International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 02 Issue: 03 | June-2015 www.irjet.net p-ISSN: 2395-0072

PRIVACY ASSURED IMAGE STACK MANAGEMENT SERVICE IN CLOUD

Ms. Shubhangi Edake[1], Prof. Sunil Rathod[2]

[1] *PG Student, Computer Engineering, Dr.D.Y.Patil School of Engineering, Lohgaon,Pune,India*
[2] *Assistant Professor, Computer Engineering, Dr.D.Y.Patil School of Engineering, Lohgaon,Pune,India*

Abstract - *In advancement of digital era and storage technology, large-set of image data are being generated now a days, image dataset categories like bio images, satellite images each dataset contains hundreds of images for processing or study. With such fast-growing trend to image storage management systems to cloud it still faces a number of basic and critical challenges, among which storage space, privacy, security is the top concern.* ***With simplified*** *image storage management and secure image access, user can also apply compression and cryptography for the purpose of storage overhead reduction. At last we will perform performance and security analysis which shows that the proposed scheme is highly effective for managing storage space required and secure data access.*

Key Words: Storage technology, security, Privacy, flexibility, availability, Compression.

1. INTRODUCTION

It is very dangerous to publish your digital data online, whether you are publishing it professionally or just putting images up on your personal blog. Watermarking, for digital media whether it is images or videos is a great way to avoid people from copying photos that you have on your website or any portal, while still allowing the image to be seen. Creating a watermark and placing it on digital media that you plan to post on the web will identify them as your own work and avoid people from copying them or claiming them as their ownership and in case of cloud storage it makes it very difficult for manage storage space, privacy and security for that matter. Cloud computing is a paradigm which is used to keep up user's data and their application by using centralized remote servers. Cloud computing can be considered a new computing paradigm for greater flexibility and availability with less cost. Because of this, Cloud computing has been gaining a good attention from many people with different work area. While using service like storage offered by Cloud service providers, it is important to provide security to information that enters the cloud, and protect the privacy associated with data, thus requires deeper security into the Clouds infrastructure. Privacy issues are sure to be central to user data concerns about the adoption of Cloud computing, building such protections into the design and operation of the Cloud is important for future success of this new networking paradigm.

2. LITERATURE SURVEY

A. Title: Towards Secure and Dependable Storage Services in Cloud Computing

1) Proposed Method:
In this paper[2] authors described Cloud storage and process to remotely storage of data and the on-demand high quality cloud applications without the burden of local hardware and software management and explained the benefits of the same. In this paper author proposed a flexible distributed storage integrity auditing mechanism, which utilizes the homomorphic token and distributed erasure-coded data. Authors designed the system in a way that allows users to audit the cloud storage with very lightweight communication and computation cost. An author mainly focuses on the correctness of the data in cloud. Proposed system is highly efficient and resilient against Byzantine failure, data modification attack and server colluding attacks.

2) Advantages:
i) Data correctness is maintained
ii) Highly efficient and resilient against Byzantine failure, data modification attack and server colluding attacks.

3) Disadvantages:
i) User's files are not encrypted on some open source cloud storage Systems.

B. Title: Ensuring Data Storage Security in Cloud Computing

1) Proposed Method:
In this paper [3], author proposed an effective and flexible distributed scheme with explicit dynamic data support to ensure the correctness of user's data in the cloud. Author proposed data correcting code in the file distribution preparation to provide redundancies and guarantee the data dependability which drastically reduces the communication and storage overhead as compared to the traditional replication-based file distribution techniques. Here also used homomorphic token with distributed verification of erasure-coded data. Proposed system is highly efficient and resilient against Byzantine failure, malicious data modification attack, and even server colluding attacks. Proposed system not only achieves the

storage correctness insurance but also data error localization.

2) Advantages:
i)Proposed system ensures data correction, storage correction and also error localization.

3) Disadvantages:
i)Anyone can intentionally access or modify the data files as long as they are internally consistent, for that author does not use any encryption scheme.

C. Title:An Efficient and Secure Dynamic Auditing Protocol for Data Storage in Cloud Computing

1) Proposed method: In proposed system[4] authors proposed their own auditing protocol, before that author studies about data owners and data consumers and their access privileges and new security challenges that comes with cloud computing, which needs an independent auditing service to check the data integrity in the cloud. Author also mentioned some existing remote integrity checking methods that can only serve for static archive data. Existing data integrity checking methods does not suffice existing cloud computing security needs because the data in the cloud can be dynamically updated. So author proposed an efficient and secure dynamic auditing protocol. Author first designed an auditing framework for cloud storage systems and proposes an efficient and privacy preserving auditing protocol and then extended their auditing protocol which supports data dynamic operations and also further extend proposed auditing protocol compatible for batch auditing for both multiple owners and clouds, without using any trusted organizer.

2) Advantages:
i)Proposed method supports data dynamic operations.
ii) Support batch auditing for both multiple owners and multiple clouds, without using any trusted organizer.

3) Disadvantages:
i) Proposed method provide consistent place to save valuable data and documents but stored files are not encrypted on cloud storage systems.

D. Title: An Efficient and Secure Protocol for Ensuring Data Storage Security in Cloud Computing

1) Proposed Method:
In this paper [5], authors first studied the problem of Integrity and Confidentiality of data storage in cloud computing. Authors proposed an efficient and secure protocol using ECC and Sobol sequence. Proposed scheme satisfies the all security and performance requirements of cloud data storage. Our method also supports public verifiability that enables TPA to verify the integrity of data without retrieving original data from the server and probability detects data corruptions. The proposed method is mainly suitable for thin users, who have less resources and limited computing capability scheme also supports dynamic data operations.

2) Advantages:
i) Provides data integrity ii)Supports dynamic data operations

3) Disadvantages:
i)Proposed system is suitable for users having fewer resources and limited computing capability.

E. Title: Privacy-Preserving Public Auditing for Secure Cloud Storage

1) Proposed Method:
In this paper[8] , author focused on eliminating the burden of cloud user from the tedious and possibly expensive auditing task author proposed a privacy-preserving public auditing system for data storage security in cloud computing and also prevent outsourced data leakage. Method also performs multiple auditing tasks in a batch manner for better efficiency. Author used Amazon EC2 cloud for demonstration. Author used the homomorphic linear authenticator and random masking techniques so to guarantee that the TPA would not learn any knowledge about the data content stored on the cloud server. Finally author performed an extensive analysis which shows that their proposed schemes are provably secure and highly efficient.

2) Advantages:
i) Proposed schemes are provably secure and highly efficient.
ii) Allows batch processing.

3) Disadvantages:
i) User's files are not encrypted on proposed open source cloud storage systems.

F. Title: Privacy-Assured Outsourcing of Image reconstruction Service in Cloud

1) Proposed Method: In this paper [1], author proposed a framework called OIRS, an outsourced image recovery service from compressed sensing with privacy assurance. Author mainly focuses on secure outsourcing of stored images which exploits techniques from different domains, and aims to take security. Author proposed an architecture that contains image processing methods like compression, encryption and decryption which assures storage redundancy and security.

2) Advantages:
i) Security is well preserved.
ii) Allows storage redundancy.

3) Disadvantages:
i) Auditing is not performed.

3. EXISTING SYSTEM

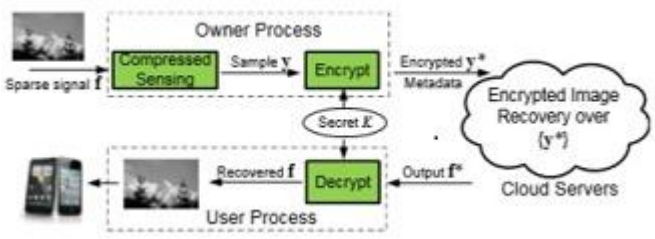

Fig. 3.1 OIRS System Architecture

Firstly, traditional cryptographic primitives for the purpose of data security protection cannot be directly adopted due to the use losses control of data under Cloud Computing. Therefore, Verification of correct data storage in the cloud must be conducted without explicit knowledge of the whole data. Considering various kinds of data for each user stored in the cloud and the demand of long term continuous assurance of their data safety, the problem of verifying correctness of data storage in the cloud becomes even more challenging.

Secondly, Cloud Computing is not just a third party data warehouse. The data stored in the cloud may be frequently updated by the users, including insertion, deletion, modification, appending, reordering, etc. To ensure storage correctness under dynamic data update is hence of paramount importance

4. PROPOSED SYSTEM

4.1 System Architecture

We propose an effective and flexible distributed scheme with explicit dynamic data support to ensure the correctness of user and user's data in the cloud. We rely on erasure correcting code in the storage preparation to provide redundancies and guarantee the data dependability. Our goal is to build up a repository to facilitate the data integration and sharing across cloud along with preservation of data confidentiality.
For this we will be using an effective encryption technique to provide data security on data storage. For storage management we simply storing the compressed images rather than the actual image which can help save the storage cost. But while compressing the image we have to maintain the quality of that image, Understanding these benefits of compressed system is pivotal, because it would allow us to explore new possibilities of establishing secure and privacy assured image service cloud computing, which

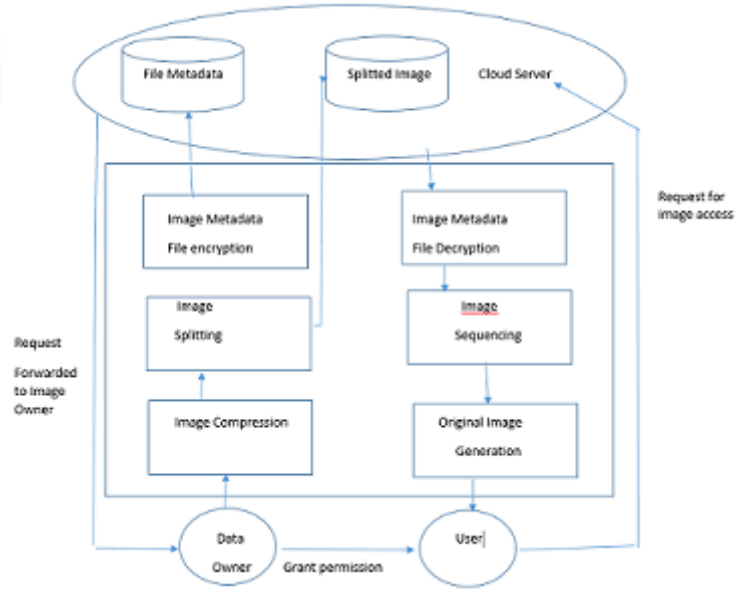

Fig 4,1 System Architecture

aims to take security, complexity, and efficiency into consideration from the very beginning of the service.

4.2 Mathematical Model

In this section we describe our mathematical model which is used to express the data storage cost, request cost, data transfer cost and average storage allocation cost in cloud computing .Our goal is to minimize storage which affect optimize cost. Our approach is to maximize storage Allocation by minimizing data size in cloud computing. For calculating the storage efficiency of proposed system we came up with some formulas as follows

Where,

1. ST - Allocation of database storage in binary

2. TR - Number of data transfers for dataset from storage to site

3. DBSize - Size of database in GB

4. DBUsage - Percentage of database accessed per user

5. DBReq - Number of monthly storage requests in database for per user

6. perReqCost Cost of each request from user

$$AvgST = \frac{STCost + TRCost + ReqCost}{Total\ GB\ stored} \quad \ldots\ldots [1]$$

$$STCost = \sum DBSize\ X\ Cst\ X\ ST \quad \ldots\ldots [2]$$

$$TRCost = \sum TR\ X\ DBSize\ X\ DBUsage \quad \ldots [3]$$

$$ReqCost = \sum ST\ X\ DBReq\ X\ perReqCost \quad \ldots [4]$$

Let S be the system where,
S={Img,Owner,User,Comp,Enc,Dec,Tpa}

Img : Image to input/upload

Owner : User who holds particular image

User : Receiver who needs particular image uploaded by owner

Comp : Perform compression on owners image before encrypting

Comp= {Iimg, Cimg,DCT}

Iimg: Input image

Cimg:Compressed image

DCT: Discrete cosine transform

Here, equation [1] computes the pixel entry that is i , jth entry of DCT of an image.

P(x,y) is the x, yth element of image represented by matrix p. N is the size of block that DCT is done on

$$D(i,j) = \frac{1}{\sqrt{2N}} C(i)C(j) \sum_{x=0}^{N-1} \sum_{y=0}^{N-1} p(x,y) \cos\left[\frac{(2x+1)i\pi}{2N}\right] \cos\left[\frac{(2y+1)j\pi}{2N}\right]$$

....[5]

N equals 8 and x and y range from 0 to 7. Therefore D(I,j) would be as in equation [7]

$$C(u) = \begin{cases} \frac{1}{\sqrt{2}} & \text{if } u = 0 \\ 1 & \text{if } u > 0 \end{cases}$$

.....[6]

$$D(i,j) = \frac{1}{4} C(i)C(j) \sum_{x=0}^{7} \sum_{y=0}^{7} p(x,y) \cos\left[\frac{(2x+1)i\pi}{16}\right] \cos\left[\frac{(2y+1)j\pi}{16}\right]$$

.....[7]

To get the matrix form of equation[5], we will use the equation [8]

$$T_{i,j} = \begin{cases} \frac{1}{\sqrt{N}} & \text{if } i = 0 \\ \sqrt{\frac{2}{N}} \cos\left[\frac{(2j+1)i\pi}{2N}\right] & \text{if } i > 0 \end{cases}$$

.....[8]

Enc : Performs encryption on owners image after compression

Enc:{Cimg,RSA,Eimg}

Iimg:Input image, here output of compressor is input for encryption module

RSA: public-key cryptosystems used for encryption

Eimg: Enrypted image

Dec : perform decryption on image before downloading by receiver/user

5. RESULTS

Here histogram are used to compare input image, encrypted image and decrypted image

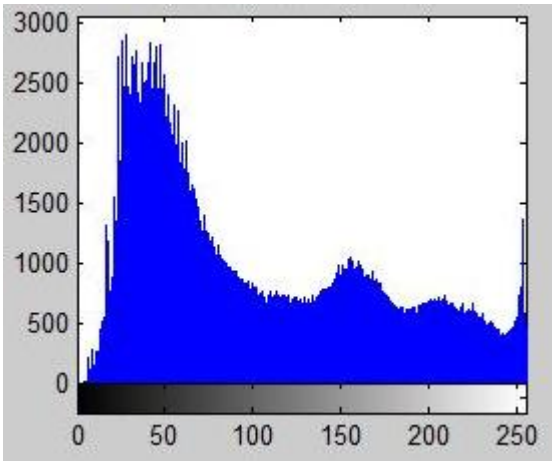

Fig 5.1Histogram of Input image

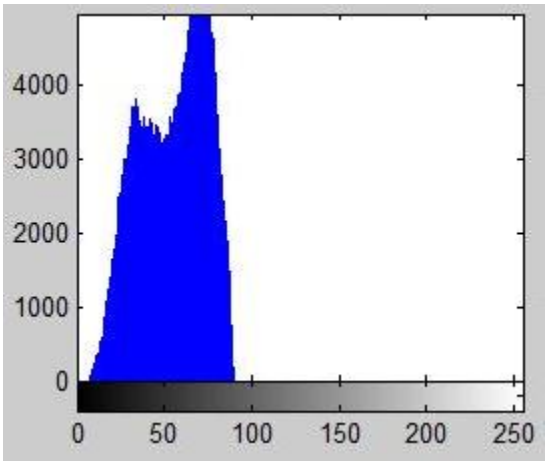

Fig 5.2Histogram of Encrypted image

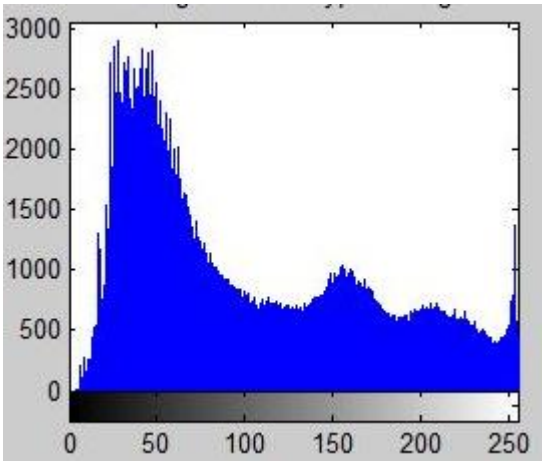

Fig 5.3Histogram of Decrypted image

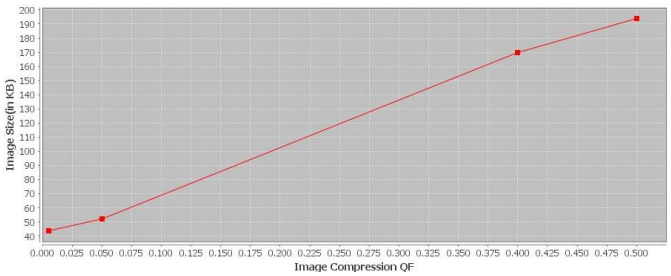

Fig 5.4Image compression QF VS Image size

Fig 5.5 Original Image

Fig5.6 Compression with QF=0.005

Fig.5.7 Compression With QF=0.5

Fig 5.8 Encrypted and decrypted image

6. CONCLUSIONS

In many organizations the main issues is maintaining the security and privacy of confidential data. Cloud store different types of data for example documents, data sheets, digital media object and it is necessary to give guarantee about data confidentiality. Data integrity, privacy and auditing are the terms which examines all stored data to maintain privacy and integrity of data and give data confidentiality. Compression technique gives more efficient result than

ACKNOWLEDGEMENT

I wish to express my sincere thanks to the guide Prof .Sunil Rathod ,PG Coordinator Prof. Pankaj Agarkar and Head of Department, Prof. Soumitra Das , as well as our principal Dr.S.S.Sonavne and last but not least, the departmental staff members for their support.

REFERENCES

[1] Cong Wang, Bingsheng Zhang, Kui Ren and JanetM. Roveda,Privacy Assured Outsourcing of Image Reconstruction Service in Cloud . IEEE Transaction on Cloud Computing, Vol. 1, NO. 1,2013.

[2] Kui Ren,Cong Wang, Qian Wang,Ning Cao,and Wenjing Lou,Towards secure and Dependable Storage Services in Cloud Computing. Proc.17th IEEE,2009,pp.1-14.

[3] Cong Wang, Qian Wang, and Kui Ren,Ensuring Data Storage Security in Cloud Computing. IEEE,US,2008 ,pp.1-9.

[4] Kan Yang and Xiaohua Jia,An Efcient and Secure Dynamic Auditing Protocol for Data Storage in Cloud Computing . IEEE Transaction on Parallel and Distributed Systems, Vol. 24, NO. 9, September 2013, pp. 1717-1726.

[5] Syam Kumar p. and Subramanian R,An Efcient and Secure Protocol for Ensuring Data Storage Security in Cloud Computing . Department of Computer Science, School of Engineering Technology Pondicherry University, Puducherry,605014, India .

[6] Sravan Kumar R and Ashutosh Saxena ,Integrity Proofs in Cloud Storage. Proc.IEEE 978-1-4244-8953-4/11, 2011.

[7] Yan Zhu, HongxinHu, Gail-Joon Ahn and Mengyang Yu,Provable Data Possession for Integrity Verication in MultiCloud Storage. in Proc. IEEE Transaction on Parallel and Distributed Systems, 10459219/12,2012.

[8] Cong Wang,Qian Wang,Sherman S.M. Chow,Kui Ren,PrivacyPreserving Public Auditing for Secure Cloud Storage. in Proc. IEEE Transaction on Computers, VOL. 62, NO. 2,February 2013.

BIOGRAPHIES

Ms. Shubhangi Edake , PG Student at Dr. D.Y.Patil School of Engineering, Savitribai Phule Pune University.

Email-shubhangi.edake@gmail.com

Prof. Sunil Rathod, Assistant Professor at Dr.D.Y.Patil School of Engineering, Savitribai Phule Pune University.

Email – sunil2k_r@yahoo.co.in

