International Journal of Computer Architecture and Mobility
(ISSN 2319-9229) Volume 1-Issue 6, April 2013

DEFENDED CLOUD DATA STORAGE

VANDANA VIJAY BELKHODE
SINPA COET, AMRAVATY
vandanabelkhode@gmail.com
GUIDE
PROF. D. M. DAKHANE

CO-GUIDE

PROF. R. L. PARDHI

ABSTRACT

Cloud computing is the next stage in providing the means through which everything from computing power to computing infrastructure, applications, business processes to personal collaboration can be delivered to you as a service, internet evolution wherever and whenever you need. There are three main service offered by cloud such as infrastructure as a service, Platform as a service and Software as a service. Cloud computing provide great security and privacy to internet communication. Information search and document retrieval from a remote database requires submitting the search terms to the database holder. However, the search terms may contain sensitive information that may be kept from the related holders the related protocol private information retrieval provide useful cryptographic tool to hide the data. The coming of cloud computing the user can access data remotely from anywhere at any time cloud services provider play a great role in providing data security, but it is not enough. For a data security provide a sufficient number of solutions offered to make the retrieval of data from the CSP. In this paper we study about security and privacy in cloud computing.

1. INTRODUCTION

The "cloud" in cloud computing can be defined as the set of networks, storage, hardware, services, and interfaces that combine to deliver aspects of computing as a service. Cloud service includes the delivery of software, storage and infrastructure over the Internet (either as separate components or a complete platform) based on user demand. Cloud computing has four essential characteristics: elasticity and the ability to scale up and down, application programming interfaces, self-service provisioning and automatic deprovisioning billing and metering of service usage in a pay-as-you-go model. This flexibility is what is attracting individuals and businesses to move to the cloud. One of the major merit of cloud storage is user can access data in a cloud anytime and anywhere using device.

In Infrastructure service, the service provider provides the hardware and necessary servers, networking components to an organization for a fee. The organization in turn installs the necessary programs in the service provider's server and uses them. The service provider is responsible for the maintenance of the servers. In Infrastructure service, the service provider provides the necessary software and the tools for creating software which are installed in their server to an organization for a specified amount. The organization creates the necessary software. On his platform and uses them. It's like renting in a house which has all the necessary things. In Platform service, the applications hosted in the service provider s server are made available to customers via the internet. The provider also interacts with the user through a front end panel. The provider provides the necessary support to the customer. The services range from electronic mail to data processing. In Software service, the applications hosted in the service provider s server are made available to customers via the internet. The services range from e-mail to data processing. Retrieved; both need to be hidden. Today's security and privacy are major issues in internet or electronic communication. This security and privacy are greatly handle by cloud computing. There are several privacy issues regarding to accessing data on such servers; two of them can easily be ideated sensitivity of I) keywords sent in queries and ii) the data.

Cloud service providers (CSP) are separate administrative entities; data outsourcing is actually relinquishing user's ultimate control over the fate of their data. As a result, the correctness of the data in the cloud is being put at risk due to the following reasons. First of all, although the infrastructures under the cloud are much more powerful and reliable than personal computing devices, they are still facing the broad range of both internal and external threats for data integrity. Examples of outages and security breaches of noteworthy cloud services appear from time to time. Secondly, there do exist various motivations for CSP to behave unfaithfully towards the cloud users regarding their outsourced data status. For examples, CSP might reclaim storage for monetary reasons by discarding data that has not been or is rarely accessed, or even hide data loss incidents to maintain a reputation. In short, although outsourcing data to the cloud is economically attractive for long-term large-scale storage, it

does not immediately offer any guarantee on data integrity and availability. This problem, if not properly addressed, may impede the success of cloud architecture.

2. Security problems in cloud storage

In cloud computing, cloud storage security is the major problem of virtual storage, resources are highly centralized, and the super storage, and the super storage, service for users by virtualization technology. The basic problem of cloud storage was to selection on documents storage services for data owner, rebound human general activities onto the internet in diminutive. Cloud privacy is not only a general technical problem, but also a social problem in attribute. For example, UDP and TCP/IP protocol provides a best-effort and up-to date service rather than a unique precise one. The quality of service can be optimized constantly by collective intelligence. The interaction of human machine on the internet forms many communities, while protection and belief are the quality aggregate by community evolvement. For the credit of producer and online shopping will be selected.

3. Related work

The problem of Private Information Retrieval was introduced by Chord. Recently Growth proposes a multi-query PIR method with constant communication rate. Ogata and Kurosawa show privacy preserving keyword search protocol based on RSA blind signatures. The scheme requires a public-key operation per item in the database for every query and this operation must be performed on the user side. Freedman, proposed an alternative implementation for private keyword search that uses homomorphism encryption and oblivious polynomial evaluation methods. The computation and communication costs of this method are quite large since every search term in a query requires several homomorphism encryption operations both on the server and the user side. A recent work proposed by Wang allows ranked search over an encrypted database by using inner product similarity. However, this work is only limited to single keyword search queries.

One of the closest methods to our solution is proposed by Cao et al. [3]. Similar to our approach presented here, it proposes a method that allows multi-keyword ranked search over encrypted database. In this method, the data owner needs to distribute a symmetric-key which is used in trap door generation to all authorized users. Additionally, this work requires keyword in the index. This means that the user must know a list of all valid keywords and their positions as compulsory information to generate a query. This assumption may not be applicable in several cases. Moreover, it is not client due to matrix multiplication operations of square matrices where the number of rows is in the order of several thousands. Wang propose a trapdoor less private keyword search scheme, where their model requires a trusted third party which they named as the Group Manager. We adapt their indexing method to our scheme, but we use a totally different encryption methodology to increase the security and efficiency of the scheme.

4. Problem hazard

4.1 *Hazard Model*

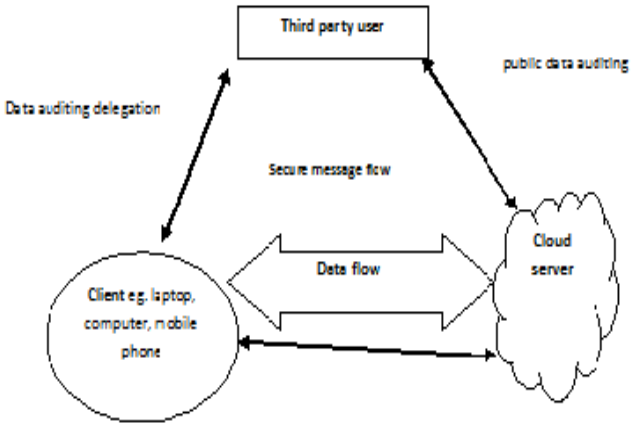

Fig. Hazard Model

Consider a cloud data storage service including three main module as illustrated in fig. the user, cloud server and third party. User contain large amount data and file to be stored in cloud; cloud service provider (CSP) can manage the cloud server (CS) to provide data storage service and has significant storage space and computation resources, the third party auditor has more expert and capability than user. It more trusted to access the cloud storage service trustworthy on behalf of the user upon request. User can depend upon CS for cloud data storage maintenance. They also interested in update and access their storage data for various application and other official purposes. It is most important for user to ensure that their data are correctly stored and maintained. To save the computation resource as well as the online burden potentially brought by the periodic storage correctness verification, cloud users may resort to TPA for ensuring the storage integrity of their outsourced data, while hoping to keep their data private from Tate data integrity threats towards users 'data can come from both internal and external attacks at CS. These may include: software bugs, hardware failures, bugs in the network path, economically motivated hackers, malicious or accidental management errors, etc.Besides, CS can be self-interested.

4.2 Goals

There are four design purposes,

1. To allow the third party auditor to check the accurateness of the stored data on demand without getting back a copy of the whole data.
2. To ensure that there exists no cheating cloud server that can pass the TPA's audit without indeed storing users' data intact.
3. During the auditing process user ensure that the TPA cannot the derive user data content.

4. With minimum communication and computation allow TPA to perform auditing.

4.3 Advantages of cloud storage

1. The customer after paying the amount can get the service at any time.
2. Also there are no problems of computer crash or server down. These are the responsibility of the service provider.
3. There is no investment cost for servers, computer, hardware, software, etc.
4. Amount can be paid according to usage.

Now a day, the service providers provide the service on a monthly basis. The provider and the customer can cancel the agreement at any time. So there is no waste for anyone.

4.4 Disadvantages of cloud storage

1. Security breaches**.** Remember, I said that remote server security makes it harder, but not impossible, for hackers to reach your data. If there is a compromise of the server(s) where your data is stored, your personal information may be exposed to the world.
2. Outage**s.** Have you ever been unable to access your email due to your provider being down? Now, imagine if you needed a document for an important business meeting or presentation and your storage provider's site was down.
3. Storage limits**.** While your local hard drive may be able to hold 500GB or more of data, unfortunately a remote server may only allow you to freely store about 5GB. If you want more room, you'll have to pay.
4. Slow speeds**.** Uploading and downloading of large documents may take a long time.
5. Limited features**.** If you use remote software that's provided by the storage service to manipulate and modify your data, it usually lacks the features of a program running locally.

4.5 Application of cloud storage

1. Cloud computing used in health care.
2. The main application cloud computing is military.

5. Information hiding in cloud storage

There are three basic methods are used in cloud storage

1. Digital watermarking

2. Steganography

3. Encrypted and Decrypted

5.1 Digital watermarking

Without help of the local hardware and software cloud storage provided grand to user for stored their data and access the cloud application. For hiding the data or identifying information within digital multimedia used the Digital Watermarking Technique. Digital Watermarking Technique is a not temporarily embedded into digital data, it is a permanently embedded. It is a hold the information on copyright security and data authorized. A digital watermark is a pattern inserted into a digital images and digital signal. Since this signal or pattern is present in each unaltered copy of the original image, the digital watermark may also serve as a digital signature for the copies. An available watermark is unique to each copy e.g. steady recipient or to be some for one or more copies. In the watermarking techniques document involves translation of the original into another form. Watermarking can also be deal with public-key encryption, which also converted original document into another form. Unlike encryption, however, digital watermarking leaves the original images or files basically intact and recognizable. Nowadays without the decrypted key encrypted digital data and files become unusable. In digital watermarking signature is invalided without use of special software.

5.1.1The goal of Digital Watermarking

Digital watermarking is an unchanged or extracted, building them a very important tool when protected from copyright infringement on the internet. Digital watermarks cooperate to authorized use of content or documents, while providing privacy to the content or documents to protect from unauthorized usages. Digital watermarks are concentrated meaning they are able to bear any potential hackers or any type of manipulation and accessing on internet. There are two types of digital watermarking one is visible watermarking and another is invisible watermarking. In visible watermarking, is similar to the copyright notice and verification massages stating who own the material or digital stamp. Visible watermarks modify the appearance of images and video, they are effective in avoiding potential commercial value from internet hackers. In invisible digital watermarks, are generally not exposed by the human eye and ear, but can be exposed by computer, CD or DVD drivers, digital camera or other devices that are provided special type of software. If hacker used any image without any authorizations then invisible watermarks not only notified the user of hold authorized copyright owner, but authorized also provide prosecution method. The main purpose of the watermarking in cloud storage is to prevent user private and confidential document from hacker by using

some methods such as color changing, visible and invisible watermarks

5.1.2Comparison between visible and invisible watermarks

Visible and invisible watermarks both serve to deter theft but they do so in very different ways. Visible watermarks are especially useful for conveying an immediate claim of ownership. The main advantage of visible watermarks is that they virtually deleted the commercial value of the data to a would-be thief without lessening the document's utility for legitimate, legal purposes. A familiar example of a visible watermark is in the video domain where CNN and other television networks place their translucent logo at the bottom right of the screen image. Invisible watermarks, on the other hand, are more of an aid in catching the thief than discouraging the theft in the first place.

References

1. *C. Wang, Q. Wang, K. Ran, and W. Lou, "Privacy-preserving public auditing for storage security in cloud computing," in Proc. of IEEE INFOCOM'10, March 2010*

2. Cloud Security Alliance, "Top threats to cloud computing," 2010, http://www.cloudsecurityalliance.org.

3. M. Arrington, "Gmail disaster: Reports of mass email deletions,"2006.

4. Amazon.com, "Amazon s3 availability event: July 20, 2008," http: //status.aws.amazon.com/s3-20080720.html, 2008.

5.Q. Wang, C. Wang, K. Ran, W. Lou, and J. Li, "Enabling public audit ability and data dynamics for storage security in cloud computing," IEEE Transactions on Parallel and Distributed Systems, vol. 22, no. 5, pp. 847–859, 2011.

6. G. Attendees, R. Burns, R. Carmela, J. Herring, L. Kisser, Z. Peterson, and D. Song, "Provable data possession at entrusted stores," in Proc. of CCS'07, 2007, pp. 598–609.