IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 7, Issue 1, January 2018

Secure Image Data Storage using Hybrid Cloud

M. Elakkiya

B.Tech, (M.E.), Department of Computer Science and Engineering,

Gojan School of Business and Technology, Chennai, India

Abstract: In IoT, increasing usage of image sensors and devices has led to a concern for storing the captured images and securing it, especially for big images. We make use of hybrid cloud structure for providing the framework for efficiently storing the images. The concept is to partition the image into most significant and less significant (remaining) image parts. The most significant part which is very less in size is stored in private cloud. The less significant part which constitutes major storage space is stored in public cloud. The two partitions are merged to form a full actual image when the user wants to retrieve the actual image. Sobel edge operator is used to partition the image. Encryption and compression schemes are employed to ensure privacy and reduce transmission bandwidth respectively.

Keywords: Hybrid cloud, private cloud, public cloud, image storage.

I. INTRODUCTION

In IoT, multiple devices exist, especially image sensors. The increasing usage of these image devices is due to their application in security and surveillance purposes. Images captured by these devices need to be stored securely for future reference. The main aspects of efficient storage system are sufficient space and security. Nowadays, organizations prefer clouds as the primary option for storage because of its advantages such as pay-per-use, flexibility, minimal supervision, easier accessibility, faster change synchronization and data recovery etc. The two main cloud storage services are private and public cloud. Private cloud is an on-premise storage service which provides a private network with dedicated hardware and software resources within an organization. In public cloud, the hardware, storage and network devices are shared with many organizations. Public cloud is the common cloud deployment model and is delivered over the internet.

Users tend to store data in their own private cloud to ensure privacy and better control over the data. But, as the image data increases, there would not be sufficient storage space. In order to meet the demand of abundant storage space, public cloud can be used. But public cloud may subject to security risks. So there is a need of hybrid cloud structure which combines the advantages of both private and public cloud. We can use the public cloud for higher volume and low security needs and private cloud for sensitive and business critical functions.

II. RELATED WORK

The concept of partitioning a file and storing in different locations makes it secure against various attacks. One such example is splitting a file into eight parts and encrypting each part using different algorithms is shown in [1] but images are not included. Also hybrid cloud is not used. Partitioning of images is can be carried out using separating the edges from the image. A novel approach for image representation based on edge structural features is detailed in [2]. Here the edge pixel segments are obtained through geometric partitioning but it involves Complex computation. So a simple way of edge partitioning is required. Once the partitioning of image is completed, the partitions have to be appropriately encrypted and compressed. [3] shows that it is not an easy task to exploit the image compression over encrypted domain. Compressing encrypted image data appropriately before transmission is essential to reduce the consumption of communication resources.

In [4], Images are encrypted by using random permutation and then performed a lossy compression with iterative reconstruction. In [5], the compression of encrypted images is based on diffusing single pixel value.

From [6] and [7] we have learnt about image reconstruction outsourcing services but there is no private cloud providing image service in these concepts.

III.SECURE IMAGE STORAGE USING HYBRID CLOUD

We propose a concept of storing image data in hybrid cloud structure. Users will be interacting only with the private cloud.

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319-5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 7, Issue 1, January 2018

A. Architecture

The architecture of the proposed system is shown as below. The four main processes involved are Partitioning, Encryption, Compression and Image assembling.

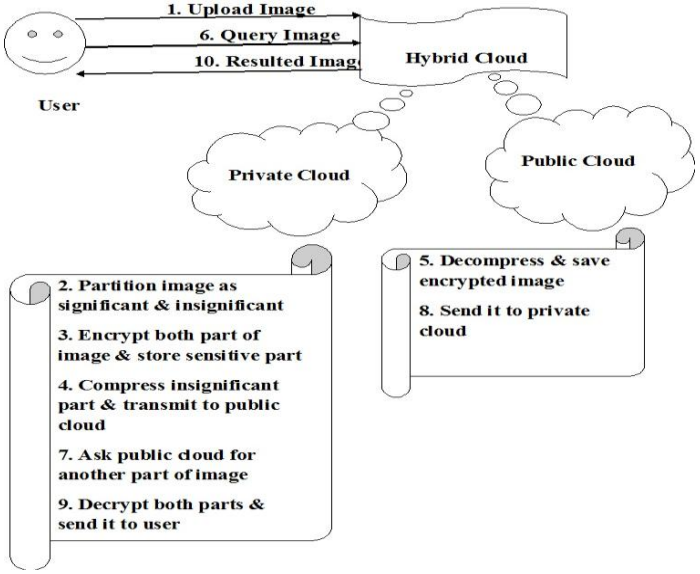

Fig 1: Architecture diagram for secure storage of images using hybrid cloud

B. Partitioning Process

Image partitioning process is carried out in private cloud. The first step is to determine the data that needs to be stored in private and public cloud.

Private cloud has limited storage space with privacy assurance. So the data that has to be stored should have less storage size but it can be a significant data. Public cloud has abundant storage space but with security risks. So the data to be stored may have large storage size but with no significant data.

Partitioning of image is carried out using edge detection method. Important features can be extracted from the edges of an image (e.g., corners, lines, curves). Edges are significant local changes of intensity in an image - a jump in intensity from one pixel to the next. The change in intensity of a point in an image can be measured by image gradient. An image gradient is a directional change in the intensity or color in an image. Pixels with large gradient values become possible edge pixels.

Sobel edge detection method is used to partition the image data. Sobel operator can be used to create an image emphasizing edges. It computes an approximate gradient of the image. The concept is based on convolving the image with a small, separable, and integer-valued filter in the horizontal and vertical directions. The operator uses two 3×3 kernels which are convolved with the original image to calculate approximations of image gradients.

The sobel mask for x and y directions are:

x:	-1	-2	-1	y:	-1	0	1
	0	0	0		-2	0	2
	1	2	1		-1	0	1

These masks are applied to the input image matrix, the derivatives Gx and Gy in x and y directions respectively are calculated. The gradient √Gx^2 + Gy^2 has to be calculated. This absolute magnitude gives the output edges.

Steps for partitioning process:

1. Represent input image in matrix form
2. Gaussian blur is applied to the image to reduce image noise and reduce detail
3. Apply sobel mask to the image matrix (for each 3x3 window)
4. The gradient of the image is calculated for each pixel position
5. The edge detected image can be obtained from the sobel gradient by using a threshold value.
6. If the sobel gradient values are lesser than the threshold value then replace it with the threshold value.
7. Assume the threshold value to be the average hue(color) value of the image

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319-5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 7, Issue 1, January 2018

C. Encryption process

Once the partitions are obtained, it has to be encrypted. Significant part of the image is straight away encrypted and stored in private cloud itself. Less significant part of the image is also encrypted but it needs to be sent to public cloud for storage. The counter mode encryption method can be applied since parallelism is one of its benefits. Also it is a common block cipher mode.

AES Encryption method is used to encrypt the image parts. Advanced Encryption Standard(AES) is the most popular and widely adopted symmetric encryption algorithm. It is based on a design principle, "substitution-permutation" network. It comprises of a series of linked operations, some of which involve replacing inputs by specific outputs (substitutions) and others involve shuffling bits around (permutations). It performs all its computations on bytes rather than bits. The input has a fixed block size of 128 bits, and a key size of 128, 192, or 256 bits. It is an iterative algorithm and key size used for an AES cipher specifies the number of repetitions of transformation rounds.

Each round comprises of four sub-processes.

- Add round key: The 16 bytes of the matrix are now considered as 128 bits and are XORed to the 128 bits of the round key. If this is the last round then the output is the cipher text.
- Byte Substitution: The input bytes are substituted by looking up S-box. AES defines a 16 x 16 matrix of byte values, called an S-box that contains a permutation of all possible 256 8-bit values.
- Shift rows: Each of the four rows of the matrix is shifted to the left.
- Mix Columns: It operates on each column individually. Each byte of a column is mapped into a new value that is a function of all four bytes in the column.

D. Compression process

Before sending the less significant image part to public cloud, it needs to be compressed to save the bandwidth during data transmission. Higher compression rate may reduce the image quality during reconstruction. So compression should be employed only as necessary. The compressed image data is sent to public cloud and is stored.

E. Image Assembling Process

If the user wants to retrieve the image stored in hybrid cloud system, reconstruction of image will happen. Significant image part is decrypted in the private cloud. Insignificant part which is stored in public cloud is decoded there and then received by private cloud. The private cloud decrypts the insignificant part. Both the decrypted parts are then assembled to get the actual complete image.

IV. EXPERIMENT ANALYSIS

Let us take an image for analysis. The original image uploaded for the proposed system is shown Fig 2. The outcome of partition process is shown in Fig 3. The significant image partition is stored in private cloud after encryption and insignificant image partition is stored in public cloud after encryption and compression.

Fig 2: Original image

Fig 3: Outcome of Partition process

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 7, Issue 1, January 2018

V. CONCLUSION

This paper proposed an efficient secure storage for big image data using hybrid cloud. In an image, the significant data (significant portion of the image e.g., edges) are securely stored in the private cloud while the insignificant data are encrypted then compressed and stored in the public cloud. The significant data account for a very small percentage of whole image data. So instead of 100% storage space of the original image, only about 20-30% storage space is being used in the private cloud thus saving major storage space for the private cloud. Even though major portion of the image is stored in public cloud, the privacy of images is assured since the storage consists of only part of the image and that too in encrypted form.

REFERENCES

[1] Punam V. Maitri, Aruna Verma "Secure file storage in cloud computing using hybrid cryptography algorithm", Wireless Communications, Signal Processing and Networking (WiSPNET), International Conference, March 2016
[2] Xiao-Meng Jia, Guo-Yu Wang, "Geometrical partition of edge image: a new approach for image structural features description", Machine Learning and Cybernetics, 2002.
[3] M. Johnson, P. Ishwar, V.Prabhakaran, D. Schonberg, K. Ramchandran, "On compressing encrypted data", IEEE Transactions on Signal Processing (Volume: 52, Issue: 10, Oct. 2004)
[4] Xinpeng Zhang, "Lossy Compression and Iterative Reconstruction for Encrypted Image", IEEE transactions on information forensics and security, vol. 6, no. 1, March 2011
[5] Wei Liu, *Member*, Wenjun Zeng, Lina Dong, and Qiuming Yao, "Efficient Compression of Encrypted Grayscale Images", IEEE transactions on image processing, vol. 19, no. 4,April 2010
[6] C. Wang, B. Zhang, K. Ren, and J. M. Roveda, "Privacy-assured outsourcing of image reconstruction service in cloud," IEEE Trans. Emerg. Topic. Comput., vol. 1, no. 1, pp. 166–177, 2013.
[7] Y. Zhang, J. Zhou, Y. Xiang, L. Y. Zhang, F. Chen, S. Pang, and X. Liao, "Computation outsourcing meets lossy channel: Secure sparse robustness decoding service in multi-clouds," IEEE Trans. Big Data, in press, 2017.
[8] Wikipedia, "AES Encryption"
[9] Wikipedia, "Sobel edge detector"