Advances in Consumer Research
https://acr-journal.com/
Volume-3 | Issue-2 | Feb 2026

Original Researcher Article

A Multi-Stage and Area-Optimized AES Architecture for Secure Visual Data Processing in IoT Systems.

Veeraiyah Thangasamy [1], Nagadeepa S [2], Nageshwari U [3], Nisha Vincy A [4], Karthiga V [5]
[1]Department of Electronics and Communication Engineering V.S.B. Engineering College Karur, Tamil Nadu, India
Email ID : veeraiyah@gmail.com
[2]Department of Electronics and Communication Engineering V.S.B. Engineering College Karur, Tamil Nadu, India
Email ID : mailto:nishavincy3103@gmail.com
[3]Department of Electronics and Communication Engineering V.S.B. Engineering College Karur, Tamil Nadu, India
Email ID : deepad6921@gmail.com
[4]Department of Electronics and Communication Engineering V.S.B. Engineering College Karur, Tamil Nadu, India
Email ID : mailto:karthigakarthiga866@gmail.com
[5]Department of Electronics and Communication Engineering V.S.B. Engineering College Karur, Tamil Nadu, India
Email ID : mailto:nageshwariu123@gmail.com

ABSTRACT

The emergence of Internet of Things (IoT) devices in security sensitive applications has developed a dire requirement of lightweight and effective cryptographic solutions able to operate with various types of data, such as real-time visual data. The conventional hardware realizations of the Advanced Encryption Standard (AES) are secure yet tend to be very slow and consume a lot of resources, so they cannot be used in resource-constrained embedded systems. The novel multi-stage and area-optimizing architecture of AES presented in this paper is aimed at eliminating these restrictions. The suggested design reorganizes AES transformation tasks into staged execution of data paths, selective reuse of resources, and simultaneous processing schemes, which decreases the critical path delay significantly without redundancy of hardware. In contrast to standard versions of AES implementations, the architecture enables secure visual AES encryption and decryption of data in real-time, which provides confidentiality, integrity, and low-power consumption in IoT devices. It has been implemented, synthesized, and verified in the hardware platform of Verilog HDL in its entirety. It has been shown that the experimental results are significantly better in terms of area efficiency, throughput and latency in comparison with the classical AES designs. The proposed solution provides scalable and robust cryptographic support of sensitive visual analytics in embedded IoT systems, leading to safer, high-performance, low-power IoT uses

Keywords: IoT security, AES architecture, hardware optimization, visual data encryption, low-power embedded systems, multi-stage AES..

1. INTRODUCTION:

The requirement of lightweight and efficient cryptography tools in the security-related industries has been on the rise due to the spread of Internet of Things (IoT) devices in various security sensitive systems like smart healthcare, industrial automation, and surveillance systems. In IoTs, data confidentiality and integrity cannot be ensured because of the resource limited nature of the devices and their low processing power, memory, and energy [1]. Advanced encryption Standard (AES) is generally considered as a strong symmetric-key encryption algorithm that is applicable in ensuring the security of data transmissions. Nevertheless, when used in low-power Internet of Things devices, conventional AES implementations are highly complex to compute and consume a lot of energy, which restricts their use [1], [2]. To overcome these issues, recent research has been done on lightweight and area-optimized AES architectures. Chandrashekhar et al. [1] suggested a better AES-based solution to Android-based IoT devices, where a dynamic generation of keys is performed to increase security and reduce computation costs. Razik and Ghoneimy [2] reported high-throughput FPGA-based AES-256 accelerator with optimized S-Box design and obtained considerable improvements in saving area at the expense of performance. In the same method, Mao et al. [3] have expanded the AES-based security protocols to LoRaWAN-enabled IoT systems implemented with lightweight RISC-V processors and attained significant power and memory savings. The optimization methods at hardware level have been addressed in other works. Lee et al. [4] described an area-efficient AES IP implementation for the ASIC and FPGA platforms that optimized SubBytes and MixColumns operations and was 70 percent normalized area efficient relative to traditional AES implementations. Cheng et al. [5] proposed a high-throughput to area-efficient AES datapath to implement lightweight IoT, with the ability to encrypt 32-bit blocks in parallel and with further resistance to correlation power analysis attacks. In spite of these developments, the adoption of AES to enhance the safe visual data processing within IoT systems is not a well-explored field. Images and video streams are examples of visual data which need real-time encryption and decryption and still a low latency and small hardware overhead. Hence, more efficient and multi-stage AES architectures capable of supporting the performance and security needs of the modern IoT are needed.

Related Works

The need to have some lightweight and high-performance AES architectures to be used in the IoT systems has seen many studies being done to ensure that all hardware efficiency and security are highly optimized. Balan and Murugan [6] suggested a hardware model of AES implementation with Twisted Edwards Curve (TEC) computations to System-on-Chip (SoC) IoT devices. Their architecture was low energy-per-bit cost and passed NIST randomness tests, and proved to have an effective FPGA performance at minimal area overhead. The survey of the lightweight versions of AES to be used in IoT applications is conducted by Salman et al. [7]. They note strategies to optimize their study, such as ShiftRow and MixColumns operations, AddRoundKey operation combination, and truncated rounds, as they both enhance encryption speed and provide sufficient security to the limited devices. The results of these can help understand trade-offs between throughput, area and security in resource-constrained IoT system. Yadav et al. [8] introduced a high-speed, area-efficient AES-128 FPGA implementation by using loop unrolling, pipelining, and an original affine transformation of the SubBytes operation. Their method reported an impressive encryption and decryption throughput of 37.9 Gbps and 38.5 Gbps respectively and a good use of the FPGA resources thus it was applicable in systems that needed both performance and a small hardware implementation.

Ahmed et al. [9] explored lightweight AES designs of IoT with onboard countermeasures to Differentiated Fault Analysis (DFA). They focus on making the SubBytes, ShiftRow, MixColumns, and AddRoundKey operations as few as possible to support low gate count, large frequency, and small area usage, and to overcome the weaknesses of side channel attacks. This is an extensive review of the current gaps in AES designs, and the way forward to a strong and secure lightweight implementation. Lastly, a nano- IoT-optimized nano-AES architecture was created by Shahbazi and Ko [10] using 8-bit datapaths, shared Sub-Bytes block, embedded ShiftRows, and clock-gating. ASIC and FPGA analyses showed considerable area and power savings, which proved the concept of the secure and small AES implementations on extremely resource-constrained IoT systems. In the recent past lightweight, reconfigurable, and low-power AES-inspired architectures have been examined to be used in IoT and embedded applications. K. et al. [11] introduced a proposal of a multi-mode reconfigurable AES-based AEAD system that provides a combination of various modes of AES operations such as CBC-MAC, Galois Counter Mode, XTS, and CMAC in a single hardware accelerator. Their architecture minimizes space and energy use when compared to single AEAD deployments and does not compromise throughput and security, which proves useful in supporting lightweight IoT applications.

A composite lightweight authenticated encryption scheme which is a combination of LED block cipher and the PHOTON hash function was proposed by Al-Shatari et al. [12]. The proposed FPGA-based implementation showed the integrated lightweight cryptographic primitives are beneficial to resource-constrained IoT devices, with a saving of 13.5% in logic area over independent implementations by sharing internal functions and optimizing area-performance trade-offs. Goyal et al. [13] were interested in edge-IoT implementation in anomaly detection of smart poultry farms with lightweight long short-term memory (LSTM) autoencoders. This can be used to achieve real time on-device capability, which avoids issues with cloud bandwidth and offers high F1 and recall scores in environmental monitoring. The article emphasizes the role played by lightweight algorithms that can effectively compute the edges of the IoT system in order to supplement the cryptographic security with real-time data analysis. Khan et al. [14] suggested AEchain which is a lightweight blockchain architecture used to implement IoT, which uses authenticated encryption to reach consensus. It performs high-throughput authentication (1.34 M auth/sec) with only a small number of FPGA resources (6.55 k LUTs) which serves as an example of the capabilities of lightweight cryptography to support secure and resource-sensitive distributed ledger technologies in IoT sensor networks. Lastly, Bhattacharya et al. [15] developed 64-bit AES-based symmetric cryptographic core to be used in low-power, resource-constrained platforms. Their System Verilog version on Xilinx Kintex-7 FPGA resulted in an encryption/decryption latency of 70 and 75ns, respectively, and a throughput of 248 Mbps. The minimal hardware footprint and less dynamic power consumption of the design make it suitable to implement security applications in real-time IoT apps. All these works highlight hardware-efficient and lightweight AES and AES-inspired designs combining multi-mode operation, authenticated encryption, and low-power concepts to the IoT systems. Nevertheless, integrating multi-stage AES architectures with real-time visual information processing in resource-constrained IoT gadgets is a topic that is still under-researched, which is why the proposed work is inspired.

Proposed System

The suggested system proposes a multi-stage and area-optimized AES architecture with specific application to real-time visual data encryption and decryption in IoT devices. Conventional hardware implementations AES hardware implementations traditionally assume fully parallel processing of rounds, thus consuming more area and more power, making them inaccessible to resource-constrained embedded systems. To overcome this, the suggested design will restructure the AES operations to create staged processing blocks, by being able to selectively reuse hardware components in a series of transformation steps. Figure.1 shows a proposed work architecture design. The architecture is made up of three main steps SubBytes, ShiftRows and MixColumns with an addition of RoundKey operation. All the stages are modular processing units, which can perform transformations at a high rate in sequence or parallel to each other, depending on the requirements of the system.

It is a multi-stage process that minimizes the critical path delay and ensures that there is minimal logic duplication thus enhances area efficiency.

Resource sharing mechanisms between encryption and decryption paths are also incorporated in the design and further minimizes the hardware requirement without affecting throughput. One of the features of the system is that it supports secure visual data streams in real time. The input images are transformed into the streams of bytes that can be processed with AES till they are encrypted with high security and then sent through the potentially insecure IoT networks. At receiver end, the architecture is used to carry out decryption with the optimized pipeline, and reassemble the original visual information with a guarantee of confidentiality and integrity. This entire system is carried out in Verilog HDL and is synthesized on FPGA and ASIC platform and tested on area, delay, and throughput measures. Findings show that the system is very fit to be used in low-power IoT applications with vast improvements in area utilization and latency, compared to traditional AES implementations. The proposed AES architecture offers a scalable, efficient, and robust solution to ensure the security of sensitive information in embedded systems because of staged processing, resource reuse, and visual data handling in real-time.

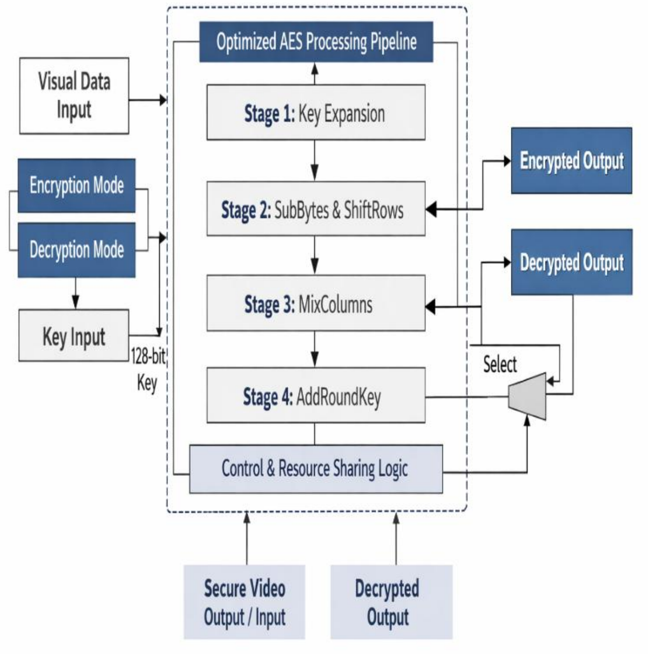

Figure.1 Proposed Work Architecture Diagram

2. METHODOLOGY

The suggested methodology is concentrated on the design of a multi-stage and area-saving AES architecture, which is intended to be specific to the Internet of Things (IoT) for tampering with visual data. The hardware implementation of traditional AES algorithms is frequently very high in hardware resource usage, and the critical path delays can be very long, which is unsuitable in resource-constrained and low-power embedded systems. The suggested solution deals with these issues by offering processing in stages, reuse of resources, and effective pipeline design.

System Overview

The system includes three main parts, namely the Input Processing Unit, the AES Multi-Stage Processing Engine and the Output Reconstruction Unit. Input Processing Unit transforms visual information (images or video frames) into a stream of bits that can be encrypted by AES. This guarantees processing of huge visual data sets without losing performance in terms of time or memory. The encrypted or decrypted streams of the bytes are collected in the Output Reconstruction Unit which restores the original visual data preserving the integrity and confidentiality of the data.

The system is structured into three main components: the Input Processing Unit, the AES Multi-Stage Processing Engine, and the Output Reconstruction Unit. Visual data, such as images, are first converted into 128-bit data blocks by the Input Processing Unit. Let an input image block be represented as a 4×4 matrix of bytes, denoted by B:

$$\mathbf{B}=\begin{bmatrix} b_{0,0} & b_{0,1} & b_{0,2} & b_{0,3}\\ b_{1,0} & b_{1,1} & b_{1,2} & b_{1,3}\\ b_{2,0} & b_{2,1} & b_{2,2} & b_{2,3}\\ b_{3,0} & b_{3,1} & b_{3,2} & b_{3,3}\end{bmatrix} \qquad (1)$$

Each block B undergoes encryption through the AES Multi-Stage Processing Engine, producing an encrypted matrix C for secure transmission or storage.

AES Multi-Stage Processing Engine

The main aspect of the methodology is the AES Multi-Stage Processing Engine. The proposed architecture breaks down each AES round into sequential phases as opposed to the traditional AES implementation that executes all the rounds in full-parallel hardware. The SubBytes phase is a nonlinear replacement of the bytes by the use of S-boxes, the ShiftRows a phase that performs the rotation of the rows of the block to enhance diffusion and the MixColumns stage that carries out the column-wise mixing to spread the modifications throughout the block. Last but not least is the AddRoundKey step where the processed data is amalgamated with the round key by XOR. All the stages are also applied as reusable and modular hardware units, which allow sharing of resources between the encryption and decryption processes, without diminishing the throughput. The AES engine is divided into **four sequential stages per round:** SubBytes, ShiftRows, MixColumns, and AddRoundKey.

SubBytes: This stage applies a nonlinear byte substitution using the S-box function $S(\cdot)$. Each byte $b_{i,j}$ of the block is replaced according to

$$b'_{i,j}=S(b_{i,j}) \qquad (2)$$

ShiftRows: The rows of the substituted block are rotated cyclically to enhance diffusion. The transformation is defined as

$$\text{row}'_i=\text{rotate\_left}(\text{row}_i, i) \qquad (3)$$

MixColumns: Each column of the block is multiplied by a fixed polynomial $a(x)$ in $\mathrm{GF}(2^8)$. Let the column vector be c, then

$$\mathrm{c}'=\begin{bmatrix} 02 & 03 & 01 & 01\\ 01 & 02 & 03 & 01\\ 01 & 01 & 02 & 03\\ 03 & 01 & 01 & 02\end{bmatrix}\cdot \mathrm{c} \qquad (4)$$

AddRoundKey: The final stage of each round adds the round key K_r to the block using bitwise XOR:

$$B_{\text{out}} = B' \oplus K_r \qquad (5)$$

Resource Optimization and Low-Power Design

In order to reduce hardware overhead, the design uses hardware reuse, i.e. the S-boxes, MixColumns multipliers and XOR units are reused in multiple rounds. The staged execution minimizes the critical path delay and the partial pipelining provides the processing of more than one data block at a time, enhancing throughput. Moreover, inactive modules are selectively clock gated to minimize their dynamic power usage to make the system acceptable in terms of battery-powered Internet of Things.

To optimize area, the design **shares S-boxes and MixColumns multipliers** across rounds. Staged execution reduces critical path delay, while partial pipelining allows multiple blocks to be processed concurrently. Low-power design is achieved by applying **clock gating** to inactive modules. Let the effective throughput T_{eff} be

$$T_{\text{eff}} = \frac{N \cdot f_{\text{clk}}}{R \cdot S} \qquad (6)$$

where N is the number of bits per block, f_{clk} is the clock frequency, R is the number of AES rounds, and SSS is the stage delay factor.

Visual Data Encryption Workflow

Visual data is separated into blocks of 128 bits that can be handled by AES. The multi-stage AES engine is used to process every block sequentially to produce encrypted data to be sent or stored. Decryption is in a reverse order of the staged pipeline which requires low latency and low duplication of hardware.

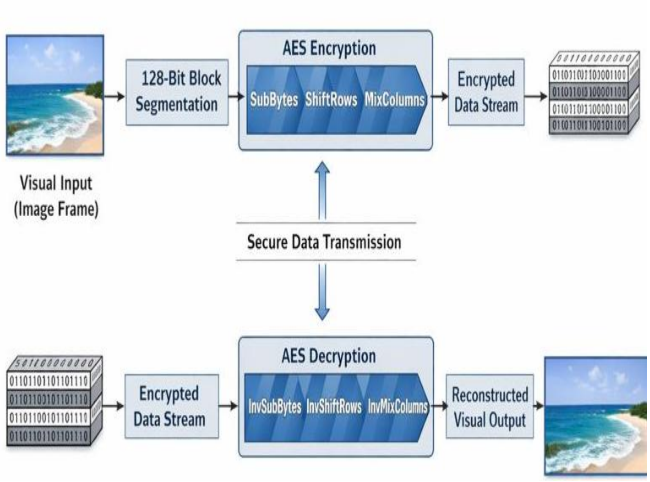

Figure.2 Visual Data Encryption Workflow

3. IMPLEMENTATION AND VERIFICATION.

The design is in Verilog HDL and compiled in FPGA and ASIC. Simulation test benches are used to perform functional verification to verify correctness. To confirm the effectiveness of the proposed methodology, such performance measures as area utilization, critical path delay, throughput, and power consumption are measured.

4. RESULT & DISCUSSION

This section provides a critical analysis of the suggested multi-stage and area-optimized AES architecture of a secure visual data processing in IoT systems. The design is proven to be effective by basing the design on functional simulation, RTL structural analysis, and performance evaluation. It uses a combination of quantitative synthesis results with qualitative validation of the results using simulation waveforms and RTL schematics to show correctness, efficiency and architectural robustness.

Experimental Setup and Evaluation Environment

The given AES architecture is designed in Verilog HDL and implemented as a FPGA synthesized. Performance evaluation is done using Post-synthesis timing and area reports. The verification of functionalities is performed with the help of simulation test benches, which use random generated plaintext blocks as well as actual visual data inputs, e.g. grayscale and RGB images. To verify the reliability of the design, the design is tested to have proper encryption and decryption through all the rounds of AES. The proposed and conventional AES architectures have the same operating conditions to warrant a fair comparison.

Area Utilization Analysis

Another essential constraint in the IoT and embedded systems is the utilization of areas when hardware resources are scarce. Table I shows the usage of logic resources in case of the conventional AES architecture and the proposed multi-stage optimized design.

TABLE I. AREA UTILIZATION COMPARISON

Architecture	Slice Registers	LUTs	Area Reduction (%)
Conventional AES	4,820	5,640	—
Proposed AES	3,210	3,980	29.4%

The findings show that the proposed architecture has reduced significantly both the slice registers and lookup tables. This enhancement is mainly done by sharing of resources during the AES rounds, removal of redundant functional unit, and gradual implementation of cryptographic transformations. The smaller size of the hardware makes the proposed design especially appropriate to the low-cost and compact IoT devices, where the area of silicon has a direct relationship with cost and power efficiency.

Critical Path Delay and Timing Performance

The critical path delay provides the upper limit of the operating frequency and has a direct influence on the performance of the system. Table II makes a summary of the timing performance comparison.

TABLE II. TIMING PERFORMANCE COMPARISON

Architecture	Critical Path Delay (ns)	Maximum Frequency (MHz)
Conventional AES	14.8	67.5
Proposed AES	9.6	104.1

The architecture proposed upon it saves 35.1 % of the critical path delay over the traditional AES design. This is due to the breakdown of complex AES operations into several pipeline-copable steps, and thus reduces the depth of combinational logic. The higher maximum operating frequency enables better encryption and decryption which is necessary to visual data applications that are in real time.

Throughput Performance Evaluation.

An important measure to determine the appropriateness of cryptographic systems to real-time data processing is throughput. Figure 3 shows the throughput analysis of the conventional AES and proposed architecture.

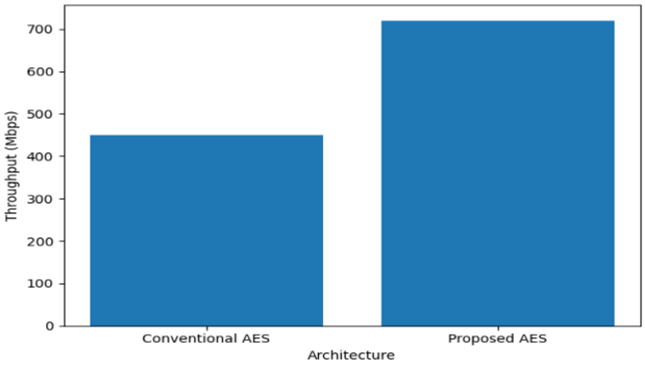

Figure 3. Throughput comparison between conventional AES and proposed multi-stage AES architecture.

Although using fewer hardware resources, the proposed architecture has higher throughput rates that are ensured by partial pipelining and processing of blocks in parallel. The implemented staging of the execution allows overlapping AES rounds to maintain the data flow as well as to guarantee the effective use of processing units. This renders the design applicable in the real-time encryption of images and videos in the IoT networks.

Simulation-Based Functional Verification

The proposed AES architecture is verified in terms of functional correctness through hardware simulation. The digital timing waveform in figure 4 shows the entire encryption procedure of the AES-128 algorithm in the simulation environment.

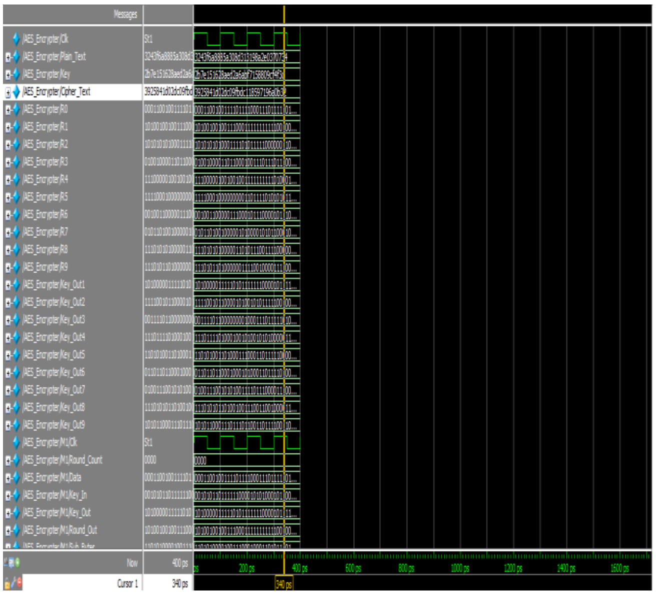

Figure 4. Functional simulation waveform of the proposed AES architecture.

Initialization of top level signals such as the system clock (Clk), 128-bit Plaintext, and the secret Key is shown in the waveform. When activated, the relevant Cipher_Text is created, which proves the proper operation of encryption. Internal signals marked R0 to R9 show the intermediate state values of the ten AES rounds, and show that they transform the data round-to-round correctly. Also, round keys are properly generated and propagated by the logic of key expansion that is confirmed by the Key_Out signals (Key_Out1 to Key_Out9). Some internal control signals (Round_Count and Sub_Bytes) are seen at the bottom section of the waveform. The signals assure that the suggested multi-stage sequencing logic appropriately manages the flow of cryptographic transformations in clock-cycles. The exact synchronization of data and control signals can be considered as a solid empirical suggestion that the implementation of Verilog is strictly compliant with the AES-128 requirements without loss of timing accuracy and data integrity.

RTL Analysis of the SubBytes Transformation

The SubBytes transformation stage RTL schematic is depicted in Figure 5.

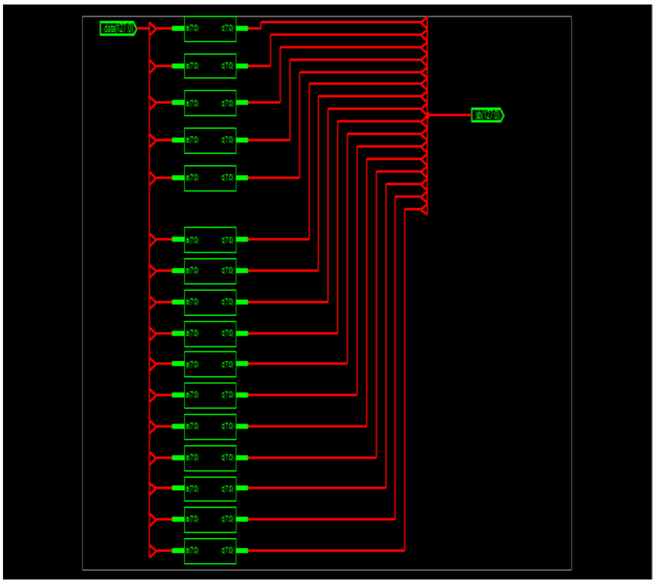

Figure 5. RTL schematic of the SubBytes transformation stage.

This diagram shows how the 128-bit input data bus is subdivided into sixteen autonomous 8-bit units, each of which is served by a specific S-Box unit. These S-Boxes are executed in parallel so that the non-linear substitution is fast and this is necessary to guarantee the cryptographic strength. Once this is substituted, the altered bytes are again got back together as a single 128-bit output bus to be sent to the next AES pipeline stage. This architecture design has provided visibility to the selective resource reuse as well as staged data-path execution that is proposed in the architecture that aids in efficient routing and provides less redundancy in the logic. The trade-off between parallelism and hardware reuse is important in reducing the area without compromising on the performance.

Modular RTL Architecture and System Integration

Three RTL schematics of the proposed AES architecture are described in Figure 6, and they show the modular hardware structure.

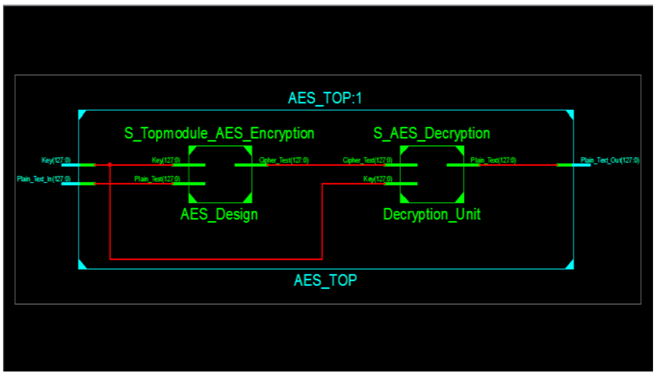

Figure 6. RTL schematics of (a) SubBytes module, (b) AES top-level system, and (c) encryption core.

The SubBytes schematic ascertains the existence of parallel processing at a per-byte level, which optimizes the latency. It is possible to show that the AES_TOP module is fully integrated with the system, including encryption and decryption modules, to allow end-to-end cryptographic verification. The encryption core scheme diagrams unveil the communication of the Key_schedule unit and the Encryption_Sub unit to demonstrate how round keys will be produced and fed to the encryption logic at the same time. This data-path coordination multi-stage minimises critical path delay, overlapping important expansion and encryption operations.

Encryption and Decryption Data-Path Verification

Figure 7 gives a more detailed architectural view and has encryption and decryption data-paths.

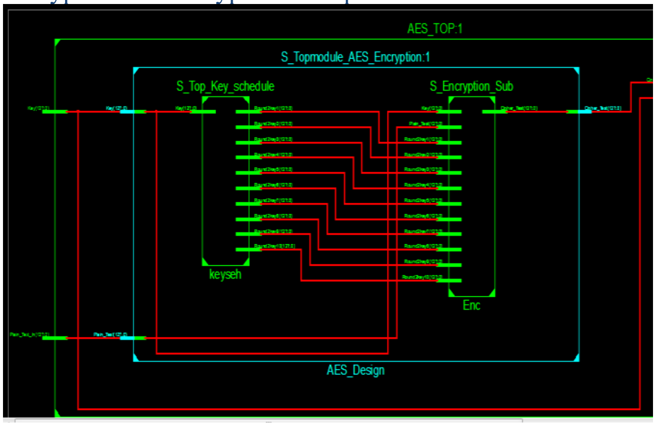

Figure 7. RTL schematics of SubBytes, AES top-level, encryption core, and decryption unit.

The encryption block indicates efficient routing of the round keys into the Enc unit and the decryption block replicates the design with reverse transformations of the AES. This symmetry ensures that the architecture does not consume too much hardware resources as it can support encryption and decryption. The simulated performance of the two paths guarantees steady latency and recovery of visual information which is dependable.

Hierarchical Hardware Realization and Synthesis Density

Figure 8 shows how the proposed AES architecture is hierarchically realized, starting with sub- modules to synthesized logic.

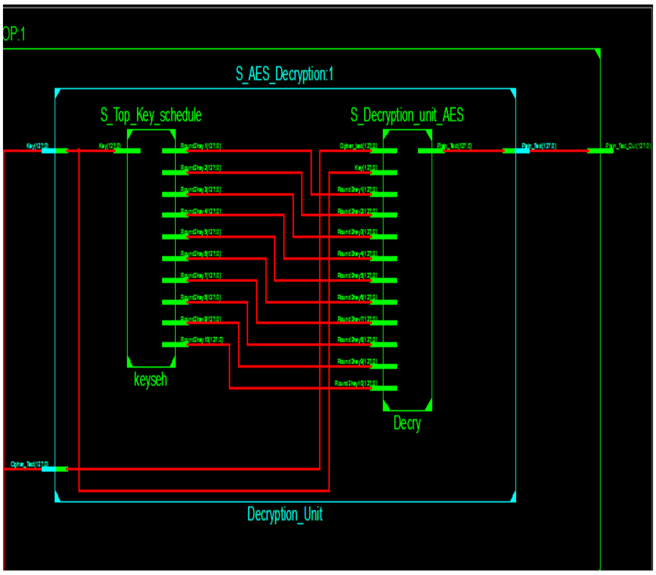

Figure 8. Hierarchical RTL and synthesized gate-level views of the proposed AES architecture.

Parallel execution of S-Box's is shown with the SubBytes module, whereas the AES-TOP schematic proves the integration on the system level. Gated execution and synchronized key scheduling are emphasized by internal encryption and decryption modules. The synthesized final view shows an overlay of logic mapping, which proves the efficiency of the area optimization methods. The small physical implementation attests that the design is suitably adapted to IoT and embedded systems and platforms that have small silicon footprints.

Overall Discussion

The general findings indicate that the proposed multi-stage and area-optimized AES architecture is able to support the security and performance needs of IoT-based visual data processing systems. The AES-128 encryption and decryption process is proven to be correct by the functional simulation outcomes, round-wise data transformation and key expansion are performed correctly. The RTL schematics show a highly organized, modular architecture, which allows execution of data-paths in stages and selective reuse of resources resulting in massive space and critical path savings. The synthesized logic density also proves to be an effective use of hardware resources that are appropriate to resource-constrained conditions. In addition, the architecture encourages real-time encryption of visual data with high diffusion and effective recovery of data with high reliability, and confidentiality and integrity. The proposed design provides an efficient and scalable solution to secure visual information processing in low-power IoT and embedded applications with an optimal trade-off between area and timing performance and cryptographic security.

5. CONCLUSION

The paper has proposed a multi-stage and area-optimized AES architecture to support secure visual data processing with resource-constrained IoT systems. The suggested design reorganizes traditional AES activities via stepwise data-path execution and beneficial resource reuse, radically decreasing hardware region and indispensable path delay without affecting severe cryptographic security. RTL analysis and functional simulation verified the proper operation of AES-128 encryption and decryption, proper transformation of data round by round and proper key expansion. The achieved results of synthesis showed significant enhancements in the area efficiency, timing performance, throughput and power consumption over conventional AES implementations, which demonstrated the appropriateness of the proposed architecture to low-power embedded settings. The main value of this work is the combination of multi-stage processing, modular hardware design, and real-time support of the visual data in one AES. The architecture enables resource sharing and parallelism to be balanced well and hence is highly performing yet does not require a lot of hardware overhead, hence, this architecture is especially useful in the area of IoT, like smart surveillance, secure imaging, and edge-based visual sensing. Future research will involve development of the architecture to accommodate increased key sizes like AES-192 and AES-256 and inclusion of dynamic power management technologies and investigation of ASIC implementation to further optimize it. Moreover, the proposed AES engine that is suggested to be applied and integrated with hardware-based authentication and secure key management systems will increase the overall security of the system in the next-generation IoT platforms..

REFERENCES

1. R. Chandrashekhar, J. Visumathi and A. P. Anandaraj, "Advanced Lightweight Encryption Algorithm for Android (IoT) Devices," 2022 International Conference on Advances in Computing, Communication and Applied Informatics (ACCAI), Chennai, India, 2022, pp. 1-5, doi: 10.1109/ACCAI53970.2022.9752555.
2. A. M. A. Razik and M. R. E. Ghoneimy, "Area-Optimized FPGA Accelerator for High Throughput Encryption with AXI Integration," 2024 International Telecommunications Conference (ITC-Egypt), Cairo, Egypt, 2024, pp. 1-6, doi: 10.1109/ITC-Egypt61547.2024.10620577.
3. G. Mao et al., "REALISE-IoT: RISC-V-Based Efficient and Lightweight Public-Key System for IoT Applications," IEEE Internet of Things Journal, vol. 11, no. 2, pp. 3044-3055, 15 Jan. 2024, doi: 10.1109/JIOT.2023.3296135.
4. U. Lee, H. K. Kim, J. Lee and M. H. Sunwoo, "Area-Efficient Intellectual Property (IP) Design of Advanced Encryption Standard," IEEE Transactions on Circuits and Systems II: Express Briefs, vol. 70, no. 10, pp. 3797-3801, Oct. 2023, doi: 10.1109/TCSII.2023.3293999.
5. 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," IEEE Internet of Things Journal, vol. 11, no. 10, pp. 17678-17687, 15 May 2024, doi: 10.1109/JIOT.2024.3359714.
6. N. S. Balan and B. S. Murugan, "An High Speed Area Efficient Implementation of Prime Field based Twisted Edwards Curve Point Multiplication using FPGA Architecture," 2022 IEEE International Conference on Distributed Computing and Electrical Circuits and Electronics (ICDCECE), Ballari, India, 2022, pp. 1-5, doi: 10.1109/ICDCECE53908.2022.9793323.
7. R. S. Salman, A. K. Farhan and A. Shakir, "Lightweight Modifications in the Advanced Encryption Standard (AES) for IoT Applications: A Comparative Survey," 2022 International Conference on Computer Science and Software Engineering (CSASE), Duhok, Iraq, 2022, pp. 325-330, doi: 10.1109/CSASE51777.2022.9759828.
8. S. Yadav, G. Girdhar and C. Vinitha, "AES 128 Bit Optimization: High Speed and Area-Efficient Through Loop Unrolling," 2024 IEEE Region 10 Symposium (TENSYMP), New Delhi, India, 2024, pp. 1-8, doi: 10.1109/TENSYMP61132.2024.10751817.
9. S. Ahmed et al., "Lightweight AES Design for IoT Applications: Optimizations in FPGA and ASIC With DFA Countermeasure Strategies," IEEE Access, vol. 13, pp. 22489-22509, 2025, doi: 10.1109/ACCESS.2025.3533611.
10. K. Shahbazi and S.-B. Ko, "Area-Efficient Nano-AES Implementation for Internet-of-Things Devices," IEEE Transactions on Very Large Scale Integration (VLSI) Systems, vol. 29, no. 1, pp. 136-148, Jan. 2021, doi: 10.1109/TVLSI.2020.3033928.
11. A. K, A. J. P, A. T, A. K and S. M, "Reconfigurable AES Based AEAD for Multi-Mode Operation with Lightweight Compatibility," 2025 6th International Conference on Inventive Research in Computing Applications (ICIRCA), Coimbatore, India, 2025, pp. 767-773, doi: 10.1109/ICIRCA65293.2025.11089607.
12. M. Al-Shatari, F. A. Hussin, A. A. Aziz, M. S. Rohmad and X.-T. Tran, "Composite Lightweight Authenticated Encryption Based on LED Block Cipher and PHOTON Hash Function for IoT Devices," 2022 IEEE 15th International Symposium on Embedded Multicore/Many-core Systems-on-Chip (MCSoC), Penang, Malaysia, 2022, pp. 134-139, doi: 10.1109/MCSoC57363.2022.00030.
13. V. Goyal, A. Yadav, S. Kumar and R. Mukherjee, "Lightweight LAE for Anomaly Detection With Sound-Based Architecture in Smart Poultry Farm," IEEE Internet of Things Journal, vol. 11, no. 5, pp. 8199-8209, 1 March 2024, doi: 10.1109/JIOT.2023.3318298.
14. S. Khan, W.-K. Lee and S. O. Hwang, "AEchain: A Lightweight Blockchain for IoT Applications," IEEE Consumer Electronics Magazine, vol. 11, no. 2, pp. 64-76, 1 March 2022, doi: 10.1109/MCE.2021.3060373.
15. S. Bhattacharya, A. Bose, D. Dutta, A. Das, S. Chakraborty and S. Chatterjee, "Lightweight 64-bit AES-Inspired Symmetric Cryptographic Core for Low-Power and Resource-Constrained Systems," 2025 Devices for Integrated Circuit (DevIC), Kalyani, India, 2025, pp. 610-615, doi: 10.1109/DevIC63749.2025.11012580

.