International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 11 Issue 05, May-2022

Securing IOT Systems using VHDL Implementation

Dr. S. Vijaya Lakshmi[1], R. Giridhar[2], A. Jhansi Priyanka[3] and K. Sreekar[4]
[1,] Assistant Professor,
[2, 3,] 4Final Year,
Department of Electronics & Engineering, Vel Tech Rangarajan
Dr. Sagunthala R&D Institute of Science and Technology, Chennai, Tamilnadu.

***Abstract*:- The risks encountered in digital communication system are unauthorized access, denial of service, data corruption, leakage, attack monitoring, authentication and destruction, etc. These problems arise while performing various electronic activities such as video/text transfer, communication, e-commerce, etc. More algorithmic procedures/steps are released to reduce risk. The AES algorithm was used as part of this study. This type of security algorithm makes it possible to analyze performance research. All encoding and decoding transformations are simulated using an iterative design approach to minimize hardware consumption.Design was performed in Xilinx Vivado software. The results obtained for the encryption and decryption procedures show a significant improvement in the performance of the algorithm. In this project, AES 128-bit encryption and decryption was performed using the Verilog hardware description language and simulated using Vivado.**

Keywords: Digital Communication System, Authentication, AES, Encryption, Decryption.

1 INTRODUCTION

The risks encountered in digital communication systems are unauthorized access, denial of service, data corruption, leaks, attack monitoring, authentication and trashing, etc. These problems arise while performing various electronic activities such as video/text transfer, communication, e-commerce, etc. More algorithmic procedures/steps are released to reduce risk. We may use firewalls, detection systems, security through cryptography and other algorithms. The need for secure data communication is increasing with the development of several cryptographic algorithms such as DES, 3DES, AES, RSA, SHA, RC5, etc. The basic idea of a cryptocurrency algorithm is to secure data while transmitting data in the network. The data that needs to be transmitted from the sender to the receiver in the network must be encrypted using an encryption algorithm. By using a decoding technique, the receiver can view the original data. The AES algorithm has been proven in many papers to be effective in hardware and software implementations. It can use data of different length, e.g. 128,192 or 256 bits to deal with a private key of the same length. Subbyte, Shift row, Mixed Column and Add Round are the four basic The basic plot of Algorithm is shown in the figure 1.. operations performed in 10, 12, or 14 rounds/rep. The Mixed Column operation will not be performed on the last turn.

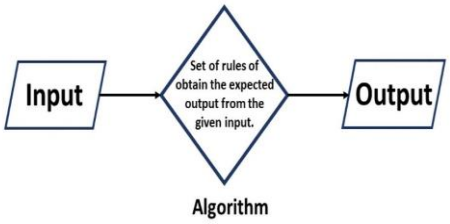

Fig 1: General view of Algorithm

A. Background of AES Algorithm

The National Institute of Standards and Technology (NIST) has begun a process to develop a The Information Processing Standard (FIPS) for Advanced Encryption Standard (AES), specifies an advanced encryption algorithm to replace the expired Data Encryption Standard (DES) in 1998. Rijndael was chosen because it has the best overall score in Safety, Performance, Efficiency, performance and flexibility.

The Rijndael algorithm is a symmetric block cipher that can process 128-bit data blocks via uses encryption keys of length 128, 192, and 256 bits. AES algorithms like Rijndael are also a A symmetric block cipher can encrypt (encode) and decrypt (decrypt) information [1]. encode converts data into a cryptic form called ciphertext. Decrypt the data transformation ciphertext in its original form, called the plaintext. The number of spins depends on the key length as described in Table I [3].

The basic AES encryption and decryption structure with different stages is shown in FIGURE I. This block diagram is general to the AES specifications. It consists of a number of different transformations applied consecutively on the bits of the data block, in a fixed number of iterations, known as loops [2]. The number of rounds depends on the length of the key used for the encryption process. The Advanced Coding Standard can be programmed in software or built in pure hardware [5].

Table 1: Key-Block- Round Combinations

Bit Size	Key Length	Number Of Rounds
128	4	10
196	6	12
256	8	14

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 11 Issue 05, May-2022

2 PROPOSED ARCHITECTURE

AES is mainly composed of two units namely Computer Science the other unit is the main expansion unit. Data processing unit with four main modules or transformations where subbyte toggles, row changes, column shuffles, and adding round keys are all involved and the key expansion unit generates the round key for the next round. Total encryption and decryption process is shown in the figure 2 and figure 3.

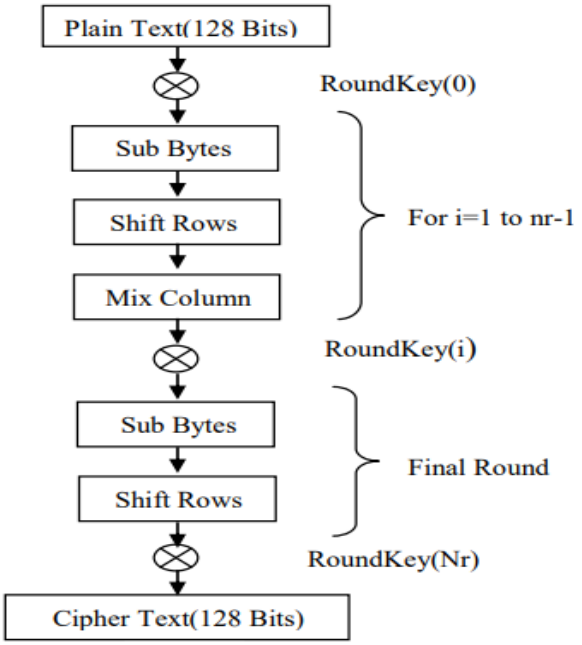

Fig .2: AES Encryption Process

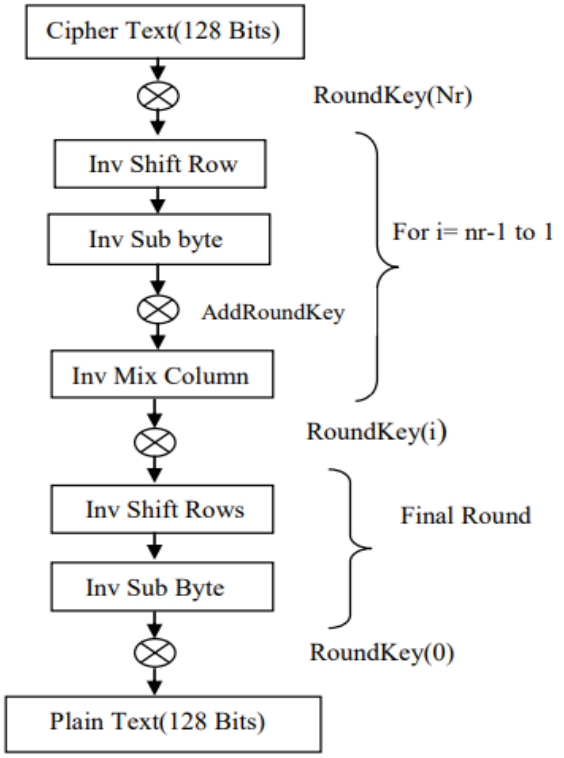

Fig.3 AES Decryption Process

3 TRANSFORMATION PROCESS IN AES

a. Sub-Byte Transformation

The Byte Substitution transformation is a nonlinear substitution of bytes that operates independently on each byte of state uses an alternate table (Sbox) [2]. The subbyte transformation is shown in figure 4 . In the AES implementation, the design of the Sbox plays an important role in the optimization. There are two approaches to Sbox design. Design a multiply inverse and a separate affine transform or Build a logic circuit that defines the input and output of the Sbox function.

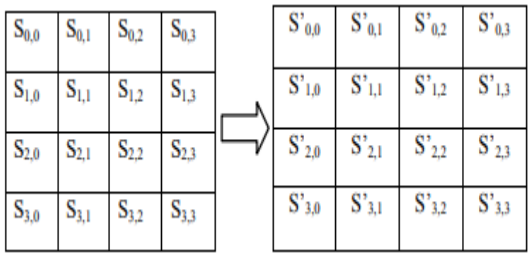

Fig .4: Expansion of Sub Byte Transformation.

b. Shift-Row Transformation

In Shift row shifting, the bytes of the last three rows of the report are shifted cyclically
different number of bytes (difference). The first row, r = 0, is left unshifted, while the second, third, and fourth rows cyclically shift one byte, two bytes, and three bytes to the left, respectively [3]. The row shift transformation is shown in figure 5.

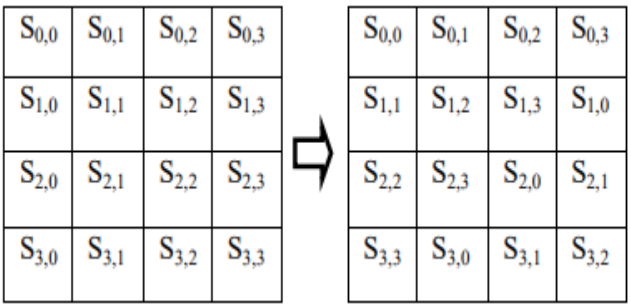

Fig .5: Row shift Transformation.

c. Mix Column Transformation

This process is used to shuffle the bytes of each column separately during the transfer. The corresponding transformation in decoding is denoted by Inv Mix columns and means inverse mixture transform column [3]. The goal here is to continue shuffling the 128-bit input block.
The mix column implementation is shown in figure 6.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 11 Issue 05, May-2022

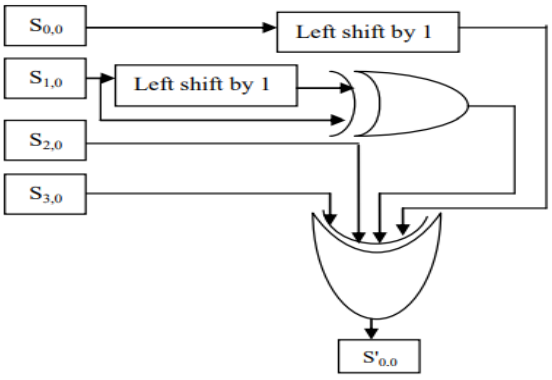

Fig .6: Mix Column Implementation.

d. Adding Round Key

In this operation, the round key is applied to the State by a simple bitwise XOR [4]. Basically, the Key Extender is used to generate the next round key because for three different key sizes AES consists of 10, 12 or 14 rounds. So, after each round, a new round lock must be produced. So this unit generates this turn key for each turn [5]. This unit also uses the concept of byte shifting and byte substitution that was used in the data processing unit [6].

4 RESULTS AND DISCUSSION

VHDL is used because the hardware description language due to the ability to trade among environments. The software program used for this paintings is Xilinx 6 and the waveforms are simulated with the assist of version sim simulator. This is used for writing, debugging, simulating and checking the overall performance outcomes the use of the simulation equipment to be had on Xilinx 6. All the outcomes are primarily based totally on simulations from the Xilinx, the use of Timing Analyzer and Waveform Generator. All the character transformation of each encryption and decryption are simulated the use of FPGA ACEX1K own circle of relatives.

In order to permit a complete parallel technique of the nation, it's miles important to put in force all of the adjustments over 128 bits. The maximum high-priced one is the Byte substitution, due to the fact it's miles a desk research operation, applied as ROM. Each eight bits calls for a 2048 bit ROM. To technique 128 bits it's miles important 32768 bits. The Key Expansion makes use of a Byte substitution operation over 32 bits also, so any other 8192 bits need to be allocated. This layout makes use of 32% of the location of EP1K100FC484-1, round 1631 good judgment factors are ate up to put in force simplest eight-bit S-container research desk. Hence, about 20,000 good judgment factors are important to put in force the entire 128-bit byte substitution transformation. It may be finished through the APEX20K own circle of relatives devices.

The decryption implementation outcomes are much like the encryption implementation. The key time table technology module is changed with inside the opposite order. In which final spherical secret is handled because the first spherical and lowering order follows. The inputs are clock of 100ns time period, Active High reset, and eight-bit nation as a popular good judgment vector, whose output is eight-bit Inverse S-container research substitution. This layout makes use of 50% of the location, round 877 good judgment factors are ate up to put in force simplest eight-bit S-container research desk. The final encryption and decryption result for AES algorithm using VHDL is shown in figure 7 and 8.

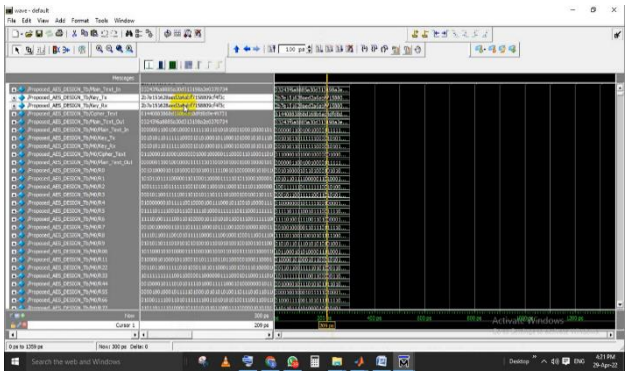

Fig .7: Result obtained for encryption in AES algorithm

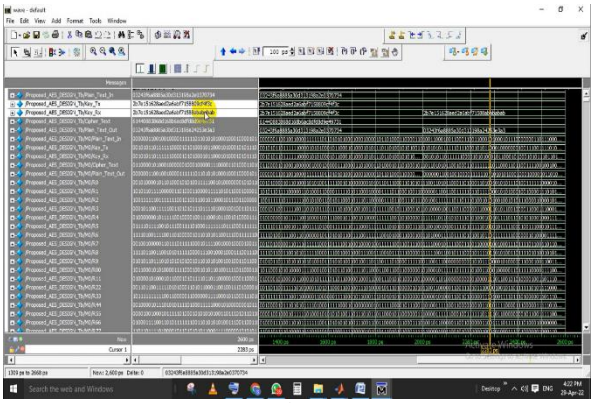

Fig .8: Result obtained for decryption in AES algorithm

5 CONCLUSION

Because encryption plays a leading role in today's world. Therefore, frequency is the main issue You can minimize the time. Optimized and synthesizable VHDL code was developed to implement both encryption and decryption processes. This report explained the basics of the AES algorithm and how to implement it using VHDL. This is a simulation It runs on different device families. The software used is Xilinx and the waveforms are simulated using a model simulation simulator. Therefore, AES can actually be implemented on the FPGA with reasonable efficiency, using encryption and decryption, respectively.

REFERENCES

[1] Manteena R. A VHDL Implemetation of the Advanced Encryption Standard-Rijndael Algorithm.
[2] Sharma R, Gehlot P, Biradar SR. VHDL Implementation of AES-128. UACEE International Journal of Advances in Electronics Engineering–IJAEE. 2013 Jun 5;3(2):17-20.
[3] Gehlot P, Sharma R, Biradar SR. VHDL Implementation of AES Algorithm.
[4] Subbarao D, Swapnakumari B. Implementation of AES-256 encryption algorithm on FPGA. International Journal. 2015 Apr 4;104.
[5] Sumathi, M., Nirmala, D. and Rajkumar, R.I., 2015. Study of Data Security Algorithms using Verilog HDL. International Journal of Electrical & Computer Engineering (2088-8708), 5(5).

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 11 Issue 05, May-2022

[6] Florin, R. and Ionut, R., 2019, October. FPGA based architecture for securing IoT with blockchain. In 2019 International Conference on Speech Technology and Human-Computer Dialogue (SpeD) (pp. 1-8). IEEE.

[7] Anitha Kumari, S. and Mandi, M.V., Implementation of Present Cipher on FPGA for IoT Applications.