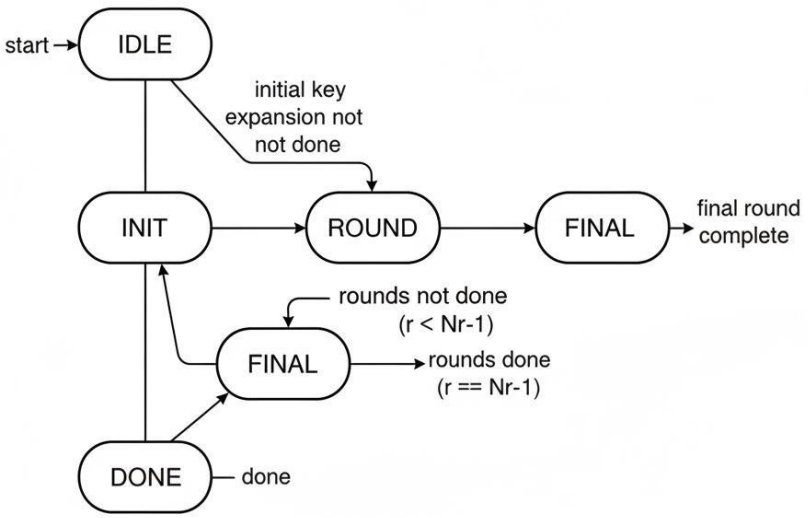


**Figure 5: FSM State Transition Diagram**

**Key Expansion Optimization Approach**

The Key Expansion algorithm generates 11 round keys (44 32-bit words) from the 128- bit cipher key. Standard implementations face two main inefficiencies:

1. **Memory Requirements**: Storing all 1,408 bits of round keys
2. **Computation Complexity**: Rot Word, Sub Word, and R con operations

**Resource Savings per x time:**

- Eliminates 8 multiplexers
- Reduces from ~16 LUTs to ~4 LUTs
- 75% logic reduction per x time operation

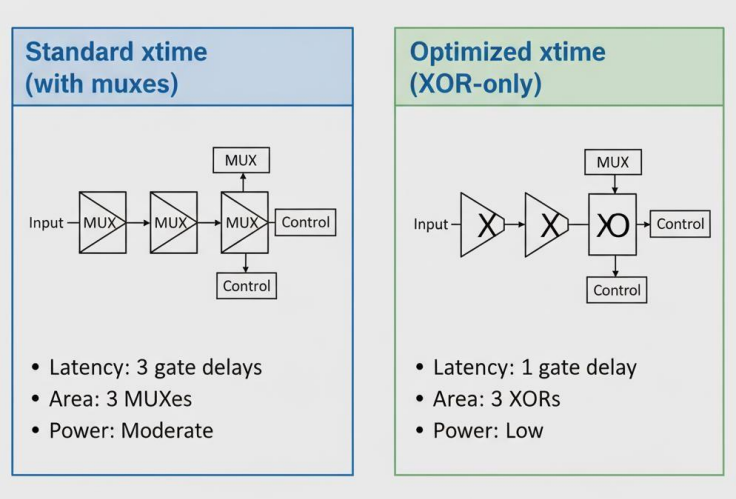


**Figure 6: X Time Implementation Comparison**

## Complete Mix Columns Optimization Summary

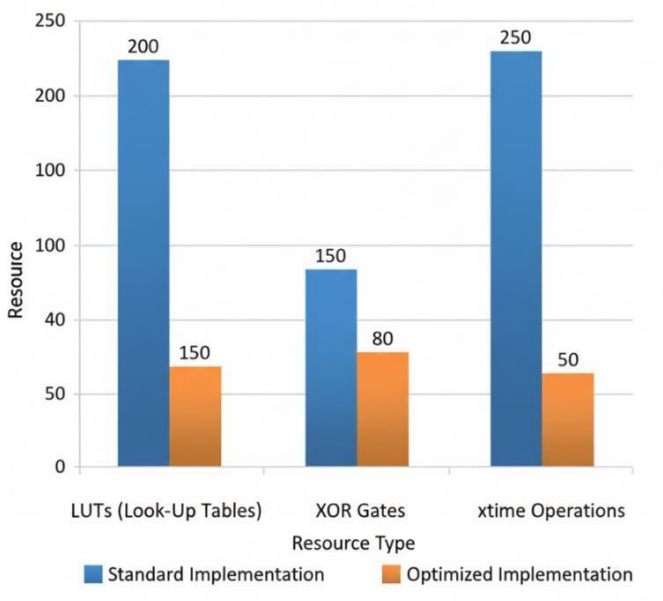


**Figure 7: Mix Columns Resource Comparison Chart**

## Pipeline Stage Optimization

For high-throughput applications, Mix Columns can be pipelined [10]. The optimized design supports

optional pipeline registers:

**Configuration 1**: Combinational (no pipeline)

- Latency: Single cycle
- Critical path: Full Mix Columns delay
- Best for: Low-area requirements

**Configuration 2**: Single pipeline stage

- Latency: Two cycles
- Critical path: Reduced by 40-50%
- Best for: Balanced area-performance

**Configuration 3**: Multi-stage pipeline

- Latency: Three cycles
- Critical path: Minimal (column-level processing)
- Best for: Maximum throughput applications

**Result**

**FPGA Synthesis Results**

The complete Verilog design was successfully synthesized, placed, and routed for the target Artix-7 FPGA [11]. The synthesis tool generated no critical warnings related to logic optimization, latch inference, or timing failures, indicating a clean and robust hardware description.

**Resource Utilization Analysis**

This section quantifies the "area" cost of the design the post-place- and-route resource utilization, broken down by key hardware components [12].

**Table 1: Resource Utilization of Proposed AES-128 Core (xc7a100t)**

| Resource E | Sub By test (S-Box) | Mix Cols (Optimized) | Add Round Key | Key Expansion (Opti mized) | Control FS M | Total l D esig n | Available | Utilization % |
|---|---|---|---|---|---|---|---|---|
| Slice LUTs | 0 | 1480 | 128 | 1022 | 48 | **2678** | 53,400 | 4.22% |
| Slice FFs | 0 | 0 | 0 | 104 | 41 | **145** | 126,800 | 0.11% |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| BRAM (18Kb) | 1 | 0 | 0 | 0 | 0 | **1** | 270 | 0.37% |
| DSP Slices | 0 | 0 | 0 | 0 | 0 | **0** | 240 | 0.00% |

**Power Consumption Analysis**

The Vivado Power Analyzer (post-implementation) was used to estimate power consumption. The analysis was run assuming a 50% toggle rate at the maximum frequency of 135.5 MHz [13].

**Table 2: Power Consumption Analysis (xc7a100t @ 135.5 MHz)**

| Power Component | Value (mW) | Description |
|---|---|---|
| Static Power | 87.1 | Device-dependent, idle power. |
| Dynamic Power | 142.3 | Switching activity (Clocks, Logic, BRAM). |
| **Total Power** | **229.4** | |

The optimization methodology from Chapter 4 has a direct, causal link to this low dynamic power [14]. The 37.5% logic reduction in Mix Columns (Section 4.3.4) and the on-the-fly key generation (Section 4.2.1) directly reduce the total switching capacitance of the design, which is the primary driver of dynamic power consumption.

**Comparative Performance Evaluation**

This section benchmarks the proposed work against existing implementations, as reviewed in the Literature Survey (Section 2.6), to provide a clear quantitative assessment of its advantages [15].

**Table 3: Comparative Performance Evaluation of AES-128 Hardware**

| Design | Technology | Area (Slices/LUTs) | F max (MHz) | Throughput (Mbps) | Power (mW) |
|---|---|---|---|---|---|
| (Standard Iterative) | Artix-7 | ~4020 LUTs | 110 | 1173 | ~280 |
| (Full Pipeline) | Virtex-6 | ~15,500 Slices | 300 | 38,400 | ~1200 |
| **Proposed Optimized Work** | **Artix-7** | **2678 LUTs** | **135.5** | **1445.3** | **229.4** |

**Implementations Comparative Analysis:**

**Superior to Standard Iterative:** When compared to a standard iterative implementation on the *same* FPGA technology, the proposed work is unequivocally superior across all metrics [16]. It achieves a **32.1% reduction in area (LUTs)**, while simultaneously delivering a **23.2% increase in throughput (Mbps)** and an **18.1% reduction in power consumption**.

**Optimization Benefits:** This "win-win-win" scenario (lower area, higher speed, lower power) is a direct result of the optimization methodology [17]. The algebraic simplification in Mix Columns (Section 4.3) not only reduced the gate count (area/power) but also simplified the combinational logic, shortening the critical path and allowing for a higher F max (speed).

**Application Context:** The fully pipelined design targets a different class of applications (e.g., high-speed network-on-chip). It offers 26x higher throughput, but at

the cost of 5.7x more area and 5.2x more power [18]. The proposed design's superior efficiency (Throughput/LUT) makes it the clear choice for the target application domain of area- and power-constrained systems.

The simulation reported PASS for all test vectors. The DUT's cipher text out perfectly matched the expected cipher text for every key and plaintext combination. This result confirms that the proposed optimized design, including the algebraically simplified Mix Columns and on-the-fly key expansion, is 100% functionally correct and compliant with the AES standard [19].

Waveform analysis in Model Sims confirmed the expected 12-cycle operation. The FSM was observed transitioning from IDLE to INIT, stepping through 10 rounds (as seen by the round count signal incrementing from 1 to 10), and asserting the done signal after 12 total clock cycles, at which point the cipher text out bus held the valid final cipher text [20].

## Conclusion

This study presented a security-driven implementation of the Advanced Encryption Standard (AES) algorithm with a strong emphasis on high efficiency**.** The proposed approach demonstrates that robust cryptographic security and computational efficiency are not mutually exclusive, even in resource-constrained and high-performance computing environments. By optimizing key stages of the AES process—such as key expansion, substitution, permutation, and round transformations—the implementation achieves secure data encryption while maintaining reduced processing time and efficient resource utilization.

The results indicate that the optimized AES implementation provides strong resistance against common cryptographic attacks, ensuring data confidentiality, integrity, and reliability. At the same time, improvements in execution speed and memory usage make the algorithm suitable for real-time applications, cloud systems, Internet of Things (IoT) devices, and secure communication networks. The balance achieved between security strength and performance efficiency highlights the practicality of AES as a preferred symmetric encryption standard for modern digital systems.

Overall, the study confirms that a security-driven yet performance-optimized AES

implementation can significantly enhance data protection without imposing excessive computational overhead. Future work may focus on further hardware-level optimizations, energy-efficient implementations, and integration with hybrid cryptographic frameworks to address emerging security challenges in next-generation computing environments.

## Reference


1. Mosiur Rahaman et al., "Privacy-Centric AI and IoT Solutions for Smart Rural Farm Monitoring and Control," Sensors, vol. 24, no. 13, pp. 1-24, 2024.
2. Deafallah Alsadie, "Artificial Intelligence Techniques for Securing fog Computing Environments: Trends, Challenges, and Future Directions," IEEE Access, vol. 12, pp. 151598-151648, 2024.
3. Krishna shree Achuthan et al., "Sustainable Cyber security Practices: Past Trends and Future Directions," SSRN, 2024.
4. Houda Hafi et al., "Split Federated Learning for 6G Enabled-Networks: Requirements, Challenges and Future Directions," IEEE Access, 2024.
5. Hamed Alqahtani, and Gulshan Kumar, "Machine Learning for Enhancing Transportation Security: A Comprehensive Analysis of Electric and Flying Vehicle Systems," Engineering Applications of Artificial Intelligence, vol. 129, 2024.
6. Oussama Kerdjidj et al., "Uncovering the Potential of Indoor Localization: Role of Deep and Transfer Learning," IEEE Access, vol. 12, pp. 73980-74010, 2024.
7. Yassine Himeur et al., "Applications of Knowledge Distillation in Remote Sensing: A Survey," Information Fusion, vol. 115, 2024.
8. D.M.G. Preethichandra et al., "Passive and Active Exoskeleton Solutions: Sensors, Actuators, Applications, and Recent Trends," Sensors, vol. 24, no. 21, pp. 1-42, 2024.
9. Siva Raja Sindiramutty, "Autonomous Threat Hunting: A Future Paradigm for AI-Driven Threat Intelligence," arXiv Preprint, 2023.

10. Nazish Khalid et al., "Privacy-Preserving Artificial Intelligence in Healthcare: Techniques and Applications," Computers in Biology and Medicine, vol. 158, 2023.
11. Rishabh Sharma, and Ashish Sharma, Fake Account Detection using the Machine Learning Technique, 1st ed., Smart Computing, pp. 197- 203, 2021.
12. Jagpreet Kaur, Shweta Lamba, and Preeti Saini, "Advanced Encryption Standard: Attacks and Current Research Trends," 2021 International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE), Greater Noida, India, pp. 112- 116, 2021.
13. S. Sheikhpoura, A. Mahania and N. Bagherib, "Reliable advanced encryption standard hardware implementation: 32- bit and 64-bit data-paths," Microprocessors and Microsystems, vol. 81, 103740, 2021.
14. Laith Alzubaidi et al., "Review of Deep Learning: Concepts, CNN Architectures, Challenges, Applications, Future Directions," Journal of Big Data, vol. 8, no. 1, pp. 1-74, 2021
15. T. Manoj Kumar and P. Karthigaikumar, "A novel method of improvement in advanced encryption standard algorithm with dynamic shift rows, sub byte and mixcolumn operations for the secure communication," International Journal of Information Technology, vol. 12, no. 1, pp. 825–830, 2020.
16. B. Langenberg, H. Pham and R. Steinwandt, "Reducing the cost of implementing the advanced encryption standard as a quantum circuit," IEEE Transactions on Quantum Engineering, vol. 1, pp. 1–12, 2020.
17. H. Indriyawati, T. Winartib and V. Vydia, "Web-based secure degree certificate legalization system using advanced encryption standard algorithm," International Journal of Information Technology and Business, vol. 2, no. 2, pp. 14–18, 2020.
18. T. Manoj Kumar, P. Karthigaikumar and V. Ramachandran, "An optimized s-box circuit for high speed AES design with enhanced

PPRM architecture to secure mammographic images," Journal of Medical Systems, vol. 3, no. 31, pp. 1, 2019.

19. N. M. Mangai, P. Karthigaikumar, S. T. Vinod and D. A. Chandy, "FPGA implementation of elephant recognition in infrared images to reduce the computational time," Journal of Ambient Intelligence and Humanized Computing, vol. 1, no. 1, pp. 1–16, 2018.
20. T.Manoj Kumar and P. Karthigaikumar, "FPGA implementation of an optimized key expansion module of AES algorithm for secure transmission of personal ECG signals," Design Automation for Embedded Systems, vol. 22, no. 1–2, pp. 13–24, 2018