www.ijecs.in

International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 2, Issue 6 June, 2013 Page No. 2030-2032

DATA STORAGE IN CLOUD COMPUTING

Shachindra Kumar Dubey, Prof. Ashok Verma

Computer Science & Engg. *Department* Gyan Ganga Institute of Technology and Sciences Jabalpur, India
sachindrakumar000@gmail.com
HOD Computer Science & Engg. Department Gyan Ganga Institute of Technology and Sciences Jabalpur, India
ashokverma@ggits.org

Abstract— Cloud Computing is an emerging as well as the next generation technology. It provides different services such as SaaS, PaaS, IaaS. It is an Internet based technology where quality services are provided to users including data and software, on remote servers. In order to achieve secure cloud, there exists certain techniques such as erasure-coded data, authentication, message-digest algorithms. There are a number of algorithms and their methodologies available for achieving data security. In this paper we look at the current researchers related to data security issues like confidentiality and authentication. In particular, we will discuss how to secure data on certain servers.

***Keywords*—Cloud computing, authentication, confidentiality, auditing, data-correctness, security.**

I. INTRODUCTION

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. Cloud computing is the use of computing resources (hardware and software) that are delivered as a service over a network (typically the Internet).

A cloud storage system is considered as a large scale distributed storage system that consists of many independent storage servers. In the process of storing data to the cloud, and retrieving data back from the cloud, there are mainly three elements that are involved, namely the user, the server and the communication between them. In order for the data to have the necessary security, all these elements must have a solid security. Example of cloud computing: Amazon Cloud Drive, G Space, Minus, Web e-mail providers like Gmail, Hotmail and Yahoo! Mail store e-mail messages on their own servers, A Drive YouTube, Social networking sites like Facebook and MySpaceSites like Flicker and Picasa host millions of digital photograph. While these internet-based online services do provide huge amounts of storage space and customizable computing resources, this computing platform shift, however, is eliminating the responsibility of local machines for data maintenance at the same time. As a result, users are at the mercy of their cloud service providers for the availability and integrity of their data. Recent downtime of Amazon's S3 is such an example.

As with any storage system, there are certain security properties that are desirable in a cloud storage system: confidentiality, integrity, write- serializability and read freshness. These properties ensure that user's data is always secure and cannot be modified by unauthorized users and the data is always at the latest versions when being retrieved by the user. In this paper, we propose an effective and flexible distributed scheme with explicit dynamic data support to ensure the correctness of users' data in the cloud.

II. PROBLEM STATEMENT

Security and Reliability are main challenges of cloud computing. Clients aren't likely to entrust their data that on cloud will not be accessed by other clients. To achieve security on cloud there are so many techniques and algorithm available. Some of these techniques are:

Encryption**:** technique use complex algorithm to hide the original information with the help of encryption key. Authentication processes, which require creating a user name and password. Authorization practices – firstly list of authorized clients, who can access data stored on cloud system.

However, many people worry that data saved on a remote storage system is vulnerable. . Hackers could also attempt to steal the physical machines on which data are stored. A disgruntled employee could alter or destroy data using his or her authenticated user name and password. Cloud storage companies invest a lot of money in security measures in order to limit the possibility of data theft or corruption.

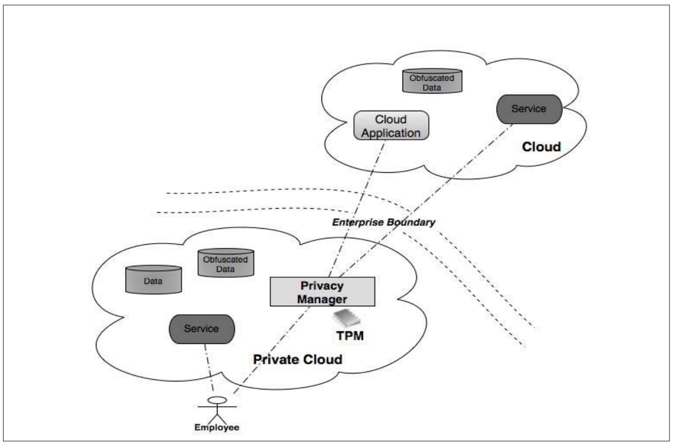
We are discussing some techniques that are helping how to get security at administrative level and for different clients by doing survey and reading the different research paper.

III. METHODS

A. Concept of Transparent security

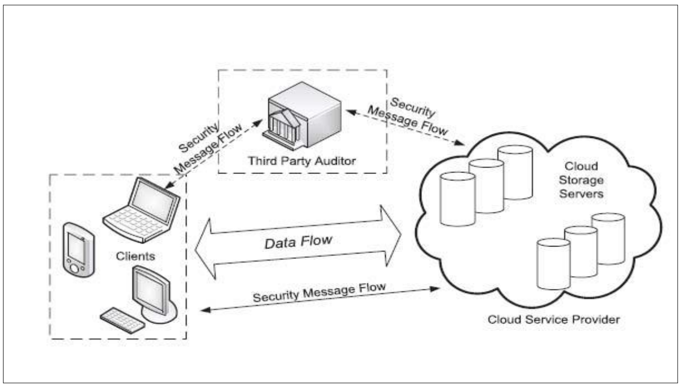
According to NIST (National Institute of Standards and Technology) Cloud computing is a model for enabling convenient, on - demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

B. Third party auditing



Third party auditing is an entity, which has expertise and capabilities that clients do not have, is trusted to assess and expose risk of cloud storage services on behalf of the clients upon request. The task of TPA is to verify integrity of the dynamic data stored in the cloud. Users rely on the CS for cloud data storage and maintenance. They may also dynamically interact with the CS to access and update their stored data for various application purposes. The users may resort to TPA for ensuring the storage security of their outsourced data, while hoping to keep their data private from TPA. However, during providing the cloud data storage based services, for their own benefits the CS might neglect to keep or deliberately delete rarely accessed data files which belong to ordinary cloud users. Moreover, the CS may decide to hide the data corruptions caused by server hacks or Byzantine failures to maintain reputation. We assume the TPA, who is in the business of auditing, is reliable and independent, and thus has no incentive to collude with either the CS or the users during the auditing process.

Fig:- A Cloud Data Storage Architecture



C. Authentication

The process of identifying an individual, usually based on a username and password. In security systems, authentication is distinct from authorization , which is the process of giving individuals access to system objects based on their identity. Authentication merely ensures that the individual is who he or she claims to be, but says nothing about the access rights of the individual.

Network security starts with authenticating, commonly with a username and a password. Since this requires just one detail authenticating the user name —i.e. the password— this is sometimes termed one-factor authentication. With two-factor authentication, something the user 'has' is also used (e.g. a security token or 'dongle', an ATM card, or a mobile phone); and with three-factor authentication, something the user 'is' is also used (e.g. a fingerprint or retinal scan).

D. Secret sharing and Erasure coding

1) Secret sharing: Shamir proposed an (m, n) Secret Sharing (SS) scheme based on polynomial interpolation, in which m of n shares of a secret are required to reconstruct the secret.

2) Erasure code: An (k, n) erasure code encodes a block of data into n fragments, each has 1/k the size of the original block and any k fragments can be used to reconstruct the original data block. Examples are Reed Solomon (RS) codes and Rabin's Information Dispersal Algorithm.

In the basic scheme, suppose a sensor node v has data to be stored locally. To protect data, it can perform the following operations to ensure the data integrity and confidentiality:

- *Step 1:* Generate a random session key kr and compute the keyed hash value h(data, kr) of data.
- *Step 2:* Encrypt data, h (data, kr) with kr and obtain {data, h (data, kr)}kr .
- *Step 3:* Encrypt kr using the key KUV shared between the authorized users and itself. This key can be either symmetric or asymmetric depending on the chosen user access control mechanism, which is independent to our design here and will not be discussed in this paper.
- *Step 4:* Store DATA =< {data, h(data, kr)}kr , {kr}KUV > and destroy kr.

IV. ARCHITECTURES

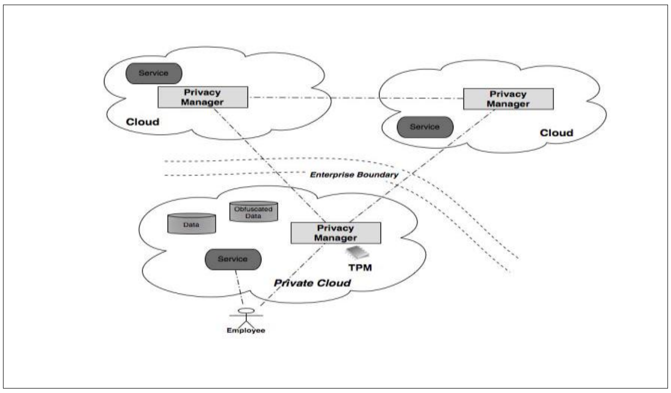
A. Privacy manager in a hybrid cloud

Privacy manager may be deployed in a local network, or a private cloud, to protect information relating to multiple parties. This would be suitable in environments, such as enterprise environments, where local protection of information is controlled in an adequate manner and its principal use would be to control personal information passing to a public cloud.

Fig: Enterprise-focused Privacy Manager

Advantages to this approach include that the benefits of the cloud can be reaped within the private cloud, including the most efficient provision of the Privacy Manager functionality. It can provide enterprise control over dissemination of sensitive information, and local compliance. The Privacy Manager would act on behalf of the user and decide the degree of data transfer allowed, based upon transferred user policies and the service context, and preferably also an assessment of the trustworthiness of the service provision environment.

Fig: Privacy Manager within the Cloud



B. Privacy manager in the cloud

Privacy Manager Software on the client helps users to protect their privacy when accessing cloud services. A central feature of the Privacy Manager is that it can provide obfuscation and de-obfuscation service, to reduce the amount of sensitive information held within the cloud. Privacy Manager allows the user to express privacy preferences about the treatment of their personal information, including the degree and type of obfuscation used. Personae – in the form of icons that correspond to sets of privacy preferences – can be used to simplify this process and make it more intuitive to the user.

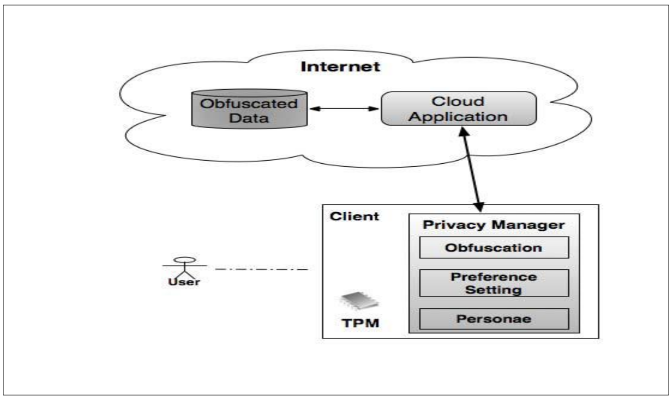


Fig: Client based privacy manager

V. CONCLUSION

In this discussion we found various solutions to enforce the security for data stored on cloud. In this paper we demonstrate how confidentiality and authentication security can be achieved by using Erasure Coding and TPM techniques. This paper dealt with different security models to protect the data which is stored in the cloud. According to the user requirements, they may choose the most appropriate model. However, in the case of Third Party Auditing (TPA), cloud data storage security is critical because of its poor service quality. This paper also dealt with different architectural representations for privacy management. We provide the extension of the proposed one to support TPA, so that the users can safely delegate the integrity checking tasks.

REFERENCES

[1] http://en.wikipedia.org/wiki/Cloud_computing#History

[2] http://mp3.about.com/od/glossary/g/Cloud-Storage-Definition-What-Is-Cloud-Storage.htm

[3] A berkeley view of cloud computing. http://www.eecs.berkeley.edu/Pubs/TechRpts/2009/EECS-2009-28.html.

[4] C.Wang, Qian Wang, Kui Ren, Wenjing Lou, “Ensuring Data Storage Security in Cloud Computing,” Proc. IWQoS „09, pp. 1–9, July 2009.

[5] K. Ren, C. Wang, and Q. Wang, “Security Challenges for the Public Cloud,” IEEE Internet Computing, vol. 16, no. 1, pp. 69-73, 2012.

[6] Q. Wang, C. Wang, J. Li, K. Ren, and W. Lou, “Enabling Public Verifiability and Data Dynamics for Storage Security in Cloud Computing,” Proc. 14th European Conf. Research in Computer Security (ESORICS’09), pp. 355-370, 2009.

[7] S. Pearson, Y. Shen, and M. Mowbray, “A Privacy Manager for Cloud Computing,” Proc. Int’l Conf. Cloud Computing (CloudCom), pp. 90-106, 2009.

[8] A. Squicciarini, S. Sundareswaran, and D. Lin, “Preventing Information Leakage from Indexing in the Cloud,” Proc. IEEE Int’l Conf. Cloud Computing, 2010.