International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2018 IJSRCSEIT | Volume 3 | Issue 1 | ISSN : 2456-3307

Secure Prominent Data Transmission through Advance Encryption Standard

[1]V. Swarupa, [2]Ch. Loknadh
[1]M.Tech-Scholar, Department of ECE, Malineni Perumallu Educational Society, Guntur, , Andhra Pradesh, India
[2]Associate Professor, Department of ECE, Malineni Perumallu Educational Society, Guntur, , Andhra Pradesh, India

ABSTRACT

To implement the advanced encryption standard (AES) algorithm in efficient way throughput architecture is proposed. In this proposed architecture we are using integrated AES encryption and decryption designs. Now the entire architecture consists of 128 bits which are divided into two parts mainly they are higher and lower parts. But the proposed AES will perform the operation at lower part. In proposed architecture we perform some operations like sub-byte substitution and INV sub-byte substitution. At each stage of this substitution, it will perform a normal AES Operation but the computation is reduced by half. So in the proposed architecture the sub-type and INV sub-byte substitutions will give reduction in critical path delay and also the key expansion modules.

Keywords : Advanced Encryption Standard (AES), Sub-Byte Substitution Cloud Computing

I. INTRODUCTION

From past ten years the internet, wireless communication and high security communications have increased a lot. But for all these communications we need reliable computations. Now an advanced encryption standard AES algorithm is proposed for the purpose of high security and internet applications.

This advanced encryption standard AES algorithm is approved by the national institute of standards and technologies. This institute will give high security for many applications. Various modifications are done at each level Of AES encryption and decryption techniques. The main intent of this proposed approach is to decrease the critical path delay with fewer computations and to reduce the area. Next coming to the model of cloud computing, it integrates the much technological advancement like virtualization, web services and service level agreement.

Because of huge development in technologies many number of customers and service providers has increased and all users move towards the cloud environment. Generally, different cloud services are used by the government, military and commercial systems to provide the network connectivity and service availability to end users. Here the cloud provides three fundamental models to provide services to the users. The three fundamental models are given as 1. Infrastructure as a service (Iaas) 2. Platform as a service (Paas)and 3. Software as a service (Saas). As there are different advantages in the cloud computing but security is the major issue. Many researchers have focused on this issue to overcome.

Basically, cloud infrastructure is mainly available in private and public cloud. Coming to the private cloud, it consists of only one organisation or customer where the hosted services are given to limited number of people's. Next coming to the public cloud, the entire infrastructure is owned and managed by the cloud provider by itself. Here the security and data confidentiality are more important. Here the quality of service management is an important issue because of increase in number of cloud users. In cloud computing this quality of service management is referred as the activities of quality service management should meet the end to end user's applications.

Here the cryptography is nothing but converting the plane text to cipher text at the transmission end and by using a channel this data is transmitted and again the cipher text is converted into plane text. We use different types of algorithms in cryptography but get highly security we use the AES algorithm. The AES algorithm will provide the FIPS approved cryptographic algorithm for providing secure data transmission. Here the AES algorithm will perform the byte wise operations in four ways they are 1. Byte substitution using substitution table 2. By using different offsets shift row operations are performed on state array. 3. The data is mixed with the each column of state array and 4. At last adding round key to the state. The AES algorithm is most widely used in voice communication, network appliance's, virtual private network.

As discussed earlier about the operations AES performs four basic operations, let us first discuss about the first operation that is sub-byte operation. This sub-byte operation is also known as non linear byte substitution method. Here the each byte operation is performed individually. Coming to shift row operation, the first row will not be shifted and second row is shifted by one circular shift and third row is shifted by two circular shifts. Next is mix column operation, here each column occupies 4 bytes of linear transformation. It takes four inputs and produces four outputs. The last operation is add round key operation, this operation is performed on simple bit wise XOR and block length is equal to 16 bytes. These are the operations which are performed by the AES algorithm. Now let us discuss about the proposed system of AES encryption standard algorithm

II. PROPOSED SYSTEM

The below figure (1) shows the block formation of AES algorithm. Depending upon the online file processing applications the proposed system will use a prototype. Here this appliance is hosted by the online cloud data base which is provided by the cloud provider go daddy. Basically it is an US based cloud service provider. The main purpose of using this service is to run the applications in very fast way. In this model one system acts as microcontroller where the user can access the information from anywhere at any time from the internet. The main intent of this proposed system is to secure the data with confidentiality.

Let us discuss this with an example, if the user wants to access the information for uploading then he or she should have to register with their email-id and phone number to the system. Here the username and password should be created by the user not by the system. After the process of registration the user can login and upload the data with confidentiality. Before uploading the file to cloud the use will get an encryption file as individual blocks. Now at last click on the save button to use that file for future use. This is the normal way to secure data in cloud computing. Coming to the medical applications, there is no need to carry hard copy or soft copy, instead of that the user can share the copy at anytime from anywhere. But here the important thing is to remember the secret file-id. The file id may in the form of numbers, alphanumeric characters and special characters. Here to upload a file there is no limit of length but it takes time to upload the file. In the proposed encryption algorithm we use 128 bit keys and they perform 10 rounds for this 128 bit keys in proposed system. Depending upon the file size, the file splits into different blocks.

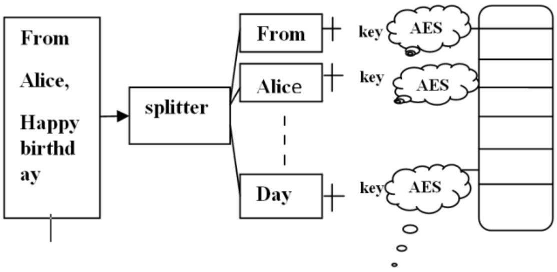


FIG. 1. Proposed System

These blocks are encrypted individually and block wise encryption is uploaded to the cloud. The upload process is done in different locations by using block-id and file-id. Now in such a case if anyone like the cloud and wanted to get a file from the server then the clod doesn't give total information of that file because it is saved in different locations and the information is in encrypted form. So the person who knows the secret-id can get the total information from the cloud. Here the proposed system provides the data by using online editing facility. In this process the user can edit the data and as well as upload the data without downloading. This process is done by only the actual users only the other users can only view the data. So from this we can say that the proposed system will secure the data in a confidential way.

III. RESULTS

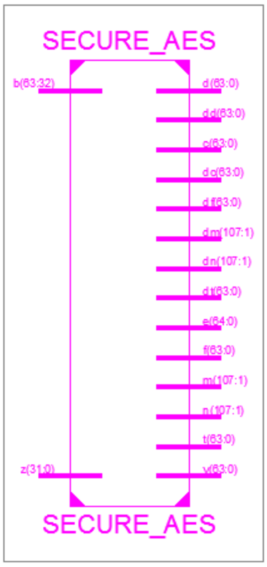


FIG.2 RTL Schematic

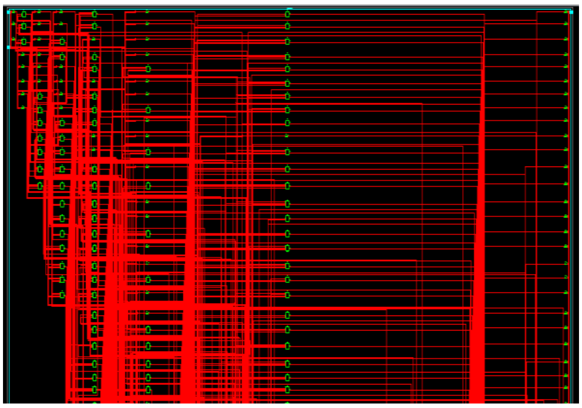
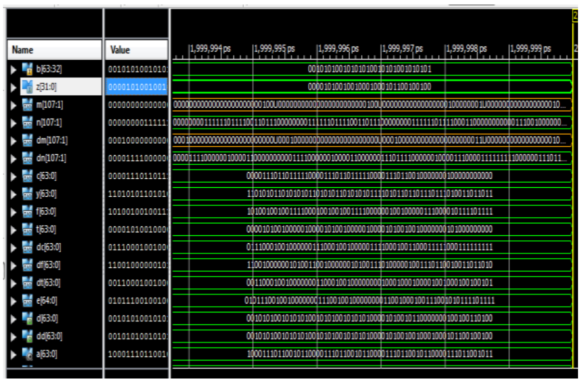


FIG.3 Technology Schematic



```
Name        Value
b[63:32]    001010100101010
z[31:0]     000010100100100
m[107:1]    000000000000000
n[107:1]    000000000111111
dm[107:1]   000100000000000
dn[107:1]   000011110000000
c[63:0]     000011101101101
y[63:0]     110101011010101
f[63:0]     101001001001011
t[63:0]     000010100100000
dc[63:0]    011100010010010
df[63:0]    110010000001010
dt[63:0]    001100010010010
e[64:0]     010111001001001
d[63:0]     001010100101010
dd[63:0]    001010100101010
a[63:0]     100011101100100
```

FIG.4 Output Waveform

IV. CONCLUSION

The proposed method is designed by using the novel method. As discussed earlier that AES algorithm performs four basic operations. In this the sub byte substitution method utilizes the less blocks of RAMs and as well as some modifications are done in mix column substitution. By using the sub byte and INV sub byte modules in proposed system there will be less delay and low power consumption. The proposed system provides better security compared to the existed one. 128 bit encryption is provided for the purpose of data confidentiality. Depending upon the performance of delay the proposed approach is analysed. So from this we can say that if the delay is increased then the size of file will be increased. This problem is overcome in our proposed system.

V. REFERENCES

[1]. National Institute of Standards and Technology, "Advanced Encryption Standard (AES)," 2001.

[2]. S. K. Mathew, et al. "53 Gbps native GF(24)2 composite field AES-encrypt/decrypt accelerator forcontent-protection in 45nm High performance microprocessors, "IEEEJournalOfSoli d-StateCircuits,vol.46,no.4,pp.767 776,April2011.

[3]. M. Mozaffari-Kermani and A. Reyhani-Masoleh, "Efficient highperformance parallel hardware architectures for the AES GCM,"IEEETransactions on Computers, vol. 61, no. 8, pp. 1165-1178, August2012.

[4]. S.-F. Hsiaso, M.-C. Chen and C.-S. Tu, "Memoryfree low cost Designs of Advanced Encryption Standard using common sub expression elemination for Sub functions in transformations,"IEEE Transactions on Circuits and Systems, vol. 53, no. 3, pp. 615-626,March 2006.

[5]. X. Zhang and K. K. Parhi, "High speed VLSI architectures for theAES algorithm,"IEEE Transactions on Very Large Scale Integration (VLSI) Systems, vol. 12, no. 9, pp. 957-967, September 2004.

[6]. S. K. Reddy S, R. Sakthivel and P. Praneeth, "VLSI implementation of AES crypto processor for high throughput,"International Journal ofAdvanced Engineering Sciences and Technologies, vol. 6, no. 1, pp.022-026, 2011.

Authors :

V. SWARUPA completed her B.Tech at Priyadarshini College of Engineering and Technology, Guntur and puring M.Tech at Malineni Perumallu Educational Society, Guntur. Her area of interest is VLSI.

CH. LOKNADH completed his B.Tech at Nalanda Institute of Engineering and Technology, Kantepudi and M.Tech at RVRJC College of Engineering. He has 5 years of teaching experience and at present he is working as Associate professor at Malineni Perumallu Educational Society, Guntur.