ISSN: 2278 – 909X
International Journal of Advanced Research in Electronics and Communication Engineering (IJARECE)
Volume 5, Issue 1, January 2016

A Review on Low Latency for File Encryption and Decryption Using BRA Algorithm for Secure Transmission of Data

Kalyani V. Gulhane[1], Prof.G.D.Dalvi[2]

Abstract -

The need of reliable and effective security mechanisms to protect information systems is increasing due to the rising magnitude of identity theft in our society. Cryptography involves various techniques for taking user data, readable data, and transforming it into unintelligible form, for the secure transmission over the network, and then using a key to transform it back into readable data when it reaches its destination. The main aim of this study is to increase security in communication by encrypting the information using a key that is created through using an image. Often information security is major obstacle in different areas like bank, transaction ,military, network application. Whenever we want to send file from one location to another location in the network, many unauthorized users are illegally access the information. There are different algorithms like Blowfish, DES,AES, RC5 that achieve more security but increases the complexity of the algorithm and also takes more time for encryption and decryption of files. Our algorithm proposes a method for low latency encryption decryption algorithm that will take smallest amount of time for file encryption and decryption and provide more security. This algorithm can be applied on different types of files. In Byte Rotation Algorithm a random key generation technique is used.

Keywords- Byte Rotation Algorithm, Encryption time, Decryption time, Key generation , Parallel process

I. INTRODUCTION

Cryptography is the art of achieving security by encoding a messages to make them non-readable. It ensures the information security such as confidentiality, data integrity, entity authentication and data origin authentication, also it means hidden writing, and it refers to the technique of using encryption to hide text. Encryption is changing the original data to a secret message, while Decryption is the reverse. Algorithm is the process of encryption and decryption of the data based on a mathematical procedure. Every algorithm and techniques has its own different advantages and disadvantages. Delay, throughput, energy consumption are the important QoS of the Sensor networks. Voice, video, images, and text are examples of real time applications that need to be transmitted quickly with a high level of security. Nowadays, there are many applications that provide real time services , such as Skype and Tango. On the other hand ,there are many suggested algorithms that can be used to protect these applications and to guarantee that unauthorized persons cannot access these services.

The conventional methods of encryption can only maintain the data security. The information could be easily accessed by the unauthorized users for malicious purpose. Therefore it is necessary to apply effective encryption/decryption methods to enhance data security. The multiple encryption and multilevel encryption system provides sufficient security. But as security level is increased, the time for encryption and decryption along with the complexity of algorithm is also increased. Also speed and performance of these system is low. This is the major cause of decreasing the speed and efficiency of the encryption system. In this work we will implement a new encryption algorithm "Byte–Rotation Algorithm" which enhances the security as well as speed of the encryption scheme.

II. LITERATURE REVIEW

Sunita Bhati, Anita Bhati, S. K. Sharma [1] presented a new approach towards Encryption Schemes: Byte – Rotation Encryption Algorithm.The BREA is applied on different blocks of plain text and executes in parallel manner through multithreading concept of single processor system. BREA which is a block cipher and used with Block Wise Parallel Encryption Model. The model has been written into two steps. In the first step, the plaintext has been broken into number of blocks. Each block size is of 16 bytes. So the number of blocks depends on the total input bytes of plain text. Each

block is represented by 2D array. These arrays of blocks are passed into BREA in parallel manner to execute simultaneously by using multithreading concept. The concept will allows all the blocks to process parallel in CPU. Because of parallel execution, the processing speed of the system will enhance.

Kawser Wazed Nafi, Tonny Shekha Kar, Sayed Anisul Hoque Dr. M.M.A Hashem [2] This proposed architecture is based on cloud computing platform. This ensures secure communication system and hiding information from others. AES based file encryption system and asynchronous key system for exchanging information or data is included in this model. This structure can be easily applied with main cloud computing features, e.g. PaaS, SaaS and IaaS. This model also includes onetime password system for user authentication process.

Sonalina Chowdhury[3] this system proposed a new algorithm NCADET (New Combinational Approach using Different Encryption Technique) implemented which was hard to crack as well as give proper security to the information transferred. It is a key exchange Block cipher algorithm .Each block of plain text size 16 bytes. Two different key matrix generated by sender and Receiver must be send to each other with the help of two different channels secretly. Size of key matrix generated by sender and Receiver are 16 bytes each and their value is randomly generated by sender & receiver respectively. The size of actual key matrix use for cryptography is 16 bytes which is obtained from both sender and receiver. The disadvantage of the system is its computation which is very complex and time consuming.

III.PROPOSED WORK

The cryptography is divided into two main categories, the first and the most common category is called classical cryptosystems encryption algorithms (also called single-key or symmetric) which uses a single shared key to encrypt and decrypt a message. The most common algorithms within this category are called Data Encryption Standard AES, Triple DES (data encryption standard), RSA, Blowfish etc. In this system we will implement Byte Rotation Algorithm which gives higher quality result in parameters like encryption time and decryption time as compared to others.

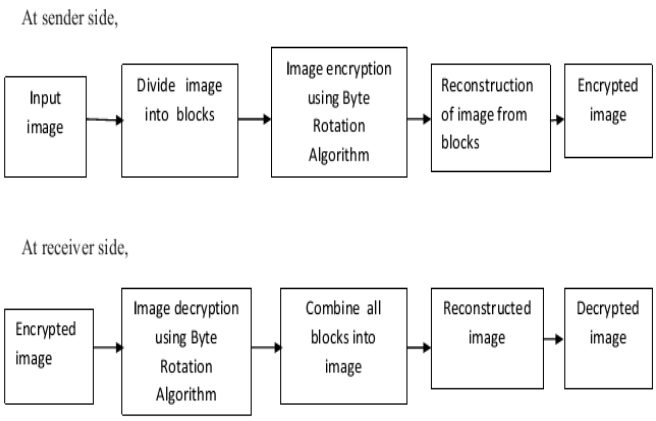

Fig. 1 Block diagram of BRA

.

In architecture diagram shows sender side in which the image file is divided into small number of blocks and BRA encryption technique applied on small block of data to get encrypted image. This encrypted image is decrypted using BRA decryption algorithm and combines the divided blocks into image. At receiver side we get decrypted image i.e. recovered image.

IV.CONCLUSION

In this paper, a low latency for file encryption and decryption technique for secure transmission of data is discussed. This system will give the effective and efficient strategy of making most out of the advantage of Byte Rotation algorithm. The performance of the system will enhance speed of encryption and decryption system. Thus the system is justified for its use in securing files.

ACKNOWLEDGEMENT

I would like to express my sincere thanks towards my guide Prof. G .D. Dalvi for their valuable guidance and constant supervision as well as for providing necessary information regarding the project & also for their support in completing the project. However, it would not have been possible without the kind support and help of many individuals and organizations. I would like to express my special gratitude towards my guide & member of Electronics and Telecommunication Engineering for their kind co-operation and encouragement which help me in completion of this project.

REFERENCES

1] Sunita Bhati, Anita Bhati, S.K. Sharma," A New Approach towards Encryption Algorithm: BREA", Research Paper Published in WCECS 2012,October 24-26,2012,San Francisco, USA.

2] Kawser Wazed Nafi, Tonny Shekha Kar, Sayed Anisul Hoque Dr. M.M.A Hashem "A New User Authentication", File encryption and Distributed Server Based Cloud Computing security architecture" IJACSA Vol. 3, No. 10, 2012.

3]Sonalina Chowdhury, "A New Combinational Approach Using Different Encryption Technique", IJARCSSE, vol-3, Issue-8, ISSN 2777-128X PP.1022-1026, August 2013

4] Gaurav R. Patel, Prof. Krunal Panchal, Sarthak R. Patel "A Comprehensive Study on Various Modifications in RSA Algorithm" ISSN: 2321-9939

5] Nidhi Gouttam, "Implementation of Simulation of Byte Rotation Encryption Algorithm", IJARCSSE, VOL 2, Issue-5, ISSN 2347-4289,2014.

6] Punam V. Maitri, Dattatray S. Waghole, Vivek S. Deshpande "Low latency for file encryption and decryption using Byte Rotation Algorithm",ICPC,2015.

7] Ali M Alshahrani and Prof. Stuart Walker "New Approach in Symmetric Block Cipher Security Using a New Cubical Technique" (IJCSIT) Vol 7, No 1, February 2015.

8] William Stallings, "Cryptography and Network Security", ISBN 81-7758-011-6, Pearson Education, Third Edition.

BIOGRAPHY

Kalyani V. Gulhane is a student of Master of Engineering in Electronics and Telecommunication at P.R. Pote College of Engineering Amravati, India. She is graduated from G.H. Raisoni College of Engineering ,Amravati, India.

Prof. G.D. Dalvi received his M. Tech degree from SSCOE & T, Durg, India. He is a principal of P.R. Pote College of Polytechnic, Amravati in department of Electronics and telecommunication Engineering.