International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347 - 6435 (Online) Volume 13, Issue 02, February 2024)

Review of Area-Efficient Nano-AES Implementation for Internet-of-Things Devices

[1]Sarvesh Kumar Rai, [2]Dr Anshuj Jain

[1]Research Scholar, Dept. of Electronics and Communication Engineering, SCOPE College of Engineering, Bhopal, India,
[2]Associate Professor & HOD, Dept. of Electronics and Communication Engineering, SCOPE College of Engineering, Bhopal, India

***Abstract*— With the widespread adoption of Internet-of-Things (IoT) devices, there is a growing need for secure communication and data encryption in resource-constrained environments. Advanced Encryption Standard (AES) is a widely used symmetric encryption algorithm that ensures confidentiality and integrity of data. However, the implementation of AES on IoT devices is challenging due to their limited computational resources and power constraints. Therefore, there is a need for area-efficient nano-AES implementations specifically designed for IoT devices. This paper presents a comprehensive review of area-efficient nano-AES implementations for IoT devices. It begins by discussing the key challenges in implementing AES on resource-constrained devices, including limited memory, low processing power, and energy constraints. Various techniques to overcome these challenges are then explored, including lightweight and compact designs, efficient key scheduling algorithms, and optimized hardware architectures.**

***Keywords*— Encryption, Security, Internet of Things (IoT), Privacy.**

I. Introduction

The development of IoT by utilizing the new form of IP address (IPv6), which goes past the constraints of IPv4, will change the universe of Web by giving the network to a tremendous number of keen associated gadgets close to 70 billion, or considerably more. Prospering this innovation has been called as the Second Economy or the Modern Web revolution. It will create an enormous market with different administrations, and the extent of this market is assessed in the trillions of dollars. This market is a promising plan to be effective, anyway just if the security viewpoints get into record before this tremendous procedure begins to be actualized generally.

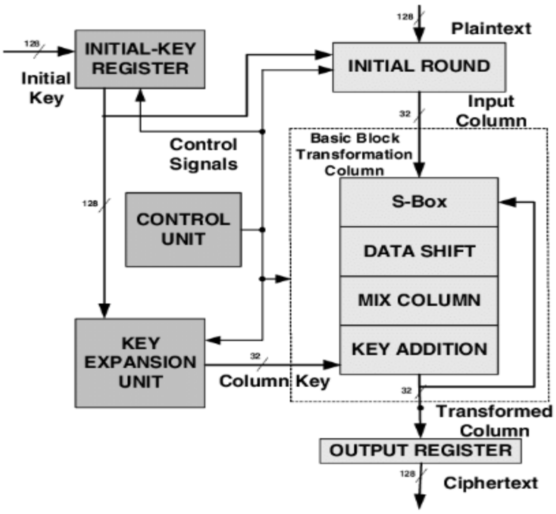

Figure 1: AES block diagram

The IoT's anyplace, anything, whenever nature could undoubtedly change these points of interest into disservices, if security viewpoints would not be given enough. For instance, if anyone can approach any close to home administrations and data, or if the data of an extensive variety of individuals can be come to by nature consequently, the IoT would not have a dependable situation. Multimedia data (text, audio, image, animation and video) have been widely used in the past few years for advanced digital content transmission. With the network technology focusing on Internet of Things (IoT) nowadays, the security of the multimedia content has raised researchers' concerns. The exchange of digital data over a network has exposed the multimedia data to various kinds of abuse such as Brute-Force attacks, unauthorized access, and network hacking. Therefore, the system must be safeguarded with an efficient media-aware security framework such as encryption methods that make use of standard symmetric encryption algorithms, which will be responsible for ensuring the security of the multimedia data.

For the encryption of electronic data, one of the most prominent cryptographic algorithms is the Advanced Encryption Standard algorithm. The Advanced Encryption Standard (AES) has been lately accepted as the symmetric cryptography standard for confidential data transmission. However, the natural and malicious injected faults reduce its reliability and may cause confidential information leakage. The review covers a range of area-efficient nano-AES implementations proposed in recent years, highlighting their strengths and limitations. These implementations utilize techniques such as algorithmic optimizations, hardware sharing, and reduced memory footprints to achieve efficient and compact designs. The performance metrics considered in the review include area utilization, power consumption, and throughput.

Additionally, the paper discusses the security implications of area-efficient nano-AES implementations and the trade-offs between security and efficiency. It addresses the potential vulnerabilities and attacks associated with lightweight designs and provide insights into mitigating these risks.

Furthermore, the review identifies future research directions and emerging trends in the field of area-efficient nano-AES implementations for IoT devices. It discusses the integration of hardware and software optimizations, the exploration of new cryptographic algorithms, and the utilization of emerging technologies such as reconfigurable hardware and machine learning.

II. LITERATURE SURVEY

K. Shahbazi et. al., [1] presented work carries out a Very Large Scale Integration (VLSI) implementation of the Advanced Encryption Standard (AES) symmetric cipher to investigate for its best-suited architecture for IoT applications. Standard architectures, such as, rolling, unrolling and combinational were examined. S-box, which forms the core of AES was designed using composite field arithmetic and an optimized form was used in each architecture design to improve hardware efficiency. The design, verification and RTL synthesis of the algorithm was done using Xilinx Vivado 2018.3 simulator. Stringent area and power requirements being the prior criteria for IoT devices, the rolled architecture turned out to be the favorite candidate upon analysis of the result.

A. R. Chowdhury et al.,[2] Recently IoT devices are dominating the world by providing it's versatile functionality and real-time data communication. Apart from versatile functionality of IoT devices, they are very low-battery powered, small and sophisticated, and experience lots of challenges due to unsafe communication medium. It is present MAES, a lightweight version of Advanced Encryption Standard (AES) which meets the demand. A new 1-dimensional Substitution Box is proposed by formulating a novel equation for constructing a square matrix in affine transformation phase of MAES. Efficiency rate of MAES is around 18.35% in terms of packet transmission.

M. Xie et al.,[3] In this work, author propose a fast and efficient AES in-memory (AIM) implementation, to encrypt the whole/part of the memory only when it is necessary. Rather than adding extra processing elements to the cost-sensitive memory, we take advantage of NVM's intrinsic logic operation capability to implement the AES algorithm. We leverage the benefits (large internal bandwidth and dramatic data movement reduction) offered by the in-memory computing architecture to address the challenges of the bandwidth intensive encryption application. Embracing the massive parallelism inside the memory, AIM outperforms existing mechanisms with higher throughput yet lower energy consumption.

D. Bui et al.,[4] In this work, it is present propsoed hardware optimization strategies for AES for high-speed ultralow-power ultralow-energy IoT applications with multiple levels of security. Our design supports multiple security levels through different key sizes, power and energy optimization for both data path and key expansion. The estimated power results show that our implementation may achieve an energy per bit comparable with the lightweight standardized algorithm PRESENT of less than 1 pJ/b at 10 MHz at 0.6 V with throughput of 28 Mb/s in ST FDSOI 28-nm technology.

S. Chen et al.,[5] presented a very large-scale integration (VLSI) circuit design of a micro control unit (MCU) for wireless body sensor networks (WBSNs) in cost-intention. The proposed MCU design consists of an asynchronous interface, a multisensor controller, a register bank, a hardware-shared filter, a lossless compressor, an encryption encoder, an error correct coding (ECC) circuit, a universal asynchronous receiver/transmitter interface, a power management, and a

QRS complex detector. A hardware-sharing technique was added to reduce the silicon area of a hardware-shared filter and provided functions in terms of high-pass, low-pass, and band-pass filters according to the uses of various body signals.

A. Jabbar et al.,[6] presents security architecture is designed that secures the data using encryption/decryption algorithm where the proposed algorithm is a hybrid encryption algorithm that uses the concept of EC-RSA, AES algorithm and Blowfish algorithm along with SHA-256 for auditing purpose. Presented experiment results show that the proposed concept is reasonable, it enhancing efficiency about 40% in terms of execution time i.e. encryption as well as decryption time and security and providing confidentiality of cloud data at could end.

Q. Wu et al.,[7] Broadcast encryption (BE) schemes allow a sender to securely broadcast to any subset of members but require a trusted party to distribute decryption keys. Group key agreement (GKA) protocols enable a group of members to negotiate a common encryption key via open networks so that only the group members can decrypt the cipher texts encrypted under the shared encryption key, but a sender cannot exclude any particular member from decrypting the cipher texts. In this work, we bridge these two notions with a hybrid primitive referred to as contributory broadcast encryption (ConBE).

A. Moradi et al.,[8] In this work. The attack is based on an also recently published correlation collision attack, which avoids the need for a hypothetical timing model for the underlying combinational circuit to recover the secret materials. The target platforms of our proposed attack are 14 AES ASIC cores of the SASEBO LSI chips in three different process technologies, 13 nm, 90 nm, and 65 nm. Successfully breaking all cores including the DPA-protected and fault attack protected cores indicates the strength of the attack.

B. Liu et al.,[9] By exploring different granularities of data-level and task-level parallelism, we map 16 implementations of an Advanced Encryption Standard (AES) cipher with both online and offline key expansion on a fine-grained many-core system. The smallest design utilizes only six cores for offline key expansion and eight cores for online key expansion, while the largest requires 107 and 137 cores, respectively. In comparison with published AES cipher implementations on general purpose processors, our design has 3.5-15.6 times higher throughput per unit of chip area and 8.2-18.1 times higher energy efficiency.

M. M. Wong et al.,[10] In this work, we derive three novel composite field arithmetic AES S-boxes of the field GF(((22)2)2). The best construction is selected after a sequence of algorithmic and architectural optimization processes. Furthermore, for each composite field constructions, there exists eight possible isomorphic mappings. Therefore, after the exploitation of a new common subexpression elimination algorithm, the isomorphic mapping that results in the minimal implementation area cost is chosen. High throughput hardware implementations of our proposed CFA AES S-boxes are reported towards the end of this work.

III. ADVANCE ENCRYPTION STANDARD CONSTRAINT

AES is the short form of Advanced Encryption Standard.

• It is FIPS approved cryptographic algorithm used to protect electronic data.

• It is symmetric block cipher which can encrypt and decrypt information.

• Encryption part converts data into cipher text form while decryption part converts cipher text into text form of data.

• AES algorithm used different keys 128/192/256 bits in order to encrypt and decrypt data in blocks of 128 bits.

• AES is implemented in both hardware and software to protect digital information in various forms data, voice, video etc. from attacks or eavesdropping.

AES is slower than symmetric encryption. Therefore it is in general just used to encrypt a symmetric key that is used to encrypt the rest of the message. The main disadvantage of using a shared key in encryption is that you cannot use it to ensure non-repudiation. Every block is always encrypted in the same way.

- Hard to implement with software.
- AES in counter mode is complex to implement in software taking both performance and security into considerations.

IV. DIFFERENT SECURITY APPROACHES

A. Privacy preserving

Privacy preservation in data mining is an important concept, because when the data is transferred or communicated between different parties then it's compulsory to provide security to that data so that other parties do not know what data is communicated between original parties. Preserving in data mining means hiding output knowledge of data mining by using several methods when this output data is valuable and private. Mainly two techniques are used for this one is Input privacy in which data is manipulated by using different techniques and other one is the output privacy in which data is altered in order to hide the rules.

B. ID Cryptography

Identity-based cryptography is a type of public-key cryptography in which a publicly known string representing an individual or organization is used as a public key. The public string could include an email address, domain name, or a physical IP address. This approach allowed users to verify digital signatures using only public information such as the user's identifier. Under Shamir's scheme, a trusted third party would deliver the private key to the user after verification of the user's identity, with verification essentially the same as that required for issuing a certificate in a typical PKI.

C. Ad-Dissemination

Dissemination takes on the theory of the traditional view of communication, which involves a sender and receiver. The traditional communication view point is broken down into a sender sending information, and receiver collecting the information processing it and sending information back, like a telephone line.

D. Token Based

Token-based confirmation plans, for example, Pledge 2 and OpenID Interface Combined Validation give helpful options in contrast to shared insider facts and testaments, and furthermore take into consideration the presentation of far reaching strategy controls connected to IoT get to necessities. Testament based confirmation in examination with shared mystery validation is progressively useful with vast number of gadgets, on the grounds that the overhead about dealing with the insider facts ends up huge for countless. Testament based verification utilizes deviated calculations and manages the handling of authentications

C. Frame-work

While the broadly useful key trades are security arrangements at the Web space, TCP/IP security conventions are one of the essential parts of structuring IP-based IoT security arrangements. Numerous conventions, for example, IKEv2/IPsec, TLS/SSL, DTLS, HIP, PANA, and EAP are conceivable arrangements in the 6LoWPAN and Center IETF working gatherings to give a progressively secure IoT information transmission

V. CONCLUSION

This paper present the literature survey and study of security algorithms for high speed and internet of things application and also introduced briefly the main ideas of IoT and called attention to the significance of having a protected structure for this new encouraging innovation. We went over the present difficulties related with giving protection which is the best basic segment, on the grounds that without enough security. Secondly different security techniques discussed and compare their performance. Also discuss existing AES algorithm studied and analyzed well to promote the performance of the encryption methods also to ensure the security proceedings. Therefore AES has many advantages but if it will use IOT application then give more delay and consume large area and more power. In future it can be modified and design MAES sothat requirement of security in IOT application can be fulfill.

REFERENCES

1. K. Shahbazi and S. -B. Ko, "Area-Efficient Nano-AES Implementation for Internet-of-Things Devices," in IEEE Transactions on Very Large Scale Integration (VLSI) Systems, vol. 29, no. 1, pp. 136-148, Jan. 2021, doi: 10.1109/TVLSI.2020.3033928.

2. A. R. Chowdhury, J. Mahmud, A. R. M. Kamal and M. A. Hamid, "MAES: Modified advanced encryption standard for resource constraint environments," *2018 IEEE Sensors Applications Symposium (SAS)*, Seoul, 2018, pp. 1-6
3. M. Xie, S. Li, A. O. Glova, J. Hu and Y. Xie, "Securing Emerging Nonvolatile Main Memory With Fast and Energy-Efficient AES In-Memory Implementation," in *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 26, no. 11, pp. 2443-2455, Nov. 2018.
4. D. Bui, D. Puschini, S. Bacles-Min, E. Beigné and X. Tran, "AES Datapath Optimization Strategies for Low-Power Low-Energy Multisecurity-Level Internet-of-Things Applications," in *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 25, no. 12, pp. 3281-3290, Dec. 2017.
5. S. Chen, M. Tuan, H. Lee and T. Lin, "VLSI Implementation of a Cost-Efficient Micro Control Unit With an Asymmetric Encryption for Wireless Body Sensor Networks," in IEEE Access, vol. 5, pp. 4077-4086, 2017, doi: 10.1109/ACCESS.2017.2679123.
6. A. Jabbar and P. U. Lilhore, "Design and Implementation of Hybrid EC-RSA Security Algorithm Based on TPA for Cloud Storage", IJOSCIENCE, vol. 3, no. 11, p. 6, Nov. 2017.https://doi.org/10.24113/ojsscience.v3i10.148
7. Q. Wu, B. Qin, L. Zhang, J. Domingo-Ferrer, O. Farràs and J. A. Manjón, "Contributory Broadcast Encryption with Efficient Encryption and Short Ciphertexts," in *IEEE Transactions on Computers*, vol. 65, no. 2, pp. 466-479, 1 Feb. 2016.
8. A. Moradi, O. Mischke and C. Paar, "One Attack to Rule Them All: Collision Timing Attack versus 42 AES ASIC Cores," in *IEEE Transactions on Computers*, vol. 62, no. 9, pp. 1786-1798, Sept. 2013.
9. B. Liu and B. M. Baas, "Parallel AES Encryption Engines for Many-Core Processor Arrays," in *IEEE Transactions on Computers*, vol. 62, no. 3, pp. 536-547, March 2013.
10. M. M. Wong, M. L. D. Wong, A. K. Nandi and I. Hijazin, "Construction of Optimum Composite Field Architecture for Compact High-Throughput AES S-Boxes," in *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 20, no. 6, pp. 1151-1155, June 2012.