Survey of Advance Encryption Standard Algorithm Based Security Approach

[1]Akash Kumar, [2]Dr. Bharti Chourasia
[1]M.Tech Scholar, [2]Professor & HOD
[1]Department of Electronics & Communication,
[1]RKDF Institute of Science & Technology Bhopal, India.

Abstract : Security is key parameter of communication between or with the internet of things. A symmetric block cipher that was established by the U.S. National Institute of Standards and Technology (NIST). However, some of the challenges arising from the use of this algorithm are computational overhead, use of a fixed S-Box and pattern problems, which occur when handling more complex multimedia data such as text, image and video. Many researchers have carried out research aiming at improving the algorithm's performance. This paper summarizes the various research work based on Advance Encryption Standard algorithms and observed some constraint using in internet of things application.

IndexTerms – AES, NIST, Internet of Things (IoT), security.

I. INTRODUCTION

The internet of things (IoT) is the system of gadgets, vehicles, and home apparatuses that contain hardware, programming, actuators, and availability which enables these things to interface, collaborate and trade information. IoT includes expanding internet network past standard gadgets, for example, work areas, workstations, cell phones and tablets, to any scope of customarily stupid or non-web empowered physical gadgets and ordinary items. Inserted with innovation, these gadgets can convey and communicate over the Web, and they can be remotely observed and controlled. 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. In this paper, study concurrent fault detection schemes for reaching a reliable AES architecture. Specifically,

As networking technology advances, the gap between network bandwidth and network processing power widens. Information security issues add to the need for developing high-performance network processing hardware, particularly that for real-time processing of cryptographic algorithms.

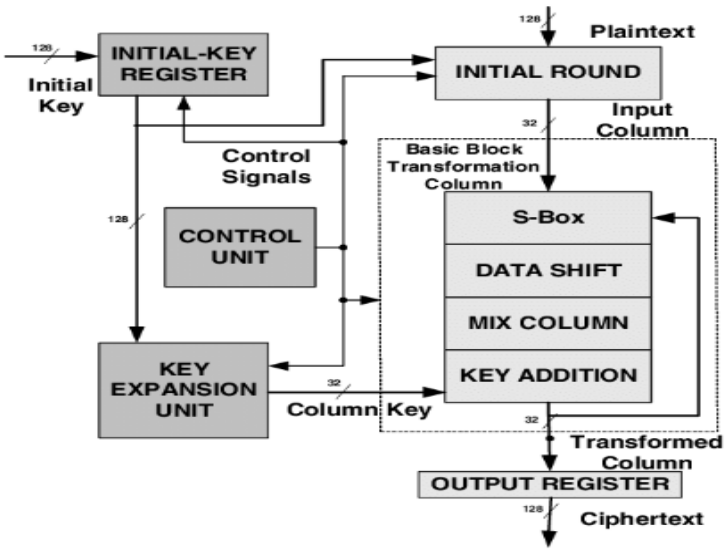

Figure 1: AES block diagram

AES have 128, 192 and 256 bit key size with 10, 12 and 14 rounds respectively. In AES the data and key is mixed to form key by implying, following steps.

a. Key Expansion:

Initially the key is expanded into two halves to form a bigger key using addition of padding bits.

b. Round Key:

Then add round key (k1) with the initial key using XOR operation.

c. Round operation (N-1) rounds:

Usually 10, 12 and 14 rounds here, follow the same steps for first(N-1) rounds and last Round will be different, here firstdo substitution operation using look up table then rows are shifted, the Columns are mixed, each time round key is added to form new key.

d. Final Round:

In final round, when previous round key is added then do substitution, then shifting of rows and round key is added. Then finally all round keys are added to form a strong key.

II. LITERATURE SURVEY

A. R. Chowdhury et al.,[1] 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 which indicates MAES consumes less energy than AES and it is applicable for Resource Constraint Environments.

M. Xie et al.,[2] 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,take advantage of NVM's intrinsic logic operation capability to implement the AES algorithm. 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.,[3] In this work, it is present proposed 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. In terms of security evaluation, our proposed data path, 32-b key out of 128 b cannot be revealed by correlation power analysis attack using less than 20 000 traces.

Q. Wu et al.,[4] 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, bridge these two notions with a hybrid primitive referred to as contributory broadcast encryption (ConBE).

A. Moradi et al.,[5] 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.,[6] By exploring different granularities of data-level and task-level parallelism, 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. Moreover, the design shows 2.0 times higher throughput than the TI DSP C6201, and 3.3 times higher throughput.

M. M. Wong et al.,[7] In this work, derive three novel composite field arithmetic (CFA) Advanced Encryption Standard (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 exist 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. Through the exploitation of both algebraic normal form and seven stages fine-grained pipelining, our best case achieves a throughput 3.49 Gbps on a Cyclone II EP2C5T144C6 field-programmable gate array.

Abhiram L S, Sriroop B K, Gowrav 2015 [8] In this work, System security is a rising area of correspondence. Cryptography assumes an imperative job in giving a protected system to correspondence. The most secure square figure today is Rijndael figure otherwise called AES. Yet, with cutting edge investigate occurring in the field of cryptography, the regular plan of AES is powerless for cryptanalysis. Subsequently a great deal of changes have been proposed on this calculation.

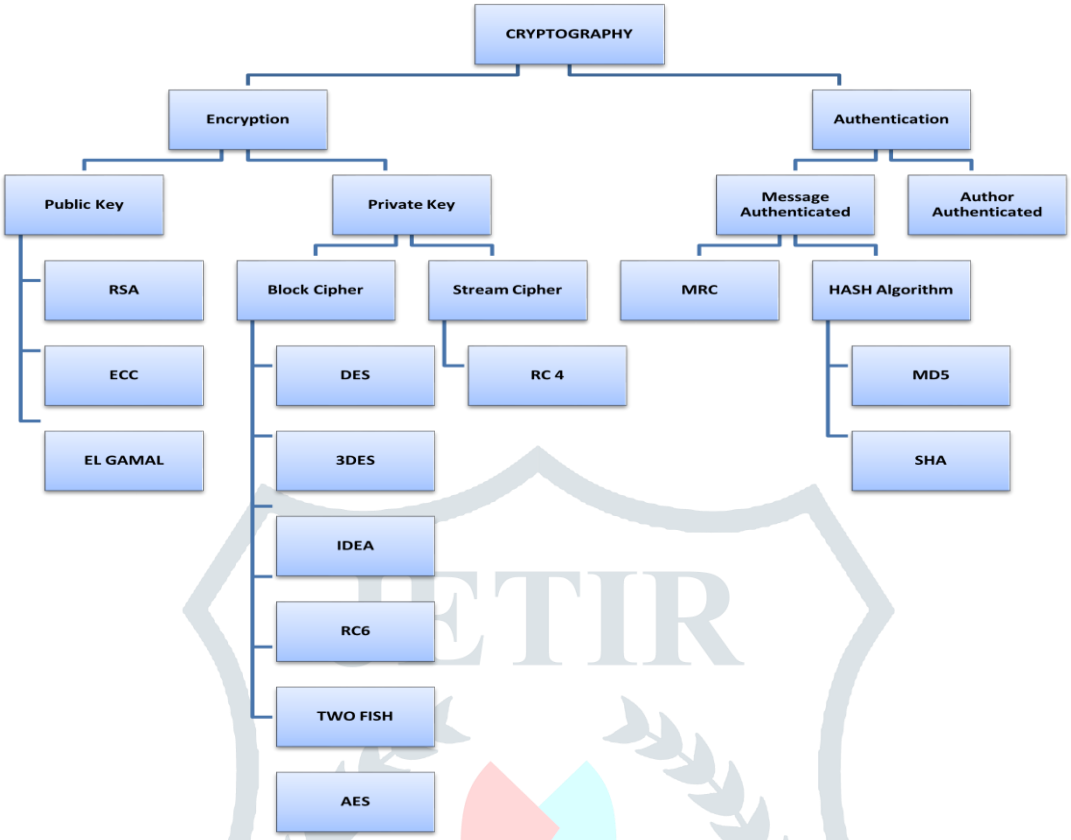

Figure 1.2 Classification of Cryptography

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. CONCLUSION

In this paper present the survey and study of AES algorithm for high speed and wireless communication application and also discuss the classification of cryptography. Further 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. Therefore, implement MAES for 128 bit data encryption and decryption sothat more number of data value can be encrypted with high speed.

REFERENCE

1. 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
2. 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.

3. 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.
4. 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.
5. 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.
6. 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.
7. 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.
8. M. Mozaffari-Kermani and A. Reyhani-Masoleh, "A Lightweight High-Performance Fault Detection Scheme for the Advanced Encryption Standard Using Composite Fields," in *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 19, no. 1, pp. 85-91, Jan. 2011
9. M. Mozaffari-Kermani and A. Reyhani-Masoleh, "Concurrent Structure-Independent Fault Detection Schemes for the Advanced Encryption Standard," in *IEEE Transactions on Computers*, vol. 59, no. 5, pp. 608-622, May 2010.
10. S. O'Melia and A. J. Elbirt, "Enhancing the Performance of Symmetric-Key Cryptography via Instruction Set Extensions," in *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 18, no. 11, pp. 1505-1518, Nov. 2010.
11. M. Wang, C. Su, C. Horng, C. Wu and C. Huang, "Single- and Multi-core Configurable AES Architectures for Flexible Security," in *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 18, no. 4, pp. 541-552, April 2010.
12. F. Mace, F. -. Standaert and J. -. Quisquater, "FPGA Implementation(s) of a Scalable Encryption Algorithm," in *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 16, no. 2, pp. 212-216, Feb. 2008.