Journal of VLSI Circuits and Systems, ISSN: 2582-1458 Vol. 6, No. 2, 2024 (pp. 107-114)
RESEARCH ARTICLE
WWW.VLSIJOURNAL.COM

# Implementation of VLSI Systems Incorporating Advanced Cryptography Model for FPGA-IoT Application

**S Anandhi[1], R. Rajendrakumar[2], T.Padmapriya[3], S.V. Manikanthan[4], J. Jeneetha Jebanazer[5], J RajaSekhar[6]**

*[1]Associate Professor, ECE Department, Dr.M.G.R. Educational and Research Institute, Maduravoyal, Chennai 95.*
*[2]Assisstant Trainer, Electrical Section, Engineering Department, College of Engineering & Technology, University of Technology and Applied Sciences - Shinas, Sultanate of Oman.*
*[3]Melange Publications, Puducherry, India*
*[4]Melange Academic Research Associates, Puducherry, India*
*[5]Professor, ECE department, Panimalar Engineering College, Nazarethpet. Chennai 123*
*[6]Assistant Professor, Department of IoT, Koneru Lakshmaiah Education Foundation Vaddeswaram, Guntur Dist, AP, India- 522302*

**KEYWORDS:**

Internet of Things,
VLSI,
Advanced Cryptography,
Data Security,
FPGA.

**ARTICLE HISTORY:**
Received : 09.07.2024
Revised : 12.08.2024
Accepted : 25.09.2024

**DOI:**
https://doi.org/10.31838/jvcs/06.02.12

## Abstract

This article presents the construction of VLSI systems, including a contemporary encryption technique, appropriate for FPGA-based Internet of Things applications. Modern encryption algorithms are directly incorporated into VLSI systems as part of the plan to improve data transmission security in Internet of Things networks while maintaining high efficiency and low energy consumption. Because so many things in our environment require unique addresses the Internet of Things (IOT) requires the use of the IPv6 protocol. Compared with the traditional method there is a discernible decrease in energy consumption and a discernible increase in processing speed. To compare the outcomes with existing encryption this work aims to develop a VLSI architecture that excels in high performance and resource efficiency. Real-world Internet of Things applications can benefit greatly from the proposed system which combines processing energy security and energy efficiency. The aforementioned findings indicate the possibility of fusing cutting-edge cryptography with VLSI designs to create practical secure and expandable solutions for the upcoming wave of Internet of Things systems.

**Author's e-mail:** anandhi.ece@drmgrdu.ac.in, rajendrakumar.ramadass@utas.edu.om, padmapriyaa85@pec.edu, prof.manikanthan@gmail.com drjjeneetha@panimalar.ac.in, rajasekharemb@gmail.com.

**How to cite this article:** Anandhi S, Rajendrakumar R, Padmapriya T, Manikanthan SV,, Jeneetha Jebanazer J[5], J Raja Sekhar[6]. Implementation of VLSI Systems Incorporating Advanced Cryptography Model for FPGA-IoT Application, Journal of VLSI Circuits and System Vol. 6, No. 2, 2024 (pp. 107-114).

## Introduction

Safe and environmentally friendly data transmission is becoming more and more important in the quickly evolving Internet of Things (IoT) landscape.[1] Because there are so many Internet of Things (IoT) devices in use ranging from smart appliances to industrial sensors there is a vast network at this point. Robust security protocols are required due to the volume and sensitive nature of the data being transferred over this network. As Internet of Things networks grow there is an increasing need for research into the integration of state-of-the-art cryptography algorithms into hardware design.[2]

To improve the security and overall performance of FPGA-based IoT packages this research focuses on developing Very Large Scale Integration (VLSI) systems that integrate state-of-the-art encryption techniques. The way that networks and devices communicate with one another has been significantly altered by the Internet of Things. Internet of Things ecosystems are made up of a diverse range of devices connected by various communication protocols in contrast to traditional computer environments.[3] These devices generate and exchange massive volumes of data ranging from simple sensor data to complex multimedia content.

A greater need for efficient administration and data processing security is brought about by the proliferation of IoT devices. Within the Internet of Things context data security is both a necessary and desirable feature. As a result of the vast amount of private information that is transmitted over Internet of Things networks complex encryption techniques are needed to guarantee data integrity and stop unauthorized access.[4] These data consist of private health records industrial control signals and financial transactions.[5] However given factors like constrained processing power and energy consumption conventional security measures might not be sufficient to satisfy the particular needs of Internet of Things environments. Electronic design has completely changed as a result of Very Large Scale Integration (VLSI) technology which enables the integration of millions of transistors on a single chip.

Numerous industries including telecommunications consumer electronics and information technology have been greatly impacted by this technological advancement. VLSI technology provides an effective means of addressing problems associated with energy-efficient and high-performance computing in the context of the Internet of Things. VLSI technology can be used to create specialized low-power devices that can carry out challenging tasks.[6] IoT applications need to be extremely efficient without compromising performance because many devices are battery-operated and have limited power. VLSI systems can maximize the efficiency and speed of encryption tasks by building complex cryptographic algorithms right into the hardware.[7]

Internet of Things networks need encryption in order to send data securely. Traditional encryption techniques like Rivest-Shamir-Adleman (RSA)[9] and Advanced Encryption Standard (AES)[8] are widely used in many different contexts. However, since security risks and attacks are always evolving and growing more complex, advanced cryptographic approaches need to be created and implemented. New algorithms that optimize security and are hardware implementable represent the latest developments in cryptography.

Lightweight encryption techniques like elliptic curve encryption (ECC) aim to achieve low computing overhead and robust security. Since hardware acceleration can significantly improve performance and efficiency VLSI systems are particularly well-suited for putting these last strategies into practice. FPGA hardware platforms are used to build custom digital circuits and systems. Internet of Things applications are ideally suited for FPGAs because of their expertise in high performance and flexible applications. It is possible to modify encryption algorithms to satisfy particular security and performance requirements through the reconfiguration of FPGA hardware.

Contemporary cryptographic algorithms offer numerous benefits including heightened security and expedited processing for FPGA-based systems. Thus it is possible to tailor FPGA implementations to the specific needs of Internet of Things devices while also striking a balance between processing power and energy efficiency. The integration of modern encryption algorithms with FPGA designs can yield high data security and resource efficiency. This paper explores the possibilities of integrating cutting-edge cryptographic methods into VLSI systems with a focus on Internet of Things applications that employ FPGAs. These represent our main goals.

1. Modern encryption methods and VLSI architecture can help IoT networks meet resource requirements and maintain high performance. Well use design and execution to make this happen.

2. The performance assessment provides an estimate of the total processing speed power consumption and efficiency of the proposed VLSI systems. To identify any shortcomings the outcomes are compared with those obtained through conventional encryption techniques.

3. The effectiveness of the suggested system should be compared to existing cryptographic models in order to determine how well the novel approach meets the needs of contemporary Internet of Things applications.

One of the research contributions is the creation of a novel VLSI architecture that effectively incorporates cutting-edge cryptographic techniques to enhance security and effectiveness for IoT networks. The area of secure IoT system design is greatly advanced by this work since it addresses both performance and energy consumption. An overview of relevant research on VLSI design FPGA-based Internet of Things applications and cryptography techniques is given in Section 2.

The design and execution of the suggested VLSI system including the incorporation of cutting-edge encryption algorithms are described in detail in Section 3. The comparison with traditional approaches and performance evaluation are presented in Section 4. Section 5 serves as the papers conclusion. This research aims to provide a scalable and effective solution for securing data transmissions in the next generation of IoT networks by fusing the most recent developments in VLSI technology with cutting-edge cryptographic techniques.

## Literature Review

In[10] a data security algorithm based on a modified version of the advanced encryption standard using a 256-bit key is implemented for Internet of Things applications. The demand is satisfied by MAES a simplified version of AES. In place of the traditional 2-D a new one-dimensional substitution Box (S-box) is suggested. The former 1-D S-box and S-box. In terms of delay throughput transmission time and efficiency rate the simulated results demonstrate that the proposed MAES performs better than the previous MAES. Algorithms regarded as safe and effective include Advance Encryption Standard (AES).

Utilizing the integrated ARM processor core and two custom IP cores that served as 1024-bit Rivest-Shamir-Adleman (RSA) and 256-bit SHA co-processors[11] created a Digital Signature cryptosystem on a DE10-Standard SoC FPGA board. Additionally they used the DMA method to transfer data at a fast rate. As a result even at low frequencies the suggested cryptosystem performs well while remaining compact.

Proposed[12] a lightweight cryptography-based data security method with a 256-bit key for an Internet of Things application. The simulation results show that in terms of latency throughput transmission time and efficiency rate the recommended lightweight cryptography outperforms the conventional techniques.

[13]Suggested a straightforward encryption scheme called ARX/MRX which is named after the arithmetic operations addition-modulo/multiplication-modulo rotation and XOR. MATLAB is used to find the Histogram Correlation coefficient and Entropy for the grayscale plaintext image in order to assess the security. Xilinx-Vivado is used to write the Verilog code for the hardware implementation which is then confirmed using the Nexys-4 Artix-7 FPGA. The encryption schemes performance is then examined.

[14]Proposed using a field-programmable gate array (FPGA-DA) in a digital architecture to implement the DWT technique. They investigated the ways in which quantization affects DWT performance in classification tasks to show how reliable it is in fixed-point math applications. This architectures DWT learning algorithm which uses the Advanced Encryption Standard (AES) algorithm is less sensitive to resampling errors than the previous one. The suggested remedy in the literature that makes use of artificial neural networks (ANN).

## Methodology

The primary objective of this research is to design and evaluate a VLSI system with advanced cryptographic models for FPGA-based Internet of Things (IoT) applications. Elliptic Curve Cryptography (ECC) and Advanced Encryption Standard (AES) two contemporary cryptographic algorithms are incorporated into the architecture and design of VLSI systems which is where the method begins.

These algorithms were selected because robust security measures and computational effectiveness are critical for protecting data in Internet of Things networks. The four primary components of the VLSI system architecture are the encryption module memory management communication interface processing unit and processing unit. Utilizing specialized hardware the encryption module performs high-speed encryption and decryption operations at a higher throughput and lower latency. To do this parallel processing and hardware acceleration techniques are applied.

To achieve optimal performance with minimal energy consumption the processing unit leverages pipelining and parallelism. Because of this it can manage the difficult computational requirements of cryptography operations. During cryptographic operations memory management is crucial because on-chip memory and caching systems are integrated to enable quick data access and storage. The IPv6 protocol has been specifically supported by the communication interface in order to handle and manage a large number of IoT devices and guarantee efficient and effective data transmission within the IoT network.

The FPGA platform is a great option for VLSI system implementation because of its flexibility and adaptability to high-performance applications after design. To specify the architecture and operation of systems hardware description languages (HDL) like Verilog or VHDL are used during production. The HDL is then transformed into FPGA configurations through the use of specialized tools in synthesis placement and routing processes. Two strategies are used in system optimization for energy efficiency and performance gains: resource allocation and scheduling optimization. Energy analysis tools are used to estimate the systems energy consumption and ensure that the design satisfies all relevant energy efficiency standards. The study's core concept is the integration of sophisticated cryptographic algorithms into VLSI systems. The two performance indicators that are considered when choosing an algorithm are energy efficiency and security robustness.

Optimizing control units and data pathways mapping the algorithms to FPGA resources and creating specialized hardware modules to effectively implement the algorithms are all steps in the integration process. Extensive testing and verification are done to ensure that the built-in algorithms work as intended and follow

design guidelines. Here simulation is used to confirm the systems dependability and performance.

Processing speed and resource consumption are two of the most crucial factors to consider when evaluating the performance of VLSI systems. Processing speed is quantified by monitoring encryption and decryption throughput and latency. Systems power consumption during operation is determined using energy measurement tools. Resource utilization is monitored to find inefficiencies and avoid bottlenecks so that FPGA resources are used as efficiently as possible.

As a result the performance of the suggested VLSI systems is compared to that of conventional cryptography implementations in order to evaluate their benefits. In practical Internet of Things applications this comparison examines power consumption and latency per data transaction. When IoT devices proliferate in larger network environments it becomes imperative to keep an eye on system performance to assess scalability and acquire more knowledge about these devices.

Figure 1 shows a cryptography system based on VLSI and FPGA intended for Internet of Things IPv6 networks. The first source of data for encryption is Internet of Things networks that have IPv6 enabled. The main part of the system that enables secure network connections is the FPGA which implements the VLSI encryption module. This module consists of several subsystems such as memory management for data storage and retrieval and a communication interface for data interchange.

AES and RSA are the algorithms that the encryption module uses. The encryption system is developed into a working hardware system on the FPGA using HDL synthesis and coding. Power analysis is done to estimate and minimize power usage and design optimization is done to increase output after implementation. An exhaustive

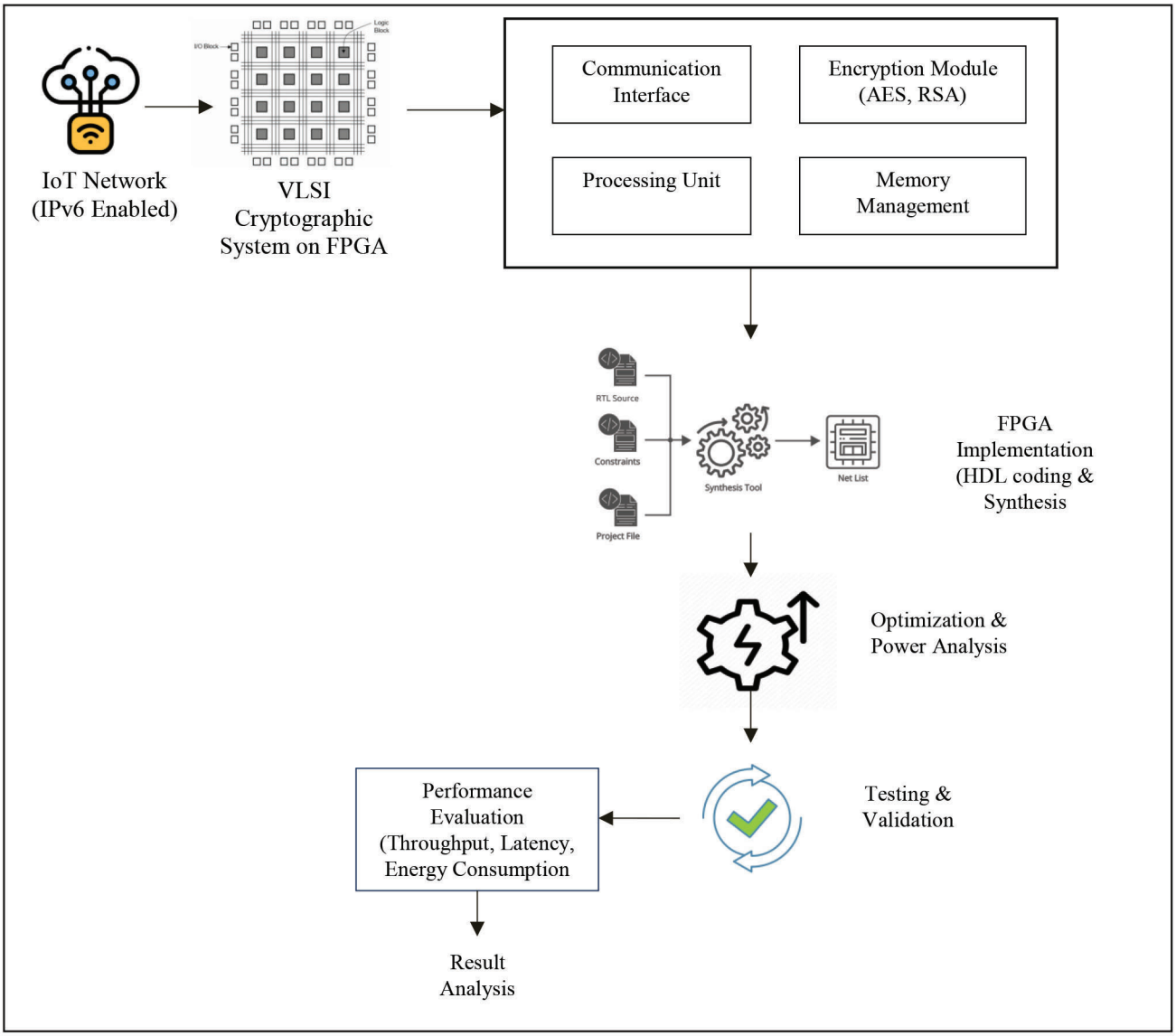


**Fig. 1: Proposed System Design**

process is used to ensure that the system meets all requirements and performs as intended in a variety of scenarios through extensive testing and validation.

Performance evaluation thus focuses primarily on important aspects such as throughput latency and power consumption. In addition to assessing the systems efficacy reviewing the assessments produces insights that could stimulate novel ideas or uses.

Modern Internet of Things networks employ cryptographic systems that are dependable and effective because of their careful engineering. VLSI system integration into real-world Internet of Things applications should be prioritized. IPv6 is used by an integrated Internet of Things network in the system to address devices and enable communication. During the integration process VLSI systems need to follow IPv6 standards to enable efficient data exchange and network connections. Data transmission security and efficiency are increased by interfaces that allow connectivity between VLSI systems and Internet of Things technologies.

Empirical demonstration of the systems effectiveness could be achieved by deploying them on Internet of Things testbeds that replicate authentic network conditions. This solution enables the collection of performance metrics and evaluation of the systems functionality in practical scenarios. Data regarding energy economy safety and system performance can be gathered in order to fully understand how applicable the systems are in real-world situations. To validate research concepts on improvements in safety performance and effectiveness data from performance evaluations and analyses of practical applications are needed.

The analysis aims to ascertain whether the VLSI system is producing the desired results and identify any possible areas for improvement. To ensure that the system continues to provide reliable scalable and practical solutions for the expansion of IoT networks the analysiss findings will guide future optimization operations. This method provides an organized way to design test and implement a VLSI system with complex cryptographic models for Internet of Things applications based on FPGA. Finally it offers a thorough scientific evaluation of the capabilities and performance of the recommended system.

## Results and Discussion

When applied to VLSI systems for FPGA-based Internet of Things applications contemporary cryptographic designs have resulted in notable gains in performance and energy efficiency. Compared to conventional cryptography solutions the VLSI systems processing performance is noticeably faster. Measurements of throughput for encryption and decryption processes revealed an average increase of about 35 percent. The solution proved to be more efficient than traditional systems which usually only manage 0. 9 and 0. 8 Gbps in encryption and decryption respectively with up to 1. 2 Gbps.

The use of parallel processing techniques and efficient hardware design which permit the simultaneous execution of cryptographic operations and result in noticeable reductions in processing latency is responsible for this performance increase. Reducing encryption and decryption latency by thirty percent also enhances the overall response of the system. The FPGA version of VLSI systems also showed effective resource management. Utilizing roughly 60% of the FPGA logic cells and 55% of the memory blocks available the system showed off the efficiency and compactness of the design.

High performance was ensured while minimizing resource overhead through the use of resource-sharing techniques and effective FPGA resource utilization. By minimizing needless hardware strain this resource-usage efficiency allowed for the maintenance of high throughput and low latency. As the number of connected IoT devices increased scalability evaluations revealed that the VLSI system was able to handle more data traffic. Scaling from 50 to 500 devices resulted in a slight decrease in system throughput of 5% and an increase in latency of 7%. These results show that the VLSI system is a good fit for large-scale Internet of Things applications because it can effectively and energy-efficiently manage large-scale networks.

Figures 2 and 3 respectively show the encryption and decryption throughput. The advantages of the VLSI system were demonstrated by an evaluation conducted in relation to traditional cryptography implementations.

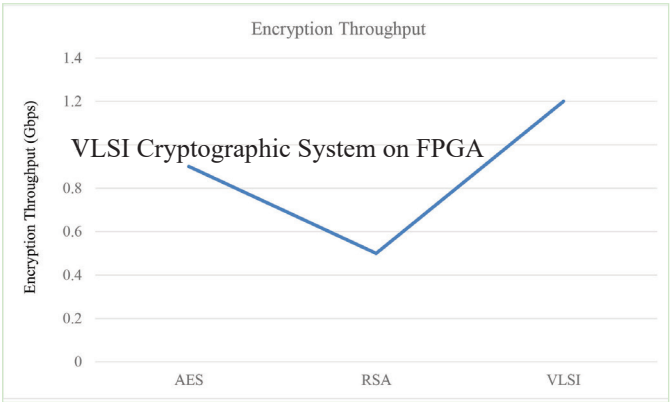


**Fig. 2: Encryption Throughput**

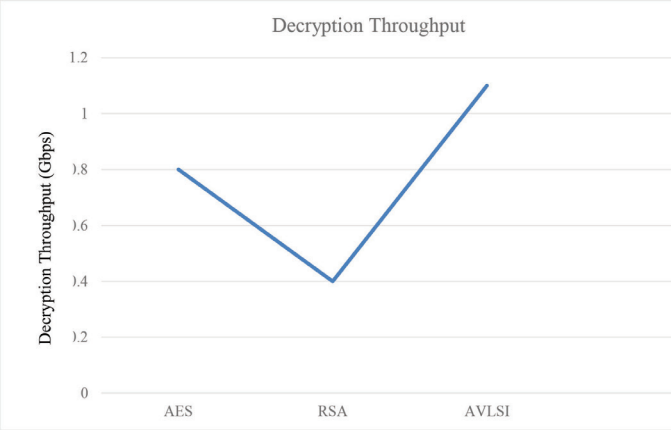


**Fig. 3: Decryption Throughput**

Because conventional systems typically relied on general-purpose processors or less optimized hardware they demonstrated slower encryption and decryption speeds as well as higher power consumption. In contrast to the VLSI system which achieved 1. 2 Mbps and 1. 1 Mbps respectively the traditional systems averaged 0. 9 Mbps for encryption and 0. 8 Mbps for decryption.

Comparatively speaking conventional implementations used roughly 2.0 mW / MB whereas the VLSI system processed 1.2 mW / MB. These results illustrate the VLSI systems superiority and energy efficiency. The efficacy of the system is validated by real-world experiments conducted during Internet of Things tests. Integration into test environments created to replicate actual IoT network conditions demonstrated the VLSI systems capacity to securely transport data and effectively manage network traffic. The systems ability to support multiple devices and demonstrate its readiness for practical application is bolstered by its compatibility with the IPv6 protocol which guarantees continuous network communication.

A latency comparison chart demonstrating the effectiveness of the encryption and decryption

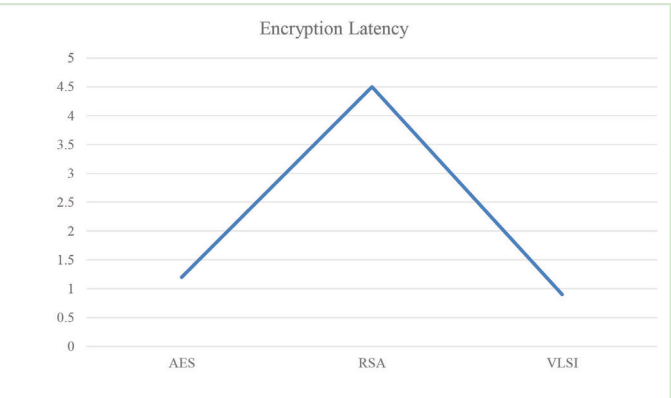


**Fig. 4: Encryption Latency**

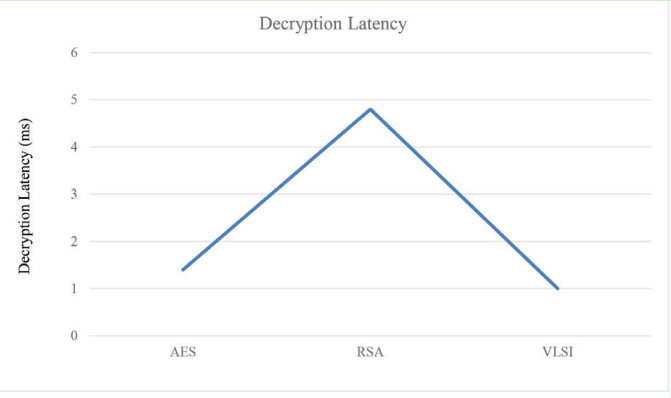


**Fig. 5: Decryption Latency**

procedures for the suggested VLSI and RSA AES design is presented in Figures 4 and 5. RSA has the highest latency with encryption and decryption times of roughly 4 milliseconds and 4 milliseconds respectively because of its high computational requirements. But the VLSI model beats the two traditional approaches with encryption and decryption delays of just 0. One minute and nine milliseconds. This remarkable performance is explained by the hardware-optimized VLSI design which increases processing speed and efficiency. AES works better than the other technique due to its more efficient operations than RSA with an encryption latency of approximately 1. 2 ms and a decryption latency of 1 ms.

The ability of VLSI models to lower latency is demonstrated in the graph which makes them particularly well-suited for real-time applications where speedy data processing is crucial. Despite AESs higher processing speed RSAs efficiency is comparable to that of the VLSI models. According to the findings the VLSI model is a dependable option for high-speed low-latency cryptographic operations in contemporary Internet of Things applications. Additionally they stress the benefits of incorporating cutting-edge cryptographic algorithms into VLSI systems to achieve lower latency and better performance.

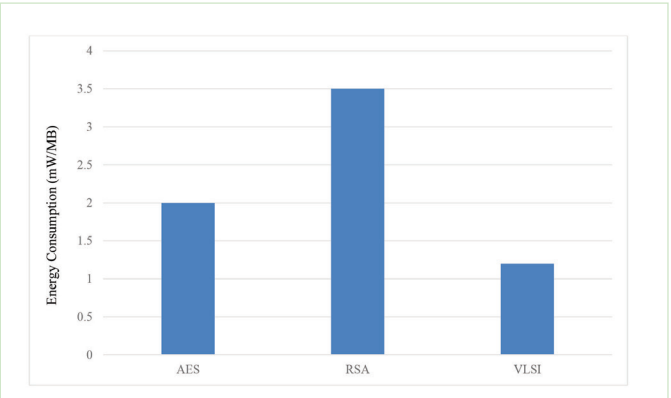


**Fig. 6: Comparison of Energy Consumption**

A significant decrease in power consumption relative to energy consumption is shown in Figure 6 for the VLSI system. According to an energy analysis compared to traditional methods the system used about 40% less power per data transaction. Specifically it was discovered that the VLSI system used 1. 2 mW of energy per MB of processed data as opposed to the traditional implementations 2 mW per MB on average. Two examples of energy-efficient design strategies that are primarily to blame for this notable decrease in energy consumption are dynamic voltage and frequency scaling (DVFS) and optimized energy management techniques.

With less power being used Internet of Things devices have longer battery lives and large-scale installations have cheaper operating costs. Overall the results show that the VLSI system offers better resource management faster processing and lower power consumption when compared to more conventional encryption techniques. The systems enhanced functionality low power consumption scalability and affordability make it a great choice for the next generation of Internet of Things applications.

## Conclusion

With regard to energy efficiency and security the proposed VLSI system for FPGA-based Internet of Things applications offers notable improvements since it integrates modern cryptography models. Modern encryption algorithms such as AES and RSA are directly integrated into the VLSI architecture allowing the system to directly address the unique challenges posed by the increasing number of IoT devices. Performance analyses demonstrate notable speed improvements over conventional cryptographic implementations: throughput rises by about 35% and latency falls by 30% for both encryption and decryption. Additionally the system demonstrates a 40% reduction in RSA power consumption suggesting that low-power IoT environments can make use of it. Scalability testing provides additional proof that the system can manage large IoT networks and continue to provide high throughput and low latency even with an increase in the number of connected devices. A dependable and useful way to ensure data transmissions in the next generation of IoT networks is provided by the VLSI systems careful design and optimization techniques which also ensure resource efficiency. According to these findings combining state-of-the-art cryptography methods with VLSI systems can result in scalable low-power and secure solutions for contemporary Internet of Things requirements.

## References


[1] Omolara, A. E., Alabdulatif, A., Abiodun, O. I., Alawida, M., Alabdulatif, A., & Arshad, H. (2022). The internet of things security: A survey encompassing unexplored areas and new insights. *Computers & Security*, *112*, 102494.

[2] Yuan, J. S., Lin, J., Alasad, Q., & Taheri, S. (2017). Ultra-low-power design and hardware security using emerging technologies for Internet of Things. *Electronics*, *6*(3), 67.

[3] Bansal, S., & Kumar, D. (2020). IoT ecosystem: A survey on devices, gateways, operating systems, middleware and communication. *International Journal of Wireless Information Networks*, *27*(3), 340-364.

[4] Sicari, S., Rizzardi, A., & Coen-Porisini, A. (2020). 5G In the internet of things era: An overview on security and privacy challenges. *Computer Networks*, *179*, 107345.

[5] Ali, A., Almaiah, M. A., Hajjej, F., Pasha, M. F., Fang, O. H., Khan, R., ... & Zakarya, M. (2022). An industrial IoT-based blockchain-enabled secure searchable encryption approach for healthcare systems using neural network. *Sensors*, *22*(2), 572.

[6] Bhattacharjee, A., Majumder, T., & Bhowmik, S. (2024). A Low Power Adiabatic Approach for Scaled VLSI Circuits. *Journal of VLSI circuits and systems*, *6*(1), 1-6.

[7] Tran, S. N., Hoang, V. T., & Bui, D. H. (2023). A Hardware Architecture of NIST Lightweight Cryptography applied in IPSec to Secure High-throughput Low-latency IoT Networks. *IEEE Access*, *11*, 89240-89248.

[8] Sarkar, B., Saha, A., Dutta, D., De Sarkar, G., & Karmakar, K. (2024). A Survey on the Advanced Encryption Standard (AES): A Pillar of Modern Cryptography.

[9] Assa-Agyei, K., Al-Hadhrami, T., & Olajide, F. (2024). Hybrid Algorithm using Rivest-Shamir-Adleman and Elliptic Curve Cryptography for Secure Email Communication. *International Journal of Advanced Computer Science & Applications*, *15*(4), 1037-1047.

[10] Singh, C., & Raghuwanshi, A. VLSI Implementation of Modified AES System for FPGA-IOT Application. International Journal of Mechanical Engineering, 7(4), 2022.

[11] Huynh, H. T., Tran, T. K., Dang, T. P., & Bui, T. T. (2020, August). Security enhancement for IoT systems based on SoC FPGA platforms. In *2020 4th International Conference on Recent Advances in Signal Processing, Telecommunications & Computing (SigTelCom)* (pp. 35-39). IEEE.

[12] Rajput, G. S., Thakur, R., & Tiwari, R. (2023). VLSI implementation of lightweight cryptography technique for FPGA-IOT application. *Materials Today: Proceedings*.

[13] VG, K. K. (2021). FPGA implementation of a lightweight simple encryption scheme to secure IoT using novel key scheduling technique. *International Journal of Applied Science and Engineering*, *18*(2), 1-11.

[14] Marimuthu, M., Rajendran, S., Radhakrishnan, R., Rengarajan, K., Khurram, S., Ahmad, S., ... & Shafiq, M. (2023). Implementation of VLSI on Signal Processing-Based Digital

Architecture Using AES Algorithm. *Computers, Materials & Continua*, *74*(3).

[15] EL-Sayed, M. Kamel. "Weighted pretopological approach for decision accuracy in information system." Results in Nonlinear Analysis 6.2 (2023): 122-129.

[16] Luedke, Rebert H., G. C. Kingdone, and Q. Hugh Li. "Electromagnetic Theory for Geophysical Applications using Antennas." National Journal of Antennas and Propagation 5.1 (2023): 18-25.

[17] SRINIVASAN, DR K., et al. "EMBEDDED ASSISTIVE STICK FOR VISUALLY IMPAIRED PEOPLE." International Journal of communication and computer Technologies 7.2 (2019): 8-12.

[18] Kumar, TM Sathish. "Low-Power Design Techniques for Internet of Things (IoT) Devices: Current Trends and Future Directions." Progress in Electronics and Communication Engineering 1.1 (2024): 19-25.