ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 6, Issue 12, December 2017

Reliable Private Image Storage in Cloud Storage Devices

John Devakumar

Senior Faculty Member, Dept. of Electronics and Communication, Pusa Institute of Technology, Pusa Campus , New Delhi, India

ABSTRACT: Cloud computing storage is a service where data is remotely maintained, managed and backed up by third parties like storage service providers. It is a data storage model where clients can upload data to a network of remote connected servers with massive disk spaces. Clients can access the data from anywhere where there is Internet access. Users on move need not carry storage devices with them .Organizations can avoid the expense of buying their own storage devices and maintaining them. Unlike other data, high quality Images occupy huge disk space. Hence storage of images in cloud computing storage systems is a natural choice

The main concern in cloud storage is data security. Data stored in cloud be corrupted or misused. Service providers can give data access to unauthorized users. Malicious data can be easily embedded in images. This paper suggests a simple method to store securely private images in cloud storage systems and resolve disputes between service providers and clients who used storage space to store images. Engineers, doctors, designers, photographers etc can store their private high resolution images securely in cloud and access them from anywhere in the world through internet without fear of data getting corrupted or misused. Two steps are suggested in this paper. First is encryption at client site before uploading images. Second step is to resolve disputes between clients and service providers using a two level information sequence exchange mechanism. First step prevent misuse of data at service provider site. Second step resolves all disputes on validity of image between clients and service providers.

KEY WORDS: Cloud storage, Private data, RGB image ,Image Encryption ,Image Decryption

I. INTRODUCTION

Engineers, Doctors , Photographers, reporters and other professionals who are on move have lot of private data. Most of them are high resolution images which are to be stored securely and retrieved whenever required . Building Designs, medical images, photographs etc require large storage space. Storing large number of images and managing them by people who are on move is difficult. Possibility of loss/theft/damage of data storing devices is high. Storing images in cloud is a very good option for people who are frequently moving .Storing images in cloud raise genuine concern regarding security of image data. Owners of image data worry that their images can be misused in the cloud. Service providers can be dishonest. This paper provides a simple method to securely store image data in cloud storage systems.

II. RELATED WORK

Lot of work has been done on data storage in cloud storage systems. Many security mechanisms are suggested. Most of the works do not distinguish between different types of data. Generalized methods are developed for securely storing data. Most of them are complex methods and time consuming. Here we are suggesting a simple method to securely store private image data. By private image data we mean that are only stored by owner of data and accessed only the owner of image or people who are authorized by owner of image,that is data that are not made available to the general public .Aaron Wheeler and Michel Winburn's[1] book, Cloud Storage Security: A practical Guide , gives the history and the evolving nature of cloud storage and security. It also looks into the threats to privacy and security when

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 6, Issue 12, December 2017

using free social media applications that use cloud storage. It includes case studies and best security checklist for selecting a cloud service provider. But unfortunately it assumes some cloud storage service providers are reliable because of their previous records. Past performances of service providers cannot not be always relied upon. Ashwin Dhivakar [2]in his book, A Multilevel Security in Cloud Computing Image Sequencing and RSA algorithm, discuss various security issues in cloud storage .In this book also the security of cloud data is left in the hands of service providers. Moreover general data security issues are discussed. Image and multimedia data is susceptible to unique type of risks like hidden malicious data that is hard to detect. Mai Mansour Dahshaw [3], in his Thesis work on Data security in Cloud storage services uses third part trusted (TTP) service that can be employed either locally on users' machine or premises, or remotely on top of cloud storage services. This service shall encrypts users data before uploading it to the cloud and decrypts it after downloading from the cloud; therefore, it remove the burden of storing, managing and maintaining encryption/decryption keys from data owner's. In addition, this service only retains user's secret key(s) not data. Moreover, to ensure high security for these keys, it stores them on hardware device. Problem with approach is it absolves the cloud service provider from all responsibility. Most of the other works are either assuming service provider takes care of data security or using complex algorithms to ensure security.In this paperwork we suggest a method to securely store images in cloud and can hold service provider accountable for corruption and modification of images.

III. METHODOLOGY

True color images from a camera that produce MxN pixel photograph can be represented by a three dimensional array of size MxNxQ.

Where M = No of pixels in X –axis
N=No of pixels in Y-axis
Q= Color (1-Red,2-Green,3-Blue)

We can consider image as three channels of MxN," n" bit values. The first MxN n bit values represent the red channel, the second MxN n bit values represent the green channel and the final MxN n bit values represent the blue channel. Each channel contains MxN "n" bit values representing intensity of the pixel for that color. Each channel consisting of n bit MxN array can be considered as "n" separate planes of bits. The least significant bits of each n bit value of a channel represent one plane and next significant bits form another plane and so on. Thus there are totally 3n bit planes, n for each channel.

To store the properties of image and other related data ,(like date, camera type ,owner etc)the least significant bit plane of one of the channels can be used . Here we use least significant bit plane of red channel. Changes made in LSB plane of a particular color channel will not affect the image quality much since human eyes are insensitive to such minute changes.

To prevent misuse of images at the cloud storage service provider side, the images are encrypted. The encryption key is stored in a image information block (IIB). Next a random bit sequence is generated (say S_1) and XOR operation is performed on the encrypted image block wise. Block size is taken equal to size of S_1 . The XOR operation results are added up and scaled to binary values to get say R_1.. Both K_1 and R_1 are stored in IIB. Encrypted image is uploaded in cloud and K_1 and R_1 are given to service provider. At service providers side using S_1 , XOR operation is performed on the received image block wise and the XOR operation results are added up and scaled to binary values and result is compared with R_1..

If the received bit sequence R_1 match with computed value of R_1 then at the service providers side a random bit sequence is generated (say S_2) and XOR operation is performed on the received image block wise. Block size is taken equal to size of S_2 . The XOR operation results are added up and scaled to binary values to get say R_2.. Next S_2 and R_2 are sent to image owner. The block diagram for uploading

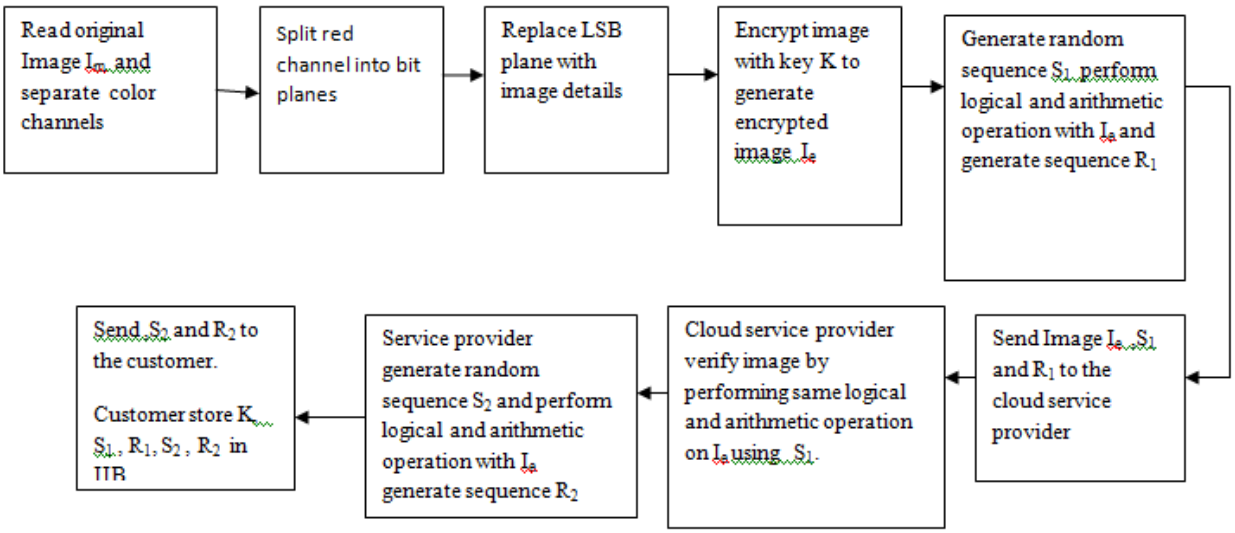
ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

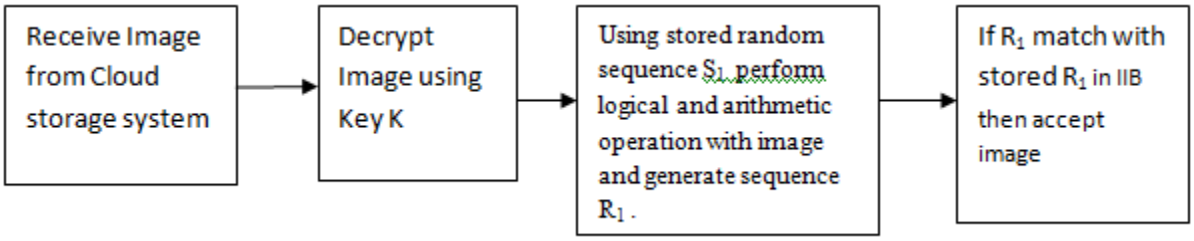
(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 6, Issue 12, December 2017



Block diagram for receiving Image



In this type of system a new data structure ,an Image Information Block (IIB) must be maintained at the customer side and service provider side. At image owner's side and server side K_1, R_1, and K_2, R_2 are stored in IIB. The image owner IIB will have also the encryption key K. IIB contain only few entries (K, S_1 , R_1, S_2 , R_2) and it does not consume much space.

At image owner's side, when they retrieve images from cloud, use sequence S_1 to perform XOR operation with the encrypted image block wise and add the results. Then scale the results in binary and check with R_1 to verify the image.. If image is found valid using key K it is decrypted to get original image.

IV. ALGORITHMS

Algorithm 1 /*Customer Side while sending image to cloud */

1. Read image **Im**
2. Determine size of image
   M= Number of pixels in row
   N = Number of pixels in column
3. Generate random binary key K of size P such that
   P = mN and (M mod m) = 0
   Where m = 1,2,…….

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 6, Issue 12, December 2017

4. Split Image into Red, Green and Blue Channels
5. Embed image details by replacing Least Significant Bit plane of Red Channel with image data
6. Divide image into blocks B_i of size P and perform the following operation
   Let number of blocks be N_b
   For i = 1 to N_b
   (B_i = (B_i XOR K))
7. Generate a random sequence S_1 of size P and perform the following operation

$$R_1 = \sum_{1}^{N_i} (B_i \text{ XOR } S_1)$$

8. Send Encrypted image to cloud and send also S_1 and R_1
9. Wait for S_2 and R_2 from service provider
10. Store S_1, R_1, S_2 and R_2 ,and Key K in IIB

Algorithm 2 /* Service Provider side while storing image*/

1. Receive image from customers
2. Using received sequence S_1 perform the following operation on received image

$$J_1 = \sum_{1}^{N_i} (B_i \text{ XOR } S_1)$$

3. If R_1 is equal to J_1 accept the image for storage and generate a random sequence S_2 of size P and perform the following operation

$$R_2 = \sum_{1}^{N_i} (B_i \text{ XOR } S_2)$$

4. Send R_2 , $S_2$to customer

Algorithm 3/*Customer Side while retrieving image */

1. Receive image from Cloud storage
2. Using received sequence S_1 perform the following operation on received image

$$J_1 = \sum_{1}^{N_i} (B_i \text{ XOR } S_1)$$

3. If R_1 is equal to J_1 accept the image and do decryption as follows
   Let number of blocks be N_b ,
   For i = 1 to N_b
   (B_i = (B_i XOR K))

Time Complexity of the Algorithm

Assuming 8 bit pixel intensities, an image of MxN pixels, for encryption MxN x8x3 bitwise XOR operations are performed .Similarly for decryption MxNx8x3 bitwise XOR operations are required. Two times XOR operation is performed on image with sequence S_i , one at the sender side and other at service provider side which require MxNx8x3x2 bitwise XOR operations. Thus total bitwise XOR operations are 96 x MxN. Thus time complexity is O(MxN).Other operations like generating key K, sequence S_1 etc take fixed time and negligible.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 6, Issue 12, December 2017

V. RESULTS

The results of above algorithm is shown below.The original image (Palace Patiala) is taken using Nikon 24 Mega pixel DSLR camera .Verification of result is simple. Encrypted data at cloud storage service provider side cannot be misused as the image is encrypted and the key is not shared with the service provider.Service provider cannot give data to third party or if third party somehow obtain the images, since key is not shared , the image is of no use.
In case any modification of image is made or malicious data is hidden in image it can be easily detected using S_1, R_1 , S_2 and R_2 and disputes can easily resolved legally in case of payment based cloud storage systems.
The algorithm suggested in this paper is run in MATLAB and outputs are shown below.

Fig 1

Fig 2

Fig 3

Fig 4

Fig 5

Fig 6

Fig 1:The original image taken using 24 Megapixel camera
Fig 2: The Red Plane of the original image where image characteristic data is hidden in LSB plane
Fig 3: The reconstructed image in which image characteristic data is hidden
Fig 4: Image after encryption that is send to cloud
Fig 5: Image received from cloud
Fig 6: Original image retrieved

VI. CONCLUSION

The original image (Fig 1) and retrieved image from cloud (Fig 6) after encryption is same. From above results we can conclude private image data can be safely stored in cloud storage systems. Confidentiality and Integrity of images can be ensured by using a private key for encryption and decryption at user end. Integrity of images can be ensured by using two pair of bit sequences (S_1, R_1) and (S_2,R_2).The complexity of algorithm used is O(MxN), where MxN is size of image in pixels. Also any dispute arise can also be resolved using this two pair of bit sequences. This paper does not address the image availability issues (means ensuring timely and reliable access to personal data always).

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 6, Issue 12, December 2017

REFERENCES

[1] Aaron Wheeler and Michel Winburn, Cloud Storage Security: A practical Guide Elsevier 06-Jul-2015
[2] Ashwin Dhivakar ,A Multilevel Security in Cloud Computing Image Sequencing and RSA algorithm , Anchor Academic Publishing
[3] Mai MansourDahshaw ,Data security in Cloud storage services, Thesis ,American University in Cairo 2014
[4] Fei Hu, CRC Press, Big Data: Storage Sharing and Security
[5]Vimal Kumar, Shivaden Chaisiri, Ryan ko, Data Security in Cloud Computing Institution of Engineers and Technology 2017
[6] Rampal Singh, Sawan Kumar, Shani Kumar Agrahari, Ensuring Data Storage Security in Cloud Computing International Journal Of Engineering And Computer Science ISSN:2319-7242 Volume 2 Issue 3 March 2013
[7] Kalpana Batra, Ch. Sunitha, Sushil Kumar ,An Effective Data Storage Security Scheme for Cloud Computing International Journal of Innovative Research in Computer and Comm. Engineering Vol.1, Issue 4, June 2013
[8] Deepanchakaravarthi Purushothaman and Dr.Sunitha Abburu An Approach for Data Storage Security in Cloud Computing International Journal of Computer Science Issues, Vol. 9, Issue 2, No1, March 2012

BIOGRAPHY

John Devakumar completed BTech in Electronics and Communications Engineering and completed MTech in Signal Processing from Delhi University. Image Processing ,Adaptive Digital Signal Processing, Microcontroller based system Design are his area of Interests .Currently working as senior faculty member in Pusa Institute of Technology, Pusa Campus New Delhi. Currently involved in projects related to Image Processing , Audio/Video encryption and Data hiding in live TV transmission.