ENSURING SECURE TRANSFER, ACCESS AND STORAGE OVER THE CLOUD STORAGE

Ramani S[1], Amol Bhatnagar[2], Anant Mehrotra[3]

[1]Assistant Professor, Computer Science & Engineering, VIT University, Tamil Nadu, India
[2]Student, Computer Science & Engineering, VIT University, Tamil Nadu, India
[3]Student, Computer Science & Engineering, VIT University, Tamil Nadu, India

Abstract

The main concern in today's growing IT sectors is the storage and maintenance of the data. As the data keep on updating according to the needs of users, there is a huge overhead in the maintenance of the hardware by the company. One of the solutions to this problem is the use of cloud storage for this enormous data. The cloud storage uses the huge data centers, which are remotely located, to store the data. In addition to the easy storage of the data, this huge data center also reduces the cost of maintenance of the data .However this distinct feature of cloud storage leads to many security issues which should be lucidly understood by the IT sectors.

One of the emerging security issue would be the integrity of the data stored in the data center i.e. to check whether the cloud provider misuses the data or not .The cloud provider can misuses the data in many ways like they can copy or modify the file .Due to the storage of data on the data center, user is not able to access the data physically thus there should be the way by which user can check the reliability of the data on the cloud. In this paper we provide the scheme to check the reliability of the data and this scheme can be agreed upon by both the user and the cloud provider.

Keywords: *Cloud Security, Masking, Cloud Storage Security, Data Center*

---***---

1. INTRODUCTION

Cloud computing has been one of the emerging technology in providing the solutions for various IT industry problem. Mostly, the cloud computing environment is used in providing the data centers for storing the data thus the main concern in cloud computing environment is the security of the data stored in data centers which are remotely located and used to store the data in the public storage.

Data center in the cloud environment is used by large number of people and different IT industries. These people used the data center to store their critical data (like a banker client will store the important information in the cloud) and none of the client knows where exactly the data is being stored. Most of the client's data is stored on the hybrid cloud which can be accessed by different clients so the security issue becomes very important in this type of environment.

There are different types of users depending on the level of security they want on their data thus the cloud storage should be able to provide different hierarchy of data security for different users depending on both types of data and the money they are paying [1].

There are different types of cloud storage depending on the level of security they provide. Public cloud is a union of set of computers and network resources based on cloud computing model. In public cloud Application, storage and other resources are provided to the every user over the internet by the cloud service provider like Amazon AWS, Microsoft and Google. As the cloud is accessed by all the general public thus the security issues is one of the biggest overhead in the public cloud.

Private cloud is a cloud infrastructure used solely for a single client and the other clients have no access to this infrastructure thus the security is not a big overhead here. Hybrid cloud is a combination of two or more clouds (private or public) having the benefits of both the environments. By having the hybrid cloud infrastructure, IT industries and different users can obtain the extended capacity or the capability of the cloud services [4].

1.1 Cloud Services

SaaS (Software as a Service): Software Application is used as an on demand service. Usually provided via the Internet Eliminates the need to install and run the application on the customer's own computer. Activities are managed from central locations rather than at each customer's site, enabling customers to access applications remotely via the Web. Examples: Google Apps, Salesforce.com

PaaS (Platform as a Service): Delivers a computing platform and/or solution stack as a service over the Internet, eliminating the need to install and run the application on the customer's own computers and simplifying maintenance and support

Facilitates deployment of applications without the cost and complexity of buying and managing the underlying hardware and software layers Examples: Google App Engine, Hadoop (Map Reduce), Microsoft Azure

IaaS (Infrastructure as a Service): Delivery of computer infrastructures such as Processors/CPUs, Memory, Storage, Networking typically via virtualization.

Rather than purchasing servers, software, data center space or network equipment, clients instead buy those resources as a fully outsourced service. IaaS clouds often offer additional resources such as a virtual-machine disk image library, raw (block) and file-based storage, firewalls, load balancers, IP addresses, virtual local area networks (VLANs), and software bundles. IaaS-cloud providers supply these resources on-demand from their large pools installed in data centers. Examples: Amazon EC2, Google Compute Engine, HP Cloud

2. BASIC CONCEPT OF CLOUD STORAGE

Nowadays, the cloud is basically used for storing the data. In cloud storage the data is stored on different data centers. While transferring data to the data center the client can only see the virtual server but in reality the cloud also uses the different data centers to store the client data.

The architecture of the storage in the cloud consists of one master data center which will store the information about the client’s data and different data centers used for storing the client data [2].

Basically the cloud storage consists of one data center and one client computer connected over the internet and sending the data to the data center.

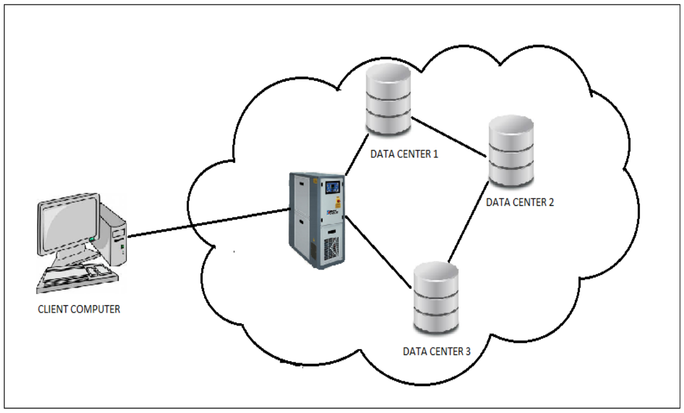

Fig -1: Cloud Storage Architecture

3. PROBLEM STATEMENT

In storing the delicate data over the data center provides the overhead of data security. To ensure the data security over the cloud storage we have to make sure that the data is secured in the three levels i.e. Client Authority, During Transfer and over the Data center.

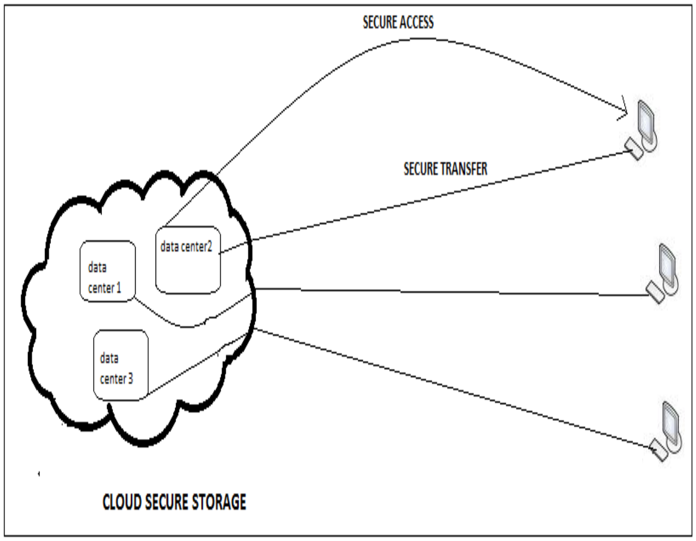

Fig -2: Secure Access, Transfer and Storage

3.1 Secure Storage Over Data Center

For the data to be secure over the data center, we have to make sure the following basic requirements of data security

- The data must be secured from the natural disaster.
- The data must be secured from the unauthorized access.

For securing the data from the natural disaster the cloud provider can divide the data into small parts and save these parts on different servers so that in case of damage to a particular server the data can be recovered. This approach will also increase the rate of access of data from different data centers because the number of clients accessing their data on a single data center will be divided among different data server [3].

The other approach can be the maintenance of the metadata or the duplicate copies of the data on the master server. In case all the files of any client get damaged than in that situation we can have this metadata which will at least provide the information about the data lost so that the client can track down his lost data.

The latter part of the security issue i.e. security from unauthorized access can be done in different ways. In order to protect the data at the data center, the cloud provider can use two approaches. In the first approach the user can randomly choose the two functions and use these functions on the data before storing it over the data center [5]. The value given by these functions should be recorded and whenever the user wants to check the integrity of the data he will going to apply the same two functions over the data stored in the data center and value obtained should be verified from the value recorded. This will ensure the secure data storage over the data center [6].

Secondly we can use the approach of masking some of the content of the file. In this case the user can mask the content of the file, thus even after getting the access to the file, the unauthorized user can't even decrypt the information from the file or he can mask the file name so that no one can predict the information in the file.

In addition to this we can also count the number of characters in the file and its size before storing it to the cloud server. In case of checking the integrity of the file, the user can count the numbers of characters in the file received from the cloud, its size and check it with the previous calculated number of characters and size. If both matches then the integrity of the file may be unhampered.

3.2 VERIFICATION

Cloud provider used to provide different resources like application and storage space to different IT industries and customers thus there is a strict need of protection of particular user data from other user's data. Whenever the user access the data in the cloud there must be some recording and tracing of the user action. It is mandatory for the security purpose that no one else other than the administrator can manage the data moreover the administrator should also have the restricted rights.

To ensure the privacy of user data there are many algorithm until the data is with user only but in cloud storage the privacy of data should not be alone maintained by the administrator. In order to protect the data at the data center, the cloud provider can use two approaches i.e. implementing the third interface that will ensure the authenticity of the user. In this approach the user cannot directly get the access of the files. He has to go through the two level of security, one is the primary authentication of the user and secondly after getting the access, the third interface should also validate that user. for example a banking client first has to login through their credentials after that for downloading or accessing the file client has to enter a secure one time password which will be send by the third interface to a secure area like email or mobile. This approach will secure most of the data and prevent unauthorized access.

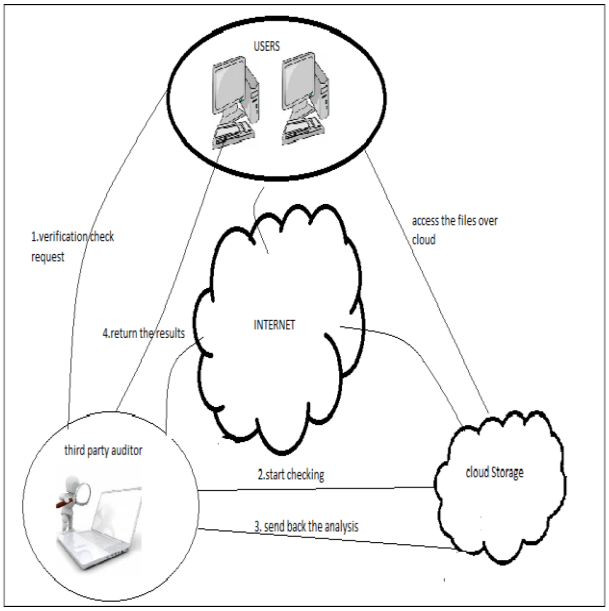

Fig -3: Third party checking the user integrity

In addition to this approach the cloud provider can use a private area designated for a particular client. This will restrict the user from accessing the file of other users as the user is having a private area on the cloud. Paper proposes to use the approach of dividing the file into small chunks of data and storing it as an individual file on different data server so that even the administrator can only view the particular part of that file on that server and will be unable to extract the data from the file.

3.3 Data Protection during Transfer

While storing data into the cloud storage the main overhead of security of the data occurs while transferring the data from the user hard disks to the designated data center. During this transfer the data is more prone to security threats.

To minimize the security threat one of the method is to setup different sub-data center between the path of user and the main data center. This will hinder the attack by the unauthorized people as the data will be going to take less time to get transfer. Moreover during the transfer we can use different cryptographic protocol like SSL and TLS that will provide security of the data over internet [7].

Another main issue is the timely delivery of the information to the user. This issue can be overcome by distributing the copies of the data to the different data center being setup near the user so as to maximize the bandwidth of access of data from the different networks. The particular user will be going to access the copy of the document that is being stored near to him. By following this approach the uses of the central data center is being reduced to minimal.

4. CONCLUSIONS

Paper proposes the models for checking the authentication of data during the transfer, storage at the data center and unauthorized access of the user. In further research we will try to improve our models in respect of the cloud storage environment.

ACKNOWLEDGEMENTS

We would like to express our sincere gratitude to my guide and the other author of this paper for their valuable help.

REFERENCES

[1]. BR Kandukuri, VR Paturi and Rakshit, A.Cloud Security Issues, Services Computing, 2009. SCC'09.IEEE International Conference on,P517-520,2009
[2]. http://en.wikipedia.org/wiki/Cloud_computing
[3]. Yan, L. and Rong, C. and Zhao, G.Strengthen cloud computing security with federal identity management using hierarchical identity-based cryptography, Cloud Computing, P167-177,2009
[4]. Lian, Q, W Chen, and Z Zhang, On the Impact of Replica Placement to the Reliability of Distributed Brick Storage Systems. Distributed Computing Systems, 2005. ICDCS 2005. Proceedings. 25th IEEE International Conference on, 2005: p. 187-196.
[5]. Wang, C., et al. Privacy-preserving public auditing for data storage security in cloud computing. in INFOCOM, 2010 Proceedings IEEE. 2010:IEEE.
[6]. Yang, K. and X. Jia, Data storage auditing service in cloud computing:challenges, methods and opportunities. WorldWideWeb, s2012.15(4):p.409-428
[7]. W. Stallings. Cryptography and Network Security: Principles and Practice. (3rd ed.). Prentice Hall, Upper SaddleRiver, NewJersey, 2003

BIOGRAPHIES

Ramani S, received his M.Tech degree from Bharathidasan Institute of Technology affiliated to Bharathidasan University, Tamil Nadu, India. He is pursuing Ph. D from VIT University Vellore, India. His area of interests includes Database, Web Technology, Data Mining. E-mail: ramani.s@vit.ac.in

Amol Bhatnagar, student of computer science engineering at Vellore Institute Of Technology, Vellore, Tamil Nadu.He is currently pursuing B.Tech in Computer science at VIT University. His current area of research includes Cloud Computing.
E-mail:amolmbd@gmail.com

Anant Mehrotra, is a student of computer science and engineering at Vellore Institute Of Technology, Vellore, Tamil Nadu.He is currently pursuing B.Tech in Computer science at VIT University. His current area of research includes data mining.
E-mail:anantm.1608@gmail.com