A Review: Importance, Implementation, and Enhancement of AES

Nadia Mustaqim Ansari[1], Rizwan Iqbal[1], Adnan Waqar[1], Sohail Rana[1], Muhammad Ismail[1], Talha Tariq[1], Syed Waqar Alam[1], Maqsood ur Rehman[1], Mustafa Mohiuddin[1] and Rohail Shaikh[1]

[1]Department of Electronic Engineering, Dawood University of Engineering & Technology, Karachi, Pakistan

Corresponding author: Adnan Waqar

Abstract- Internet of Things (IoT) connects billions of intelligent gadgets that serve various functions. To trade and gather data from one another, these devices have sensors, software, and networks built right into them. As more devices become connected daily in the IoT, researchers' top priority is securing the hardware. According to academics, the current concentrated is on observing the offensive and defensive aspects of IoT devices. The main purpose of this article is to review the work done on the security of IoT devices. This study is an elaborate Advanced Encryption Standard (AES) algorithm, which is vastly used in IoT environments against power analysis attacks. Describes the modified AES using S-BOX and makes a hybrid algorithm to create a strict environment.

Index Terms- IoT, Encryption Algorithm, Security of IoT Devices.

Introduction

IoT is a very popular topic in technology world. Smart devices are connected to make IoT environment without intervention of humans. To establish a connection, devices use different platforms like web-based and cloud-based environments. When a large number of devices are connected, security may be compromised, and it is easy for intruders to enter the system. This is also called an attack. There are different types of attacks like hardware attacks, CPA attacks, Side channel attacks, DDOS attacks, etc. Researchers find out solutions against attacks. Design many encrypted algorithms to provide security for IoT devices. All above, many researchers select Advance Encryption Standard (AES) algorithm to provide protection. There are some challenges faced by researchers when they implement AES on the system, like AES consumes more power to offer better security than other algorithms. In this context, experts focused on and studied power reduction techniques using enhanced S-BOX, which is used in AES, and the properties of AES with the combination of another encrypted algorithm. This study is based on the attack methods to give security from these attacks in IoT devices, escalate AES properties, escalate S-BOX by using mathematical models and provide improved AES by amalgamating to another cryptographic algorithm.

Section II delineates the contributions based on enhancing the properties of AES; Section III delineates the grants based on the improvement of S-BOX, section IV traces the contributions based on Image Security section V delineates the contributions based on Power Analysis Attack and their solutions, section VI delineate the contributions based on side-channel analysis (SCA) resistant VII delineates the contributions based on minimizing power consumption or reduction techniques section VIII delineate the contributions based on AES with other encryption algorithms to make Hybrid Algorithm section IX delineate the contributions based on Comparison of AES with other algorithms.

Section II

In this section 05, research contributions based on enhancing the properties of AES with different techniques like avalanche effect, strict avalanche effect, random disturbance information, hardware platform based on FPGA, confusion, and diffusion, and a combination of Feistel and SP network used to provide the strong security mechanism of IoT world. In 2020 T. M. Kumar and P. Karthigai Kumar provided the best avalanche effect and strict avalanche effect AES algorithm to make the environment secure in any remote location. Design is based on the transformation steps of AES, making dynamic AES produce the result based on the key at every round. It is designed in Verilog and verified its functionality using Modalism and implemented in Xilinx FPGA device xc6vlx75t-3ff784. The weakness of design in terms of area, time, and power is increased when redesigning and implementing of AES algorithm [1].

L. Teng, H. Li, S. Yin, and Y. Sun provide secure cloud data with a modified AES algorithm by establishing random disturbance information to increase the data security. For verification experiments are conducted by MapReduce in

Hadoop platform with the help of MATLAB. Hadoop is used for distribution and provide storage of cloud data and for calculation of data system used MapReduce [2].

S. U. Jonwal and P. P. Shingare used AES algorithm with 128-bit key size for providing hardware platform in remote area. Artix 7 Nexys 4 kit of FPGA used to set up AES with Embedded Development Kit (EDK) which is the part of Xilinx ISE design suite. MATLAB is used for interfacing FPGA board with software part of SDK (software development kit) [3].

The study of D. Khambra and P. Dabas provide secure data communication mechanism, AES algorithm used to improve the security of data with high throughput by creating confusion and diffusion, this method is constituted of some logical operations, left shifting, swapping and substitution. MATLAB used to examine the system [4].

M. Usman, I. Ahmed, M. Imran, S. Khan, and U. Ali, make a new algorithm with the help of AES "The Secure IoT (SIT)" algorithm, it is a hybrid algorithm based on Feistel and SP network architecture. The size of key in AES has great impact on the phases of encryption decryption and key setup. SIT algorithm is not scalable [5].

- *AVALANCHE EFFECT:*

The drastic effect of output when slightly changes in input bit is called Avalanche effect [6].

- *STRICT AVALANCHE EFFECT*:

To validate the Avalanche effect strict avalanche effect is used. Complemented input bit effect 50% probability of output bit changed [6].

- *HADOOP:*

Hadoop is a distributed computing framework developed by the Apache storage and calculations for large amounts of data [2].

- *MAPREDUCE FRAMEWORK:*

In MapReduce calculation, reduce process can consume time for the integrate ordering of Map. So, in the cloud computing, the division of big data should take appropriate units, otherwise, it would affect the computation time [2].

- *EMBEDDED DEVELOPMENT KIT (EDK):*

EDK is the combination of Xilinx Platform studio (XPS) and software development kit (SDK) create an Integrated Development Environment (IDE) for emerging applications which are based on embedded for executing an application [2].

- *MICROBLAZE:*

It is softcore processor and used for the interface between hardware & software. The data is transfer to the FPGA with the help of MATLAB [2].

- *SOFTWARE DEVELOPMENT KIT (SDK):*

With the help of SDK, implementation of algorithm is very easy by the writing code in C/C++ [2].

- C*ONFUSION:*

This type of process make confusion with the key to make ciphertext more secure [7].

- *DIFFUSION:*

In this process, single character change of the plain text then many characters should be changed in ciphertext and vise-versa [7].

- *FEISTEL CIPHER:*

Feistel Cipher is a symmetric pattern designed for block ciphers designing. In Feistel, Encryption and decryption use the same structure [8].

- *SP (substitute on-permutation network):*

This network based on substitution (S-BOX) and permutation (P-BOX) of cryptography [9].

Section III

In this section 04 research contributions based on improvement of S-BOX in AES with different techniques like composite field arithmetic, Chaos-Based Rotational Matrices, quantum circuit and pseudo-random algorithm which makes AES algorithm stronger.

T. B. Singha, R. P. Palathinkal and S. R. Ahamed, have focused on optimization of composite field arithmetic which is used for the formation of S-Box in AES to improve hardware efficiency. In lightweight block cipher algorithms, AES is he only algorithm which is being used for IoT proposals. The combination of design, verification, and RTL (register-transfer level) of the algorithm was done using Xilinx Vivado 2018.3 simulator [10].

The study of M. S. Mahmood Malik et al. modifies AES S-box by using chaos in affine transformation provide more stronger AES. No attack still occur that can break this algorithm [11].

B. Langenberg, H. A. I. Pham, and R. Steinwandt presents a quantum circuit and implement the S-box of AES. To decrease the quantity of T-gates and T-depth [12].

C. Yang, J. Wu, L. Wang, X. Zhang, L. Li, and S. Liu focuses for improving S-BOX and key expansions transformations of AES to monitoring smart grid. Generate a random key by pseudo-random algorithm for securing data transmission by using AES. The simulation will perform on C++ for give better result, but it takes time [13].

Section IV

In this section 02 research contributions based on Image Security by using AES with bag of word (BOW) model and changes in S-BOX with confusion and diffusion properties.

H. Wang, Z. Xia, J. Fei, and F. Xiao provide security of image in cloud server storage by using AES with block permutation modification and bag of word (BOW) model. Design an algorithm and implemented in MATLAB [14].

M. Khan and N. Munir Proposed modified AES by using Galois field which is used in S-Box and provide security of digital data like images. AES used for image security Modification of Galois field. Further improving confusion and diffusion properties [15].

Section V

In this section 04 research contributions based on Power Analysis Attack and their solutions like randomization technique, energy trace compression method, flip-chip ball grid array (FC-BGA) and dynamic partial reconfiguration.

J. Yang, J. Han, F. Dai, W. Wang, and X. Zeng, A mechanism which shows the unsuccessful efforts of correlation power analysis (CPA) attack and power analysis attack (PAA) with predicated convolutional neural networks (CNNs) when used power traces are 2000000. This process predicated on Multicore processor with SASEBO-GII FPGA board and apply RTS (Random task scheduling) and RIO (random insertion of operations) and frequency and phase randomization (FPR) schemes. In this article author additionally mention the utilization of advance encryption algorithm (AES) that AES efficiently deploys in multicore processors [16].

X. Cai, R. Li, S. Kuang, and J. Tan using system on chip with energy trace compression method AES algorithm used to secure from different attacks. AES algorithm reduces power, area of chip and cost. Energy trace compression using hamming distance. Experimental results show Limited marker points because the space is limited. Minimize the computational cost for differential power analysis attacks by proposing energy compression method and implemented in So chip with a cryptographic coprocessor [17].

A. Tsukioka et al. proposed an efficient power noise modeling technique toward the SC leakage analysis AES is used to protect against side channel attacks using correlation power analysis mostly used AES. The advanced encryption standard (AES) test chip implemented by the flip-chip ball grid array (FC-BGA) assembly technology Including more physical properties in CPS simulation to increase reliability fast power leakage simulation method power delivery network (PDN) silicon substrate chip power model (CPM) chip package system (CPS) board model. flip-chip ball grid array (FC-BGA) assembly technology efficient power noise modeling technique impedance network model [18].

Bow et al., proposed a technique called SPREAD (side-channel power resistance for encryption algorithms using DPR) for making ineffective of power analysis attack. DPR (dynamic partial reconfiguration) in the feature of modern FPGA. AES used for SCA attacks. side-channel attack countermeasure called SPREAD is used Proposed technique does not match into either of the traditional noise enhancing or signal reducing categories [19].

- *CPA (CORRELATION POWER ANALYSIS):*

A set of power traces and the subsequent sets of intermediate values, CPA analyze and recover the secret subkey by using a correlation factor between the measured power samples and the power model of the computed sensitive values [20].

- *PAA (POWER ANALYSIS ATTACK):*

Power analysis attacks are a type of side channel involves measuring the power consumption of a cryptographic device during its operation and then analyzing it using statistical techniques such as Correlation Power Analysis to derive the key [21].

- *CNN (CONVOLUTIONAL NEURAL NETWORK):*

This is a type of deep learning model for processing data which is given by grid pattern, such as images [22]

- *SASEBO-GII FPGA:*

This FPGA board is operated for transfer plaintext and ciphertext to the computer and multicore processor [16].

- *RTS (RANDOM TASK SCHEDULING):*

This type of technique is used to scheduling dynamically between two rounds implemented on multi core processor and randomly choose core to run encryption [16].

- *RIO (RANDOM INSERTION OF OPERATION):*

This type of technique is used to increase the misalignment of power. The value of true random number generator based on number of inserted operations [16].

- *FPR (FREQUENCY AND PHASE RANDOMIZATION):*

To randomize the clock frequency of each core, so producing each core's power consumption entirely random. The method of phase randomization is like the frequency randomization. Since each core runs with different clock phases.[16]

- *65-nm CMOS LP:*

The 65nm technology establishes a broad range of applications, such as mobile devices, computers, automotive electronics, IoT, and smart wearables [23].

- *DPA (DIFFERENTIAL POWER ANALYSIS):*

This type of attacks uses statistical tools to show the correlation between the key and power consumption.[17]

- *HAMMING DISTANCE:*

Distance between two same length codes are the places at which they are differ to each other [24].

Section VI

In this section 02 research contributions based on side channel analysis (SCA) resistant methods like CMOS technologies and deep learning.

S. Ghandali, T. Moos, A. Moradi, and C. Paar Propose a mechanism to protect hardware TROJAN by SCA resistant design S-BOX of AES is used in any other algorithm. This technique is used in block cipher recognized in two different CMOS technologies and generating the Trojan makes the ASIC prototypes exposed. Difficulty in embedding of clock frequency monitor [25].

Jin, S. Kim, H. Kim and S. Hong Analyze effectiveness of deep learning-based side channel analysis by using AES. AES hardware and software deployment can be analyzed with an MLP deep learning applies on SCA Select hyperparameter properly because searching of hyperparameter is costly and the performance of SCA depends on this [26].

Section VII

In this section 02 research contributions based on minimize power consumption or reduction techniques with Cooja simulator, Contiki operating system and fall chip ball grid array (FC-BGA).

Sultan, B. J. Mir, and M. T. Banday proposed mechanism shows the optimized result with power reduction using Cooja simulator. AES used to minimize the cost of hardware. With the help of Cooja simulator and Contiki operating system analyzed different encryption algorithm for reducing the power consumption [27].

V. Nandan and R. Gowri Shankar Rao Proposed mechanism used for reduction of power in AES core by *some changes in S-BOX and Galois field. In cyber process AES works against data leakage, it is well-known algorithm and gives better adoptability Implementation of AES Core in 180-nm CMOS technology and design in Verilog Proposed architecture gives better results when replacing the SHA-256 with better software. An efficient power noise modeling technique toward the SC leakage analysis. AES is used to protect against side channel attacks using correlation power analysis mostly used AES. The advanced encryption standard (AES) test chip implemented by the flip-chip ball grid array (FC-BGA) assembly technology including more physical properties in CPS simulation to increase reliability [28].

- *COOJA SIMULATOR:*

Cooja is a software simulator, it is open source, basically build in java, capable of executing C, C++ programs it is a network simulator [29]

- *CONTIKI OPERATING SYSTEM:*

It is an open-source operating system for Internet of Things (IoT) [30].

- *ZOLERTIA Z1 AND SKY MOTES IN COOJA:*

Z1 mote is a less power consumption wireless platform based on hardware i.e., Texas MSP430 F2617 microcontroller complaint with IEEE 802.15.4. Sky is an ultra-less power consumption wireless module based on Texas Instruments MSP430 F1611 microcontroller widely used in wireless sensor networks and application prototyping. It consists of 2.4GHz IEEE 802.15.4 wireless transceiver having interoperability with other IEEE 802.15.4 devices [27].

- *AES-ECB (ELECTRONIC CODE BOOK):*

In this mode Plaintext divided into blocks and generate ciphertext then encrypt every block individually with same key [27].

- *AES-CBC (CIPHER BLOCK CHAINING):*

This mode based on two ideas in first idea encrypt all blocks which is dependent on each other. Ciphertext reliant on current block as well as previous block, in second idea produce randomness in the ciphertext by using initialization vector (IV) [27].

- *AES CTR (COUNTER):*

By using this mode block cipher operate like stream cipher. An input block is used as counter (just like the initialization vector). Block size is equal to the counter. Encryption of counter using key and x-ored with first plaintext block to produce the ciphertext block [27**].**

Section VIII

In this section 04 research contributions based on AES with other encryption algorithms to make Hybrid Algorithm.

J. G. Pandey, S. Gupta and A. Karmakar focus of design based on combining AES and PRESENT algorithms is used to provide multilevel data security of audio applications. In real time applications AES gives almost infinite range of real time security. The architecture integrates AES and PRESENT block ciphers. The core has been utilized as an IP for secure audio application in an FPGA-SoC environment. weakness of the system is Difficult to ensure the reliability of the system [31].

D. Manjiang, C. Kai, W. Zengxi, and Z. Lipeng, provide security cloud data storage of power bidding system by using combination of AES and ECC algorithm AES works efficiently for big size and unstructured data. Design Hybrid Encryption Algorithm by combining AES and ECC Because AES is symmetric algorithm and ECC is asymmetric algorithm, so it is difficult to decipher of the cipher text [32].

S. Naman, S. Bhattacharyya and T. Saha Design algorithm by combining AES-253 with SHA-256 and implemented in python to provide the security of data in remote sensing. AES-256 becoming more reliable and secure for upcoming years. Design algorithm by combining AES-253 with SHA-256 and implemented in python Proposed system provide security but increase time and memory [33].

G. Mustafa, R. Ashraf, M. A. Mirza, A. Jamil and Muhammad Review cryptography and steganography in IoT devices AES and another algorithm combine makes better algorithm. Survey of different cryptography techniques [34].

- *PRESENT:*

PRESENT cipher is based on SP-network(substitution-permutation). It requires 31 internal rounds with 64-bit data and 80/128-bit keys [31].

- *FPGA-SOC (FPGA BASED SYSTEM ON CHIP):*

The electronic components are integrated on a single chip. The components can be analog, digital, or mixed signals. SoC FPGA based devices add both processor and FPGA architectures into a single device [35].

- *ASIC (APPLICATION SPECIFIC INTEGRATED CIRCUITS)*

ASICs are used for non-standard integrated circuits that have been designed for a specific use or application [36**].**

Section IX

In this section 02 research contributions based on Comparison of AES with other algorithms and 02 research papers based on current countermeasure techniques.

S. Devi and H. D. Kotha focus Xilinx 9.2i is utilized for recreation and improvement of VHDL code for proving benefits of AES over RSA and DES algorithm. AES based method is verified to be safer and more secure for transmitting and receiving data. Xilinx 9.2i is utilized for recreation and improvement of VHDL code [37].

A.Fernando, D. Agustin, M. Irsan, D. F. Murad, H. Rohayani, and D. Sujana analyze the performance of AES over DES with experiment done by Raspberry PI with PHP programming language. AES algorithm requires less time and more secure than DES Experiment done by Raspberry PI with PHP programming language. The memory of the raspberry pi is limited [38]. Authors enhanced AES algorithm apply masking technique to hide the data [39]. In paper [40] some different types of attacks are discussed and their countermeasures by using AES. Similar techniques are discussed in [41- 48].

Section X

In this section different problems and their solutions are discussed in the Table 1.

TABLE I
SUMMARY OF CURRENT DISCUSSIONS

Ref. No.	Problem	Solution
[1]	some flaws in AES	authenticate proposed system with avalanche effect
[2]	security of cloud data	using random disturbance information method on AES
[3]	hardware problem in remote area	Using FPGA with AES make platform
[4]	security of data transmission in IoT	implement modified AES algorithm
[5]	security of IoT devices	make new algorithm SIT
[10]	less hardware efficiency in AES	improved S-Box by composite field arithmetic
[11]	some flaws in AES	using chaos-based rotation metrics make strong S-Box
[12]	high production cost of AES based devices	quantum circuit engineering implemented in S-Box
[13]	security of grid monitoring system	implement AES with pseudo random algorithm
[14]	security of image retrieval	using block permutation modification in AES
[15]	digital data security	some modification in Galois field variable which is used in S-Box
[16]	power analysis attack	randomization techniques implemented in multicore processor
[17]	differential power analysis attack	energy trace compression method
[18]	side channel attacks	IC based on FC-BGA technology
[19]	side channel attacks	SPREAD is proposed
[25]	side channel hardware TROJAN	implement CMOS 90nm and 65nm
[26]	side channel analysis	deep learning with MLP
[27]	high usage of power in encryption algorithms	analyze algorithm using cooja simulator and contiki operating system
[28]	increase power when implementation of AES of the system	modified S-Box with the help of Galois field
[31]	security of multilevel data for audio applications	hybrid algorithm (AES+PRESENT)
[32]	security of large data in cloud server	hybrid algorithm (AES+ECC)
[33]	security of data in remote area	hybrid algorithm (AES+SHA)
[34]	security of IoT devices	combine cryptography and steganography to provide strong security
[37]	AES compare with another algorithm	use Xilinx 9.2i with VHDL code for comparison of AES with RSA and DES
[38]	AES compare with DES	using raspberry pi with PHP programming language

Conclusion

In this paper, we have reviewed the security issues that exist on the IoT based networks and their solutions by using cryptographic algorithm. In this regard we have reviewed implementations of AES from different types of attacks. After reviewed latest articles we conclude that AES is the more secure algorithm to provide strict security of IoT based networks also we studied AES has some limitations , but researchers enhancing the properties of AES with different techniques like avalanche effect, strict avalanche effect, random disturbance information , hardware platform based on FPGA, confusion and diffusion and combination of Feistel and SP network also modifies S-BOX with different technique like composite field arithmetic, Chaos-Based Rotational Matrices, quantum circuit and pseudo-random algorithm and BOW model. Further studied improved AES algorithm with combine and compare another algorithm to make hybrid algorithm. Specifically, to reduce the impact of power analysis attack researchers gives randomization technique, energy trace compression method, flip-chip ball grid array (FC-BGA) and dynamic partial reconfiguration. CMOS technologies and deep learning methods also studied for provide secure from side channel attacks.

References

[1] T. M. Kumar and P. Karthigaikumar, “A Novel Method of Improvement in Advanced Encryption Standard Algorithm with Dynamic Shift Rows , Sub Byte and Mixcolumn Operations for the Secure Communication,” Int. J. Inf. Technol., pp. 1–6, 2020.

[2] L. Teng, H. Li, S. Yin, and Y. Sun, “A Modified Advanced Encryption Standard for Data Security,” vol. 2019, pp. 1–6, 2019.

[3] S. U. Jonwal and P. P. Shingare, “Advanced Encryption Standard (AES) implementation on FPGA with hardware in loop,” International Conference on Trends in Electronics and Informatics ICEI 2017, IEEE, pp. 64–67, 2017.

[4] D. Khambra and P. Dabas, “Secure Data Transmission using AES in IoT,” IJAIEM, vol. 6, no. 6, pp. 283–289, 2017.

[5] M. Usman, I. Ahmed, M. Imran, S. Khan, and U. Ali, “SIT: A Lightweight Encryption Algorithm for Secure Internet of Things,” Int. J. Adv. Comput. Sci. Appl., vol. 8, no. 1, pp. 1–10, 2017.

[6] D. O. Vadaviya and P. Tandel, “Study of Avalanche Effect in AES,” Ncraes’15, no. June, pp. 183–187, 2015

[7] C. Shannon, “Diffusion and Confusion”, foundations of cryptograph, Communication theory of secrecy systems,’” vol. 28, p. 1949, 1949.

[8] E. A. Al-Bahrani and R. N. J. Kadhum, “A new cipher based on Feistel structure and chaotic maps,” Baghdad Sci. J., vol. 16, no. 1, pp. 270–280, 2019.

[9] H. M. Heys and S. E. Tavares, “The design of substitution-permutation networks resistant to differential and linear cryptanalysis,” Proc. ACM Conf. Comput. Commun. Secur., no. January, pp. 148–155, 1994.

[10] T. B. Singha, R. P. Palathinkal and S. R. Ahamed, “Implementation of AES Using Composite Field Arithmetic for IoT Applications,” pp. 115–121, 2020.

[11] M. S. Mahmood Malik et al., “Generation of Highly Nonlinear and Dynamic AES Substitution-Boxes (S-Boxes) Using Chaos-Based Rotational Matrices,” IEEE Access, vol. 8, pp. 35682–35695, 2020.

[12] B. Langenberg, H. A. I. Pham, and R. Steinwandt, “Quantum Engineering Reducing the Cost of Implementing the Advanced Encryption Standard as a Quantum Engineering,” 2020.

[13] C. Yang, J. Wu, L. Wang, X. Zhang, L. Li, and S. Liu, “Smart Grid Monitoring Systems based on Advanced Encryption Standard and Wireless Local Area Network,” IOP Conf. Ser. Mater. Sci. Eng., vol. 719, no. 1, 2020.

[14] H. Wang, Z. Xia, J. Fei, and F. Xiao, “An AES-Based Secure Image Retrieval Scheme using Random Mapping and BOW in Cloud Computing,” IEEE Access, vol. 8, pp. 61138–61147, 2020.

[15] M. Khan and N. Munir, “A Novel Image Encryption Technique Based on Generalized Advanced Encryption Standard Based on Field of Any Characteristic,” Wirel. Pers. Commun., vol. 109, no. 2, pp. 849–867, 2019.

[16] J. Yang, J. Han, F. Dai, W. Wang, and X. Zeng, “A Power Analysis Attack Resistant Multicore Platform With Effective Randomization Techniques,” IEEE Trans. Very Large Scale Integr. Syst., pp. 1–12, 2020.

[17] X. Cai, R. Li, S. Kuang, and J. Tan, “An Energy Trace Compression Method for Differential Power Analysis Attack,” vol. 4, pp. 1–9, 2020.

[18] A. Tsukioka et al., “A Fast Side-channel Leakage Simulation Technique Based on IC Chip Power Modeling,” Letters on Electromagnetic Compatibility Practice and Applications vol. 6423, no. c, 2020.

[19] I. Bow et al., “Side-Channel Power Resistance for Encryption Algorithms Using Implementation Diversity,” pp. 1–20, 2020.

[20] A. Biryukov, D. Dinu, and J. Großsch, “Correlation Power Analysis of Lightweight Block Ciphers: From Theory to Practice.” International Conference on Applied Cryptography and Network Security springer International Publishing Switzerland 2016.

[21] H. Gamaarachchi, “Power Analysis Based Side Channel Attack.” CO411/2: Individual Project I & II – Report 2020.

[22] R. Yamashita, M. Nishio, R. Kinh, G. Do, and K. Togashi, “Convolutional neural network: an overview and application in radiology,” pp. 611–629, 2018.

[23] www.tsmc.com

[24] M. Sevalnev, “Error-correcting codes introduction, Hamming distance,” 2008.

[25] S. Ghandali, T. Moos, A. Moradi, and C. Paar, “Side-Channel Hardware Trojan for Provably-Secure SCA-protected Implementations,” pp. 1–14, 2020.

[26] S. Jin, S. Kim, H. Kim and S. Hong, “Recent advances in deep learning-based side-channel analysis,” ETRI, WILEY, vol. 42, no. March 2019, pp. 292–304.

[27] I. Sultan, B. J. Mir, and M. T. Banday, “Analysis and Optimization of Advanced Encryption Standard for the Internet of Things,” pp. 571–575, 2020.

[28] V. Nandan and R. Gowri Shankar Rao, “Minimization of Digital Logic Gates and Ultra-Low Power AES Encryption Core in 180CMOS Technology,” Microprocess. Microsyst., vol. 74, p. 103000, 2020.

[29] C. Thomson, “Cooja Simulator Manual,” no. C, pp. 2015–2016.

[30] A. Dunkels, “Contiki - A Lightweight and Flexible Operating System for Tiny Networked Contiki - a Lightweight and Flexible Operating System for Tiny Networked Sensors,” no. May, 2014.

[31] J. G. Pandey, S. Gupta, and A. Karmakar, “A Unified Architecture for AES/PRESENT Ciphers and its Usage in an SoC Environment,” pp. 1–4, 2020.

[32] D. Manjiang, C. Kai, W. Zengxi, and Z. Lipeng, "Design of a Cloud Storage Security Encryption Algorithm for Power Bidding System," ITNEC, pp. 1875–1879, 2020.

[33] S. Naman, S. Bhattacharyya and T. Saha "Remote Sensing and Advanced Encryption Standard using 256-Bit Key," Emerging Technology in Modelling and Graphics, vol. 937. Springer Singapore, 2020.

[34] G. Mustafa, R. Ashraf, M. A. Mirza, A. Jamil, and Muhammad, "A Review of Data Security and Cryptographic Techniques in IoT based devices," ACM, vol. c 2018.

[35] A. Brief, "What is an SoC FPGA?" 2014 Altera Corporation.

[36] www.electronics-notes.com

[37] S. Devi and H. D. Kotha, "AES encryption and decryption standards," J. Phys. Conf. Ser., vol. 1228, no. 1, 2019.

[38] E. Fernando, D. Agustin, M. Irsan, D. F. Murad, H. Rohayani, and D. Sujana, "Performance Comparison of Symmetries Encryption Algorithm AES and des with Raspberry Pi," Proc. 2019 4th Int. Conf. Sustain. Inf. Eng. Technol. SIET 2019, pp. 353–357, 2019.

[39] N. M. Ansari, R. Hussain, S. Arif, and S. S. Hussain, "Invariant of Enhanced AES Algorithm Implementations Against Power Analysis Attacks", Computer Materilas & Continua, vol. 72, no.1, 2022.

[40] N. M. Ansari, R. Hussain, S. S. Hussain and S. Arif, "Invariant of AES Algorithm Implementations Against Power Analysis Attacks in IoT Devices", ICCOINS, IEEE 2021.

[41] Meghji, Mahir, et al. "An algorithm for the automatic detection and quantification of athletes' change of direction incidents using IMU sensor data." *IEEE Sensors Journal* 19.12 (2019): 4518-4527.

[42] Islam, Kazi Yasin, et al. "A survey on energy efficiency in underwater wireless communications." *Journal of Network and Computer Applications* 198 (2022): 103295.

[43] Waqar, Adnan, et al. "Analysis of GPS and UWB positioning system for athlete tracking." *Measurement: Sensors* 14 (2021): 100036.

[44] Waqar, Adnan, et al. "Enhancing athlete tracking using data fusion in wearable technologies." *IEEE Transactions on Instrumentation and Measurement* 70 (2021): 1-13.

[45] Waqar, Adnan, et al. "A range error reduction technique for positioning applications in sports." *The Journal of Engineering* 2021.2 (2021): 73-84.

[46] Amir, Samreen, et al. "Kinect controlled UGV." *Wireless Personal Communications* 95.2 (2017): 631-640.

[47] Khan, Imran, et al. "Comparative analysis of ANN techniques for predicting channel frequencies in cognitive radio." *International Journal of Advanced Computer Science and Applications* 8.12 (2017).

[48] Khadim, Saima, et al. "Smart Cognitive Cellular Network." *Int. J. Future Gener. Commun. Netw* 10.12 (2017): 23-34.