Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 4, Issue. 2, February 2015, pg.80 – 82

RESEARCH ARTICLE

Study of Different Algorithms and Techniques for Secure File Transmission

Siddhant Parkar[1], Neha Koli[2], Karan Shah[3], Asst. Prof. Manisha Giri[4]

[1]Department of Comp. Engineering, Atharva College of Engineering, India
[2]Department of Comp. Engineering, Atharva College of Engineering, India
[3]Department of Comp. Engineering, Atharva College of Engineering, India
[4]Department of Comp. Engineering, Atharva College of Engineering, India

[1] siddparkar@gmail.com; [2] swimmerswan@gmail.com; [3] Karan_shah108@yahoo.com; [4] manisha.giri1@gmail.com

***Abstract*— This paper proposes a method for secure, fast and easy transmission of data. Several algorithms for encryption and compression are considered and discussed for implementation. It takes a huge amount of time to send data through a network. The method proposed is to split a file into multiple parts of user specified size. Further to improve the speed of transmission, compression modules are used. For the data to not be altered or tampered with, and to keep it out of reach of unauthorized persons, encryption plays an important role.**

***Keywords*— Splitting, Merging, Compression, Decompression, Encryption, Decryption**

I. INTRODUCTION

It is vital to keep data out of reach of unauthorized people and to avoid its misuse we have to take steps for encryption of data in real time environment. It takes a huge amount to transfer large amount of data through the network. The proposed software will alter the originality of the text into some encrypted form and the split the encrypted file into user specified size. It takes very less time to send these file through the network. Flexibility of passing information, implementing the encryption standards as per the specification and the algorithm proposed is a major task of the proposed software. The stored information should be in an incomprehensible format. Upon proper request of the user. The application should have a reversal process so as to decrypt the data to its original form. While encryption and decryption is done the application should confirm the standards of authentication and authorization of the user. The user has to merge the file before decrypting them. We need to design an application which provides the users with the flexibility of sending and receiving files or messages in a secured format. In order to convert the normal text to the cipher text for a secure transfer the software design includes the encryption and decryption algorithm. The proposed software will be used to split the user specified file according to the user specified size. We provide a module for data compression as it is quite difficult to transfer one big file from one end to another through any, media like internet or a small storage like flash drive or floppy disk. Each bit of data inside the file will be manipulated by the compression algorithm to minimize the

size without losing any data after decoding which is classified to lossless compression. The basic algorithm is intended to combine with other data compression algorithm to optimize compression ratio. In this way we propose a system that will ensure maximum data security during transmission.

II. ALGORITHMS & TECHNIQUES UNDER CONSIDERATION

We consider and discuss the following encryption algorithms, compression algorithms and splitting merging techniques to find the appropriate combination for the proposed application

1. Encryption Algorithm

1.1 AES (Advanced Encryption Standard).

AES[2] is a symmetric algorithm. It is a block cipher which was adopted by US government in December 2001. Rijndael, an algorithm whose name is derived from its creators, designed and submitted in the 3rd AES[2] candidate conference, was selected in AES. It uses the block of 128 bits and key length of 128, 192 and 256 bits, which depend on the number of rounds. It does not use Fiestal cipher. There are 10, 12 or 14 rounds used for keys 128, 192 and 256 respectively. AES[2] uses the concept of 'State' which is made up of 16 bytes. The state can be represented as a 4 x 4 matrix i.e s[0,0 to s[3,3]. While generating state matrix from the given block of 16 bytes, a columnar transposition is applied on the block.

1.2 Blowfish

Blowfish[3] is a symmetric block cipher invented by Bruce Schneier in 1993.The benefit of Blowfish[3] is that no effective cryptoanalysis has been found for it till date. It provides a large number of cipher suites and encryption products amd hence provides a good encryption rate. Blowfish[3] had a variable keylength from 32 bits up to 448 bits and a 64 bit block size. Blowfish[3] is unpatented, is placed in public domain and can be used by anybody. It was developed to replace DES and was free of the constraints and problems associated with other algorithms.

1.3 CAST

CAST[4] is a 64-bit block cipher with key sizes upto 128-bit. CAST stands for Carlisle and Stafford Tavares. CAST Algorithm consists of a series of rounds of substitution in order to achieve the "confusion" and "diffusion". The algorithm encrypts by dividing the N-bit plaintext input block in half. The left half block, L1 XORs bit by bit the right half block R1which is transformed by a round function F. The two halves are then swapped. R is the number of rounds in the cipher, for which this process is repeated.

2. Data compression Techniques

2.1 G ZIP

G Zip which is a file format as well as a software application is used for compression and decompression. G Zip was shown to work better by Franceschini, Robert ; Dept. of Computer Science, Univ. of Central Florida, Orlando, FL, USA ; Mukherjee, A in their paper, "Data compression using encrypted text"[5], when used with their new text encryption algorithm. This paper presents an algorithm for text compression. The idea behind this algorithm is to define a unique encryption or signature of each word in the dictionary by replacing certain characters in the words by a special character "*" and retaining a few characters so that the word is still retrievable. "*" is the most frequently used character for any encrypted text and the standard compression algorithms can exploit this redundancy in an effective way. The paper reported better results for widely used compression algorithms such as Huffman, arithmetic, gnu-zip with respect to a text corpus. The basic assumption of this algorithm is that the system has access to a dictionary of words used in all the texts along with a corresponding "cryptic" dictionary. Two organizations must share a common dictionary if they wish to exchange information using this compression algorithm.

2.2 Huffman Coding:

Huffman coding is a lossless statistical method that find a variable length code with minimum redundancy. It was created in the early 1950s by David Huffman. The paper, "Huffman Data Compression" [6] by Joseph Lee gives a guide for implementing binary compression algorithms and examines the real life uses that binary trees offer. In Huffman coding, characters that occur most often,

are assigned as few as one or two bits while characters whose occurrence is rare are assigned more bits. In other words, characters or symbols with higher probability of difference get shorter codes. Coding a stream of data using Huffman encoding is done by forming a Huffman tree.

3. Splitting and Merging

The paper "Design and Implementation of a File Splitter and Merger Software"[7] by Muhanad Hayder describes a file splitter tool which has been developed using Java. After splitting the a file, it is saved with an extension .jfs and users have to give path of „*.jfs‟ file to utility for all files to be merged. Object oriented programming With Java2 Standard Edition (J2SE) programming language has been used by this paper. The paper describes in detail the sequence of the splitting and merging, laying a background for us to work on.

III. CONCLUSIONS

In this paper, we have reviewed various existing encryption algorithms, compression algorithms and a method for splitting files using an application developed in java. For future work an application is to be developed combining the reviewed algorithm and technologies by taking into consideration its advantages and disadvantages which will help facilitate fast easy and secure transmission of data over network.

REFERENCES

[1]Amandeep Singh Sidhu [M.Tech]1, Er. Meenakshi Garg [M.Tech]2 (2014)" An Advanced Text Encryption & Compression System Based on ASCII Values & Arithmetic Encoding to Improve Data Security"

[2]Joan Daemen, Vincent Rijmen(2002\) "The Design of Rijndael: AES - The Advanced Encryption Standard"

[3]Bruce Schneier (1993)"Description of a new variable length key, 64 bit block cipher (Blowfish)"

[4]H. M. Heys and S. E. Tavares "On the Security of the CAST encryption algorithm"

[5]Franceschini Robert.; Dept. of Computer Sci., Univ. of Central Florida, Orlando, FL, USA ; Mukherjee Amar (1996) "Data compression using encrypted text"

[6]Joseph Lee (2011) "Huffman Data Compression"

[7]Muhanad Hayder (2009) "Design and Implementation of a File Splitter and Merger Software"

