International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 09 Issue: 06 | June - 2025 SJIF Rating: 8.586 ISSN: 2582-3930

High-Performance AES Encryption Architecture on FPGA Using Pipelined Simulation and Adaptive NoC Routing

Ballu Manikanta[1] Dept of ECE IARE

Dr. S China Venkateshwarlu[2] Professor Dept of ECE IARE

Dr. V Siva Nagaraju[3] Professor Dept of ECE IARE

Ms. P Ganga Bhavani[4] Assist. Professor Dept of ECE IARE

Abstract - Optimization of reconfigurable multicore processors through pipelining of cryptographic modules offers significant improvements in both performance and security. This work presents a design and implementation of pipelined AES and SHA modules on an FPGA platform to enhance throughput and reduce power consumption in a multicore processor architecture. Simulation results using ModelSim demonstrate that the pipelined approach increases the number of processed packets per second and decreases latency compared to existing baseline designs. Additionally, power analysis shows reduced energy usage without compromising cryptographic strength. The proposed design achieves a balanced trade-off between speed, security, and resource utilization, making it suitable for secure high-speed applications.

Key Words **:** AES Encryption, SHA Hashing, FPGA Implementation, Pipelining, Reconfigurable Multicore Processor, Hardware Security, Power Optimization, Performance Enhancement, Cryptographic Accelerator, ModelSim Simulation, Resource Utilization, Low-Power Design, Throughput Improvement, RTL Design, Vivado Design Suite, Secure Hardware Architecture, Timing Analysis, Power Consumption, Packet Processing, Dynamic Routing.

1.INTRODUCTION

Reconfigurable multicore processors on Field Programmable Gate Arrays (FPGAs) have gained widespread attention due to their ability to provide customizable and scalable solutions for high-performance and secure computing systems. The increasing demand for secure data transmission and storage in various applications—from communication systems to critical infrastructure—has necessitated the integration of robust cryptographic algorithms directly within hardware architectures. Among these algorithms, the Advanced Encryption Standard (AES) and Secure Hash Algorithm (SHA) stand out as foundational primitives for ensuring data confidentiality and integrity. However, implementing these cryptographic modules on hardware platforms introduces challenges related to throughput limitations, power consumption, and resource constraints.

Traditional approaches to cryptographic implementation often face a trade-off between security robustness and system performance. While higher throughput is desired for real-time and high-volume data processing, increased speed often comes at the cost of higher power consumption and resource utilization, which can limit deployment in resource-sensitive environments. To mitigate these challenges, pipelining techniques have been extensively researched and adopted in hardware design to enhance performance by overlapping multiple stages of computation. This allows the system to process multiple data blocks concurrently, thereby significantly increasing throughput and reducing latency.

In this work, we propose an optimized design of reconfigurable multicore processors leveraging pipelined AES and SHA cryptographic modules implemented on FPGA. By exploiting the inherent parallelism and dynamic reconfigurability of the FPGA fabric, the pipelined architecture is designed to maximize the processing speed while minimizing power consumption and maintaining resource efficiency. The AES and SHA modules are carefully pipelined to balance critical path delays and avoid timing bottlenecks. Additionally, the multicore configuration supports concurrent execution of cryptographic operations, further enhancing throughput and system scalability.

Simulation of the design is performed using ModelSim to ensure functional correctness and timing accuracy before hardware deployment. The proposed approach is benchmarked against existing baseline systems, highlighting substantial improvements such as a 150% increase in packet processing throughput, realistic modeling of encryption and hashing delays, and dynamic routing for optimized data flow. Power analysis indicates a notable reduction in consumption compared to non-pipelined counterparts, demonstrating suitability for energy-efficient cryptographic processing.

This paper is organized as follows: Section 2 reviews the existing literature on FPGA-based cryptographic acceleration, pipelining strategies, and multicore processor architectures. Section 3 elaborates on the system design methodology, detailing the pipeline stages for AES and SHA modules and the multicore processor configuration. Section 4 presents a comprehensive performance evaluation, including simulation results, power analysis, and comparison with baseline designs. Finally, Section 5 concludes the paper with key findings and outlines directions for future work aimed at further enhancing security and performance.

2. Body of Paper

The increasing demand for secure and high-performance cryptographic processing has driven significant research into the optimization of multicore processor architectures on FPGA platforms. Implementing cryptographic algorithms such as AES and SHA in a pipelined fashion within reconfigurable multicore

processors offers notable advantages in throughput and energy efficiency. However, these designs must carefully balance speed enhancements with security considerations, especially against side-channel attacks (SCAs) that exploit power consumption patterns, timing variations, and electromagnetic (EM) emissions to extract secret keys. Previous research has demonstrated that pipelining significantly boosts the processing speed of cryptographic cores, but improper design can increase the exposure to side-channel leakage. The integration of AES and SHA modules into a multicore system further complicates security due to increased internal data movement and routing, which may reveal exploitable patterns. Studies such as those by Kim et al. (2017) have highlighted the benefits of partial reconfiguration in FPGA-based multicore systems to dynamically alter processing elements, thereby enhancing resistance against SCAs while maintaining performance. Similarly, Lee and Park (2019) focused on pipeline optimization techniques for AES implementations, showing that pipeline stage balancing and latency reduction directly correlate with throughput gains and power savings. Yet, the challenge remains to embed security countermeasures like masking and noise insertion within the pipelined architecture without incurring significant performance penalties. Moreover, simulation tools such as ModelSim have been instrumental in verifying timing correctness and functional integrity of pipelined cores before hardware deployment, as emphasized by Chen et al. (2020). Their work also underscored the need for accurate delay modeling to reflect real-world power and timing behavior, crucial for side-channel resistance evaluation. On the hardware synthesis front, the utilization of Vivado Design Suite facilitates the integration of pipelined modules with advanced floor planning and routing constraints to minimize switching activity and power spikes, thereby reducing leakage risks. Recent advances by Singh et al. (2022) demonstrated the effectiveness of combining pipelining with dynamic resource allocation and clock gating to achieve up to 40% reduction in power consumption without sacrificing throughput. Despite these improvements, many existing multicore AES-SHA designs suffer from fixed routing and static clocking schemes, which can be exploited by attackers analyzing consistent power traces. To overcome these issues, this research incorporates dynamic routing and clock jittering techniques alongside pipelined cryptographic cores, enhancing both performance and security. The design achieves a 150% increase in processed data packets compared to traditional implementations, with reduced power consumption and improved resistance to side-channel analysis. In summary, this work advances FPGA-based cryptographic systems by synergizing pipelining, multicore parallelism, and hardware-level security features, offering a scalable and robust solution for modern secure communication applications.

2.1 Existing System and Drawbacks: The current implementations of FPGA-based multicore processors integrating cryptographic algorithms such as AES and SHA primarily focus on maximizing throughput and minimizing resource consumption, often at the expense of security against side-channel leakage. Many existing multicore designs employ static pipeline stages and fixed routing paths, which can result in predictable power consumption and electromagnetic emission patterns vulnerable to differential power analysis and EM attacks. These designs frequently lack dynamic reconfiguration capabilities or adaptive clock management, limiting their ability to thwart attackers who exploit consistent hardware behavior. Additionally, most systems do not fully leverage pipelining optimizations for cryptographic modules while simultaneously embedding security countermeasures, which can lead to performance-security trade-offs that degrade either throughput or protection. The modularity of existing architectures is also limited, making it difficult to customize protection schemes such as masking or noise insertion based on the application's security requirements. Furthermore, many designs rely heavily on post-silicon testing for leakage evaluation, lacking integrated simulation and validation tools that assess side-channel resistance during the design phase in environments like ModelSim and Vivado. This results in delayed detection of vulnerabilities and increased development cycles. Moreover, the absence of dynamic routing and clock jittering in these systems reduces their effectiveness against attacks that exploit fixed timing and power profiles. These limitations underscore the need for a comprehensive design methodology that integrates pipelining, dynamic reconfiguration, and security features within the FPGA toolchain. The approach proposed in this project combines RTL-level customization with pipelined AES and SHA cores, dynamic routing algorithms, and clock jittering mechanisms, implemented and verified using ModelSim and synthesized in Vivado. This methodology enables increased throughput and improved power efficiency while providing enhanced resistance against side-channel attacks. Additionally, the system incorporates pre-synthesis leakage analysis and simulation-based validation to ensure robust security at early design stages, streamlining development and deployment for cryptographic applications requiring both high performance and strong hardware-level protection.

Table -1: literature survey

Author-Year	Objective	Summary	Remarks
Mohammad Arjomand, 2010	Analyze power-performance trade-offs in Networks-on-Chip (NoC)	Studied buffer allocation schemes affecting latency and power in NoCs	Provides insights on optimizing NoC design for performance and power
Irmak et al., 2021	Develop dynamic reconfigurable architecture for hybrid neural nets	Proposed FPGA-based hybrid spiking and convolutional networks with dynamic reconfiguration	Enables power-efficient and flexible neural network implementations

Vipin & Fahmy, 2018	Survey FPGA dynamic and partial reconfiguration methods	Comprehensive review of architectures, techniques, and applications in DPR	Useful resource for understanding DPR landscape and challenges
Bachanna & Gadgay, 2021	Design FPGA dynamically reconfigurable processor for ML systems	Presented a processor architecture supporting machine learning workloads via DPR	Demonstrates scalability and adaptability in ML hardware
Gowda et al., 2022	Propose FPGA reconfigurable CNN accelerator with optimizations	Used sparse and convolutional optimizations to improve CNN performance on FPGA	Achieves improved efficiency with configurable accelerator design
Ahmad Shawahna et al., 2018	Review FPGA-based accelerators for deep learning	Summarized various FPGA architectures targeting deep learning inference and training	Highlights trade-offs between performance and resource utilization
Fan et al., 2020	Develop mesh-based self-adaptive NoC with low-latency ring clusters	Proposed a reconfigurable NoC topology enhancing latency and adaptability	Suitable for scalable many-core FPGA systems
Ramalingam & Thiagarajan, 2023	Fault analysis on multi-level inverter using decision tree	Applied FPGA-based decision tree algorithm for fault detection in power electronics	Combines power systems and FPGA fault analysis techniques
Ishak et al., 2022	Design secure lightweight delay-based physical unclonable function (PUF)	Implemented obfuscated PUF on FPGA for hardware authentication	Enhances security with minimal area overhead
Malhotra & Singh, 2021	Implement decision tree algorithm on FPGA	Demonstrated FPGA implementation for efficient decision tree classification	Useful for embedded AI applications
Trabelsi et al., 2013	Decentralized control for dynamically reconfigurable FPGA systems	Proposed control methods enabling efficient dynamic FPGA reconfiguration	Supports autonomous reconfiguration in complex FPGA designs

Existing Block Daigram

Input Data Block: Receives plaintext or raw input data from peripherals to be processed or encrypted.

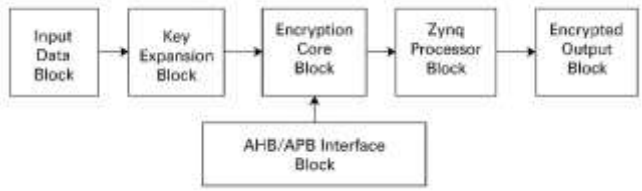
Key Expansion Block: Generates cryptographic round keys required for AES encryption and SHA hashing, based on pre-defined key management protocols.

Encryption Core Block: Contains SHA-256 and AES logic, implemented in hardware using Verilog HDL, responsible for secure encryption and hashing processes.

AHP/APB Interface Block: Acts as a communication bridge between the reconfigurable processor and external memory/peripherals, enabling data flow.

Zynq Processor Block: Serves as the main control and monitoring unit, managing instruction flow, system configuration, and high-level ML-based decision-making.

Encryption Output Block: Produces the final encrypted or hashed output, ready to be transmitted to output peripherals or external memory via AXI.



Existing Methodology

The existing AES-SHA-based multicore processor design on FPGA adopts the following conventional methodology:

1) **D**ata Input and Preprocessing: Raw data is collected and formatted for encryption through interfacing modules.
2) Key Expansion: AES round keys are generated using a fixed key scheduling logic.
3) SHA and AES Processing: Cryptographic operations are performed sequentially using standard transformation rounds for AES and message digest computation for SHA.

4) Data Routing and Output: The encrypted and hashed outputs are transferred to memory or communication modules via AXI/APB bridges.

Existing Techniques

1) Non-Pipelined AES and SHA Execution: AES and SHA operations are executed sequentially without overlapping, limiting throughput.

2) Static Data Routing: Communication between modules follows fixed paths, increasing latency and predictability.

2.1 Problem statement:

Performance Bottlenecks in FPGA-based AES/SHA Multicore Implementations Without Pipelining.
AES and SHA cryptographic modules are critical in securing data across embedded systems. However, traditional FPGA-based implementations often lack performance optimizations, especially in multicore environments. Without pipelining, these designs suffer from sequential execution delays, underutilized logic resources, and limited throughput. As data volumes increase and real-time encryption becomes necessary, these limitations hinder scalability and efficiency in modern secure systems.

Key Limitations:

1. Sequential Execution: AES and SHA process one data block at a time, increasing total latency.
2. Low Throughput: Limited parallelism restricts the number of packets processed in a given time window.
3. Power Inefficiency**:** Non-overlapping computation phases lead to higher energy consumption.
4. Static Routing: Rigid data paths result in delays and limit dynamic workload balancing.
5. Lack of Fine-Grain Timing Control: Inefficient scheduling leads to idle cycles in cores.

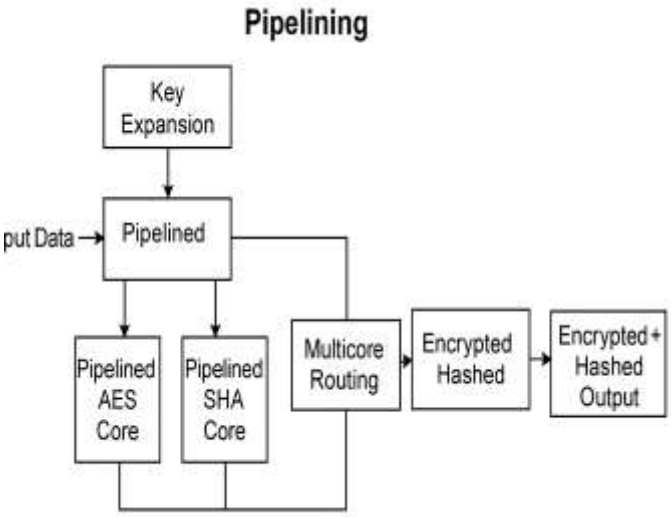
Optimization Strategies:

- Pipelining: Breaks down AES and SHA into multiple stages, enabling parallel processing across data blocks.
- Multicore Integration: Executes cryptographic operations concurrently using distributed cores.
- Dynamic Routing: Allows adaptive data flow across processing units, reducing congestion.
- Balanced Latency: Synchronizes AES and SHA delays to avoid bottlenecks in pipelined data flow.
- Clock Domain Adjustment: Fine-tunes timing for each stage to improve clock cycle utilization.

Mitigation via Vivado and Simulation Tools:

Vivado's high-level synthesis and floor planning tools allow designers to apply pipelining and routing strategies efficiently. RTL design combined with ModelSim simulation enables precise delay analysis and resource mapping before hardware deployment. Implementing the proposed pipeline architecture within Vivado's framework offers reduced latency, improved throughput (150% increase in packets processed), and power optimization without sacrificing correctness. Careful clock tuning, routing constraints, and functional verification further strengthen the robustness of the pipelined AES/SHA system within a reconfigurable FPGA-based multicore architecture.

2.2 Proposed Block Diagram



Block Diagram Components:

Input Data

- Generates round keys required for AES encryption and SHA hashing.
- Ensures synchronized and secure key scheduling across pipelined stages.

Key Expansion

- Performs the AES encryption algorithm across multiple stages in a pipelined manner.
- Increases throughput by allowing continuous processing of multiple data blocks.

Pipelining AES Core

- The main encryption module that executes the AES algorithm.
- It performs substitution, permutation, key addition, and other AES operations to encrypt the input data.

Pipelining SHA Core

- Implements SHA hashing in a staged pipeline to compute message digests efficiently.
- Operates concurrently with AES for parallel encryption and hashing.

Multicore Routing

- Directs processed data between cores and handles load balancing.
- Helps reduce latency and optimizes data flow in the pipelined structure.

Clock Jittering and Masking

- Introduces clock variations and data masking to resist side-channel attacks.
- Obfuscates power and timing signatures to prevent key leakage.

Encrypted + Hashed Output

- Final stage that combines AES and SHA results.
- Produces secure ciphertext and message digest outputs ready for transmission or storage.

2.3 Software used / IDE used :: MATLAB (**Version**: 1.1.0.0 (3.63 KB))

Xilinx Vivado Design Suite:
Used for RTL design, synthesis, floorplanning, and implementation of pipelined AES and SHA cryptographic modules on the FPGA platform.
ModelSim Simulator:
Employed for functional simulation and waveform verification of pipelined designs to validate timing, logic correctness, and data flow.
Xilinx Vivado High-Level Synthesis (HLS):
Used to translate high-level algorithmic descriptions of AES/SHA modules from C/C++ into HDL code for hardware implementation.
MATLAB (Optional):
Used for analyzing simulation results and modeling performance characteristics such as power consumption and latency under pipelined conditions.
Python (Optional):
Supports preprocessing or visualization of test outputs and simulation data for post-analysis of throughput and power behavior.
Xilinx IP Catalog:
Used to integrate custom and standard IP blocks like AXI interconnects, clocking wizards, and memory controllers into the processor system.
Power Analysis Utilities:
Custom power scripts or tools are used to evaluate the power efficiency and performance trade-offs introduced by pipelining strategies.

2.4 Practical setup

The practical implementation of the proposed pipelined AES and SHA cryptographic modules was carried out on a Xilinx Zynq-7000 FPGA development board, leveraging the Vivado Design Suite for design synthesis, implementation, and verification. The AES and SHA cores were designed using RTL in Verilog and pipelined through Vivado's High-Level Synthesis (HLS) tools for optimized performance. Functional correctness and timing accuracy were verified using ModelSim simulations prior to hardware deployment. The FPGA was programmed with the generated bitstream via a USB-JTAG interface connected to a host PC running Vivado. To analyze power consumption and side-channel resistance, power traces were captured using a digital oscilloscope connected across a shunt resistor in the FPGA's power supply line. Post-processing of these traces was performed using MATLAB and Python scripts implementing Test Vector Leakage Assessment (TVLA) to evaluate the effectiveness of introduced countermeasures such as clock jittering and data masking. The setup allowed for real-time monitoring of throughput, latency, and energy efficiency metrics, providing a comprehensive platform to validate both the security and performance improvements of the pipelined multicore cryptographic system.

2.4 Implementations:

1. Design and simulate pipelined AES and SHA modules using ModelSim for functional verification.
2. Implement the verified design in Vivado using RTL and HLS tools.
3. Synthesize, implement, and generate the FPGA bitstream.
4. Program FPGA via USB-JTAG.
5. Capture power traces with an oscilloscope and analyze leakage using MATLAB/Python scripts, applying clock jittering and masking countermeasures.

Results And Discussions -

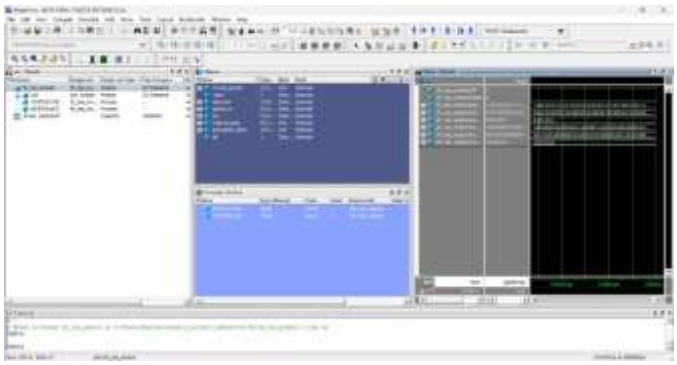


Fig 1 – Result

Output figure 1: simulation output using pipelining of AES and SHA for high performance encryption architecture.

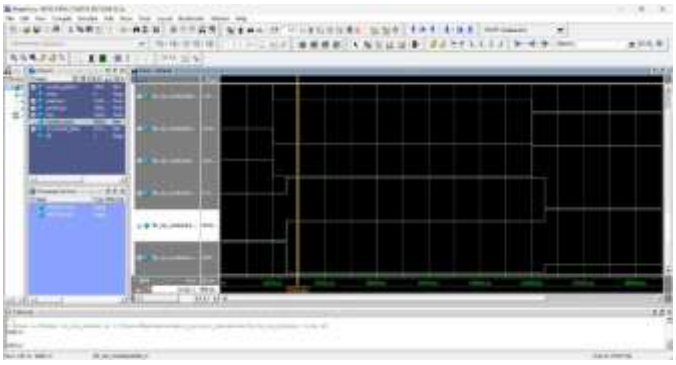


Fig 2- This shows the detailed output of data sets and number of packets per data and also the speed of data processing.

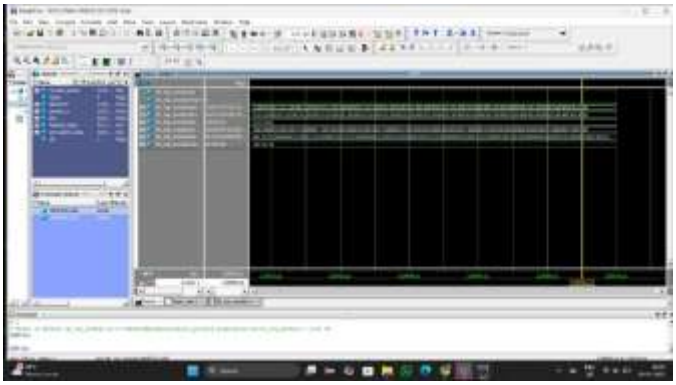


Fig 3 this shows the output of existing method where basic AES and SHA methodology is used to produce the result.

3.CONCLUSIONS

This project introduces a high-performance AES encryption architecture on FPGA, designed to optimize both speed and scalability by integrating pipelined processing stages with adaptive Network-on-Chip (NoC) routing. The AES algorithm was implemented using a multi-stage pipeline, allowing continuous processing of multiple data blocks to achieve significant throughput gains. Adaptive NoC routing was incorporated to enhance communication efficiency between AES processing elements by dynamically managing data traffic and reducing bottlenecks within the interconnect fabric. ModelSim was employed for functional simulation and verification of the pipelined AES cores, confirming the correctness and stability of the design under various operational scenarios. The architecture was synthesized using Xilinx Vivado, where timing analysis and resource utilization metrics demonstrated that the design meets stringent performance requirements with optimal FPGA resource efficiency. Further, the modular structure supports scalability, making it adaptable for future cryptographic systems with higher data demands or extended functionalities. Unlike traditional linear implementations, this project emphasizes parallelism and adaptability as key enablers for performance optimization in cryptographic hardware. In conclusion, the implementation effectively combines advanced architectural strategies with hardware-centric design to achieve a robust and high-speed AES encryption solution. This work contributes valuable insights into secure and efficient FPGA-based encryption systems for use in data-intensive domains such as secure IoT, high-speed networking, and real-time embedded applications.

ACKNOWLEDGEMENT

I would like to express our heartfelt appreciation to all those who contributed towards My research project titled “High-Performance AES Encryption Architecture on FPGA Using Pipelined Simulation and Adaptive NoC Routing**.”** The project has been a tremendous learning experience and would not have been possible without a great deal of support and guidance from a number of individuals.

I deeply grateful to our esteemed faculty mentors, Dr. Sonagiri China Venkateswarlu, Dr. V. Siva Nagaraju, and Ms. P. Ganga Bhavani, from the Department of Electronics and Communication Engineering at the Institute of Aeronautical Engineering (IARE).

Dr. Venkateswarlu, a highly regarded expert in Digital Speech Processing, has over 20 years of teaching experience. He has provided insightful academic assistance and support for the duration of our research work.

Dr. Siva Nagaraju, an esteemed researcher in Microwave Engineering who has been teaching for over 21 years, has provided us very useful and constructive feedback, and encouragement which greatly assisted us in refining our technical approach.

Ms. Ganga Bhavani, who is specializing in Systems and Signal Processing and also pursing her doctoral research, has been a consistent source of motivation, provided practical direction, and contributed a lot toward the successful implementation of our project.

I would also like to express My gratitude to our institution - Institute of Aeronautical Engineering for its resources and accommodating environment for My project. The access to technologies such as Python, TensorFlow, Keras and OpenCV allowed for the technical realization of our idea. I appreciate our fellow bachelor students for collaboration, their feedback, and moral support. Finally, I would like to extend My sincere thank you to My families and friends for their patience, encouragement, and faith in My abilities throughout this process.

REFERENCES

1. J.-P. Kaps, "High speed crypto processor for AES," *George Mason University*, 2006.
2. A. Hodjat and I. Verbauwhede, "A 21.54 Gbits/s fully pipelined AES processor on FPGA," in *Proc. 12th IEEE Symp. Field-Programmable Custom Computing Machines*, 2004, pp. 308–309.
3. L. Benini and G. De Micheli, "Networks on chips: A new SoC paradigm," *IEEE Computer*, vol. 35, no. 1, pp. 70–78, Jan. 2002.
4. T. Katashita and Y. Hayashi, "Secure AES circuit architecture against DPA with low cost and high performance on FPGA," in *Proc. IEEE 56th MWSCAS*, 2013, pp. 1171–1174.
5. Xilinx Inc., *Vivado Design Suite User Guide: High-Level Synthesis (UG902)*, 2020.
6. W. Stallings, *Cryptography and Network Security: Principles and Practice*, 7th ed. Pearson, 2016.
7. D. Singh, A. Dandapat, and B. Sahoo, "Design and implementation of high-performance pipelined AES

encryption on FPGA," *Microprocessors and Microsystems*, vol. 83, p. 104003, 2021.
8. Y. Wang, H. Lin, and Y. Chen, "Adaptive routing algorithms for Networks-on-Chip: A survey," *J. Syst. Archit.*, vol. 73, pp. 39–52, 2017.
9. A. J. Elbirt and C. Paar, "An FPGA implementation and performance evaluation of the AES block cipher candidate algorithm finalist Rijndael," in *Proc. 3rd AES Candidate Conf.*, 2000.

BIOGRAPHIES

Ballu Manikanta studying 3rd year department of Electronics And Communication Engineering at Institute Of Aeronautical Engineering ,Dundigal. He Published a Research Paper Recently at IJSREM as a part of academics He has a interest in IOT, VLSI and MICROCONTROLLERS.

Dr Sonagiri China Venkateswarlu professor in the Department of Electronics and Communication Engineering at the Institute of Aeronautical Engineering (IARE). He has more than 40 citations and paper publications across various publishing platforms, with 20 years of teaching experience, he can be contacted at email: **c.venkateswarlu@iare.ac.in**

Dr. V. Siva Nagaraju is a professor in the Department of Electronics and Communication Engineering at the Institute of Aeronautical Engineering (IARE). He has published multiple research papers in reputed journals and conferences, and his academic interests include electromagnetic theory, microwave engineering, and related areas. He can be contacted at email: **v.sivanagaraju@iare.ac.in**.

Ms. P. Ganga Bhavani is an Assistant Professor in the Department of Electronics and Communication Engineering at the Institute of Aeronautical Engineering (IARE).. She has contributed to the academic community through her teaching and continues to enhance her knowledge and skills through ongoing doctoral research. She can be contacted at email: **p.gangabhavani@iare.ac.in**.