International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2015): 6.391

Re-encryption based Attribute Revocation in Data Access Control for Multiauthority Cloud Storage

Kalyani G. Ktangale[1], Milind Penurkar[2]

[1]Student MITCOE, Pune, India

[2]Assistant Professor, MITCOE, Pune, India

Abstract: ***In Services including private users, businesses and governments, Cloud computing technologies are gaining importance at a very higher level. Cloud computing provides transparency, but sharing of resources at a distributed level has severe implications when sensitive or privacy-relevant data is concerned. To ensure the data security in cloud Data access control is an effective way . But due to the untrusted cloud servers, data access control becomes a challenging issue in cloud storage systems. However after attribute revocation if we have to provide security through re-encryption, then this is not given .In this paper we proposed certificate less encryption-based schemes by relying on a public cloud server and we apply it as underlying techniques to design the data access control scheme. Our certificate less encryption method can efficiently provide both forward security and backward security.***

Keywords: Data access control, Attribute Revocation, Re-encryption

1. Introduction

In cloud computing, security is the main important constraint which is only the main focus of this survey. Here the Encryption module, Decryption module, Splitter module and joiner module are used to provide security at a higher level. Encryption is a technique where we change the original content with some code to provide security to the data. There is some private key is used to encrypt the data.

Moving data into cloud servers provide great convenience to users because they don't have to worry about the complexities of direct hardware management and security and privacy in case of private cloud. There are several pioneers of Cloud Computing vendors for example Amazon Elastic Compute Cloud (EC2), Amazon Simple Storage Service (S3)

Current available cloud vendors provide huge amounts of storage space and customizable computing resources, and some data vendors take responsibility of data maintenance at the same time, but the security is still a major concern in case of public cloud.

Encrypted data can be re-encrypted again to provide higher level of security. During the decryption, with the help of the public key of owner we can get the decrypted data in original form to particular user, and hence security to the data is provided. Before encryption the original data is splitted into chunks with the help of Splitter module .And during Decryption all the decrypted chunks get joined together with the help of the Joiner module. Attribute revocation means to get or to revoke the original data which is encrypted. Multi-authority cloud storage means multiple users can use the data to store and download from the cloud .In such a way higher level of security is provided in cloud storage.

2. Literature Survey

[1] This paper proposed an attribute- based encryption scheme without the trusted authority, and an anonymous key issuing protocol. Authors ensured that their work give a more practice-oriented attribute based encryption system. Here author reviewed the motivation behind the use of the trusted central authority (CA) and how to avoid it.

Author also mentioned that in a multi-authority ABE scheme, different attribute-authorities monitor different sets of attributes and issue corresponding decryption keys to users and can require that a user obtain keys for appropriate attributes from each authority before decrypting a message.

Authors studied a multi-authority ABE scheme using the concepts of a trusted central authority (CA) and global identifiers (GID) but the CA in that construction has the power to decrypt every ciphertext, which they found out contradictory to the original goal of distributing control over many potentially untrusted authorities. Also in that construction, the use of a consistent GID allowed the authorities to combine their information to build a profile with all of a user's attributes, which unnecessarily compromises the privacy of the user so authors proposed a method which removes the trusted central authority, and protects the users privacy by preventing the authorities from getting their information on particular users, thus making ABE more usable in practice.

[2] In this paper, author propoed an expressive, efficient and revocable data access control method for multi-authority cloud storage, where there are multiple authorities present and each authority can issue attributes independently. Author mentioned that data access control is an effective way to ensure the data security in the cloud. Due to data outsourcing and untrusted cloud servers, the data access control becomes a challenging issue in cloud storage systems. Cipher text-Policy Attribute-based Encryption (CP - ABE) is considered as one of the most suitable methods for data access control in cloud storage, because it gives data

owners more direct control on access policies. However, it is difficult to directly apply existing CP -ABE schemes to data access control for cloud storage systems because of the attribute revocation problem. Specifically, Author proposed a revocable multi- authority CP- ABE scheme, and apply it as the underlying techniques to design the data access control scheme. Our attribute revocation method can efficiently achieve both forward security and backward security. The analysis and simulation results how that our proposed data access control scheme is secure in the random oracle mode and is more efficient than previous works.

[3] In this paper, authors first studied the problem of Confidentiality and Integrity of data storage in cloud computing and proposed an efficient and secure protocol using ECC and Sobol sequence. The proposed method is mainly suitable for thin users who have less resources and limited computing capability scheme also supports dynamic data operations. 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.

[4] In this paper, author proposed a novel patient-centric framework for data access control to Personal Health Records (PHRs) stored in semitrusted servers. To achieve scalable data access control for PHRs, author used attribute-based encryption (ABE) techniques to encrypt patient's PHR file. Author mainly focused on the multiple data owner scenario for data outsourcing and divides the users in the PHR system into multiple security domains that reduces the management complexity for owners and users.

Author first mentioned that although Personal health record (PHR) is an emerging patient-centric model of health information exchange, which is often outsourced to be stored at a third party, such as cloud providers but there have been wide privacy concerns as personal health information could be exposed to those third party servers and to unauthorized parties.

Proposed method provides high degree of patient privacy and also enables dynamic modification of access policies or file attributes, supports efficient on-demand user/attribute revocation. Author carried out extensive analytical and experimental results which showed the security, scalability, and efficiency of our proposed scheme.

[5] In this paper, author proposed an effective distributed scheme with explicit dynamic data support to ensure the correctness of users 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. This system uses 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. The main disadvantage of this system is that anyone can intentionally access or modify the data because author does not used any encryption scheme.

3. Proposed System

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 file 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.

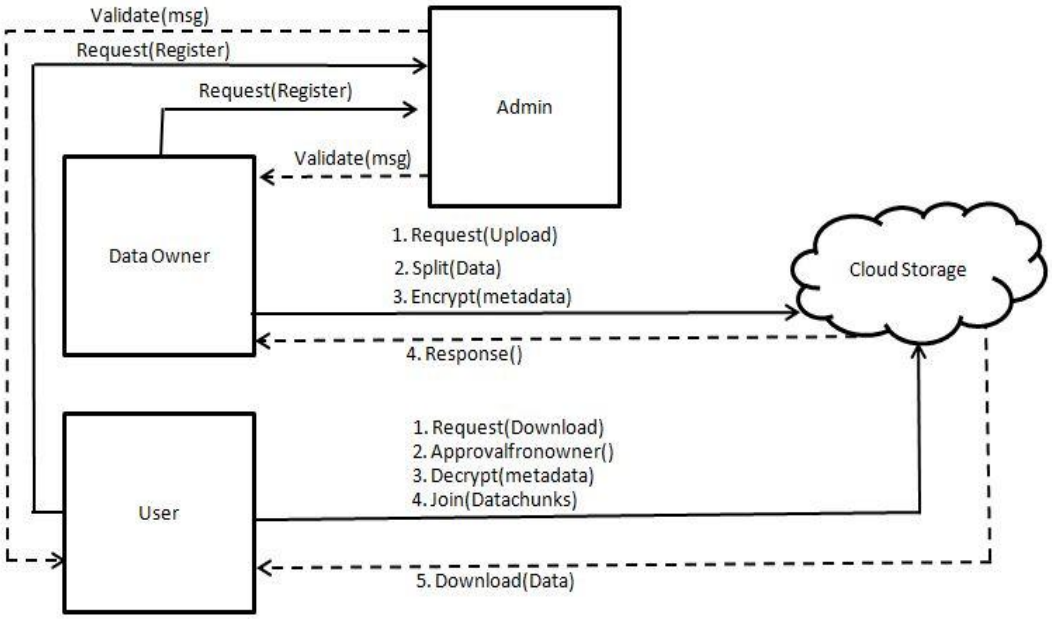

Figure 3.1: Architecture diagram

3.1 UPLOAD MODULE

3.1.1 File Compressor:
This module takes image as input and compresses the image using DCT algorithm.

3.1.2 File Splitter
This module take image as input and split it into 10 chunks and store it on cloud, while the metadata file about the split file is also stored on cloud folder

3.1.3 Encryption
This file takes metadata file as input and encrypt file. We are using AES algorithm for encryption.

3.2 Download Modules

3.2.1 File Joiner
While downloading any image file joiner get the location of image that is location of splitted file with the help of metadata file.

3.2.2 Decryption
This module is sub module of File joiner, file joiner module passes the encrypted metadata file to decryption module and this module decrypt the file and pass the file to file joiner and then file joiner get the information about chunks and joins the chunks and then joined file is a image that user requested to download.

4. Result and Alanysis

We have taken execution time as parameter for result, Various images were considered with different sizes and for each image of different size the total compression time and splitting time were calculated for images of different sizes. As the table 4.1 shows various images with different storage size in KB and respective execution time for each image

Table 4.1: Execution time for compression

Image	Size (KB)	Execution time
Allante	130	156
imagerain	256	203
sounchy	319	297
violine	455	302

Graph 4.1: Execution time for compression

Table 4.2: Execution time for splitting

Image	*Size (KB)*	*Execution time*
Allante	130	47
imagerain	256	49
sounchy	319	78
violine	455	84

Graph 4.2: Execution time for spliting

5. Storage Cost

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.

ST - Allocation of database storage in binary
TR - Number of data transfers for dataset from storage to site
DBSize - Size of database in GB
DBUsage - Percentage of database accessed per user
DBReq - Number of monthly storage requests in database for per user
perReqCost – Cost of each request from user

$$AvgST = \frac{STCost + TRCo.}{Total\ GB} \quad \ldots\ldots [1]$$

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

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

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

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 stated earlier.

6. Conclusion

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 are the terms which examines all stored data to maintain privacy and integrity of data and give data confidentiality.

References

[1] Kan Yang, and Xiaohua Jia, " Expressive, Efficient, and Revocable Data Access Control f or Multi-Authority Cloud Storage*", IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS,*Vol.25, No.7*,* pp. 1735-1744*,* July 2014.

[2] Sherman S.M. Chow " Improving Privacy and Security in Multi- Authority Attribute-Based Encryption" *Melissa Chase Microsoft Research 1 Microsoft Way Redmond, WA 98052, USA melissac@microsoft.com Department of Computer Science Courant Institute of Mathematical Sciences New York University, NY 10012, USA schow@cs.nyu.edu 2013*

[3] "Ming Li, Member, IEEE, Shucheng Yu, Member, IEEE, Yao Zheng, Student Member, IEEE, Kui Ren, Senior Member, IEEE, and Wenjing Lou, Senior Member, IEEE "Scalable and Secure Sharing of Personal Health Records in Cloud Computing Using Attribute-Based Encryption*" IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 24, NO. 1, JANUARY 2013*

[4] Syam Kumar P, Subramanian R Department of Computer Science, School of Engineering & Technology Pondicherry University "An Efficient and Secure Protocol for Ensuring Data Storage Security in Cloud Computing*" IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 6, No 1, November 2011*

[5] Cong Wang, Qian Wang, and Kui Ren Department of ECE Illinois Institute of Technology "Ensuring Data Storage Security in Cloud Computing" *Email: cwang, qwang, kren}@ece.iit.edu Wenjing Lou Department of ECE Worcester Polytechnic Institute Email: wjlou@ece.wpi.edu JULY 2012*