Multi-Level Attack with Dynamic S-Box Variable Key Pattern Generation for Key Cohort Using AES

Anusha Padmavathi Rajendran
Department of Electronics and Communication Engineering, Government College of Engineering, India
anushvathi@gmail.com

Dhanalakshmi Krishnan Sadhasivam
Department of Electronics and Communication Engineering, Kalasalingam Academy of Research and Education, India
k.s.dhanalakshmi@klu.ac.in

Abstract: *In recent times, data transmission in electronic medium is found to be more susceptible to several attacks. The study aims to control the multi-level attacks in encryption and decryption process by using Advanced Encryption Standard (AES) algorithm based Simulation Box (S-Box) operations. In AES based variable key generation pattern, every round generates the new key. The generation of multiple keys strengthen the operation of AES-dynamic S box. The AES algorithm performs operation on a 128 bit plain text and utilizes identical key for decryption and encryption process. The proposed algorithm shows significant improvements in the quality of encryption and decryption. The performance of the proposed system has been analysed in accordance with delay, power consumption and number of slices. Further the efficiency of the proposed system has been compared with other existing methods such as Positive Polarity Reed Muller (PPRM), Modified Positive Polarity Reed Muller (MPPRM) Twisted Binary Decision Diagram (TBDD) and Composite Field (CF) architecture. The results exposed that the proposed system outperforms with superior performance.*

Keywords: *Advanced encryption standard, S box, variable key generation, encryption, decryption.*

Received August 23, 2021; accepted December 15, 2022
https://doi.org/10.34028/iajit/20/5/7

1. Introduction

With the advancing trends, expansion, and applications of the data communication system, there is a great demand for research to increase the security system and devices. One of the main technique to protect the user information sent through the transmission channel is the data encryption Tsai *et al*. [25] In general, symmetric or asymmetric cryptosystems were utilized extensively for securing the information, in which symmetric method uses a key that is similar to the transmitter and receiver and asymmetric key make use of variable key generation for data encryption and data decryption Alruily *et al*. [4]. Our study employed AES algorithm and Simulation Box (S-Box) with variable key pattern generation for securing the huge data against multi-level attacks. AES has been considered as the strong and best cryptography algorithm mainly due to its effectiveness in three areas such as cost, security and implementation Alassaf *et al*. [3]. Further from the existing studies it has been proved that AES is more secure against various attacks like differential, linear and brute force attack Saha *et al*. [21]. The strength and design of all the key lengths of AES algorithm are adequate for the protection of classified data up to the secret level. High level secret information needs the usage of 192 or 256 key lengths and hence using of the Brute Force attack is generally not possible Naman *et al*. [16]. Very strong confusion and diffusion offered by the integration of sub bytes, mix columns, and shiftrow transformation remove any kind of frequency pattern in plaintext.

Additionally, AES could be implemented easily with the use of cheap processors and a minimum memory. Despite these facts, there exists several works that attempts to attack AES with the use of various crypto-analysis methods Nyarko-Boateng *et al.* [18]. Various attacks called as side channel attacks will not attack the underlying cipher text and security, but attack the implementation. The proposed variable key generation system based on AES S-box cryptographic system generate various sub keys from the corresponding original keys. Then the sub keys are utilized for encrypting one AES block cipher. The three possible key length that has been supported by AES enable the user to pick a tradeoff between the security and speed. The increased key length possible increase the time of execution in terms of encryption and decryption Acholli and Ningappa [1]. All the three lengths are regarded as secure and the more prevalent attacks against AES decrease the effective key length. AES utilize a single S Box for all the bytes in all the rounds Nissar *et al*. [17]. The ideas of integrating both stream cipher and block cipher comprise the following two stages which are sub key generation and encryption/ decryption process Dhall *et al*. [8]. Accordingly, widespread research has been carried out for the identification of novel methods in securing AES algorithm. The study utilized the main advantages of AES like its ubiquity, comparatively fast in both software and hardware. This work strengthens the existing AES algorithm against multilevel attacks Khan *et al*. [13]. The methods adopted in our study are

synchronized at decryption and encryption for obtaining a reliable and secured AES algorithm.

The main contribution of the work is:

- To control multi-level attacks by AES based variable key generation pattern for encryption and decryption.
- To strengthen AES-dynamic S-box operation with the generation of multiple keys for encryption and decryption.
- To validate the performance measures in terms of performance metrics such as critical path analysis, delay, number of slices, power consumption and throughput.
- To perform comparative analysis with the existing methods such as MPPRM, PPRM, TBDD as well as CF methods.

1.1. Paper Organization

The paper has been organized as follows Initial section of the paper introduces the need and objectives of the work. Section 2 provides the related work in accordance to the proposed work. Section 3 deliberated the proposed methodology in detail and section 4 provides the performance analysis and comparative analysis. Section 5 concludes the work.

2. Related Works

In general, encryption is essential for preserving the confidentiality of data, in such way, various encryption algorithm exists for protecting data. The AES algorithm is widely used because of its speed as well as easier implementation on smaller devices. The implementation of decryption and encryption of AES algorithm has been introduced with a lower power and highly secured Multiplexer Look Up Table (MLUT)-based S-Box by Ratheesh and Narayanan [20]. Further, key feature in suggested system was implemented on 256 to 1 byte multiplexer. This implementation method was much simpler when compared to existing methods. From the experimental outcomes, the study depicted very minimum power dissipation. Additionally, the power dissipation for various processed data seemed to be highly uniform, thereby representing a reduction in variance. Finally, the study stated that the suggested method is more secured when compared to traditional methods.

Moreover, the AES algorithm is widely utilized in the cryptographic applications Sarkar and Singh [22] as well, such that an AES algorithm with high throughput and low power has been implemented by the study Kalaiselvi and Mangalam [11], by utilizing key expansion technique. This study significantly reduced the critical path delay as well as power consumption by utilizing the suggested high performance framework. The experimental outcomes deliberated that, the suggested method provides better performance than the prevailing AES frameworks in terms of critical path delay, throughput as well as power consumption. However, this study failed to use newer FPGAs, which further increases the overall performance. Similarly Manojkumar *et al*. [15] suggested a highly efficient and low power S-Box based circuit framework over composite fields. In this model, only Hazard transparent XOR gates and AND gates were utilized for the elimination of dynamic hazards in the consumption of power in the S box. When compared to the conventional model, low propagation delay of 4.58 ns has been achieved by the suggested model. The discussed model was effectively utilized for the protection of mammographic images from being accessed by unauthorized users. In recent days, the digital sensing processing, optical computing and bio-information applications requires a highly secured algorithms for preserving information. However, there are various challenges in mathematically securing these cryptographic protocols. In order to overcome these challenges, Karunamurthi and Natarajan [12] introduced a Reversible Logic Cryptography Design (RLCD) framework for designing the decryption and encryption. Further, a Linear Feedback Shift Register (LFSR) was required by the study for generating a key for decryption and encryption block. The study evaluated Field Programmable Gate Array (FPGA) as well as Application Specified Integrated Chip (ASIC) performances for the suggested method and other prevailing methods. From the comparative analysis, the study observed a 7% of performance improvement in RLCD LFSR approach, when compared to other methods. Nevertheless, the study failed to implement various kind of RLCD cryptography for improvising FPGA and ASIC performances.

With an aim of protecting the data for a secured communication, Zodpe and Sapkal [28] suggested a novel hybrid non-pipelined AES algorithm with improvised security features. Further, this method was presented to generate S-box values as well as initial key for decryption/encryption by utilizing PN sequence generator. The study stated that, this suggested method depicts significant improvements in the quality of encryption, when compared to conventional AES algorithms. Additionally, this method is also synthesized on different FGPA devices, which also deliberated improvised throughput performance. The rapid development of computational clouds has gained more attention and allowed intense computation on the resource constrained client devices. Nevertheless, it is more challenging in outsourcing of confidential and personal data to remote data servers. Hence, the conventional AES algorithms must be enhanced for handling security threats in Cloud Computing Environment (CCE). An architecture with enhanced security was presented by Awan *et al*. [6]. This framework modifies AES algorithm by increasing encryption speed by doubling the round key feature i.e.,

(1000blocks/ second). Moreover, the suggested architecture deploys AES with 16, 32, 64, and 128 byte plain texts. From the simulations, the outcomes of the study depicted that, suggested method has reduced about 14.43% of energy consumption, 15.67% of delay and 11.53% of network usage. Thus, this method enhances the security, reduces the utilization of resource, as well as reduces delay.

In recent years, the increasing number of wireless network and internet users' accelerated the concept of encryption mechanisms for protecting the user data across networks. The AES and DES algorithms provides information security in both applications and hardware, which provides improvised safety and performance. An exhaustive research of implementing AES and DES of FPGAs was performed by Yazdeen *et al*. [26]. Even though the development of earlier Data Encryption Standard (DES) algorithms were developed data encryption, it cannot cope up with technical advancements, and also it cannot provide better security. Therefore, Madhavapandian and MaruthuPandi [14] developed an effective field programmable gate array implementation of AES targets for investigating various security processes, which are followed in Transmission Control Protocol (TCP)/Internet Protocol (IP) protocol, and also suggested a new architecture for prevailing version. Further, this research projects the implementation on the basis of modification in the Mix column in AES methods that provides an effective Boolean expression. The suggested method was employed in low power FPGA, and when comparing chip usage and overhead with existing methods, the suggested system uses very less area.

In recent researches, the Very Large Scale Integration (VLSI) designs as well as implementing VLSI plays a significant role. Nevertheless, it undergoes certain security threats such as brute force attacks, suspicious data attacks, leaking confidential information as well as Differential Power Attacks (DPA). Further, Dhanalakshmi and Padmavathi [9] focussed on cryptographic methods, implemented for enhancing security levels for the VLSI devices. Also, the study analysed various techniques for implementing AES algorithms in VLSI devices. From analysis, the study stated that, AES with dynamic S-Box makes the system more dynamic, unbreakable as well as nonlinear framework. This work provided guidelines for implementing VLSI in secured manner with the cryptographic algorithms. AES is a standardized algorithm for the block chippers to provide security services. Even though AES possess potent security features, AES was broken down by cryptanalysis. Hence, it needs to improvise the security of algorithm. Such that, Saha *et al*. [21] depicted the causes of loopholes in AES, as well as provided solutions by utilizing the suggested Systematic Random Function Generator (SRFG). Further, the utilization of randomness in the process of key generation was considered as novelty. Also, the study compared the outcomes with actual AES algorithm on the basis of certain parameters like immunity, propagation characteristics, resiliency as well as nonlinearity. These outcomes depicted that the suggested method of AES performed much better in tolerating attacks.

Privacy is considered as major parameter of the communication with Internet of Things (IoT). Nevertheless, certain challenges such as computational overhead, pattern issues as well as using fixed S-Box that occurs in managing complex data like video, image and text. Several researchers intended to improvise the performance of algorithm. In such a way, Choudhary *et al*. [7]; Al-Mashhadani and Shujaa [2] discussed various research works on the basis of encryption security algorithms, as well as observed certain constraints by utilizing IoT applications. Likewise, Ramya *et al*. [19] discussed novel and significant modification to the prevailing hardware architecture of AES algorithm. The study stated that, by implementing these methods, speed efficacy over 1.41 times has been accomplished when compare to existing methods. Furthermore, from VLSI perspective, 3 times more optimization was achieved. A low complexity design method for S-Box and inverse S box was implemented by Hamzah *et al*. [10] in FPGA utilizing Quartus II and field arithmetic tool for obtaining the simulation results via Verilog Hardware Description Language (HDL). Further, this device used 94 slices, and it is suitable for applications that needs data security with minimal power consumption and less area. The AES 128 encryption iterative framework has been designed by Arul Murugan *et al*. [5] for achieving minimum hardware usage as well as less area. The minimized hardware usage was done by including Vedic multiplier in mix column transformation, whereas, area reduction was obtained by introducing S-Box structure in AES algorithm. The experimental outcomes revealed that, the suggested method possessed smaller area than prevailing methods. A Vedic design framework has been implemented by Sumalatha *et al*. [23] for performing Finite Impulse Response (FIR) filter with Electro Cardiogram (ECG) signal. The study evaluated ASIC and FPGA performances by using Verilog code. However, the study failed to implement various kind of frameworks for improvising the performance of hardware with efficient diagnosis process.

3. Methodology

This section comprehensively deliberates the proposed, which designed a variable key pattern generation that generates different keys for every messages, thereby controlling multi-level data attacks.

Figure 1 represents overall architecture of propose model. This basically incorporates key expansion unit, data encryption unit as well as simple control logic. A

128 bit plaint text is sent as input value, such that encryption process begins with add round key operation. Every round generates new key based on AES algorithm, such that a round key is 4x4 array of 128 bits. In Sub-Bytes phases, it splits inputs to bytes and every bytes via S-Box. In shift row, every row of cipher is shifted. Similarly in Mix column, every column of cipher is shifted. By doing so, input text is encrypted as cipher text. In order to decrypt, every operations such as add round key, mixed column operation and shift row operation is performed in reverse manner. This work introduced Variable key pattern generation, through which it can generate different keys to every messages, such that it controls multi attacks.

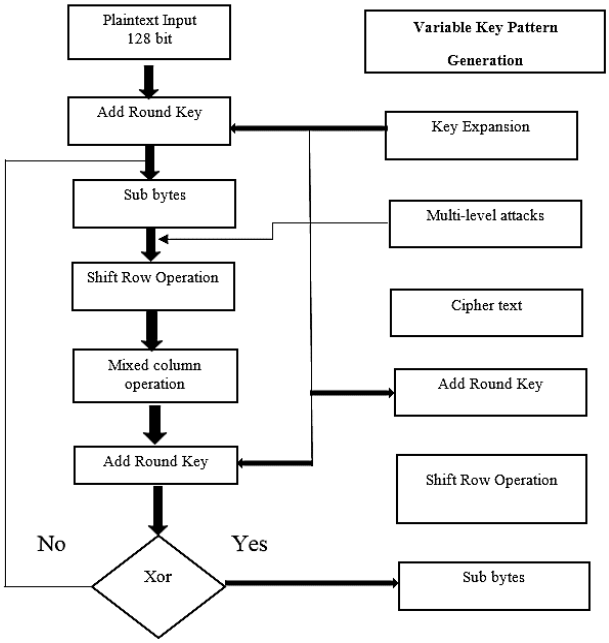

Figure 1. Overall architecture of the proposed method.

3.1. AES Algorithm Overview

The AES algorithm performs operation on a 128 bit plain text, and utilized identical key for decryption and encryption process. This algorithm performs 10, 12 as well as 14 rounds of operation by applying cipher secret of 128, 192, and 256 bit duration. Further, the algorithm operates on a data block, which consists 4x4byte matrix, and it can also be called state, in which the procedures of this algorithms were implemented. AES-128 algorithm is segregated in three states such as addition of initial round key, 1 to 9 rounds as well as the final round. Such that, in every cipher round, transformations like Sub-Byte, shift row, mix column as well as add round key will be performed. Also, in final round, sub byte, shift row as well as add round-key operations will be performed.

3.1.1. Sub-Byte Transformation

The Sub-byte transformation in invertible byte transformation that makes AES strong enough to handle attacks. Further, this substitutes each and every byte from the state matrix in S-Box, which is formed by lookup table of 256 bytes. These values were estimated by the multiplicative inverse, where the input element were mapped.

3.1.2. Encryption and Decryption Operation in AES

Decryption and encryption incorporates 4 steps, which are repeated in every round, expect the final round. Further, the decryption and encryption possess the operations like Inverse byte-substitution/ byte substitution, inverse-shift rows/ shift rows, Inverse-mix-column/ mix column as well as add round key. In the operations of final encryption round and first decryption round, the mix-column step isn't included as it is invertible. In the first two steps, the shift rows as well as the byte substitution could be interchanged without impacting the operation of encryption. Here, every byte replaces with other byte by utilizing S-Box, which provides non-linearity to the encryption data. Figure 2 represents sub byte transformation.

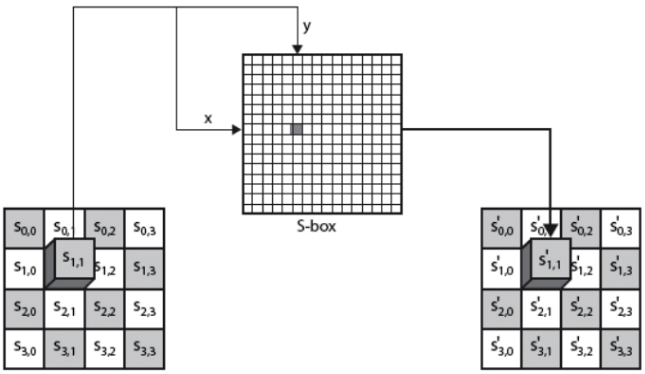

Figure 2. Transformation of sub-byte.

3.1.3. Shift Row Operation

In the shift row transformation, 1st, 2nd and 3rd rows of state matrix are cyclically shifted to left by the corresponding positions respectively. Further, offset value depends on the row number, and hence 1st row is not changed. Further, the cyclic rotation imparts the diffusion property in the AES algorithm. Figure illustrates the shift row transformation. Here, the data matrix row is cyclically shifted towards left, where 1st row remains unchanged, 2nd row shifts 1 byte towards left, 3rd row shifted 2 bytes towards left side and finally, 4th row shifts 3 bytes towards left as demonstrated in the Figure 3.

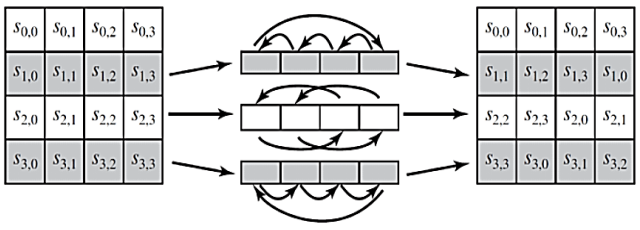

Figure 3. Operation of Shift row.

3.1.4. Mix Column Transformation

Figure 4 represents mix column transformation, in which every column of the input data matrix is transferred to new column in the matrix of output data. Here, each column of input data is considered as polynomial vector, which is multiplied with a constant matrix. Further, this multiplied operator utilized a polynomial mathematical as illustrated in Figure 4.

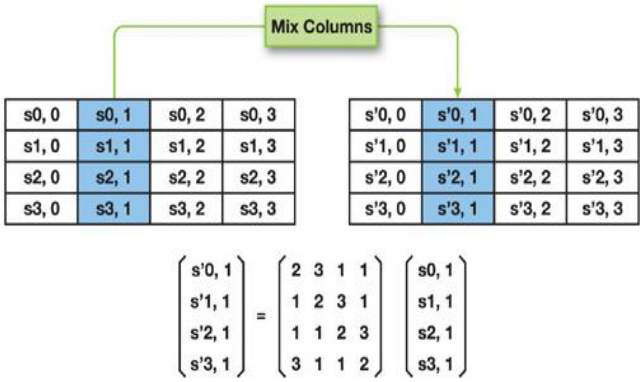

Figure 4. Mix column operation.

3.1.5. Transformation of Add Round Key

This is the final transformation in every round, such that in this transformation, XOR is the obtained round key. Add round key is common among decryption and encryption, and it is applied before decryption and encryption iterations, in which 1st 128 bits of input key is added to actual data-block as represented in Figure 5.

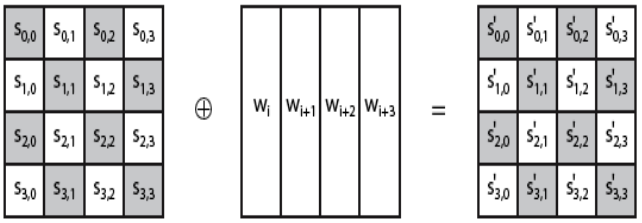

Figure 5. Transformation of add round key.

3.1.6. Key Expansion Module

This module produces 128-bit keys, which are needed for every rounds on the basis of initial key. Further, this module incorporated the functions such as Round cons, shift rows and sub byte functions. A bitwise XOR operation is performed by the round cons function by utilizing round constant array, and the values are obtained by [1, (Zhu *et al*. [27]), {00}, {00}] with xi.

3.1.7. S-Box Architecture

The byte substitution offers one byte non-linear transformation by utilizing 128 bit S-Box. Every entry is multiplicative inversion on Galois Field (GF). As S-Box transformation are only nonlinear function, the AES security depends upon implementation of S-Box. The S box architecture could be realized in software and hardware techniques also.

3.2. Variable Key Generation

Key generation reduces the usage of pre-defined keys. Furthermore, the key, which is generated depends on the feedback taps as well as seed value (initial). The variations in the parameters changes the value of initial key. For instance, an attacker tries to decrypt data by utilizing brute force attack, the attacker cannot decrypt any kind of information since there are different keys for every messages. Even though brute force attack identifies initial key, the attacker cannot decrypt input text. These modification assures high quality encryption for cipher. The flow of methodology regarding variable key pattern generation is depicted in the Figure 6.

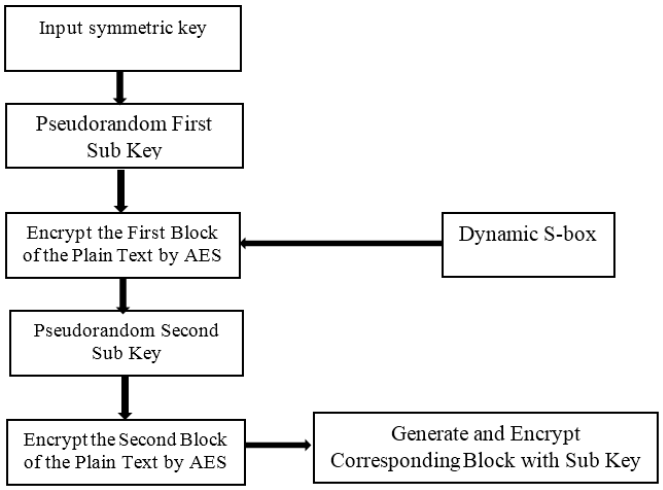

Figure 6. Variable key pattern generation.

The following depicts the algorithm for the proposed methodology.

Algorithm 1: AES Algorithm

. $S_1(y_i) = Affine\ transform\ (y_i^{-1})$

$$= \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \end{bmatrix} * \begin{bmatrix} i_7 \\ i_6 \\ i_5 \\ i_4 \\ i_3 \\ i_2 \\ i_1 \\ i_0 \end{bmatrix} + \begin{bmatrix} 0 \\ 1 \\ 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \end{bmatrix}$$

Where $S_1 refers\ to\ ShiftRows$, y_i^{-1} *refers to input text File*

Key Generation
For (n=1; n<=9; n=n+1)
'n' refers to number of iteration key expansion

{
Shift Rows transformation
}

Mix Columns transformation
If XoR Operation
Key Generation Operation
Else
Add Round key

Key Generation
For (n=1; n<=9; n=n+1)
{
Add Round Key transformation
}
$(P'_{i0,c}, P'_{i1,c}\ P'_{i2,c} P'_{i3,c}) = [P_{i0,c}, P_{i1,c}, P_{i2,c}, P_{i3,c}] \oplus [W_{round,Nb} + c_i]$
Variable Key Pattern Generation
Key expansion module

$$\begin{cases} N_i(r-1,c_i) + Sbox[R_i Word(N_i(r-1, C+3))] \\ \quad +R_i(con(r-1) \\ N_i(r,c-1) + N_i(r-1,c) \end{cases}$$

$(r-1,)$ refers $c_i th$ 32-bit column of rth round key, where $1 \le c_i \le 4\ and\ r > 1$. The initial key $(ri=1)$ is XOR with input 128-bit plaintext before the first round.

Initial round key, round 1-9 and final round are the three stages of AES-128 algorithm. At initial round, 128 bit plain-text has Exclusive-O-Red with 128 bit primary key. In every cipher round, ShiftRows(), AddRoundKeys(), MixColumns() and SubBytes() transformations have been carried out on 2-Dimensional 4*4 array of bytes which is represented as states. AddRoundKeys(),ShiftRows() and SubBytes () operations have been performed in final round. In shift row transformation, the shift rows 1, 2, and 3 of state matrix has been transformed clinically towards left to the positions of 1, 2, and 3 respectively. Based on the row number, offset value has been determined and the first row has no change. In AES algorithm, cyclic rotation of rows have carried the diffusion property. The process of linear diffusion, in which every column of the input data matrix is transferred to new column in the matrix of output data. Here, each column of input data is considered as polynomial vector, which is multiplied with a constant matrix and the multiplied operator utilized a polynomial mathematical, and represented as

$$a_i(y_i) = \langle 03 \rangle y_i^3 + \langle 01 \rangle y_i^2 + \langle 01 \rangle y_i^1 + \langle 02 \rangle$$

$$P'_i(y_i) = a_i(y_i) * P_i(y_i)$$

$$\begin{bmatrix} P'_{i0,c} \\ P'_{i1,c} \\ P'_{i2,c} \\ P'_{i3,c} \end{bmatrix} = \begin{bmatrix} 02\ 03\ 01\ 01 \\ 01\ 02\ 03\ 01 \\ 01\ 01\ 02\ 03 \\ 03\ 01\ 01\ 02 \end{bmatrix} \begin{bmatrix} P_{i0,c} \\ P_{i1,c} \\ P_{i2,c} \\ P_{i3,c} \end{bmatrix}$$

Where y_i refers to input variant, a_i refers to polynomial variant, P_i refers to polynomial mathematical, C refers to constant.

4. Performance Analysis

This section deliberates the performance analysis of proposed method compared to other existing methods like MPPRM, PPRM, TBDD, and CF.

Figure 7 represents simulation result for encryption. From this figure, it is observed that, data encryption is carried out in first phase, in which input plain text is encrypted by using cipher key as mentioned in the Table 1.

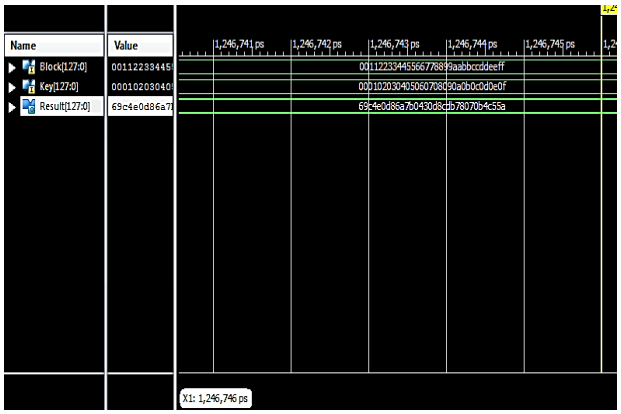

Figure 7. Simulation result for encryption.

Table 1. Block input data, cipher key and encrypted data.

Input/ Output Data	VALUES
Block Input data	00112233445566778899aabbccddeeff
Cipher Key	000102030405060708090a0b0c0d0e0f
Encrypted data	69c4e086a7b0430d8cdb78070b4c55a

Figure 8 illustrates the simulation result for decryption. From this figure, it is observed that decryption of data is performed, where the encrypted data is decrypted by using cipher key, as mentioned in Table 2.

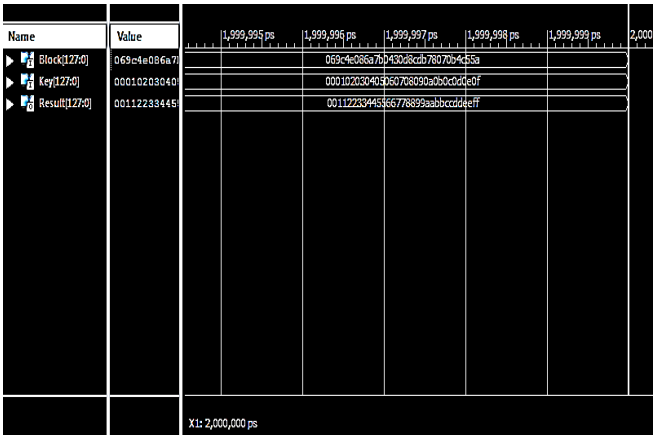

Figure 8. Simulation result for decryption.

Table 2. Block input data, cipher key and encrypted data.

Input/Output Data	Values
Encrypted data	69c4e086a7b0430d8cdb78070b4c55a
Cipher key	000102030405060708090a0b0c0d0e0f
Decrypted data	00112233445566778899aabbccddeeff

Figure 9 illustrates the propagation delay of proposed with other existing methods like MPPRM, PPRM, TBDD and CF. From this Figure 9, it is observed that, the proposed method had least propagation delay, whereas high propagation delay was obtained by CF method when compared to other existing methods. (MPPRM, PPRM, and TBDD).

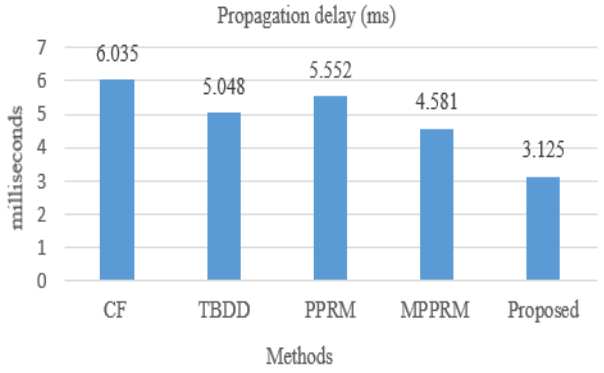

Figure 9. Propagation delay of proposed method and existing methods Manojkumar *et al*. [15] 2019.

Figure 10 represents the power consumption of the proposed method. From this Figure 10, it is noted that, the proposed method has consumed minimum power than other methods. Likewise, when considering the number of slices, the proposed method has very minimum number of slices, whereas TBDD method has more number of slices. Less number of slices, the proposed method surpasses the existing methods in terms of power consumption and number of slices.

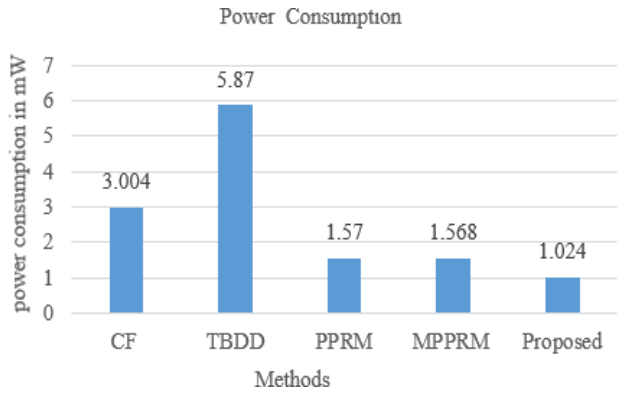

Figure 10. Power consumption of proposed method and existing method Manojkumar *et al*. [15] 2019.

Figure 11 illustrates the number of slices in proposed method and other existing methods. Such that, from the Figure 11, it is understood that, the proposed method has very minimum number of slices, whereas TBDD method has more number of slices.

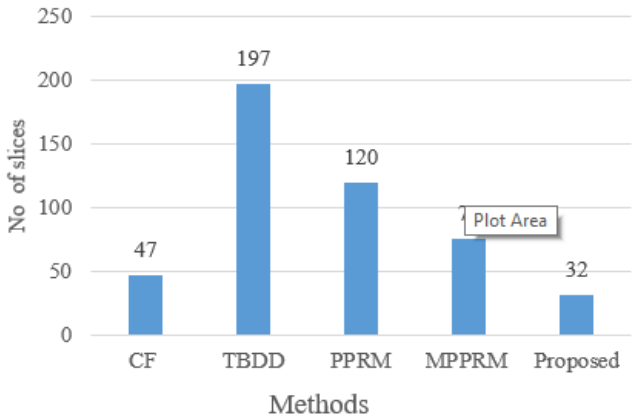

Figure 11. Number of slices in the proposed and existing system Manojkumar *et al*. [15] 2019.

From Table 3 and Figure 12, it has been found that the proposed system has enhanced values in terms of Throughput (Gbps), Max. Frequency (Mhz) and Throughput/Area(Mbps/Slice) as 2.86, 348.295 and 26 respectively in comparison with the existing study Teng *et al*. [24].

Table 3. Comparative analysis of the existing study Teng *et al*. [24] with proposed system.

Devices	Slices	Max.Frequency (Mhz)	Throughput (Gbps)	Throughput/Area (Mbps/Slice)
Virtes-6 xc6vlx240t	32	699.37	5.57	170
Virtes-6 xc6vlx240t	31	724.638	5.79	187
Virtes-5 xc5vlx20t	36	571.91	4.57	126
Virtes-5xc5vlx50t	31	512.821	4.102	132
Virtes-5 xc5vlx20t	34	303.79	2.43	71
Virtes-5 xc5vlx20t	37	571.91	4.575	124
Virtes-5 xc5vlx20t	32	523.56	4.188	131
Virtes-5 xc5vlx20t	35	617.25	4.938	141
Virtes-5 xc5vlx20t	17	644.33	5.514	303
Virtes-4 xc4vf100	45	209.61	1.68	37
Virtes-4 xc4vf100	48	549.753	4.39	91
spartan-3 xc3s200	69	327.22	2.62	38
spartan-3 xc3s200	63	338.295	2.71	43
(proposed) spartan-3 xc3s200	62	348.295	2.86	26

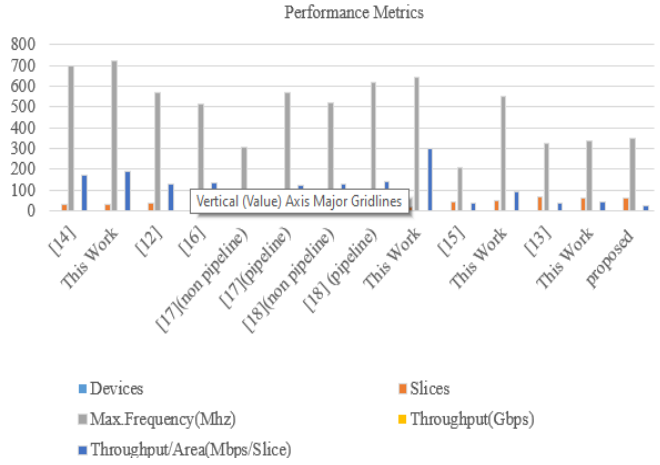

Figure 12. Comparative analysis of the existing study Teng *et al*. [24] 2021 with the proposed study.

Table 4. Performance metrics of the proposed method.

Methods	Critical path time (ns)	Throughput	Power (mW)
NIST	5.68	175.8	47.94
DOR	4.62	216.3	23.33
Dual stage	3.63	277.4	13.21
Proposed	2.04	312	10.78

The Table 4 demonstrates the performance metrics such as throughput, power and critical path time of proposed method and prevailing methods. From the above table, it is observed that, when considering throughput, proposed system possess highest throughput than the other methods. When considering power, the proposed system consumes least amount of power when compared to other existing methods. Likewise, when considering critical path time, the proposed method has very minimum critical path time than the prevailing methods.

In general, time or memory has been required for the theoretical computation of proposed algorithm where ‘n’ refers to the problem size or number of items.

Usually, $f_o(n_i)=O(g_i(n))$ denotes it is lesser than the constant multiple of$(g_i(n))$. Hence, the notation is given as "$f_o(n_i)$ *of* n_i *is Big O of* g_i *of* n_i ".

$f_o(n_i)=O(g_i(n))$ refers to the +ve constants c and k, in which $0 \leq f_o(n_i) \leq \mathcal{C} g_i(n_i)$ for all $n_i \geq k_i$. $\mathcal{C}$ and k_i values are fixed for function f which is not depends on n_i.

5. Conclusions

In AES, while implementing in high speed as well as low power circuits, total time consumed by framework must be significantly considered. Further, the implementation of S Box takes majority of time in total time. Such that, the major advantage in this method is, the dynamic hazards in combinational circuits are significantly reduced. In accordance to this, the paper employed AES based S box operations for variable key generating pattern that generates several key from the symmetrical keys. Hence modern attacks could be easily overcome by the proposed system more effectively. The efficiency of the proposed system has been validated in terms of power consumption, throughput, critical path time, number of slices and delay and compared with other existing methods such as MPPRM, PPRM, TBDD and CF. Inspite of the effective performance, the study had some drawbacks such as Rivest-Shamir-Adleman (RSA) algorithm used only asymmetric encryption. The proposed method had slow data transfer rate as it had large numbers and sometimes it may require third party to verify the reliability of public keys. Another drawback of the proposed method was it can work only with 128-bit key. In future, Hybrid Diffie-Hellman and Elliptic Curve Cryptography (ECC) algorithm can be considered to improvise the performance with regards to security.

References

[1] Acholli S. and Ningappa K., "VLSI Implementation of Hybrid Cryptography Algorithm Using LFSR Key," *International Journal of Intelligent Engineering and Systems*, vol. 12, no. 4, pp. 10-19. DOI:10.22266/ijies2019.0831.02

[2] Al-Mashhadani M. and Shujaa M., "IoT Security Using AES Encryption Technology Based ESP32 Platform," *The International Arab Journal Information Technology*, vol. 19, no. 2, 214-223, 2021. DOI: https://doi.org/10.34028/iajit/19/2/8

[3] Alassaf N., Gutub A., Parah S., and Al Ghamdi M., "Enhancing Speed of SIMON: A Light-Weight-Cryptographic Algorithm for Lot Applications," *Multimedia Tools and Applications*, vol. 78, no. 23, pp. 32633-32657, 2019. DOI: https://doi.org/10.1007/s11042-018-6801-z

[4] Alruily M., Shahin O., Al-Mahdi H., and Taloba A., "Asymmetric DNA Encryption and Decryption Technique for Arabic Plaintext," *Journal of Ambient Intelligence and Humanized Computing*, pp. 1-17, 2021. DOI: https://doi.org/10.1007/s12652-021-03108-w

[5] Arul Murugan C., Karthigaikumar P., and Priya S., "FPGA Implementation of Hardware Architecture with AES Encryptor Using Sub-Pipelined S-Box Techniques for Compact Applications," *Automatika*, vol. 61, no. 4, pp. 682-693, 2020. DOI: https://doi.org/10.1080/00051144.2020.1816388

[6] Awan I., Shiraz M., Hashmi M., Shaheen Q., Akhtar R., and Ditta A., "Secure Framework Enhancing AES Algorithm in Cloud Computing," *Security and Communication Networks*, vol. 2020. DOI: https://doi.org/10.1155/2020/8863345

[7] Choudhary A., Pandey N., and Agwekar A., "Review of VLSI Architecture of Cryptography Algorithm for IOT Security," IEEE Project paper, 2021.

[8] Dhall S., Pal S., and Sharma K., "A Chaos-Based Probabilistic Block Cipher for Image Encryption," *Journal of King Saud University-Computer and Information Sciences*, vol. 34, no. 1, pp. 1533-1543, 2022. DOI: https://doi.org/10.1016/j.jksuci.2018.09.015

[9] Dhanalakshmi K. and Padmavathi R., "A Survey on VLSI Implementation of AES Algorithm with Dynamic S-Box," *Journal of Applied Security Research*, vol. 17, no. 2, pp. 241-256, 2022. DOI: https://doi.org/10.1080/19361610.2020.1870403

[10] Hamzah H., Ahmad N., Jabbar M., and Soon C., "AES S-Box/Inv S-Box Optimization Using FPGA Implementation," *Journal of Telecommunication, Electronic and Computer* Engineering, vol. 9, no. 3-8, pp. 133-136, 2017.

[11] Kalaiselvi K. and Mangalam H., "Power Efficient and High Performance VLSI Architecture for AES Algorithm," *Journal of Electrical Systems and Information Technology*, vol. 2, no. 2, pp. 178-183, 2015. DOI: https://doi.org/10.1016/j.jesit.2015.04.002

[12] Karunamurthi S. and Natarajan V., "VLSI Implementation of Reversible Logic Gates Cryptography with LFSR Key," *Microprocessors and Microsystems*, vol. 69, pp. 68-78, 2019. DOI: https://doi.org/10.1016/j.micpro.2019.05.015

[13] Khan S., Parkinson S., and Qin Y., "Fog Computing Security: A Review of Current Applications and Security Solutions," *Journal of Cloud* Computing, vol. 6, no. 19, pp. 1-22, 2017. DOI: https://doi.org/10.1186/s13677-017-0090-3

[14] Madhavapandian S. and MaruthuPandi P., "FPGA Implementation of Highly Scalable AES Algorithm Using Modified Mix Column With Gate Replacement Technique for Security Application in TCP/IP," *Microprocessors and*

Microsystems, vol. 73, 2020. DOI: https://doi.org/10.1016/j.micpro.2019.102972

[15] Manojkumar T., Karthigaikumar P., and Ramachandran V., "An Optimized S-Box Circuit for High Speed AES Design with Enhanced PPRM Architecture to Secure Mammographic Images," *Journal of medical Systems*, vol. 43, no. 31, 2019. DOI: https://doi.org/10.1007/s10916-018-1145-9

[16] Naman S., Bhattacharyya S., and Saha T., "Remote Sensing and Advanced Encryption Standard Using 256-Bit Key," *Emerging Technology in Modelling and* Graphics, pp. 181-190, 2020. DOI: https://doi.org/10.1007/978-981-13-7403-6_18

[17] Nissar G., Garg D., and Khan B., "Implementation of Security Enhancement in AES by Inducting Dynamicity in AES S-Box," *International Journal of Innovative Technology and Exploring Engineering*, vol. 8, no. 11, pp. 2364-2373, 2019. DOI: 10.35940/ijitee.J9311.0881019

[18] Nyarko-Boateng O., Asante M., and Nti I., "Implementation of Advanced Encryption Standard Algorithm with Key Length of 256 Bits for Preventing Data Loss in an Organization," *International Journal of Science and Engineering Applications*, vol. 6, no. 03, pp. 88-94, 2017.

[19] Ramya B., Reddy K., and Pasula Sravanthi N., "VlSI Implementation of Modified Aes Cryptography Using Sbox," *Complexity International*, vol. 25, no. 1, 2021.

[20] Ratheesh T. and Narayanan S., "FPGA Based Implementation of AES Encryption and Decryption with Low Power Multiplexer LUT Based S-Box," *IOSR Journal of Electronics and Communication Engineering*, vol. 12, no. 2, pp. 57-61, 2017. DOI:10.9790/2834-1202015761

[21] Saha R., Geetha G., Kumar G., and Kim T., "RK-AES: An Improved Version of AES Using a New Key Generation Process with Random Keys," *Security and Communication Networks*, vol. 2018. DOI: https://doi.org/10.1155/2018/9802475

[22] Sarkar A. and Singh B., "A Review on Performance, Security and Various Biometric Template Protection Schemes for Biometric Authentication Systems," *Multimedia Tools and Applications*, vol. 79, no. 3, 2020. DOI:10.1007/s11042-020-09197-7.

[23] Sumalatha M., Naganjaneyulu P., and Prasad K., "Low Power and Low Area VLSI Implementation of Vedic Design FIR Filter for ECG Signal De-Noising," *Microprocessors and Microsystems*, vol. 71, no. 102883, 2019. DOI: https://doi.org/10.1016/j.micpro.2019.102883

[24] Teng Y., Chin W., Chang D., Chen P., and Chen P., "VLSI Architecture of S-Box with High Area Efficiency Based on Composite Field Arithmetic," *IEEE Access*, vol. 10, pp. 2721-2728, 2021. DOI: 10.1109/ACCESS.2021.3139040.

[25] Tsai K., Leu F., You I., Chang S., Hu S., and Park H., "Low-Power AES Data Encryption Architecture for a Lorawan," *IEEE Access*, vol. 7, pp. 146348-146357, 2019. DOI: 10.1109/ACCESS.2019.2941972.

[26] Yazdeen A., Zeebaree S., Sadeeq M., Kak S., Ahmed O., and Zebari R., "FPGA Implementations for Data Encryption and Decryption Via Concurrent and Parallel Computation: A Review," *Qubahan Academic Journal*, vol. 1, no. 2, pp. 8-16. 2021.

[27] Zhu Y., Yang M., Yao Y., Xiong X., and Li X., Zhou G., and Ma N., "Effects of Illuminance and Correlated Color Temperature on Daytime Cognitive Performance, Subjective Mood, and Alertness in Healthy Adults," *Environment and Behavior*, vol. 51, no. 2, pp. 199-230, 2019. DOI:10.1177/0013916517738077

[28] Zodpe H. and Sapkal A., "An Efficient AES Implementation Using FPGA with Enhanced Security," *Journal of King Saud University*, vol. 32, no. 2, pp. 115-122, 2020. DOI: https://doi.org/10.1016/j.jksues.2018.07.002

Anusha Padmavathi Rajendran working as Assistant Professor in the department of Electronics and Communication Engineering, in Government College of Engineering, Thirunelveli, TamilNadu, India. I had graduated with BE degree in Electronics and Communication Engineering from Anna University, Chennai in 2012 and M.E in Vlsi Design from PSN Engineering College in Thirunelveli 2017. My area of interest is Wireless Network Security, Image Processing and VlSI Design.

Dhanalakshmi Krishnan Sadhasivam working as Assistant Professor in the department of Electronics and Communication Engineering, Kalasalingam Academy of Research and Education, Krishnankoil, Virudhunagar District, TamilNadu, India. I am graduated with BE degree in Electronics and Communication Engineering from Anna University, Chennai in 2007 and M.Tech in Digital Communication and Network Engineering from Kalasalingam University, Krishnankoil in 2011. I have received the PhD degree in Intrusion Detection System for Wireless Networks from Kalasalingam Academy of Research and Education, Krishnankoil in 2018. My area of interest is Wireless Network Security, Satellite Communication and Signal Processing.