ISSN:0975-9646

Faster Transfer of AES Encrypted Data over Network

Suvarna Patil[#1], Rahul Patil[*2],

[#]*M. E. Computer Department, Pune University*
PCCOE College INDIA

[*]Assist. Prof. Department of Computer Engineering &
In-charge Systems, Pimpri Chinchwad College of Engineering, Pune 44, India

***Abstract*— Cryptographic algorithm can be used to transfer the encrypted data securely on the network. AES encryption algorithm is used in many cryptographic applications. For this, various cryptographic algorithms are used for the security of different types of data like audio or video data transfer on the network. Advanced Encryption Standard (AES) is a NIST (National Institute of Standards and Technology) specification of the encryption and decryption electronic data. AES suffered the drawback of slow processing and large time of data transferring, so to speed up the process of the AES algorithm, we apply AES algorithm in parallel. Following is four sections that describe the paper: First is, we presented basic introduction of AES algorithm, Second is, a survey on related algorithms has been presented, third, discusses the proposed model and finally forth concludes.**

***Keywords*— AES algorithm, HD images, Security, Cryptography.**

I. INTRODUCTION

In 2001 Joan Daemen and Vincent Rijmen was developed AES algorithm and in 2002 NIST selected AES as standard ciphering algorithm in. AES algorithm has three versions which are dependent on the key length like AES128 bit, AES192 bit, and AES 256 bit and 128 bit block data which constructed in 4x4 matrixes called state.
AES algorithm is a very popular and strong encryption algorithm which has a number of advantages in data ciphering. Encryption algorithm is best method used to keeping the information security. The information is changed into an inapprehensible form in the encryption algorithms. AES is one of the public cryptography and widely used in large number of applications such as smart card, cell phone, automated teller machines, and www servers. The AES algorithm is suffer from some drawbacks like, patterns appearance, long encryption and decryption time in the ciphered image.

This document is a template. An electronic copy can be downloaded from the conference website. For questions on paper guidelines, please contact the conference publications committee as indicated on the conference website. Information about final paper submission is available from the conference website.

A. *BACKGROUND AES ALGORITHM*

The DES algorithm is replaced by the AES algorithm in 1997 by NIST. The 64-bit block triple-DES had become very popular at that time, but this block length was very small and it was as well slow. The double-DES algorithm is not very harder to break.
The NIST has selected a block cipher which is to be effective from May 26, 2002 that is called as the RIJNDAEL. Previously the AES algorithm has given this name because Vincent Rijmen and Joan Daemen have created this algorithm. The symmetric key encryption algorithm is used to encrypt sensitive information. The RIJNDAEL encryption algorithm was originally a variable block size 16, 24, 32 bytes and variable key size 16, 24, 32 bytes. The NIST decided that define AES with a block size of 16 bytes.
The private-key cryptography must be implemented by the AES algorithm. AES algorithm is a block cipher, it is also called as an iterated cipher because it repeating the steps multiple times and fixed number of bytes it operates, which makes it simpler to explain and implement. AES algorithm is used as a secret key encryption algorithm. AES algorithm and most of the encryption algorithms are the reversible type. In the AES algorithm the encryption and decryption has performed reverse action in both the steps.

B. *AES REQUIREMENT*

The AES algorithm is work on 128-bit blocks and it support 3 different keys sizes: 128, 192, and 256 bits. Following is the size of N rounds which is dependent on the key length: N = 10 for 128-bit keys, N = 12 for 192-bit keys, and N = 14 for 256-bit keys. The AES algorithm is available on a royalty free basis for the world if it is selected.
The AES algorithm rounds depend on the following key size.

TABLE 1

Key Size(bytes)	Block Size(bytes)	Rounds
16	16	10
24	16	12
32	16	14

AES perform following four operations:

I. ADD ROUND KEY (XORs the round key with the state),
II. BYTE SUB (a substitution using an S-box),
III. SHIFT ROW (a permutation),
IV. MIX COLUMN (unless it is the last round),

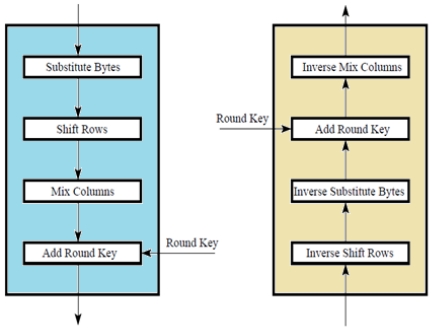


Fig. 1 The encryption process step is shown at left and decryption process step is shown at right.

To make the AES algorithm reversible in the decryption process, the last round step Mix Column is not performed.

II. Related Work

Previously, in paper [1] different security encryption mechanism for wireless network was described. In this paper cryptographic algorithms AES, CAST and RC5 is analyzed. It provides major security services like confidentiality. In paper [2] the concept of steganography is used to transmit the data secretly and safely and hide behind image. In this only authorized user is able to get the original data. In paper [3] first transforms the text into an image using an RGB substitution method, and after that it encrypts the image using AES algorithm will lead to a highly secure transmission of text. In paper [4] at bit level the parallel AES algorithm is diffusing the blocks and the Bit-Ratio analysis is increased and hence the AES algorithm becomes stronger against Brute-Force. In paper [5] conversion of file containing text is done using AES algorithm and key will be encrypted using Elliptic Curve Cryptography (ECC) algorithm which is called as the hybrid cryptography.

III. Proposed Work

Traditionally while transferring secured data over network lot of time is wasted in encrypting and decrypting audio data, video data and image at sender's and receiver's end. The ciphered images have created the problem of patterns appearance in the AES algorithm because in these images similar colour is present in the original image. Here we used the AES algorithm that was proposed in [8]. The modification is mainly focused on ShiftRow transformations, if the value of 1'st element in state is even, the second and third rows are shifted right one and two times respectively, else the first and third rows are unchanged and each byte of the second and fourth rows of the state are cyclically shifted left over different number of bytes. This modification allows to remove the patterns appear.

This paper has focused on reducing the time of encryption and decryption using parallel processing. Consider following scenario to understand the proposed work.

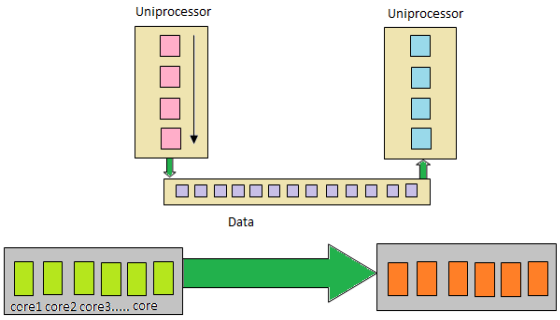
There is a file of 5 megabit (5242880 bits) which needs to be sent from sender to receiver. Using a 128 bit AES algorithm the number of steps required will be 5242880/128=40960. This means 40960 data blocks will be created on which AES will be applied individually. But using the parallel approach the number of steps required will be 40960/64=640 where 64 is number of processors. The total time required to process the data will be reduced by number of processor time's Uniprocessor time. The proposed approach initially breaks the input file into 128 partitions.

Total Time required for Uniprocessor = $\frac{N}{128} * \text{AES Execution Time}$ ….. (1)

Total Time required for Parallel approach = $\frac{N}{128} * \frac{\text{AES Execution Time}}{n}$ ….. (2)

Where, x = File Size in bits
n = no. of processor

Fig. 2 Transfer of Secured Data by Sequential and Parallel Method



IV. Conclusions

The cryptographic algorithm can be used for accomplishing the security of encrypted data that can be transmitted over the network. AES encryption algorithm is used in many cryptographic applications. Several techniques have been proposed for implementation of the AES algorithm. AES algorithm is working slowly because it is computationally expensive, in particular with audio, video and image data encryption. In our proposed work we managed to overcome the drawback of slow processing and the time of encryption and decryption using parallel processing.

References

[1] Bhavin Patel, Neha Pandya, "Data Transfer Security solution for Wireless Sensor Network," International Journal of Computer Applications Technology and Research Volume 2–Issue 1, 63-66, 2013.

[2] Divyani UdayKumar Singh et al, "Separable Reversible Data Hiding in Image Using Advanced Encryption Standard with Fake Data Generation," International Journal of Computer Science and Information Technologies, Volume 5 (3), 2014.

[3] Sourabh Singh, Anurag Jain, "An Enhanced Text to Image Encryption Technique using RGB Substitution and AES," International Journal of Engineering Trends and Technology (IJETT) – Volume 4, 2013.

[4] Salim M. Wadi, Nasharuddin Zainal, "Rapid Encryption Method Based on AES Algorithm for Grey Scale HD Image Encryption," The 4th International Conference on Electrical Engineering and Informatics (ICEEI), 2013.

[5] K.Brindha, G.Ramya, Rajpal Amit Jayantila, "Secured Data Transfer in Wireless Networks Using Hybrid Cryptography," International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, 2013.

[6] Adam Berent, "Advanced Encryption Standard by Example".

[7] Amin B. Mobhani, "Diffusion of Cipher Blocks at Bit Level in Parallel AES to Improve Bit – Ratio Test thus Increasing

Cryptanalysis Complexity," International Journal of Current Engineering and Technology, Volume.4, 2014.

[8] The Advanced Encryption Standard Lecture Notes on, "Computer and Network Security," by Avi Kak.

[9] Kamali, S., H., Shakerian, R., Hedayati, M., Rahmani, M. A New Modified Version of Advanced Encryption Standard Based Algorithm for Image Encryption. International Conference on Electronics and Information Engineering, IEEE, 2010.

[10] Shashank Srivastavaa, Avinash Kumar Singh, G.C. Nandi, "Inter Cipher Block Diffusion: A Novel Transformation for Proposed Parallel AES," 2nd International Conference on Communication, Computing & Security (ICCCS), 2012.