+Secured Image Storage Using Data Integrity Convergent Encryption Protocol

H N S Bhavani Eshwari[1], P N Ramya[2]
Computer Network and Information Security, Jawaharlal Nehru Technological University
[1]Department of Information Technology, GNITS, Telangana, Hyderabad, dhansu93@gmail.com
[2]Assistant Professor, Department of Information Technology, GNITS, Telangana, Hyderabad, ramyapn1@gmail.com

ABSTRACT: Cloud Computing is an emerging technology and plays key role. Cloud service provider provides the flexibility and allows users to offload their data to the cloud and leave all the data management, maintenance and security issues to the Cloud Service Provider (CSP) who manages the services.CSP charge nominal fee to the users on usage of the resources provided by them. In the cloud storage, Security of data has become a prime concern, replication and dissemination of multimedia data become increasingly. Due to the increase in data usage, the storage space had been compromised for redundant data which means occurrence of the same data provided by millions of users creates wastage of available space on the cloud. To overcome the above problem data deduplication techniques are employed. Those techniques eliminate the redundant data on cloud by using Data Integrity Convergent Encryption Protocol. In this proposed system, we employee the protocol where each image in the formats of .jpeg, .png and .tiff is divided into blocks, rehashed, encrypted and these blocks which are common between images are stored only once at the cloud and performed integrity check for the uploaded images whether the images are remained same or corrupted during data transmission by generating hamming code. We provide detailed analyses based on the theory, experiment and security aspects of the proposed scheme.

Keywords: Deduplication, Integrity, Encryption, Storage.

I. INTRODUCTION

Cloud computing is the emerging technology. Cloud computing is the availability of system resources as cloud storage, networking and computational power to the user on demand. Cloud technology offers many services e.g. Software as a Service known to be SaaS, Platform as a Service known to be PaaS, Infrastructure as a Service known to be IaaS. Cloud computing has empowered users with the expediency of data storage, data availability, data accessibility, etc. cloud computing methodology offers tremendous flexibility and allows users to offload their data to the cloud and leave all the data management, maintenance and security issues to the Cloud Service Provider (CSP) who manages the services.CSP charge nominal fee to the users on usage of the resources provided by them. This is important for CSP to maintain balance between the cost of the services they provide and the fees they charge to the users, as maintaining and storing the huge volume of user's data, along with the bandwidth usage incur costs for the service providers of cloud.

The data stored can be in various forms like text, image, audio, video and hosting applications on the cloud by users. Some of the most popular Cloud Storage Providers are Dropbox, icloud, flicker, google photos. The uses of digital cameras and social media sites such as Facebook and YouTube have contributed to the rapid growth of data being uploaded to the cloud. Images are used to communicate and convey meaningful information. The widespread usage of digital images on the internet requires a reliable, fast and powerful security to store and transmit them over the network. The use of images and multimedia content for sharing purposes is one of the most significant factors causing issues of duplicate data in the storage and increase in the bandwidth, communication.

Securing images from unauthorized users and adversaries is very important and needed in the fields of medical processing, remote sensing, military, government documents, telecommunications and other similar fields. Image encryption is needed to enforce content access control, privacy, confidentiality and provide protection of images by transforming the original content of the image into texture-like or noise-like information that is hard to understand as the quantity of data storage increases is becoming a serious issues in cloud storage services. In 2020 the amount of data storage growing about 40 trillion gigabytes and more, it will occupy lots of space in cloud storage. To overcome the problem of removing duplicate data, providing the security is explained and implemented in this paper. To remove duplicate data, where we are considering image kind of data, we proposed a method that is Data Integrity Convergent

Encryption (DICE) Protocol at client side. We are presenting a secure block level image deduplication method. In this method, identical images are identified and eliminated in encrypted form. In Data integrity convergent encryption (DICE) Protocol [1], the image uploaded by user are set into blocks, keys are generated by hashing each block of the image. Each block is encrypted using Advanced Encryption Standard (AES) which is a symmetric based algorithm with a key that is obtained from hashing the blocks of image using SHA-256 algorithm. A tag for each block is generated by hashing the cipher generated by encrypting the block and stored in the tag store to check the block availability. It means that identical blocks generate the same tags, which allows service provider to perform deduplication based on the tags generated for the image blocks. To check the integrity of the uploaded image, we use hamming code which is a block code that is used for detect bit errors. We generate a hamming code for the generated tag from the block of the image given as input, during upload and download of the image we generate a hamming code and check whether the generated hamming code during image upload and image download are remained same, during transmission or any uploaded data is tampered. As one tag is generated from cipher block that reduce the requirements of bandwidth and communication. In detail, secure image storage using Data integrity convergent encryption Protocol is explained theoretically and implemented experimentally in further sections.

In this section 1 Introduction, we deal with the introduction of the storage in the cloud and how the different formats of the data is stored. How cloud service provider facing problem of data redundancy and which protocols are used to increase the efficiency of storage, and how data integrity is done. In this paper we focused on the data of image format with different extensions of image as .png, .tiff and .jpeg. Describe about the need and objective of the study

In this section 2 Literature Review, describe about the reference of the papers considered for the data analysis and implementation of the project. describe the problem definition and proposed system.

In this section 3 Methodology, which kind of methodology architecture and block diagrams

In this section 4 describing about the algorithms and module

In this section 5 Result Analysis, describing about the implementation and performance analysis.

In the section 6 Conclusion, we consider the conclusion thus some discussions in this paper.

II. RELATED WORK

Bellare et al. have proposed the Message Locked Encryption (MLE) scheme [2], where protocol standards are defined. Convergent Encryption (CE), Convergent Encryption without Hash (HCE1), Convergent Encryption With Hash (HCE2) and Randomized Convergent Encryption (RCE) several other MLE based strategies are available [3]. These mentioned strategies provide deduplication [4].

Gang et al. [5] considered the entire image for deduplication of and applied the Convergent Encryption (CE) scheme coupled with Attribute Based Encryption to perform deduplication of image.

Fatema et al. [6] used partial encryption along with SPIHT compression characteristics and image hashing to perform deduplication. Security is provided the Cloud Service Provider using the partial encryption scheme and to identify the identical compressed and encrypted images for deduplication the image hashing technique is used. In their work, the image compression algorithm is applied first by the user, then partial encryption scheme is used and finally computed the image hash signature. The signature is then sent to the Cloud Service Provider (CSP) to check for deduplication.

Achmad Fauzi, [7] In this research, during transmission of the data, communication performed at any time may not always go well, sometimes name error happens. The author performs error detection and error correction in data transmission using the algorithm Hamming Code, this algorithm is used to in the detection and correction of bit damaged during transmission. This algorithm is applied to check the error detection which changes during the transmission of the data.

Problem Definition

With the emergence of cloud computing technology, Cloud computing is the availability of computer system resources, especially cloud storage, networking and computational power to the user on demand. Researchers introduced Message Locked Encryption (MLE) schemes based protocols such as Convergent Encryption (CE), Hash Convergent Encryption without tag check (HCE1), Hash Convergent Encryption with tag check (HCE2) which provide secured deduplication of data, where the data is generally in the format of text. As a result, multimedia data such as images, which are larger in size compared to text files, have not been given much attention and to overcome this problem to remove duplicate data in image form we apply secured data deduplication to reduce the cost and space required for their storage.

The deduplication of file is performed at the file level, where the duplicate files are detected by applying hash functions on the entire file and then checked if the hash values are the same. In case of the image data, applying hash on the entire image data may not be appropriate, as the hash value may differ even if two images are different only by a pixel value. This defeats the goal of deduplication. To overcome the existing problem, an image is set into blocks and the Data Integrity Convergent Encryption protocol is applied on block separately rather than on the entire image. As a result, the blocks which are common between two or more identical images are stored only once in the storage.

Proposed System

In the proposed system, uploaded image of a user is divided into blocks of fixed number and the Data Integrity Convergent Encryption protocol is applied on each block instead of the entire image. As a result, the blocks which are having similar images are stored only once in the cloud.

The user can upload the image format of .jpeg, .png and .tiff. The user first divides the image into blocks of fixed number. Each block size could be of variable length, anywhere from (4×4, 8×8 to 16×16) cm. After converting the image into blocks, the user runs the client portion of the DICE protocol on each block generate keys , tags for the block image and the deduplication of images is performed and images are stored only once in the cloud. In order to prove the data integrity of the image block, hamming code is generated during transmission of the image from client to the cloud service provider and vice versa. During this transmission there may be errors in data, data loss, data modification. In order to identify, we generate hamming code to check the data modifications during transmission of the image data. During uploading and retrieving of the data, generated code will be verified and check the data integrity whether the data is modified or remained same.

III. METHODOLOGY

System Architecture

In the below mentioned system architecture, users upload the data irrespective of the devices like Personal Computer (PC), laptop, mobile etc. The uploaded data is images, after uploading image is set into blocks and encrypted to store in the cloud storage. Cloud Service Provider (CSP) authorize the users, maintains the files uploaded by the user , checks the data integrity and stores the data. The existence of the identical images are checked if existed the generated block tags are updated if not request raised for the user to upload the image and perform the data depuplication by applying Data integrity convergent encryption protocol on each block and checks the duplicates in the cloud by sending a tag vector in tag store of the cloud. Data integrity for the image by generating the hamming code for the tags as input during upload and download of the image and comparison of the hamming code is performed to check whether the uploaded image is corrupted or is it remained same during its transmission of the data.

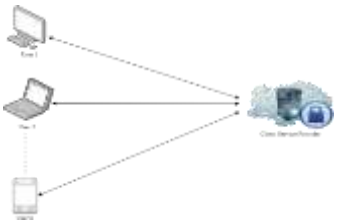

Fig 3.1 Overview of system

Block Diagram

In the block diagram, users have to register, to gain access control for uploading and downloading of the image in login page. User uploads the image and checks the existence of the image blocks, If image block is existed then it updates the existed image blocks else raise request to upload the image. If the new image is uploaded then those uploaded images are set into blocks, which are encrypted to provide confidentiality using AES and key obtained by hashing the block. Cloud Service Provider assign block ID's to the image converted blocks and maintain the files in the storage. The deduplicate method for the near identical images (blocks) is applied using Data Integrity Convergent Encryption protocol and redundant blocks. If the blocks having the same cipher, says block is existed and generated tags are updated in the cloud storage by checking the data integrity of the image block during upload and download of the image by generation of the hamming code.

Fig 3.2 Block Diagram

IV. ALGORITHM

The below mentioned algorithm gives the step by step procedure how the blocks of images are deduplicated, integrity check is done and stored image only once in the storage of cloud.

Upload of the image

Algorithm 1 Upload File
Objective: To split images into blocks
Input: User upload image

1. **Procedure** User: Upload Image File
2. Generate key by hashing the image block
   Key ⟵ Hash (Block)
3. Encrypt the image block by using AES
   Cipher ⟵ Encrypt(key, Block)
4. Generate the tags for the encrypted block
   Tag ⟵ Hash(Cipher)
5. Compute the rehashed values for the generated tags
   Tag1 ⟵ Rehash(Tag)
6. If EXISTENCE = FALSE then
   Upload(Rehash(Tag),Cipher)
7. Else
   Return
8. **Procedure** Cloud Service Provider: VERIFY EXISTENCE(Rehash(Tag))
9. If Hash(Cipher) ∈ Blocks List then
   Return "TRUE"
10. Else
11. Return "FALSE"

Storage of the image

Algorithm 2 Storage of Image
Objective: To store image blocks and update tags of image block
Input: Image blocks

1. **Procedure** CSP: Store Image Blocks
2. Computed Tags are stored in the storage
   Store ⟵ Tag1
3. If Tag1 EXISTENCE = TRUE then
   Tag 2 ⟵ Hash(Tag)
4. Else
   Return

Data integrity check

Algorithm 4 Data Integrity Check
Objective: To check data integrity
Input: Uploaded image stored in storage

1. **Procedure** Cloud Service Provider: Data Integrity Of Image
2. If Image blocks upload and download Ham_code Existence = True then
3. H(T) ⟵ Hamming(Tags of Block)
4. If H(i) = H(j) then
5. Image remained same
6. Else
7. Image corrupted

Download of the image

1. Input downloads of image.
2. User send tag and user id to CSP for tag search in tag store
3. If Ti = Ti'
4. Then match found and cipher block is send to the user.
5. Else match not found.
6. User receives the tag and cipher block
7. Computes the tag from received cipher blocks Ti''= H(Ci)
8. Match with stored tag Ti = Ti''
9. If match found
10. Start decryption Bi ← D(Ki, Ci),
11. else
12. return block is corrupted

V RESULT ANALYSIS

Implementation results

Fig 4.1 Home Page

The home page of the Secured Image Storage using Data Integrity Convergent Encryption Protocol. Here the user or cloud service provider can access the home page. User must login in order to gain access.

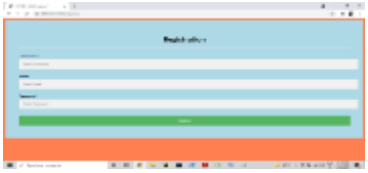

Fig 4.2 Registration

Here the user can enter his or her details in the text field like username, email id, and password in the registration page and clicks register.

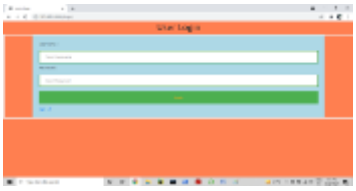

Fig 4.3 Login

Here the user can enter his or her details in the text field like username, email id, and password in the registration page and clicks register

Fig 4.4 Image Upload and Image Download

Here the user can upload and download the image in this page after getting access to the user.

Fig 4.5 Image upload

Here the user can upload the image from the local folder after getting access.

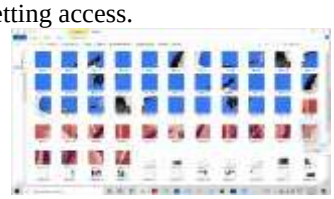

Fig 4.6 Image Blocks

The uploaded image is divided into blocks as shown in the above figure.

Fig 4.7 Generated keys

For the uploaded image by user, keys are generated by hashing the image block using SHA256, as shown in the above figure.

Fig 4.8 Generated tags

For the uploaded image by user, tags are generated by encrypting the image block using AES with the key generated from the block image, as shown in the above figure.

Fig 4.9 Cloud Tags

For the uploaded image by user in the cloud, generated tags for the image uploaded is stored only once, as shown in the above figure.

Fig 4.10 Integrity check

For the image transmission from client to cloud service provider and vice versa, hamming code is generated during this process and generated code is verified to check whether image got modified by any adversary or remained same, as shown in the above figure.

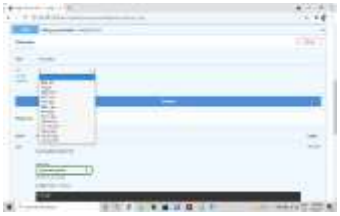

Fig 4.11 Image Download

Here the user can download the image from the uploaded images.

Fig 4.12 Image Download

The downloaded image is shown in the above figure.

Fig 4.13 Downloaded Image

The images downloaded by the user shown in the local folder of the system. In the above figure it shows the downloaded images.

Performance analysis

We have run the protocol on 10 image pairs, as 20 image dataset. Image dataset included different image formats like .png, .jpeg, .tiff. image size varied from 0.022mb to 14mb.

The images uploaded without duplication and the images uploaded with duplication is shown in the below figure.

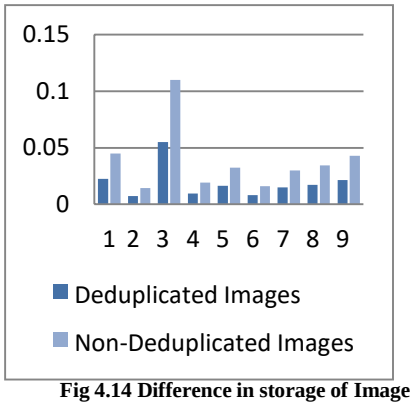

Fig 4.14 Difference in storage of Image

As the image upload and download communication costs are decreased as shown in the below figure. Where the similar images are uploaded only once in the storage along with the integrity check.

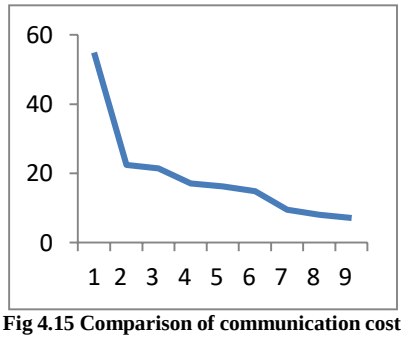

Fig 4.15 Comparison of communication cost

VI CONCLUSION

In this paper, we proposed method shows the deduplication check of the uploaded images of different formats. The integrity of the image data is modified or remained same. By using deduplication, storage efficiency is increased as the uploaded similar images are stored only once in the storage. By generating hamming code during transmission of the data from client to cloud service provider and vice versa, integrity of the data is checked and stored securely.

REFERENCES

[1] Agarwala, P. Singh, and P. K. Atrey, “DICE: A dual integrity convergent encryption protocol for client-side secure data deduplication,” in IEEE International Conference on Systems, Man, and Cybernetics, Banff, Canada, 2017, pp.2176–2181.

[2] M. Bellare, S. Keelveedhi, and T. Ristenpart, “Message locked encryption and secure deduplication,” in Advances in Cryptology – 32nd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Athens, Greece, 2013, pp. 296–312.

[3] M. Bellare and S. Keelveedhi, “Interactive message-locked encryption and secure deduplication,” in Public-Key Cryptography – 18th IACR International Conference on Practice and Theory in Public-Key Cryptography, Gaithersburg, MD, USA, 2015, pp. 516–538.

[4] J. Stanek, A. Sorniotti, E. Androulaki, and L. Kencl, “A secure data deduplication scheme for cloud storage,” in Financial Cryptography and Data Security, Berlin, Heidelberg, 2014, pp. 99–118.

[5] H. Gang, H. Yan, and L. Xu, Secure Image Deduplication in Cloud Storage. Cham: Springer International Publishing, 2015, pp. 243–251.

[6] F. Rashid, A. Miri, and I. Woungang, “Secure image deduplication through image compression,” J. Inf. Secur. Appl., vol. 27, no. C, pp. 54–64, 2016.

[7] Achmad Fauzi, Nurhayati, Robbi Rahim “Bit Error Detection and Correction with Hamming Code Algorithm” IJSRSET Journal Volume 3 Issue 1

[8] K. Keonwoo, Y. Taek-Young, J. Nam-Su, and C. Ku-Young, “Client-side deduplication to enhance security and reduce communication costs.” ETRI Journal, vol. 39, no. 2, pp. 116 – 123, 2017.

[9] W. Fitriani and A. P. U. Siahaan, "Single-Bit Parity Detection and Correction using Hamming Code 7-Bit Model," International Journal of Computer Applications, vol. 154, no. 2, pp. 12-16, 2016.

[10] V. Singh and N. Sharma, "A Review on Various Error Detection and Correction Methods Used in Communication," American International Journal of Research in Science, Technology, Engineering & Mathematics, vol. 9, no. 3, pp. 252-257, 2014.

[11] Deepika, A. Kumar, and Gurusiddayya, "A Study on Error Coding Techniques," International Journal for Research in Applied Science & Engineering Technology (IJRASET), vol. 4, no. 4, pp. 825-828, 2016.

[12] E. Torres, G. Callou, G. Alves, J. Accioly, and H. Gustavo, “Storage services in private clouds: Analysis, performance and availability modeling”, IEEE International Conference on Systems, Man, and Cybernetics, Budapest, Hungary, 2016, pp. 3288–3293.
[13] S. Anwarul and S. Agarwal, “Image enciphering using modified AES with secure key transmission”, Commun. Comput. Syst. - Prasad al., pp. 137–142, 2016.
[14] A. Kumar and A. Agrawal, “Image Encryption by 128 Bit Encryption Technique”, Int. Conf. Syst. Model. Adv. Res. Trends, pp. 106–108, 2015.
[15] P.K. Das, P. Kumar, and M. Sreenivasulu, “Image Cryptography: A Survey towards its Growth”, Adv. Electron. Electr. Eng. Res. India Publ., vol. 4, no. 2, pp. 179–184, 2014.