AN EFFICIENT IMPLEMENTATION OF AES ON FPGA FOR PROTECTION OF IOT DATA

1st .Shelly R. Wankhede [1] , 2nd Dinesh B.Bhoyar [2] 3rd Swati K.Mohod

[1] *Shelly R. Wankhede, Department of Electronics and Telecommunication , Yashwantrao chavan College of Engineering and Technology,Nagpur, Maharashtra, India*
[2] *Dinesh B.Bhoyar Department of Electronics and Telecommunication , Yashwantrao chavan College of Engineering and Technology, Nagpur,Maharashtra, India*
[3]*Swati K.Mohod, Department of Electronics and Telecommunication,Rajiv Gandhi college of Engineering and Research , Nagpur, Maharashtra, India*

ABSTRACT

The Internet of Things the internet connectivity of various devices like desktop and laptop computers, smart phones and everyday things that utilize embedded technology to interact with the environment, all through the Internet

.Encryption for protection or security of IOT Data can be done with the help of IP address which is through the internet connectivity which forms a network of physical objects. The interaction that is established between the objects and different internet enabled devices in a given area.

The encryption and decryption is been carried out on Field Programmable Gate Array (FPGA) to make the system independent cryptosystem. The proposed design on Xilinx, and is verified the result using the synthesis tool of Xilinx ISE-Design software. The encryption and decryption is being done on VHDL. In this era where the whole world are been connected to each other by the means of communication where internet plays a very important role and where Data security is also very important in this paper we present a algorithm for security of data from different attacks with the help of AES (Advanced Encryption Standard).In this algorithm where we are using the symmetric key block cipher where the key would be given same with respect to encryption. Many applications it can be used as it is lossless operation. We limit our focus on 12b8 bit AES encryption and decryption where coded in VHDL coding. The proposed paper describes the private key cryptosystems which has a key with fixed size.

Keyword : - *AES, FPGA, Key, IOT, Cloud Security, VHDL*

1. INTRODUCTION

In the cloud with the help of IOT many devices would be connected in coming years. The data in it is very important and private and the accessibility should be provided to only authorize servers.This paper highlights on the encryption of the data before transmission at the edge of IOT device by AES Hardware and protecting the decryption of the stored data by key. The key is only accessible to the authorized users [3].

In this paper describes process carried out for AES algorithm of its encryption and decryption [3]. And shows us the block diagram for the process to secure IOT data used for the transmission and receiving of the data.

Now a day's demand for Data security has been growing rapidly due to different threats which can retrieve the important data which is vital and should be secured.

As data security handles two practices for developing of security based algorithms namely:

- To store the integrity of data
- To store information of data in

Mainly the world depends on different software that protects the vital information. As we noticing that world is been using digital technology in each and every field which have increased the different threats with which data can be hacked with the help of wrong means.Cryptography is the one which can be applicable for securing data which will provide us the solution for different attacks or hacking of data.

There are different algorithms for cryptography which are divided into two;

- Stream cipher and
- Block cipher

For security purposes such as privacy of multimedia and visual surveillance systems in which block cipher cryptography is used for protection

. From the below diagram, there is plain text which is the original text which is critical in nature which is need to be protected against different threats which can be espionage and fraudulent cyber attack. Then by applying the different transformation which is called as the encryption process we get the plain text in the form of cipher text. On the other side the decryption process is been carried out which would be the inverse transformation and after this inverse transformation we get the original text or the plain text. For securing the data i.e. digital data often used as encompass mathematics, applied statistics and code programming.

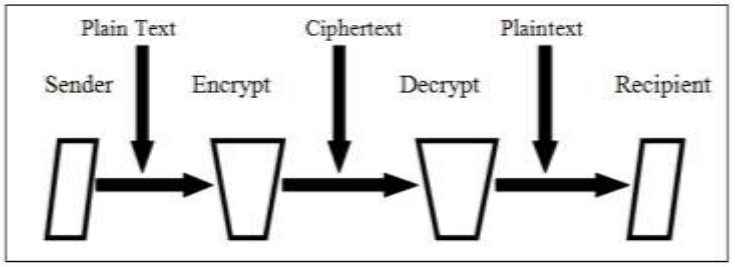

Fig 1:The Basic Encryption And Decryption Process.

2. ADVANCED ENCYPTION STANDARD(AES)

Stands for Advanced encryption standard it is approved for cryptography algorithm that is used to protect our electronic data. THE NIST has given an replacement of DES which was of 64 bits i.e. its block size was 64 bits.A new symmetric key was was used replacing the DES standard which is the AES standard. A private key block cipher is used by AES. Block size of 128 bit is been encrypted by it. There are three different key lengths in AES standard which are as 128 bit ,196 bit and 256 bit, key can't be available for public use .there are different rounds for each key length as shown in the diagram AES is an cryptographic algorithm which is used to protect data from theft and other means. The AES Algorithm can be symmetric as well asymmetric block cipher in which symmetric key is same during encryption and decryption process and asymmetric having in which key is different during encryption and decryption process.

The encryption process is used to convert Data into cipher form or coded form which could not understood by the public and the different thefts can be reduced with the help of encryption process. In Decryption the data or the cipher is again gets converted into the original form or plain text. The AES algorithm used cryptographic keys of 128, 192, and 256 bits to encrypt and decrypt data in blocks of 128 bits. The different algorithms are MARS, RC6, RIJNDAEL, SERPENT and TWOFISH. The conclusion was that the five Competitors showed similar characteristics. After having a study of the above algorithms Rijndael algorithm came to be best with respect to security,performance,efficiency,implementation and flexibility.

Table No.1 :Different Key Length

	Key Length	Block Size	Number Of Rounds
AES-128	4	4(128)	10
AES-192	6	4(128)	12
AES-256	8	4(128)	14

In this section we would we discussing different functionalities which are been used for the AES algorithm and addressing issues such as area, power and throughput. Some are very popular with respect to performance, size and power in the architectures. It is said that each and every technique has advantages and disadvantages or limitations. The excellence of cryptography is not only securing data or protecting it but also taking in considering or based on the time taken to perform the encryption[1].AES (Advanced Standard Standard) is employed for encryption which is designed which is adaptive on a development platform.

AES is an algorithm which is commonly known as Rijindael is a symmetric cipher which is been provided by NIST for protecting data.VHDL coding is been done for the employment of AES algorithm which has different transformations in the encryption process and at decryption process[1].

3. AES ENCRYPTION AND DECRYPTION

In this part we would give the encoding process for the AES algorithm. The algorithm divides different blocks of 128 bit which are the XOR block to provide the 1st round and so on which is been applied to input and output logical and no logical operations. The addition to the encryption and decryption process there is a key expansion processThe transformations that out are namely Sub Bytes, Shift Rows, Mix Columns, AddRoundKey.

The AES design has the original input and the secret key which would be the private key then by combining the original message and the cipher key we get the cipher text which could be an unintelligent form for the public. The input can be 192 bit and 256 bit also. The AES are only having three inputs which are 128 bit, 192 bit and 256 bit. We are using a 128 bit input then from cipher block; the output would be a cipher text. For 128 bit, 192bit and 256 bit we have 10, 12, 14 rounds. There are regular rounds for each bit which are 9, 11, 13 and the final round which are different i.e. 10th, 12th and 14th.

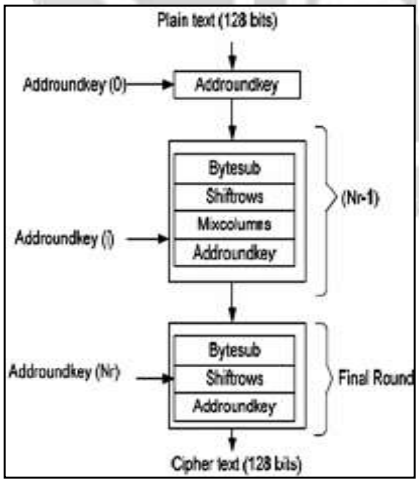

Fig 2 : Encryption Process

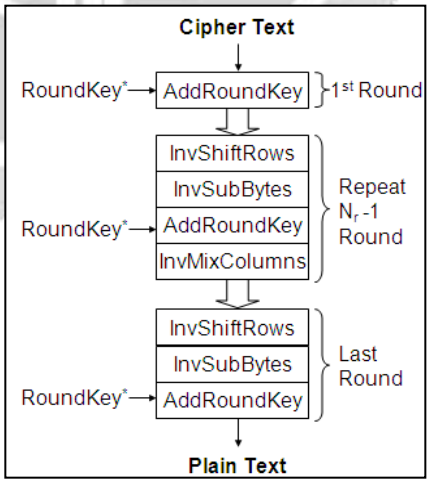

Fig 3: Decryption Process

Decryption is an inverse procedure of encryption It is used for obtaining the plain text from given cipher text. The key is same. In decryption the s-box is inverse of that which was used in encryption. With the help of VHDL the encrypted data which is the ciphered data, plain text can be obtained. Decryption is the inverse form of encryption.

The different tasks for decryption are as follows:

- Add Round Key
- Inv Mix Columns
- Inv Shift Rows
- Inv Sub Bytes

AES involves three steps which are follows:

- Key generation,
- Encryption
- Decryption

- **Key Generation**:Each round has its own round key that is derived from the original 128-bit encryption key in the manner described in this section it involves XORing of the round key with the state array.

- **Encryption** :The plain text is given to encrypt i.e. in an encoded form which is the ciphered text

- **Decryption**:The ciphered text from the encryption process is been decoded and then the plain text is obtained.

3.1 Key Expansion

Most of the key expansions are performed based on

- ROT WORD (4 bytes: circular shift)
- SUB WORD (4bytes: substitution)
- RCON
- XOR

As we know that for generating the cipher text we have to generate a series with round keys .Word is generated with help of key Expansion , word substitution i.e. subword rotation is used for two word processing Subword takes a four-byte input word and applies an S-box to each of the four bytes to produce an output word. RotWord takes a four-byte word and performs a cyclic permutation.

4.BLOCK DIAGRAM

As shown in block diagram there is an AES module which does the work of both encryption and decryption and AES encryption module can be executed by hardware and software module. In Hardware module integration is to be done and the we would be comparing the different parameters performance parameters with respect to the earlier ones. The data is taken as hexadecimal in the encryption and decryption phase.

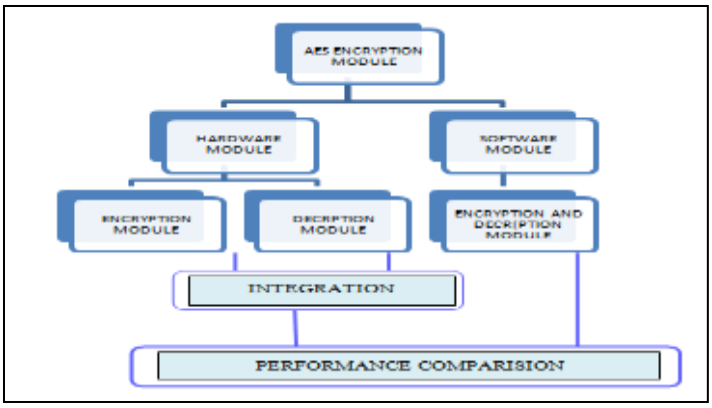

Fig 4: Block Diagram

5. PROPOSED ALGORITHM

The device that is the edge device generates the data. Firstly the data pushed to the cloud our data is the cloud offline data which is the hexadecimal data.There are different attacks such as spoofing, sniffing etc.It is very much safe to encrypt the data before transmission hence an hardware would be needed which is an AES performed on FPGA .For proper reception of encrypted data can cause attack so with the help of AES encryption and decryption

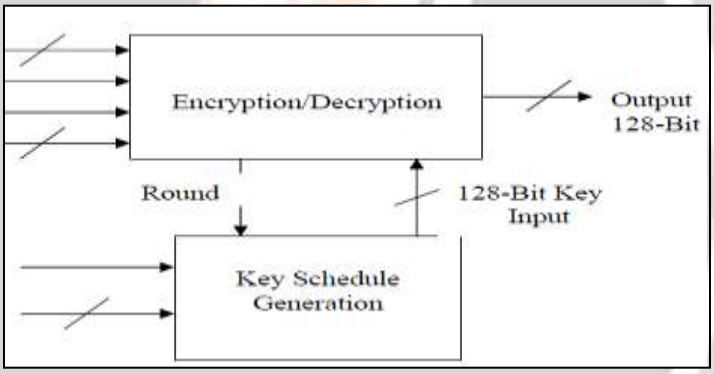

Fig 5: Proposed Algorithm

6. RESULTS

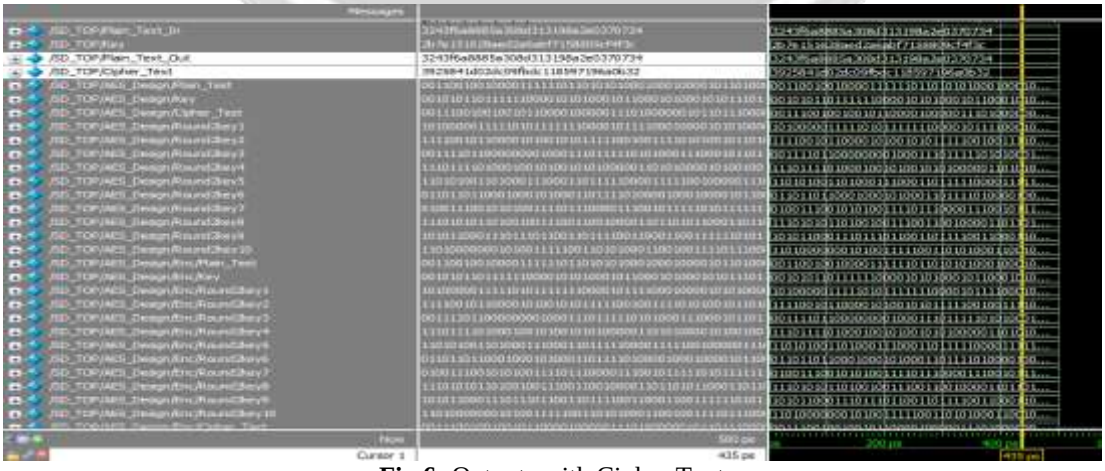

Fig 6: Outputs with Cipher Text

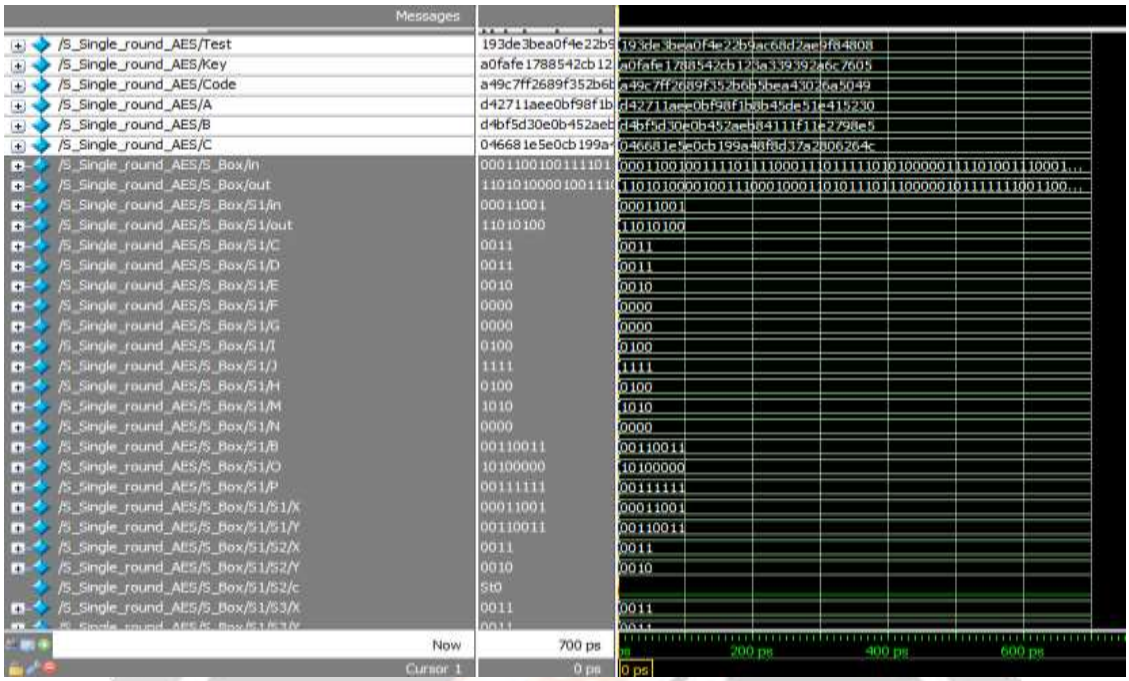

Fig 7: Output after 1st round i.e. is the plain text

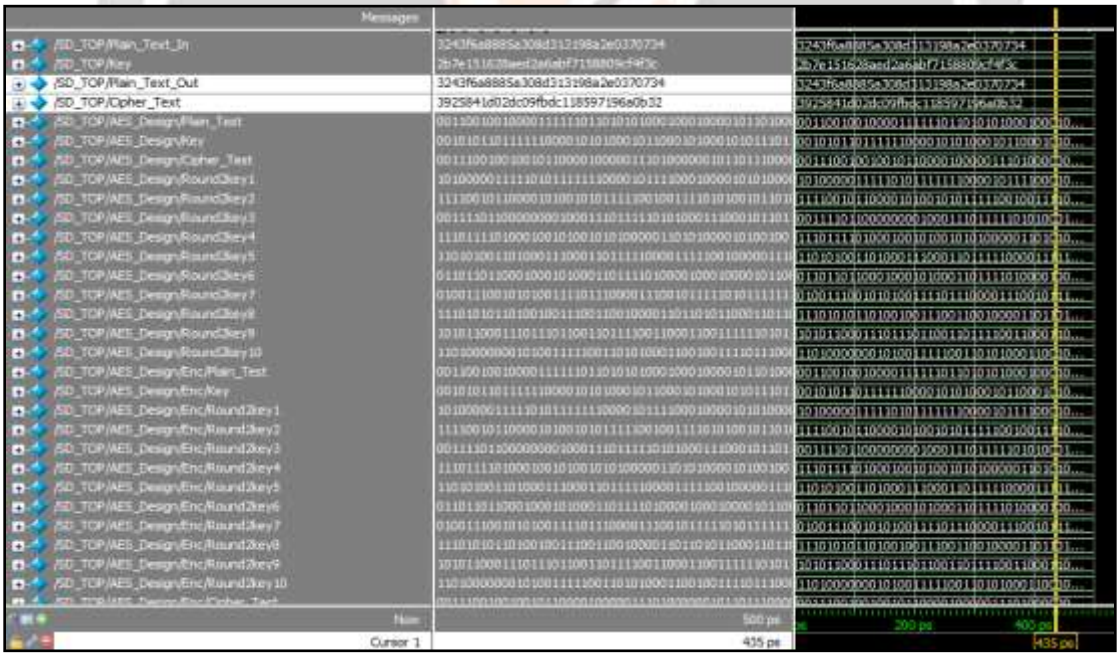

Fig 8: Output after 10th round i.e. is the plain tex

7. FUTURE SCOPE

Future scope would be that to secure IOT data the vital information generated by edge device. The algorithm can be put forward for much secured asymmetric key encryption. [3] This approach can be made complex to hack by using session key generation at the time for request. For reducing power and for faster processing an

application specific integrated circuit should be designed. The optimization of the design can be carried out to improve the power efficiency and area efficiency [1]

6. REFERENCES

[1] Abdulla El Bouchti, Samir Bahsani, Trik Nahhal "Encryption as a Service for Data Healthcare CloudSecurity ", Fifth International Conference on Future Generation Communication Technologies(FGCT 2016)

[2] Sheetal U. Jonwal, Pratibha P. Shingare "Advanced Encryption Standard (AES)implementation on FPGA with hardware in loop", International Conference on Trends in Electronics and Informatics ICEI 2017

[3] Y Chandu, K. S. Rakesh Kumar, Ninad Vivek Prabhukhanolkar, A N Anish, Sushma Rawal. "Design and implementation of hybrid encryption for security of IOT data", 2017 International Conference On Smart Technologies For Smart Nation 2017

[4] Amit Kumar, Manoj Kumar, P. Balramudu."Implementation of AES algorithm using VHDL", 2017 International Conference on Computing Methodologies and Communication (ICCMC)

[5] Ali E. Taki El_Deen, El-Sayed A. El-Badawy, Sameh N. Gobran" Digital Image Encryption Based on RSA Algorithm" IOSR Journal of Electronics and Communication Engineering (IOSR-JECE) e-ISSN: 2278-2834,p- ISSN: 2278-8735.Volume 9, Issue 1, Ver. IV (Jan. 2014), PP 69-73

[6] W. Stallings, Cryptography and Network Security: Principles and Practices, 3rd edition, Prentice Hall, NJ, 2003.

[7] R. L. Rivest, A. Shamir and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystem,'· Commun. ACM, vol.21 no. 2, pp. 120-126