ISSN: 2456-043X

International Journal of Engineering Science and Generic Research (IJESAR)
Available Online at www.ijesar.in
Journal Index In ICI World of Journals - ICV 2016 – 68.35
Volume 6; Issue 6; November-December; 2020; Page No. 01-08

A NEW AES ARCHITECTURE USING DYNAMIC KEY FOR HIGH SECURITY, LOW POWER AND HIGH-SPEED APPLICATIONS

Miss. M Leekshika[1], Mrs. M. SrilakshmiRavali[2]

[1]Research Scholar, Department of ECE, Stanley College of Engineering and Technology for Women, Hyderabad, Telangana, India

[2]Assistant Professor, Department of ECE, Stanley College of Engineering and Technology for Women, Hyderabad, Telangana, India

Abstract

Advanced Encryption Standard (AES) is the most secured encryption algorithm. It is a block cipher[1] of 128-bit size and key sizes varying from 128,256, and 512 bits. Based on the key sizes, 128, 256, and 512 bit it has 10, 12, and 14 rounds respectively. The stages in AES are add round key, sub byte, shift row, and mix column. As AES being symmetric, the security of the key is questionable and it even consumes highpower.

The proposed work is based on creating a dynamic key [11] based on the sequence of the blocks of data. Each block is considered a frame of 16 bytes and sent in a sequential manner. Based on the sequence, the dynamic key is generated by incrementing the 16 bytes of the key by one unit. The individual data frame associated with a key is passed through the AESalgorithm, which generates the Cipher Text and to the receiver.The receiver, based on the order in which the encrypted data is received, will find the key to decrypt thedata.As the number of frames increases, the security will be high because the probability of finding the key will be least. The conventional s-box is replaced with a one-dimensional s-box [7] provides low power and high speed.

Simulations and synthesis are done in Xilinx ISE 14.7 version and coding are done in Verilog HDL and the results are obtained on the Xilinx Virtex6 FPGA board.

Keywords: Advanced Encryption Standard (AES), Cryptography, DES, and Symmetric Key Algorithms.

I. INTRODUCTION

The Advanced Encryption Standard, in the following referenced as AES [4], is the winner of the contest, held in 1997 by the US Government, after the Data Encryption Standard was found too weak because of its small key size and the technological advancements in processor power. Fifteen candidates were accepted in 1998 and based on public comments the pool was reduced to five finalists in 1999. In October 2000, one of these five algorithms were selected as the forthcoming standard: a slightly modified version of the Rijndael.

The Rijndael, [6] whose name is based on the names of its two Belgian inventors, Joan Daemen and Vincent Rijmen, is a Block cipher, which means that it works on a fixed-length group of bits, which are called blocks. It takes an input block of a certain size, usually 128, and produces a corresponding output block of the same size. The transformation requires a second input, which is the secret key. It is important to know that the secret key can be of any size (depending on the cipher used) and that AES uses three different key sizes: 128, 192, and 256 bits. To encrypt messages longer than the block size, a mode of operation is chosen, after the implementation of AES. While AES supports only block sizes of 128 bits and key sizes of 128, 192, and 256 bits, the original Rijndael[6] supports key and block sizes in any multiple of 32, with a minimum of 128 and a maximum of 256 bits.

The need for privacy has become a high priority for both governments and civilians desiring protection from signal and data interception. Widespread use of personal communications devices has only increased demand for a level of security on previously insecure

communications. Both DES [2] (Data Encryption Standard) and AES are defined as symmetric key block ciphers, with the main difference being the bit length of the key (56 bit for DES).

These symmetric-key encryption schemes use the same key for both the sender and receiverand as a result, eliminate the need for the verification server needed in public keying. Symmetric keying lends itself to swork independently of an open network and in turn a higher level of system interoperability.

The aim of this project is to design a high secured advanced AES architecture for low power and high-speed applications.

II. EXISTING WORK

2.1 Advanced Encryption Standard(AES)

The Advanced Encryption Standard (AES) [5] specifies a FIPS-approved cryptographic algorithm that can be used to protect electronic data. The AES algorithm is a symmetric block cipher that can encrypt (encipher) and decrypt (decipher) information. Encryption converts data to an unintelligible form called cipher text; decrypting the cipher text converts the data back into its original form, called plaintext.

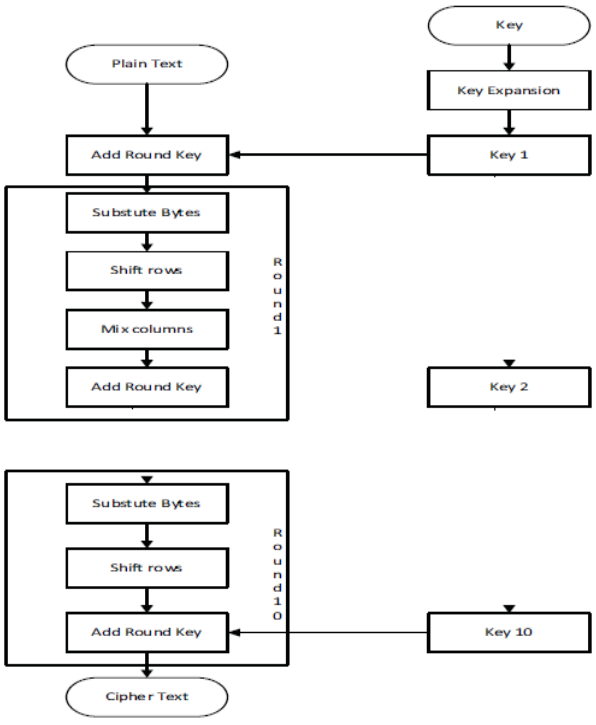

Figure 2.1: Flowchart Diagram for the AES Encryption Algorithm

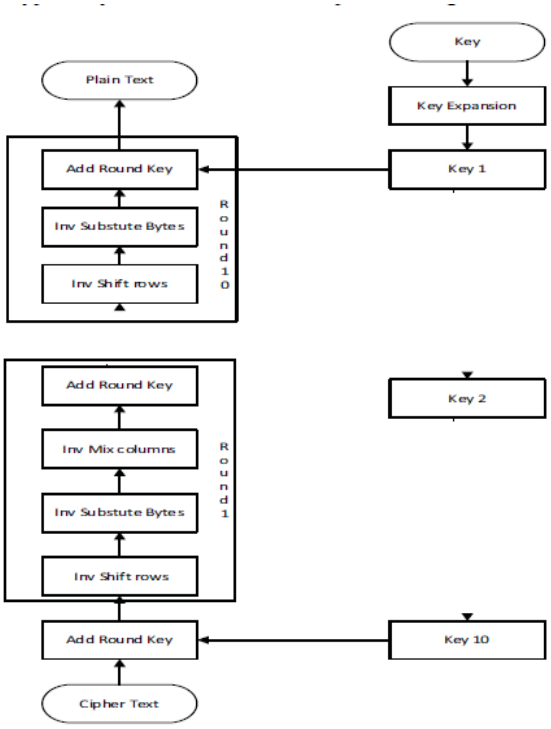

Figure 2.2: Flowchart Diagram for the AES Decryption Algorithm

Joan Daemen and Vincent Rijmen urbanized a block cipher called Rijndael. In AES the span of each block and the key can be autonomously specified to be 128, 192, or 256 bits. The AES arrangement exploits data of 128 bits and the same three key size alternatives. This 128-bit data can be divided into four operation blocks, which are represented as a square matrix of bytes. These operation blocks are copied into a state array. The state array is organized as a 4×4 matrix. The data is conceded through N rounds (N = 10, 12,14) for encryption. These rounds are performed by the following transformations

Sub Byte Transformation:

In this process 128-bit block is replaced with another 128- bit block, for substitution purpose we use an 8bit S-box.

Shift Rows Transformation:

In this process, we leave the first row of data, perform once shift left on 2nd row, two times shift left on 3rd row and three times shift left on 4th row.It is a simple Permutation.

Mix Column Transformation:

This is a substitution; where the bytes in the columns are linearly combined. The matrix multiplication is

performed over the same GF (28) as used in the design of the S-box.

Add Round Key Transformation:

When working state and expanded key are XOR with each other, this process is called Add round Key.

All four layers expressed above (including key scheduling) have analogous converse methods. The procedure of encryption follows more than a few ladders. An initial add round key is applied. After this, a round function is applied to the block. Each block consists of sub byte, shift rows, mix columns, and add round key transformation. These blocks are repeated N times, depending upon the length of the key applied. The same sequence of transformations is applied to the decryption structure as which is applied in the encryption structure. The transformations i.e. Inv-Sub byte, Inv Shift rows, Inv-Mix columns, and Add round key permit the type of key schedules to be matched for encryption and decryption. Here it must be noted that the Mix Column reverse operation requires matrix elements.

III. PROPOSED WORK

3.1 Block Diagram of Proposed AES Transmitter and Receiver

The key exchange is the common weakness of all symmetric key methods, not just AES, so a separate key exchange mechanism is necessary. Therefore, a technique to create a dynamic key based on the data transfer sequence has been presented. The system starts with 128 bits of data (16 bytes data), 128 bits in the key length.

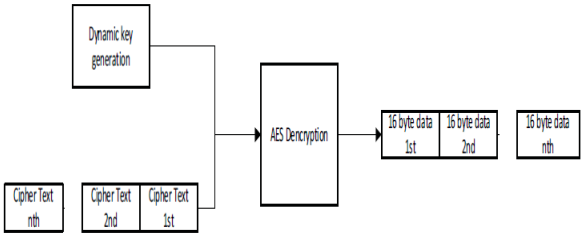

Figure 3.1: Proposed AES at Transmitter Side

The sender will make frames consisting of 16 bytes and send the frames in the sequence. Based on the sequential order, we will generate the key from the encrypted data. The receiver, based on the data frame sequence to determine the sequence of receiving data,

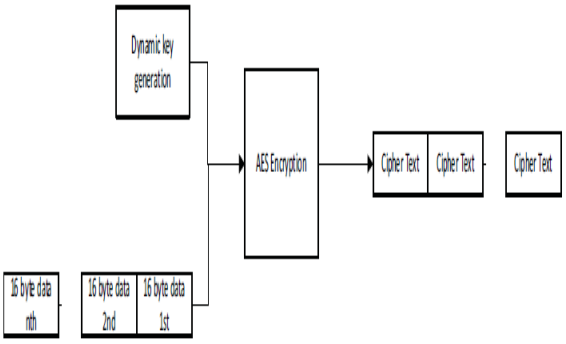

Figure 3.2: Proposed AES at Receiver Side

Will know the key sequence generated from the sending side. Here, the dynamic key generation in the transmitter is the same as in the receiver that is based on the sequence of transmitting data frames.

3.2 Dynamic Key Generation

In the proposed AES algorithm, based on 16-byte frame-by-frame data transfer, a dynamic key [11] is generated. Before transmitting data, the

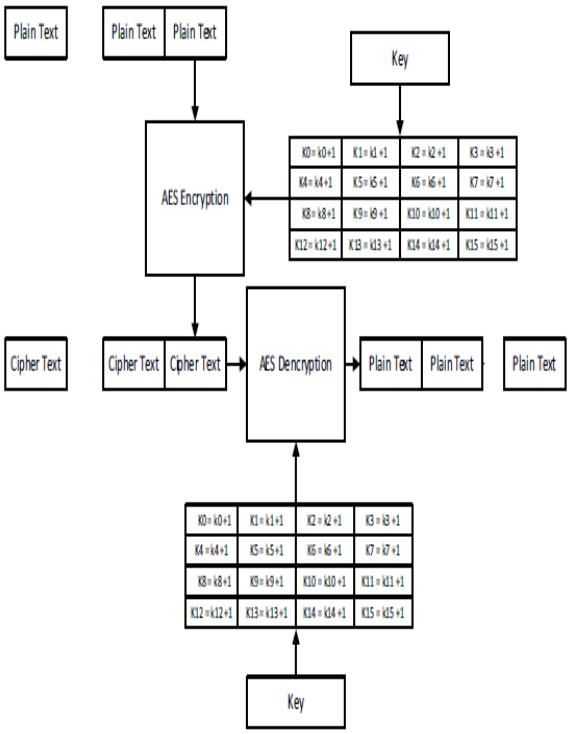

Figure 3.3: Dynamic Key Generations

Sender and the receiver must specify the key. First, the data (Plain Text) are framed each frame consists of 16 bytes and is sent in sequence.

Based on the transmitted data frame sequence, the 16 bytes of the key is changed by incrementing one unit. Each data frame associated with a key change passes through the AES algorithm, which generates the Cipher Text and sends it to the receiver. Recipients, based on the order in which the encrypted data is received, will find the key to decrypt the data.

3.3 Security Enhancement through Dynamic Key

There are two states of zero and one. So, the 128-bit key for the AES algorithm will find the 2^128states.Theprobability of finding the key to the AES algorithm is (1/2)128.With the probability above, the attacker can still find the 128-bits key and can decrypt the original data by the trial-and-error method. Here the proposed scheme to frame 16 bytes of data (128 bits) in sequential order, based on sequences to create a dynamic key has been presented. With the probability above, (1/2)^128 is the probability of finding a data frame in our algorithmic proposition. When the frame "n"transmits, the probability that our key will be (1/2)128xn where n is the number of the transmitted frames. If nincreases, the probability will be decreased very much.

3.4 Modified S-Box

In order to overcome the power constraint, we are using a 1-D S-Box [7] instead of a conventional S-Box. The following are the steps

a) Multiplicative Inverse Table: In the Rijndael AES, all the arithmetic operations are performed over the Galois Field(24). Galois Field (24) is considered in the following example where the number of irreducible polynomials of degree 4 over GF (2) are $x^4+ x + 1$, $x^4+ x^3+ x^2+ x + 1$ and $x^4+ x^3+ 1$. All the generated values of the multiplicative inverse table and substitution box depend on the selection of irreducible polynomial. For our experiment purpose, we choose x^4+x+1 as our irreducible polynomial but we can select any of the irreducible polynomials which are mentioned above. Following the Extended Euclidean Algorithm, a 1-dimensional multiplicative inverse table is formed. Figure 3.4 illustrates the multiplicative inverse table of the proposed algorithm.

0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	1	9	E	D	A	7	6	F	2	C	5	A	4	3	8

Figure 3.4 Multiplicative Inverse Table

b) Affine Transformation: This affine transformation process also follows two phases. Firstly, 4x4 square matrix's multiplication and secondly, 4x1 constant column matrix addition. The 4x4 square matrix is constructed following equation 1 and equation 2 refers to the value of di:

di = bi _ b(i+2)%4 _ b(i+3)%4 _ Ci (4)

Ci = ith bit of a specially designated byte which is hexadecimal of 3; 8; 10; 13; 15 as they don't generate any fixed points. The constant value is a little bit precarious. On calculating over the GF(24), the value of the constant column matrix ranges from 0x00 to 0x0F, we can only select 5 values from there as these values do not generate any fixed point after transformation. The fixed point refers to the generation of the output value same as the input value.

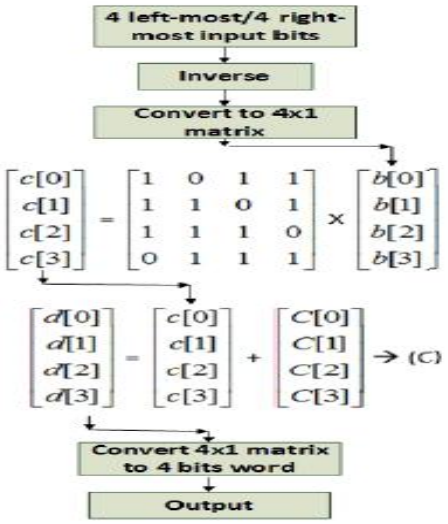

Figure 3.5: The Generation Process of Proposed MAES

Different S-Boxes and inverse S-Boxes for different values of the constant value C is given below from figures

Case-1: When C = 0x03

0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
3	4	F	B	2	1	7	0	C	D	5	9	6	E	A	8

Inverse S-box:

0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
7	5	4	0	1	A	C	6	F	B	E	3	8	9	D	2

A one dimensional S-Box can be explained mathematically from the following example.

0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	1	9	E	D	A	7	6	F	2	C	5	A	4	3	8

4 Bit S-Box Inverse Table

Example: Constant matrix C=03; and Input = 4'ha [A=10; B=11; C=12; D=13..]

4'ha = 4'b1010

Step1: Considering Inverse of Input 4'ha from the above table

4'ha=4'hc = 4'b 1100

Step2: Multiply matrix "C" with matrix "L"

$$= \begin{bmatrix} 1011 \\ 1101 \\ 1110 \\ 0111 \end{bmatrix} * \begin{bmatrix} 0 \\ 0 \\ 1 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \\ 1 \\ 0 \end{bmatrix}$$

Step3: Add C=03 to above obtained matrix we get

$$= \begin{bmatrix} 0 \\ 1 \\ 1 \\ 0 \end{bmatrix} \oplus \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \\ 1 \\ 0 \end{bmatrix} = 4'b\ 0101 = 4'h5$$

IV.RESULTS AND ANALYSIS

4.1: AES Top Module Schematic

The standard AES top module is obtained as shown below

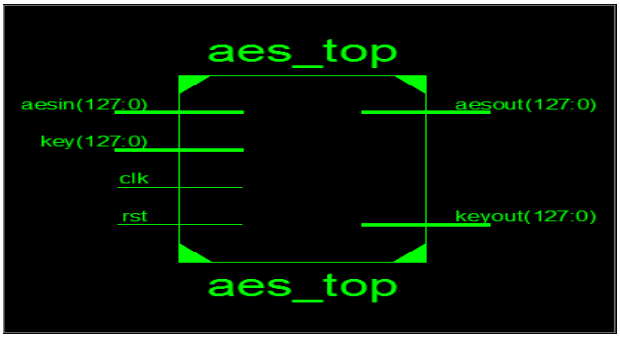

Figure 4.1: AES Schematic

4.1.2: AES Simulation Results

The simulation results of AES output when the input of 128 bit i,e.aesin[127:0] and key size of 128bit i,e. keyin[127:0] is given, we obtained output value aesout [127:0] same as AES input.

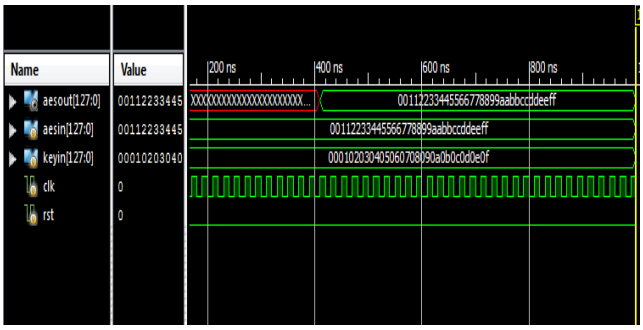

Figure 4.2: Simulation of Standard AES

4.1.3 AES Area

The device utilization summary of Standard AES is obtained as

Device Utilization Summary (estimated values)			[-]
Logic Utilization	**Used**	**Available**	**Utilization**
Number of Slice Registers	84	93120	0%
Number of Slice LUTs	6595	46560	14%
Number of fully used LUT-FF pairs	1	6678	0%
Number of bonded IOBs	514	240	214%
Number of Block RAM/FIFO	76	156	48%
Number of BUFG/BUFGCTRLs	1	32	3%

Figure 4.3 AES Area

4.1.4 AES Delay

The Timing Summary of Standard AES is obtained as shown below

```
Timing Summary:
---------------
Speed Grade: -2

   Minimum period: 4.150ns (Maximum Frequency: 240.990MHz)
   Minimum input arrival time before clock: 5.042ns
   Maximum output required time after clock: 2.126ns
   Maximum combinational path delay: 0.486ns
```

Figure 4.4: AES Delay

4.2 AES With Dynamic Key Schematic

The Dynamic Key top module is obtained as shown below

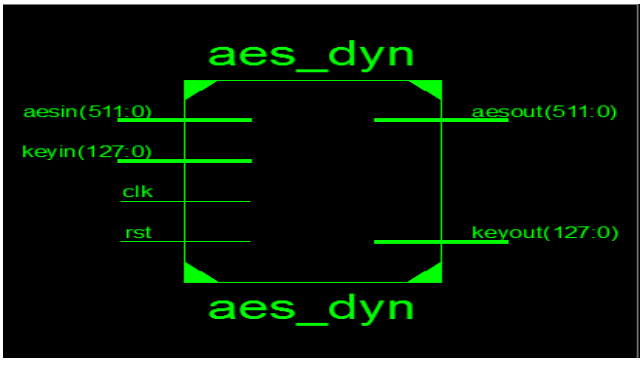

Figure 4.5: AES with Dynamic Key Schematic

4.2.1 Simulation ofAES with Dynamic Key

Thesimulation results of AES with Dynamic key when the input of 512 bit i,e.aesin[511:0] = 576 and key size of 128bit i,e. keyin[127:0] = 56 is given, we obtained output value aesout [511:0] = 576 same as AES input value.

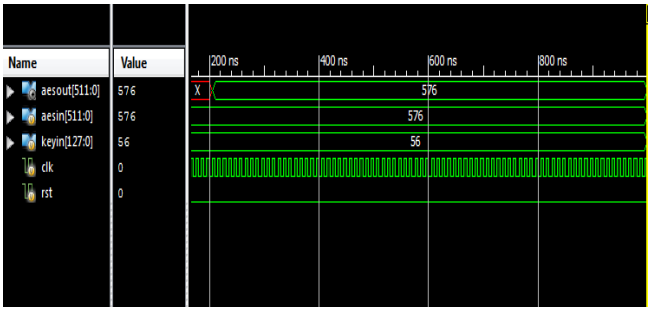

Figure 4.6: Simulation of AES with DynamicKey

4.2.2 AES with Dynamic Key Area

The device utilization summary of Dynamic Key Area is obtained as shown below

Device Utilization Summary (estimated values)			
Logic Utilization	**Used**	**Available**	**Utilization**
Number of Slice Registers	7744	93120	8%
Number of Slice LUTs	87055	46560	186%
Number of fully used LUT-FF pairs	0	94799	0%
Number of bonded IOBs	1281	240	533%
Number of Block RAM/FIFO	86	156	55%
Number of BUFG/BUFGCTRLs	1	32	3%

Figure 4.7 AES with Dynamic Key Area

4.2.3 AES with Dynamic Key Delay

This section shows the Timing Summary of AES with Dynamic Key

```
Timing Summary:
---------------
Speed Grade: -2

   Minimum period: 3.867ns (Maximum Frequency: 258.59
   Minimum input arrival time before clock: 24.220ns
   Maximum output required time after clock: 1.416ns
   Maximum combinational path delay: 4.843ns
```

Figure 4.8: AES with Dynamic Key Delay

4.3 Modified S Box Based AES With Dynamic KeySchematic

The S Box Based AES With Dynamic Key module is obtained as shown below

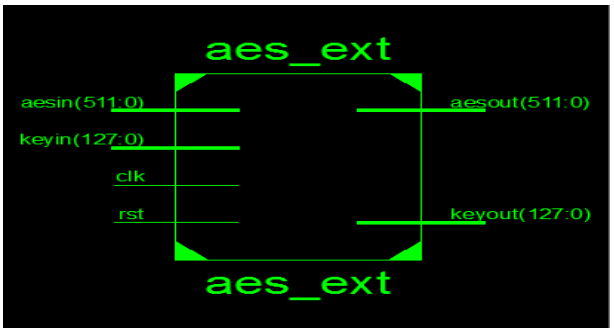

Figure 4.9: Modified S Box Based AES withDynamic KeySchematic

4.3.1Simulation of AES with Dynamic Key with Modified S Box

Thesimulation results of AES with Dynamic Key with Modified S Boxwhen the input of 512-bit i,e.aesin[511:0] = 12345 and key size of 128bit i,e. keyin[127:0] = 56 is given, we obtained output value aesout [511:0] = 12345 same as AES input.

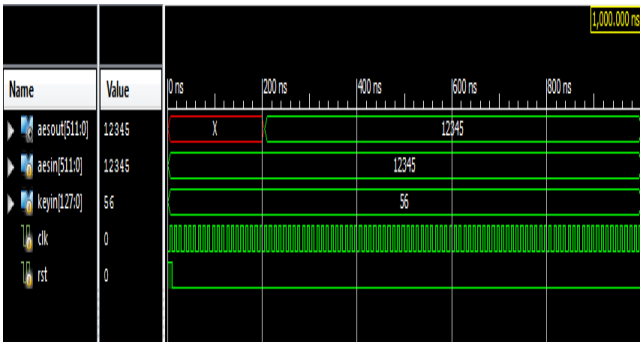

Figure 4.10: Simulation of AES with Dynamic Key with Modified S Box

4.3.2Modified S Box Based AES with Dynamic Key Area

The device utilization summary of Modified S Box Based AES with Dynamic Key Area is obtained as shown below

Device Utilization Summary (estimated values)			
Logic Utilization	**Used**	**Available**	**Utilization**
Number of Slice Registers	10240	93120	10%
Number of Slice LUTs	58557	46560	125%
Number of fully used LUT-FF pairs	9728	59069	16%
Number of bonded IOBs	1281	240	533%
Number of BUFG/BUFGCTRLs	1	32	3%

Figure 4.11: Modified S Box Based AES with Dynamic Key Area Results

4.3.3**Modified S-Box Based AES with Dynamic Key Delay Results**

The timing summary of Modified S Box Based AES with Dynamic Keyis obtained as shown below

```
Timing Summary:
---------------
Speed Grade: -2

   Minimum period: 2.557ns (Maximum Frequency: 391.129MHz)
   Minimum input arrival time before clock: 25.975ns
   Maximum output required time after clock: 1.416ns
   Maximum combinational path delay: 4.318ns
```

Figure 4.12: Modified S Box Based AES with Dynamic Key Delay Results

4.4 Comparison of Results of AES

The comparison between Existing AES, Proposed AES with Dynamic Key, and Modified AES with Dynamic Key is shown below

Parameter	Existing AES	Proposed AES with Dynamic Key	Modified S-Box Based AES With Dynamic Key
Area (LUTs)	6595	87095	58557
Delay (ns)	4.150	3.867	2.557
F_{max} (Mhz)	240.990	258.9	391.129

Table 1: Comparison of Results of AES

From the above comparison we can observe that Modified S-Box AES with Dynamic Key has a significantimprovement in power compared to Existing AES & Proposed AES with Dynamic Key that is, it occupies less area, operates with less delay, and high frequency.

4.5PowerComparison of Conventional and S-Box

The power comparison of conventional and modified S Box is shown below, says that there is a significantimprovement in power of Modified S-Box compared to Normal S-Box, where modified S-Box consumes power of 0.1118mW, whereas Normal S-Box consumes 0.8886mW

Table 2: Power Comparison of Conventional and Modified S Box

Parameter	Normal S Box	Modified S Box
Power (mW)	0.8886	0.1118

All the above results are obtained on the Xilinx Virtex6 FPGA board.

V. CONCLUSION

AES is a widely used encryption algorithm. It is a symmetric cipher that uses the same key for both encryption and decryption. Thus, the security depends on the key, and hence a new architecture with the dynamic key generation unit is proposed. This reduces the probability of finding the key least. In order to be used such architecture in low power and high-speed applications a modified s box is used.

FUTURE SCOPE

The probability of finding the key is inversely proportional to the number of transmitted frames. Thus,security can be further increased if we increase the number of frames.

REFERENCES

1. J. Daemen and V. Rijmen, “The Block cipher Rijndael”, An overview Of IEEE on smart card Research and Applications, CA, 2000, Vol.1820, pp. 227-284.
2. Judy H. Moore; Gustavus J. Simmons, “Cycle Structure of the DES for Keys Having Palindromic (or Anti-palindromic) Sequences of Round Keys”, IEEE Transactions on Engineering Management, Volume: 48, Issue: 3, Aug 2001.
3. C. Sanchez-Avilaf; R. Sanchez-Reillot, “The Rijndael block cipher (AES proposal): a comparison with DES”, Security Technology, 2001 IEEE 35th International Carnahan Conference on, 07 August
4. Federal Information Processing Standards Publications (FIPS-197), “Advanced Encryption Standard (AES)”, 2001.
5. J. Daemen and V. Rijmen, “The Design of Rijndael AES-The Advanced Encryption Standard”, Springer Publications, 2002.
6. C. Sanchez-Avilaf; R. Sanchez-Reillot, “The Rijndael block cipher (AES proposal) a comparison with DES”, Security Technology, 2001 IEEE, 07 August 2002.
7. Kishan Chand Gupta and Palash Sarkar, “Improved Construction of Non-linear Resiliant

S-Boxes", IEEE Transactions on Information Theory, Vol. 51, No.1, pp.341- 358, 2005.
8. Christof Paar and Jan Pelzl, "Understanding Cryptography", Springer Publications, 2012.
9. Vinayak Bajirao Patil, "Implementation of AES algorithm on ARM processor for wireless network", International Journal of Advanced Research in Computer and Communication Engineering, Vol. 2, Issue 8, August 2013.
10. M. Gomes, R. Da Rosa Righi, and C. A. Da Costa, "Internet of things scalability: Analyzing the bottlenecks and proposing alternatives", Int. Congr. Ultra Mod. Telecommun. Control Syst. Work., Vol. 2015–Janua.J.
11. ZuharMusliyana, "Security enhancement of advanced encryption standard (AES) using time-based dynamic key generation", ARPN Journal of Engineering and Applied Sciences, Vol. 10, No. 18, October 2015.
12. M. Gomes, R. Da Rosa Righi, and C. A. Da Costa, "Internet of things scalability: Analyzing the bottlenecks and proposing alternatives", Int. Congr. Ultra-ModeTelecommunication Control Syst. Work., Vol. 2015–Janua.J.
13. FlevinaJoneseD'souza, "Advanced Encryption Standard (AES) Security Enhancement using Hybrid Approach", in Computing, Communication, and Automation (ICCCA), 2017 International Conference on, 5-6 May 2017.
14. Ishfaq Ali; Muhammad Asif "Applying Security Patterns for authorization of users in IoT Based Applications", Engineering and Emerging Technologies (ICEET), 2018 International Conference on, 22-23 Feb. 2018.
15. This link is available at https://en.wikipedia. org/wiki/Rijndael_S-boxaccessed on 02-12-2019
16. This link is available at https://www.random.org /bytes accessed on 02-07-2019
17. This link is available at https://en.wikipedia.org /wiki/Random_number_generation accessed on 02-12-2019
18. This link is available at https://en.wikipedia.org/ wiki/Block_cipher_mode_of_operationaccessed on 05-04-2020
19. This link is available at http://www.webopedia. com /TERM/C/cryptanalysis.htmlaccessed on 30-07-2020
20. This link is available athttp://www.securearc. com /wiki/index.php.AssetValueaccessed on 12-09-2020

AUTHOR DETAILS:

	**Miss M. Leekshika** has received her **Bachelor of Engineering (B.E.)** in **Electronics and Communication Engineering (ECE)** from Stanley College of Engineering and Technology for Women, O.U affiliated college in 2016. She is pursuing her **Master of Engineering (M.E.)** in **Electronics and Communication Engineering** (**Specialization - Digital Systems**) from,O.U affiliated college in 2020.Her area of Research Interest is **Network Security & Cryptography**.
	**Mrs. M. SrilakshmiRavali** working as **Assistant Professor** at Stanley College of Engineering and Technology for Women. She received her Bachelor degree in **Electronics and Communication Engineering (ECE)** from Mahaveer Institute of Science & Technology, **M.S.ECE (VLSI)** from Southern Illinois University Carbondale. Her area of research interest is **VLSI & Communications.**