International Journal of Engineering Science Invention (IJESI)
ISSN (Online): 2319 – 6734, ISSN (Print): 2319 – 6726
www.ijesi.org ||Volume 8 Issue 02 Series. II || Feb 2019 || PP 13-16

Implementation of a Secure Encrypted data layer for IOT Applications on a reconfigurable hardware

Dr. Vijay Lakshmi.D[1], Pooja Nayak.N[2]
[1](Assistant Professor, ECE, Bangalore Institute of Technology, India)
[2](Mtech Student, ECE, Bangalore Institute of Technology, India)
Corresponding Author: Dr. Vijay Lakshmi. D

ABSTRACT : *The Advanced Encryption Standard (AES), a Federal Information Processing Standard , is an approved cryptographic algorithm that can be used to protect electronic data. The AES can be programmed in software or built with pure hardware. However, Field Programmable Gate Arrays (FPGAs) offer a quicker and more customizable solution. This project presents the AES algorithm with regard to FPGA and Verilog language. Quartus II 13.02 software is used for simulation and optimization of the synthesizable Verilog code. Synthesizing and implementation (i.e. Translate, Map and Place and Route) of the code is carried out on Cyclone II FPGA board. The DE2 FGPA device of Cyclone Family is used for hardware evaluation. This method can make it a very low-complexity architecture, especially in saving the hardware resource in implementing the AES Sub Bytes module and Mix columns module etc. The proposed architecture is suited for hardware-critical applications, such as GPON network security, ATM Machines, smart card, PDA, and mobile phone, etc.*

KEYWORDS – *AES, Cryptography, Cyclone, Encryption, Quartus II*

Date of Submission: 03-02-2019 Date of acceptance: 19-02-2019

I. INTRODUCTION

Cryptography is the science of secret codes, enabling the confidentiality of Communication through an insecure channel. It protects against unauthorized parties by preventing unauthorized alteration of use. In a broader sense Cryptography is best known as a way of keeping the contents of a message secret. Confidentiality of network communications, for example, is of great importance for e-commerce and other network applications. However, the applications of cryptography go far beyond simple confidentiality. In particular, cryptography allows the network business and customer to verify the authenticity and integrity of their transactions. If the trend to a global electronic marketplace continues, better cryptographic techniques will have to be developed to protect business transactions.

II. ADVANCED ENCRYPTION STANDARD

The Advanced Encryption Standard (AES), also referenced as Rijndael (its original name), is a specification for the encryption of electronic data established by the U.S. National Institute of Standards and Technology (NIST) in 2001. The AES is a subset of a much larger encryption algorithm known as Rijndael, which become one among many proposals to the NIST competing for becoming a widespread encryption algorithm. On October of 2000, the NIST introduced the Rijndael algorithm as the winner due to high-quality normal routing in security, overall performance, efficiency, implementation capability, and ease.

The Advanced Encryption Standard (AES) Algorithm, adopted by the U.S. government in 2001, is a block cipher transforms 128-bit data blocks under a 128-bit, 192-bit or 256-bit secret key, by means of permutation and substitution. The AES algorithm will be used for many applications within the government an in the private sector. Breaking an AES encrypted cipher text by trying all possible keys is currently computationally infeasible with technology advances.

III. AES ALGORITHM

The Advanced Encryption Standard (AES) Algorithm is a block cipher transforms 128-bit data blocks under a 128-bit, 192-bit or 256-bit secret key, by means of permutation and substitution. The AES algorithm is a symmetric cipher. In Symmetric ciphers, a single secret key is used for both the encryption and decryption, whereas in asymmetric ciphers, there are two sets of keys referred to as a private key and public keys.

For the AES algorithm**,** the length of the input block, the output block and the State is 128 bits. This is represented by Nb = 4, which reflects the number of 32-bit words (number of columns) in the State. The length of the Cipher Key, K, is 128, 192, or 256 bits**.** The key length is represented by Nk = 4, 6, or 8, which reflects

the number of 32-bit words (number of columns) in the Cipher Key. The number of rounds to be performed during the execution of the algorithm is dependent on the key size. The number of rounds is represented by Nr, where Nr =10 when Nk = 4, Nr = 12 when Nk = 6, and Nr = 14 when Nk = 8.

The transformations performed in each state array are different and each round depends on cipher key. Each round of AES cipher(except the last one) consists of all the following transformations. Sub Bytes(s-box), Shift Rows, Mix Columns, Add Round Key.

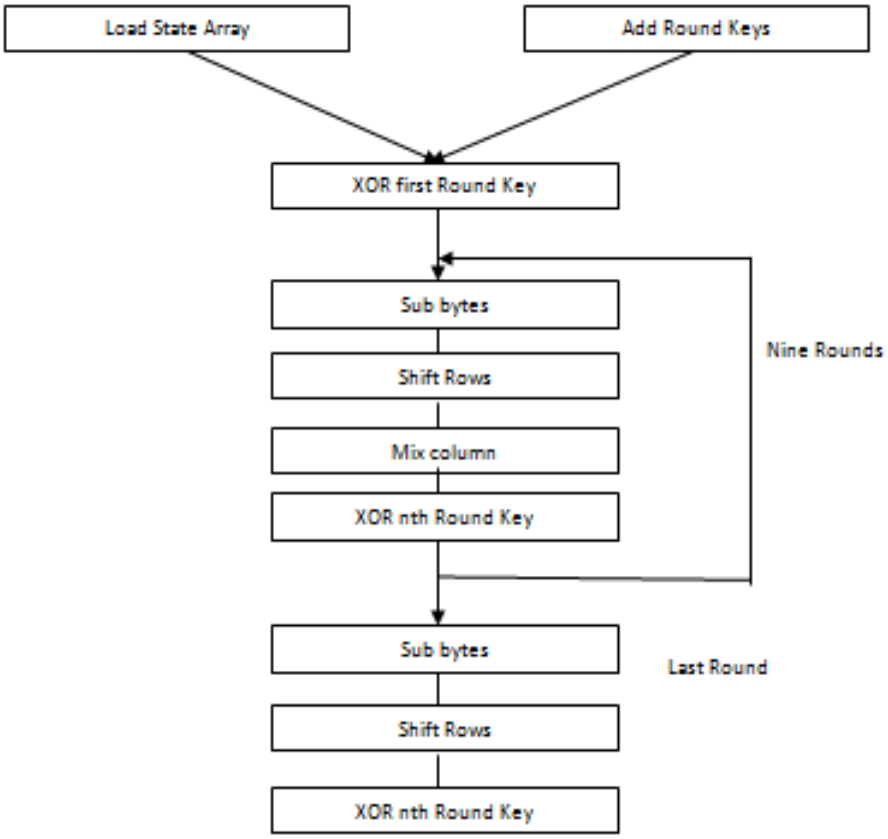

Fig.3.1 AES Algorithm

The Sub-Bytes Step**:** Sub Bytes operation is a non-linear byte substitution, operating on each byte of the state independently. The substitution table (S-Box) is invertible and is constructed by the composition of two transformations:

1. Take the multiplicative inverse in Rijndael's finite field
2. Apply an affine transformation

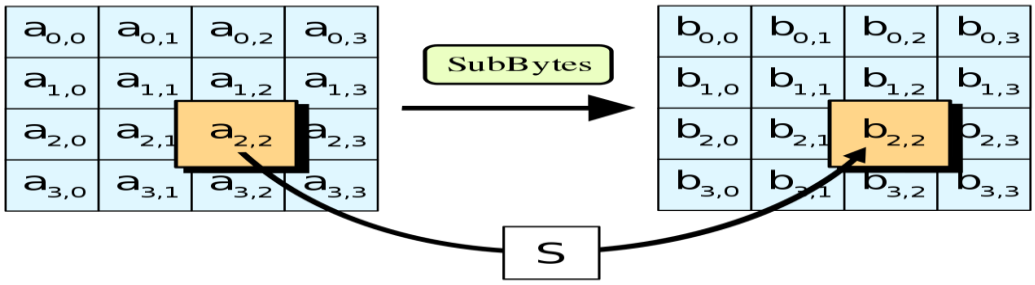

Fig.3.2 Sub Byte Operation

Shift Row Operation: In this operation, each row of the state is cyclically shifted to the left, depending on the row index. The 1st row is shifted 0 positions to the left. The 2nd row is shifted 1 position to the left. The 3rd row is shifted 2 positions to the left. The 4th row is shifted 3 positions to the left.

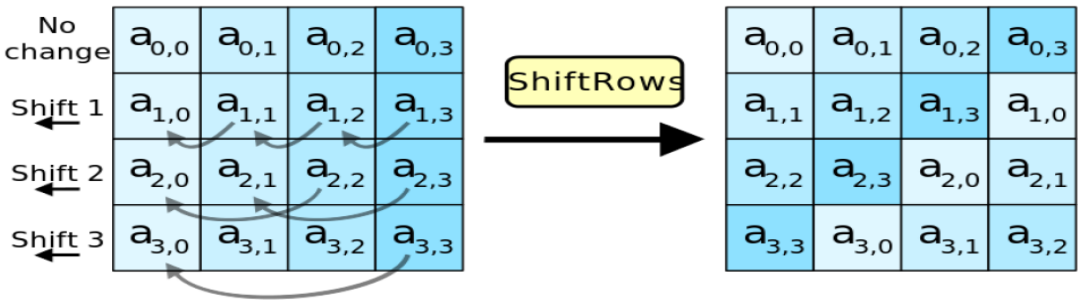

Fig.3.3 Shift Row Operation

Mix Colum Operation: In the Mix Columns step, the four bytes of each column of the state are combined using an invertible linear transformation. The Mix Columns function takes four bytes as input and outputs four bytes, where each input byte affects all four output bytes.

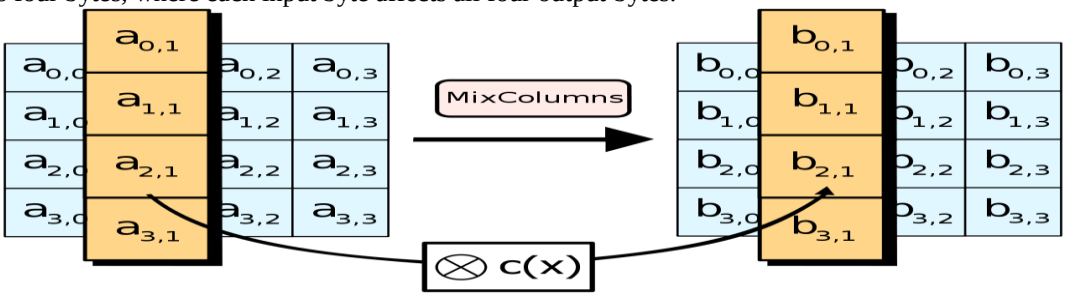

Fig.3.4 Mix Column Operation

IV. KEY GENERATOR OPERATION

The key generator circuit functions to generate unique key for every round operation in AES algorithm. Key expander (or generator) operation basically follows five steps to generate a unique key for each round. User defined is fed as an input to Key expander circuit to find the key generated output.

As shown in the figure, the key expansion takes place on a four-word to four-word basis, in the sense that each grouping of four words decides what the next grouping of four words will be.

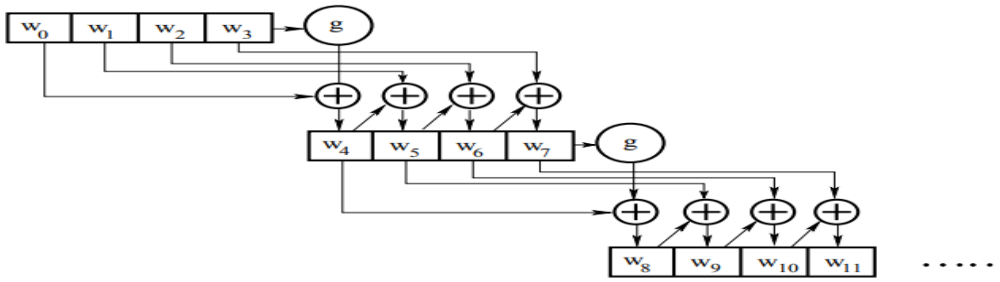

Fig.4.1 Key generation Operation

The primary function of Add Round Key Operation is to associate key expander output generated by key generator Circuit to the AES algorithm. In this operation, a Round Key is applied to the state by a simple bitwise XOR. The Round Key is derived from the Cipher Key by the means of the key schedule. The Round Key length is equal to the block key length (=16 bytes).

Add round key Output is given by XOR ing of Key expansion output and Mix column output. The above output is the encrypted output of round 1. The Add round key output is again feedback to the Sub Byte transformation through feedback loop for 2nd round of operation end the same process is repeated until it completes 10 rounds of operation.

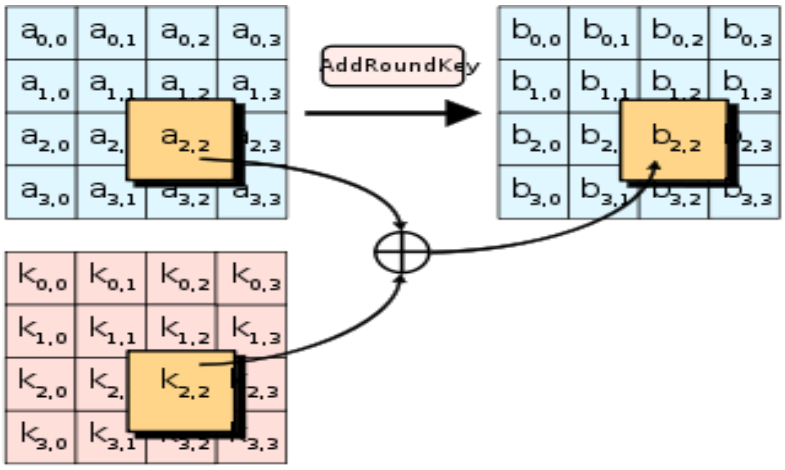

Fig.4.2Add Round Key Operation

V. CONCLUSION

Optimized and Synthesizable VERILOG code is developed for the implementation of encryption process. Each program is tested with some of the sample vectors provided by NIST and output results are perfect with minimal delay and hardware. Therefore, AES can indeed be implemented with reasonable efficiency on an DE2 FPGA. The time varies from chip to chip and the calculated delay time can only be regarded as approximate.

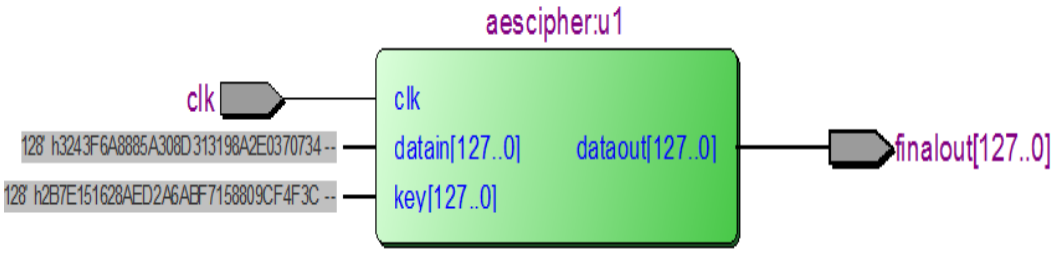

Fig.5.1 RTL Schematic

REFERENCES

[1]. Abhiram.L.S, Gowrav.L, Punith Kumar.H.L & Sriroop.B.K, Manjunath.C.Lakkannavar, "Design and synthesis of Dual Key based AES Encryption", MSRIT, Bangalore, India, 21-22 November 2014 978- 1-4799-6546-5/14/$31.00©2014 IEEE.

[2]. Milind Mathur & Ayush Kesarwani, "Comparison Between DES , 3DES , RC2 , RC6 , BLOWFISH and AES National Conference on New Horizons in IT - NCNHIT 2013 ISBN 978-93-82338-79-6.

[3]. Ankita Nampalliwar & Sheeja Suresh , "Design and Implementation of AES Algorithm Using FPGA" ISSN: 2321-7782 (Online) ,Volume 2, Issue 1, January 2014 ,International Journal of Advance Research in Computer Science and Management Studies.

[4]. Ahmed A. Mohamed & Ahmed H. Madian, "A Modified Rijndael Algorithm and its Implementation using FPGA 978-1-4244-8157 ©2010 IEEE, ICECS 2010.

[5]. Kenneth Stevens & Otmane Ait Mohamed, "Single-chip FPGA Implementation of a Pipelined, Memory-Based AES Rijndael Encryption Design" 0-7803-8886 ©2005 IEEE CCECE/CCGEI, Saskatoon, May 2005.

[6]. Cyclone II FPGA Starter Kit Board User Guide.

[7]. William Stallings, "Cryptography and Network Security Principles and Practice", Sixth Edition.

[8]. Abha Sachdev, Mohit Bhansali. (2013, April 9) "Enhancing Cloud Computing Security using AES Algorithm", International Journal of Computer Applications

[9]. Manpreet Kaur, Rajbir Singh. (2013, May 18) "Implementing Encryption Algorithms to Enhance Data Security of Cloud in Cloud Computing", International Journal of Computer Applications

[10]. Ritu Pahal, Vikas kumar. (2013, July 7) "Efficient Implementation of AES", International Journal of Advanced Research in Computer Science and Software Engineering

Dr. Vijay Lakshmi.D" Implementation of a Secure Encrypted data layer for IOT Applications on a reconfigurable hardware" International Journal Of Engineering Science Invention (Ijesi), Vol. 08, No. 02, 2019, Pp 13-16