

An Analysis on Cloud Data Storage

M. Sudha and C. Balakrishnan

*Dept. of PG Studies in Engineering, S. A. Engineering College,
Anna University, Chennai, Tamil Nadu, India.
sudha.muthuraman@gmail.com*

Abstract - Cloud data storage refers to storing data to an off-site storage system maintained by a third party. Instead of storing information to your computer's hard drive or other local storage device, you save it to a remote database. The internet provides the connection between your computer and the database. Cloud storage reduces hardware and software demands on the user's side. Accessing and storing data on cloud storage has some security risks and thus makes the cloud information inconsistent and unreliable. This paper compares the traditional data storage and cloud data storage and provides few ways to protect the data stored in the cloud. To make data in the cloud a reliable one, some auditing mechanism should be used. This auditing can be performed by a third party system which lies between cloud users and cloud data storage. Third party auditor stores the log information of all files which are accessed from cloud storage and thus assures cloud storage correctness.

Keywords - Cloud data storage, local storage, third party auditor, traditional storage.

I. INTRODUCTION

Cloud computing is such a type of computing environment, where business owners outsource their computing needs including application software services to a third party and when they need to use the computing power or employees need to use the application resources like database, emails etc., they access the resources via Internet. The operating cost of cloud computing is much cheaper than having a company's own personal IT infrastructure and managed team. [1] Security and privacy is the only concern in cloud environments, because all your files, emails, database are hosted in a third party servers in their premise. Considering the installation of network infrastructure a cloud environment can be broadly categorized into three types- public cloud, private cloud and hybrid cloud. Though from operation and maintenance point-of-view cloud computing is a great cost-effective IT solution for business of any magnitude, but it has at least two major concerns-technical developments, security and privacy. Since cloud computing is relatively a new technology in comparison to other existing computing solutions, it still has lots of scope of becoming a mature system as a reliable and cost-effective computing technology.

Since due to outsourcing all the important data resides in a third party premise, there is always a concern about the trust-worthiness of the cloud service providers. Any security and privacy violation can be fatal- keeping this in mind many business owners are still to be convinced about the security and privacy issues of cloud computing.

Despite some serious privacy related drawbacks, cloud computing is a lucrative choice to improve productivity in any business environment, where IT is in high demand. To raise the security and privacy of cloud service providers, there need to be more co-operations between world governments so as we can develop a unified global rules and guidance for running a safe cloud computing service. Since users may not retain a local copy of outsourced data, there exist various incentives for cloud service providers (CSP) to behave unfaithfully towards the cloud users regarding the status of their outsourced data. [1, 2]

In order to achieve the assurances of cloud data integrity and availability and enforce the quality of cloud storage service, efficient methods that enable on-demand data correctness verification on behalf of cloud users should be designed. These techniques can be useful to ensure the storage correctness without having users possessing local data. In this paper, traditional and cloud data storage services are compared and the security issues faced by the cloud data storage are listed and how to overcome those issues.

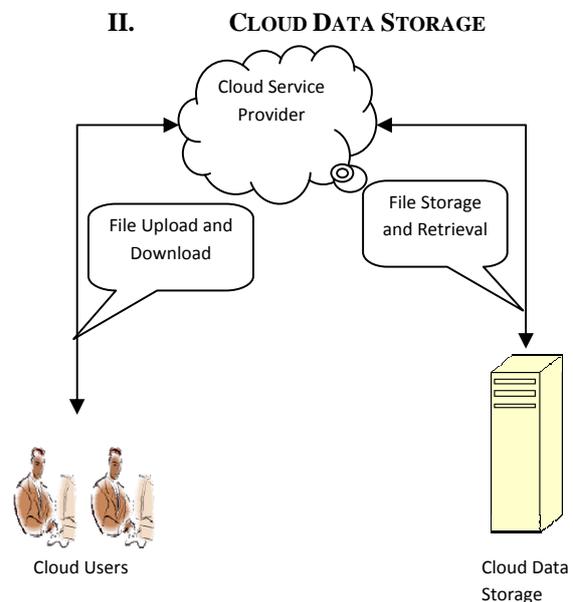


Fig. 1 General Cloud Data Storage Architecture

Data can be stored either in the form of files or blocks. Files like audio, video, text and any types are stored in the cloud. Accessing the cloud is based on internet or intranet.

Cloud supports easy scalability i.e., the network can be scaled by just increasing the nodes. Service providers are built only for the particular group of systems that access the cloud storage. Cloud storage has several advantages over traditional data storage. For example, if you store your data on a cloud storage system, you'll be able to get to that data from any location that has Internet access. You wouldn't need to carry around a physical storage device or use the same computer to save and retrieve your information. So cloud storage is convenient and offers more flexibility. Figure 1 shows the general cloud storage architecture without proper security.

A. Advantages of Cloud Storage

There are several advantages of the cloud storage model over individual storage and networked online storage. Unlike data stored in a cloud, information stored on an end user device cannot easily be accessed by others and individual storage is far more vulnerable to loss, damage or theft. Networked storage devices address those problems, but they still require both human and physical resources that an individual or a corporation may not possess. [8, 9] Cloud storage solutions are more scalable and efficient way to store data. Rather than estimating the amount of data storage needed and purchasing the hardware required, a cloud storage customer will only pay for what is needed. [4] Cloud storage is a scalable solution that can grow spontaneously to meet increased demand. There is also an inherent economy of scale when many individuals and organizations elect to store their data on the same systems managed by a single provider.

III. TRADITIONAL DATA STORAGE VS CLOUD DATA STORAGE

Traditionally, large businesses have backed up their data to either disk or tape for storage in off-site data centers. Although these disk and tape solutions require a relatively high initial capital expenditure and expansion expense. Aside from costs, these solutions result in lengthy data recovery times. Whereas cloud storage requires one-time initial investment and no expansion cost. It also provides a quicker data recovery times.

Disk-to-tape methodologies are still widely used today and have been providing businesses with full-system restores and disaster recovery for many years. At one point, higher-capacity tapes have become more expensive. Despite the increase in capacity, tapes are often unable to store the volume of data that businesses need to back up, [3, 10] resulting in the management of multiple tapes using relatively cumbersome and manual processes. Just like video tapes that must be watched sequentially, backup tapes can only access data in the order it was written. To access data directly and rapidly, the data has to be staged onto a hard disk. Finally, backup tapes are notoriously fragile and must be handled with care. But in the case of cloud data storage, data can be easily accessed directly and rapidly. It

is possible to watch video files sequentially which is stored on the cloud.

Security is a major issue in cloud data storage. Since data is stored in the third party system, it is easy for the attackers to hack and modify the data when compared to any other traditional data storage services. [5] So various security measures should be taken to protect the data stored in the cloud and make the data consistent and reliable. Security can be provided by using various encryption methods, tokens and so on. Graph in the figure 2 given below specifies that cloud data storage is always better than traditional data storage.

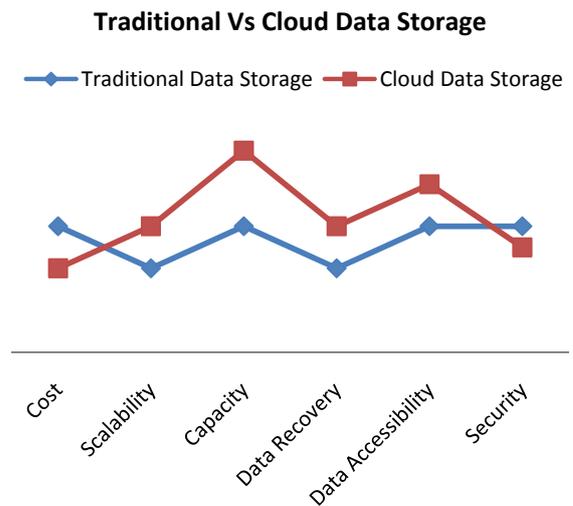


Fig. 2 Traditional Vs Cloud data storage

IV. SECURITY ISSUES

Major security issues faced by cloud data storage services are as follows. [7]

- A. *Authorized user access*
Information transmitted from the client through the Internet poses a certain degree of risk, because of issues of data ownership. Only authorized users can access the data.
- B. *Security fulfillment*
Clients are accountable for the security of their solution, as they can choose between providers that allow to be audited by third party organizations that check levels of security.
- C. *Data location*
Data can be located in any part of the world depending on the cloud service providers. Data stored in any location should support cloud storage correctness.
- D. *Data segregation*
Information from multiple companies may be stored on the same hard disk, so a mechanism to separate data should be used by the provider.

E. *Data recovery*

Each and every provider should have a disaster recovery protocol to protect user data. If the data is corrupted while retrieving, then disaster recovery protocol should act according to that.

F. *Challenge-Response proof*

If a client suspects faulty activity from the provider, it may not have many legal ways to prove the challenge made by client.

V. SECURITY MEASURES

Security measures for making the data stored in the cloud secured are as follows. [6] Figure 3 shows the cloud architecture with the specified security measures.

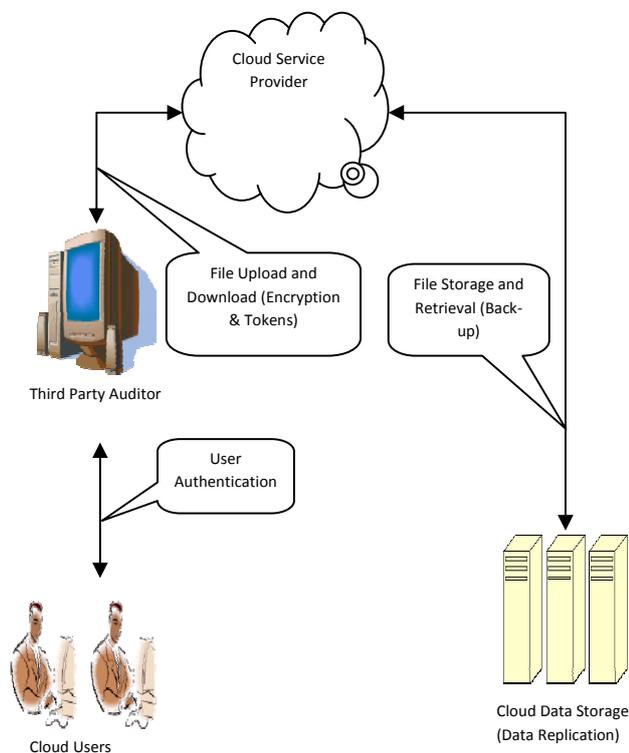


Fig. 3 Cloud Data Storage Architecture with Security measures

A. *Authentication*

Only authorized users can access the data stored in the cloud storage. Authorization is provided using username and strong password.

B. *Encryption*

Files stored in the cloud should be encrypted first and then stored. So, only the users who know the decryption key can access the file. This makes the data highly secured.

C. *Data replication*

Multiple copies of data backed up at different locations. This can be achieved by having two or more

mirrored data centers, or by keeping a local copy of the latest version of backed up data on site with the business.[1]

D. *Tokens*

Tokens are generated by Third Party Auditor for the data which is to be stored in the cloud. On retrieving the data from cloud again tokens are generated. If both the tokens are same, we can ensure that data stored in the cloud is not corrupted. [2]

E. *Back-up*

As far as the actual file uploads, there are essentially two approaches. The first is to back up entire files each and every time. Second is that if the file is modified, then the whole thing is backed-up afresh or only back up the new data. [5]

VI. CONCLUSION

Cloud storage provides a new architecture to address the storage, management and analysis of fast-growing machine-generated data. By providing advanced scalability, manageability and the potential to collapse compute and storage together on the same processing nodes, cloud storage will guide in new levels of efficiency and economics into enterprise data centers. This on-demand storage system will provide IT administrators with the capability to monitor and proactively manage their cloud environment, all with minimal effort and at a low cost.

ACKNOWLEDGMENT

I must thank, first and foremost, my Guide Mr.C.BALAKRISHNAN M.E., (Ph.D.) Assistant Professor, Department of PG studies in Engineering, without whose guidance and patience, this dissertation would not be possible. I wish to record my thanks to Mrs.UMARANI SRIKANTH M.E., (Ph.D) Head of the Department, Department of PG Studies in Engineering and staffs of the Department of PG studies in Engineering for their consistent encouragement and ideas.

REFERENCES

- [1] C. Wang, Q. Wang, K. Ren, N. Cao and W. Lou, "Towards Secure and Dependable Storage Services in Cloud Computing", May 2011, pp.1-14.
- [2] Balakrishnan.S, Saranya.G, Shobana.S, Karthikeyan.S "Introducing Effective Third Party Auditing for Data Storage Security in Cloud" in Proc. of IJCST Vol. 2, Issue 2, June 2011.
- [3] <http://bizcloudnetwork.com/pros-and-cons-of-using-cloud-storage-services>
- [4] <http://searchsystemschannel.techtarget.com/feature/The-benefits-of-cloud-storage-services>
- [5] <http://www.techairlines.com/2011/01/31/backups-local-vs-cloud-storage>
- [6] Craig Balding, "ITG2008 World Cloud Computing Summit", 2008 <http://cloudsecurity.org/>
- [7] Traian Andrei, "Cloud computing challenges and related security issues".
- [8] Jeff Boles, "The benefits of cloud-based storage", November 10, 2008
- [9] Jason, "Pros and Cons of Using Cloud Storage Services", April 18, 2011
- [10] Scott Lowe, "Block level storage vs. file level storage: A comparison", February 18, 2011.