Security for Images in Cloud Computing

Anju Rachel Oommen[1] Nisha Mohan P M[2]
[1,2]Assistant Professor
[1,2]Mount Zion College of Engineering, Kadammanitta, Kerala.

Abstract— Cloud computing has gained more popularity in the recent time and it provide numerous services. Image transfer is one of the major services it provides other than text. The Rapid growth of electronic media helps in fast exchange of images. The progress in data exchange by electronic system needed more of security and has become a necessity. Challenges in cloud computing include confidentiality, scalability in data centers. In this paper, we define a security measure for images by the use of blowfish encryption algorithm.

Key words: Cloud Computing, scalability

I. INTRODUCTION

Cloud computing provides many services which helps to store, manage and process data over a network. It helps users and enterprise to process data in third party data centers. It needed more of security and has become a necessity. Challenges in cloud computing include confidentiality, scalability in data centers. In this paper, we introduced define an image data transfer by the use of encryption algorithm. Due to the growth of multimedia applications, the security of multimedia application needs to be done most efficiently. As the world changes we need to provide more security when we transfer data over network.

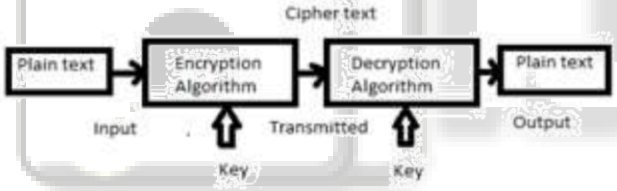

Fig. 1:

is a process of transforming the data i.e. images into another form. It takes input as plain text. An encryption algorithm is applied to the plain text and generating cipher text. It is then decrypted using decryption algorithm to generate the output which is the plain text itself. Traditional encryption algorithm like DES has lot of deficiencies when the image size is large. There are many techniques which help in achieving security to the images like steganography, Digital watermarking etc. The major focus of this paper is to provide secure image transfer over the network using improved encryption techniques. The security breach may deface the a particular persons in image or any important images in use for military or Government usage. The data in the cloud like images will be frequently updated i.e. it will be dynamic storage area. In the proposed method we divide the image into different number of splitted blocks (2^n) times where n is the number of splitted part instead of a single image data transfer over network from cloud.

II. RELATED WORKS

Image encryption techniques have been in use for providing real time image security stored in the cloud. Traditional algorithm has lot of disadvantages which does not provide good efficiency when the image size is large. Image encryption technique is a method which converts the image into another form which is hard to understand by others. Image decryption method will retrieve back the encrypted image back into the original image. Image encryption algorithm can be classified into (i) position permutation based algorithm (ii) value transformation based algorithm (iii) visual transformation based algorithm. There are 2 major groups of image encryption (a) Chaos based selective or non selective methods (b) Non chaos selective methods. The different image encryption techniques involve:

A. Selective Encryption:

In selective encryption, only a part of the data will be encrypted rather than the whole data. The subset of data will be only encrypted. In this we will reduce the amount of data to be encrypted and preserve sufficient security.

B. Visual Cryptography:

It is an encryption technique in which encrypted images can be decrypted by human eyes if the correct key is used. It uses two transparent images. One image contains secret information and other random pixels. We will not get key from any one of the images. Both the images should be combined together to generated the original data. The image will be divided into 2 parts – a key and a cipher. Separately they are random noises but together they will generate images.

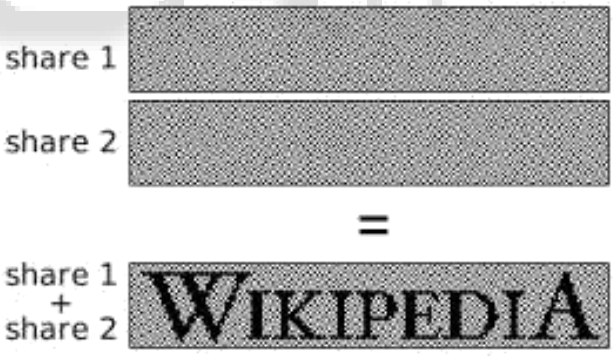

Fig. 2: Visual Cryptography

C. Data Encryption standard:

DES is a symmetric key algorithm for multimedia data. DES was developed in the 1970's. It is a block cipher. To encrypt a plaintext message, DES groups it into 64-bit blocks. Each block is enciphered using the secret key into a 64-bit cipher text by means of permutation and substitution. It has 16 rounds.

III. PROPOSED METHOD

In the proposed method, the original image will be divided into different k*k parts. Each part of the image will be treated as a single image. This single image will be encrypted using blowfish algorithm. Blowfish is a 64 bit symmetric block cipher which uses variable length keys from 32 to 448 bits. It

uses 16 round Fiestel network for encryption and decryption. It encrypts data on a 32 bit microprocessor. In each round of Blowfish, the left and right 32- bits of data are modified unlike DES which only modifies right 32 bits. Blowfish uses a bitwise exclusive-or operation to be performed on the left 32-bits before being modified by the F function or propagated to the right 32-bits for the next round.

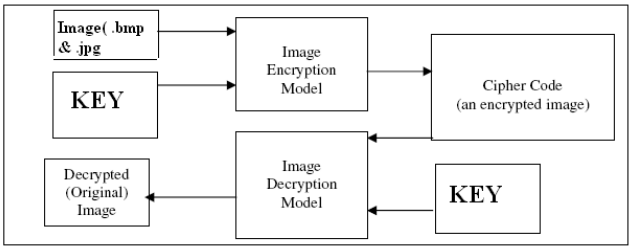

Fig. 2: Proposed Architecture

The basic algorithm used for blowfish encryption and decryption is:
Divide X into two 32 bits halves XL and XR
For I = 1 to 16
XL=XL Pi
XR=F(XL)XR
SAWP XL and XR
END FOR
SWAP XL and XR
XR=XR P 17
XL=XL P18
RECOMBINE XL and XR
Output X
In decryption process the sub key Pi must be in reverse order. In this every half is swapped for next round.

IV. Conclusion

In this paper, we have discussed how images in a cloud can be securely transferred over network using secured encryption method. The method explained is blowfish encryption which securely transmits image. Previous methods like DES, AES can be replaced Blowfish to give more effectiveness on security. It can't be correctly broken by hackers until the correct combinations are found. As a future work of Blowfish to increase the strength, the number of rounds can be increased. It takes less time to encrypt and decrypt.

References

[1] J Mahalakshmi, Dr. K Kuppuswamy, "Security as a service for files in Cloud computing- A Novel Application Model "
[2] Pooja Rani, Apoorva Arora, " Image security systemusing Encryption and Security", vol 4, Issue 6,June 2015.
[3] Mohammed Sajid Quamruddin Khizrai, "Image encryption using different techniques for High security transmission over a network ", IJERGS, vol 2,Issue 4 June-July 2014.
[4] Pia singh, " Image Encryption and Decryption using Blowfish algorithm in Matlab", IJSER, vol 4 Issue 7, July 2013.
[5] Rupinder Kaur, Rekha Bhatia," Image Privacy Protection for Online storage Using Adaptive Security Model", IJARCSSE, vol 5, Isuue 8, July 2015.

