International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 03 Issue: 06 | June-2016 www.irjet.net p-ISSN: 2395-0072

Security in Data Storage in Cloud Computing

Janhavi Puranik, Prof.Anandhi Giri

Janhavi Puranik
M.C.A
Y.M.T College of Management
Kharghar, Navi Mumbai

Prof .Anandhi Giri
M.C.A
Y.M.T College of Management
Kharghar, Navi Mumbai

Abstract - *Cloud Computing is considered as the next-generation computing technology in IT industry. In cloud environment client and servers are responsible for data transfer among them. Speed of data transfer is the key issue in networking. Our research paper gives one way to securing the data and also protects data from unauthorized users in cloud servers, data is secured as per user choice so that high security is maintained .Cloud moves data to large data warehouse where frequent manipulation and maintenance of data may not be secured. In this paper, we focus on cloud data storage security, which is an important aspect of quality of service. To ensure correctness of data in cloud, we proposed one of the flexible distributed scheme. Cloud allows its users to remotely access and store data.*

Key Words: **Cloud computing, storage, Security,framework, data transffer.**

1.INTRODUCTION

Cloud computing refers to the shared pool of IT resources where each resource provides global access to its users. Cloud enable it users a large storage space to store and manipulate the data. The Amazon Simple Storage Service (s3) and Amazon Elastic Computer Cloud (EC2) are the most popular vendors of cloud.

Cloud reduces the storing of data at local storage space, instead it offers a global storage space by using data warehouses. Such a data centers allows its users to frequently manipulate the data by using the operations such as adding, deleting, updating, recording, moving the data. Hence security in the storage of cloud data is necessary and it is the important aspect of quality of service .As cloud offers global storage it comes up with various security threats. To ensure the cloud security and correctness of data to its users in private cloud is the main aim of our paper.

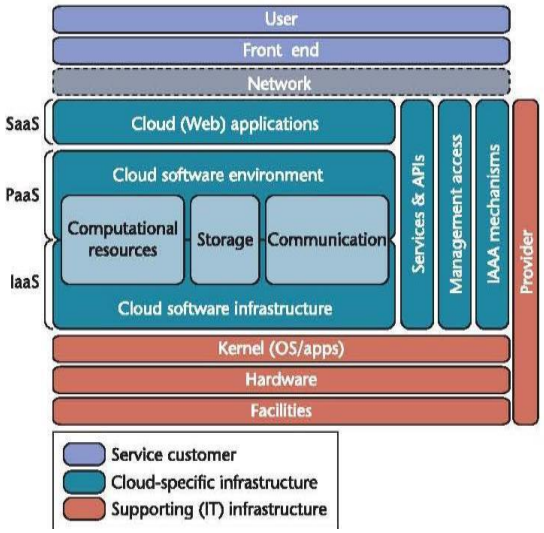

Figure 1: Architecture of Cloud Computing[8].

SYSTEM MODEL

In fig.1 and fig.2 The model for storage in cloud is illustrated

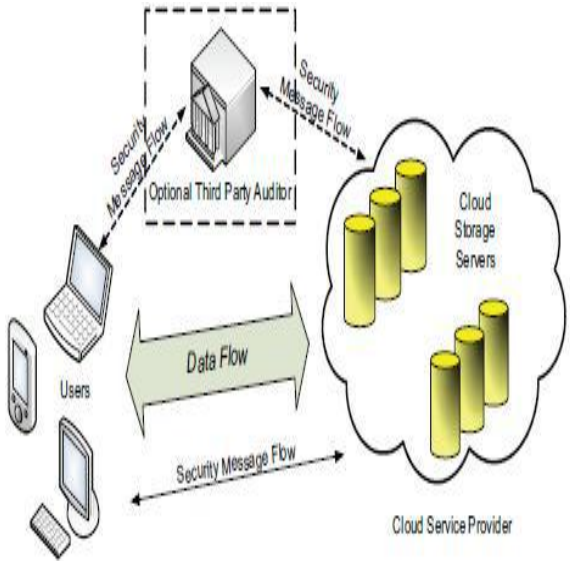

Figure 2:Cloud data storage architecture[4].

The entities in above model are given as follows[5]:

• User: users, who have data to be stored in the cloud and rely on the cloud for data computation, consist of both individual consumers and organizations.
• Cloud Service Provider (CSP): a CSP, who has significant resources and expertise in building and managing distributed cloud storage servers, owns and operates live Cloud Computing systems.
• Third Party Auditor (TPA): an optional TPA, who has expertise and capabilities that users may not have, is trusted to assess and expose risk of cloud storage services on behalf of the users upon request.
In cloud data storage, a user stores his data through a CSP into a set of cloud servers, which are running in a simultaneous, cooperated and distributed manner. Data redundancy can be employed with technique of erasure-correcting code to further tolerate faults or server crash as user's data grows in size and importance. Thereafter, for application purposes, the user interacts with the cloud servers via CSP to access or retrieve his data. In some cases, the user may need to perform block level operations on his data. The most general forms of these operations we are considering are block update, delete, insert and append. In our model, we assume that the point-to-point communication channels between each cloud server and the user is authenticated and reliable, which can be achieved in practice with little overhead. Note that we don't address the issue of data privacy in this paper, as in Cloud Computing, data privacy and storage is orthogonal to the problem we study here.

ADVERSARY MODEL

Security threats faced by cloud data storage can come from two different sources[5]. On the one hand, a CSP can be self-interested, un-trusted and possibly malicious. Not only does it desire to move data that has not been or is rarely accessed to a lower tier of storage than agreed for monetary reasons, but it may also attempt to hide a data loss incident due to management errors, convoluted failures and so on. On the other hand, there may also exist an economically motivated adversary, who has the capability to compromise a number of cloud data storage servers in different time intervals and subsequently is able to modify or delete users' data while remaining undetected by CSPs for a certain period. Specifically, we consider two types of adversary with different levels of capability in this paper:
Weak Adversary: The adversary is interested in corrupting the user's data files stored on individual servers. Once a server is comprised, an adversary can pollute the original data files by modifying or introducing its own fraudulent data to prevent the original data from being retrieved by the user.
Strong Adversary: This is the worst case scenario, in which we assume that the adversary can compromise all the storage servers so that he can intentionally modify the data files as long as they are internally consistent. In fact, this is equivalent to the case where all servers are colluding together to hide a data loss or corruption incident.

DESIGN GOALS

The major goal of paper is to ensure the cloud data by protecting it for that we designed one framework.Also another goal is to provide a secure way to transffer the data in cloud.Some more design goals are as follows:
(1)Prevention of unauthorised access: It allows only authorised users to manipulate cloud data
(2) Data security:By using framework it ensures data transffer security.

SECURITY ARCHITECTURES

The above contents are from many security related research literature . The contents describes issues and solutions of security in cloud.The literture described previously gives many security architectures and frameworks. Some of the architectures given by researchers are described below:
According to Wikipedia, there are a number of security concerns associated with cloud computing. These issues fall into two broad categories: security issues faced by cloud providers (organizations providing software-, platform-, or infrastructure-as-a-service via the cloud) and security issues faced by their customers (companies or organizations who host applications or store data on the cloud).The responsibility is shared, however. The CSP enables the security of data in cloud by providing strong password protection and protects the data from unauthorized access.
When an organization elects to store data or host applications on the public cloud, it loses its ability to have

physical access to the servers hosting its information. Hence insider attacks harms the cloud data. According to a recent Cloud Security Alliance Report, insider attacks are the third biggest threat in cloud computing. Therefore, CSP's must monitor the data centers which having physical access by employees . Additionally, data centers must be frequently monitored for suspicious activity.

According to Symantec research, they found many issues with how the security of IaaS environments was managed. One of the main issues that we observed was incorrectly configured access permissions that allowed anyone to access sensitive information stored in the cloud. They were able to identify over 16,000 cloud domains by enumerating domain prefixes with words from a dictionary. Of the discovered domains, 0.3 percent had guessable folder structures that could be read by everyone, leading to over 11,000 publicly accessible files. Some of these files contained highly sensitive information such as user names, passwords, credit card transaction logs, and email addresses. Another problem that we observed in cloud environments were leaked credentials, which could be used to access and modify stored data. These credentials were often hardcoded in applications and were unprotected, potentially allowing attackers to extract them. Furthermore, administrators often did not properly enable logging in their cloud services, making it difficult for them to investigate incidents.

SECURITY FRAMEWORK FOR SERVER-CLIENT NETWORK

To ensure the security in cloud storage we have proposed a framework. The Fig 3 is the two tier model for data transfer by key exchange.

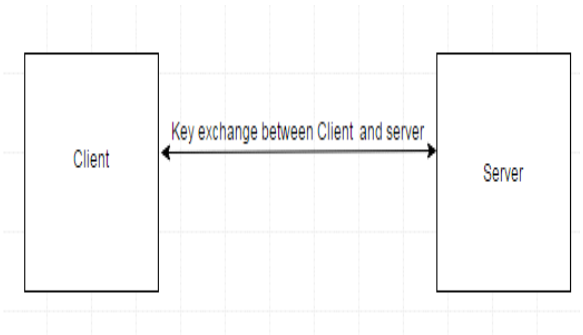

Fig:3 Design of client server Security framework

The client and server will start data transfer after exchanging keys between them by using traditional key exchange mechanisms such as deffie-helman key exchange, public key cryptography etc. The Keys are stored at both sides. Whenever client sends request to server the authentication is done at both ends and session is started. The semaphore is then set at server side for each client with each having unique id shared with that client only. A semaphore is a variable or abstract data type that is used for controlling access, by multiple processes, to a common resource in a concurrent system such as a multiprogramming operating system[10]. The semaphore have a critical section with lock facility to acquire and release the lock which allows only one process to access the shared resource(usually shared memory) at a time. A critical section is a part of a multi-process program that may not be concurrently executed by more than one of the program's processes[11].The typical working of semaphore[13] is given in Fig.4

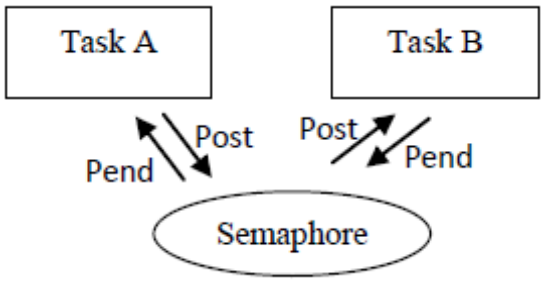

Fig.4 Working of semaphore[7].

This will prevent the other processes to access and store data in the cloud storage space such as shared memory. This will restrict the other processes of that client to enter into the critical section. It will also restrict the data transfer from other users processes. The shared unique id allows only that client's process to enter into the critical section while other users are restricted . After one process releases the lock and moves out of critical section, other process allowed with clients unique id to enter into the critical section and acquire lock. This will ensure secured storage of data over the cloud network.

CONCLUSION

In this paper, we investigated the problem of data security in cloud data storage and data transfer, which is essentially a distributed storage system. To ensure the secure storage of users' data in cloud data storage, we proposed a security framework. Our framework achieves the secure storage of data. After authentication and key exchange, security framework generates the unique id and sets semaphore at server side which ensures only one process to access and store the data in cloud. Hence other users are restricted to do so in that critical section. Thus, ensuring cloud users a cloud storage security.And hence the proposed framework will work as design model to ensure secure data transfer in cloud computing.

REFERENCES

[1] Cong Wang, Qian WangKui Ren, Ning Cao, and Wenjing Lou "Toward Secure and Dependable Storage Services in Cloud Computing" IEEE transactions on services computing, vol. 5, no. 2, april-june 2012

[2] Qian Wang,Cong Wang, Kui Ren, Wenjing Lou Jin Li "Enabling Public Auditability and Data Dynamics for

Storage Security in Cloud Computing" IEEE transactions on parallel and distributed systems, vol. 22, no. 5, may 2011

[3] Patrick McDaniel, Sean W. Smith, "Outlook: Cloudy with a chance of security challenges and improvements," IEEE Computer and reliability societies (2010), pp. 77-80.

[4] Pradnyesh Bhisikar, "Security in Data Storage and Transmission in Cloud Computing", International Journal of Advanced Research in Computer Science and Software Engineering Volume 3, Issue 3, March 2013 ISSN: 2277 128X.

[5]Farzad Sabahi,"Virtualization for Cloud Environment Using Hypervisor-based Technology", International Journal of Machine Learning and Computing, Vol. 2, No. 1, February 2012.

[6] Abhishek Pandey , R.M.Tugnayat , A.K.Tiwari," Data Security Framework For Cloud Computing Networks", International Journal Of Computer Engineering & Technology (Ijcet) Volume 4, Issue 1, January- February (2013), pp. 178-181.

[7]J.Ramprabu,G.Sindhuja,"Performance Analysis of Open-Source Real Time Operating Systems", International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 4 Issue 2, February 2015.

[8] Santosh Kumar and R. H. Goudar,"Cloud Computing – Research Issues, Challenges,
Architecture, Platforms and Applications: A Survey", International Journal of Future Computer and Communication, Vol. 1, No. 4, December 2012.