Efficiency on Public Cloud Storage Providers in Cloud Computing

E. Srimathi, SP. Chokkalingam

ABSTRACT: ***Storage plays an important role in cloud computing, the information are stored in data centre on cloud to access the data from anywhere throw internet. Three different types of clouds are available for storing the data such as Private Cloud, Public Cloud and Hybrid Cloud. This paper is to know the flexibility and efficiency of Cloud Computing in Public Cloud. Now a day's various cloud storage applications are available in Public Cloud, in low cost with lots of flexibility to the user. Among this three different clouds, Public Cloud is available for all types of web user but its security risk factor is high because data can be hack by intruders on brute force attack. Cloud storage makes the person to do their work easily from anywhere with the help of internet connection, it reduce the secondary device to store the data.***

Keyword: Cloud Storage, Distributed Computing and Data Centre.

1. INTRODUCTION

Cloud computing makes the web user to access the information all over the world through internet. Cloud storage reduces the secondary device, user no need to carry their information in external devices, whatever the details they kept in cloud can be accessible from anywhere. User can store all types of information such as text, picture, audio, video and application can also be deployed in cloud storage. In cloud three major services are provided to the user such as [1]Software as a Service (SaaS), [2]Platform as a Service (PaaS) and [3]Infrastructure as a Service (IaaS).

[1]SaaS is used to build the software according to user requirements. [2]PaaS provides an individual framework for the user to run or install their software in system according to their use. [3]IaaS provides an infrastructure for the user to store, to retrieve, to search the data in cloud. Cloud computing offers three different types of clouds such as private cloud, public cloud and hybrid cloud.

All this three clouds can be used to store the data in cloud, private cloud is secure to store the data because the details stored in that cloud can be access by individual user who paid to use that cloud so, security risk is very low in private cloud.

Figure 1: Services of Cloud Computing

In public cloud all types of user can access in free of cost for certain limitations but security risk is high in this cloud because n numbers of hackers are involved to hack the data. Hybrid cloud can be used as both private and public cloud so security risk is low while comparing with public cloud.

2. DATA STORAGE IN PUBLIC CLOUD

Public cloud provides the services with the use of internet to make resources such as application and storage, available to the general public user on the public cloud. It contains computing service and storage service, computing serves the user to do all types of their work through internet connection. Storage is used to store public user data in cloud to access their information from any type devices through internet such as laptop, tablet and mobile.

Cloud Storage provides the flexibility to the user to access the data from anywhere threw internet, encryption is a technique to secrete the data from hackers. The original data which is said to be normal human readable text/data are converted to human unreadable text/data because if the hackers hack the information from cloud they cannot able to read the text which is stored in the cloud. The data which is stored can text, image, audio, video or any other type of format according the user. Main risk arise in public cloud is "Brute Force Attack".

Public cloud data can be hacked by tracing the user name and password of the account or by guessing the password (brute force attack) of the account to hack the data from the cloud; this type of hackers are involved at the end point of the application but some hackers are involved at the point of communication channel itself, so on that time our cloud storage providers should be secure to protect the data from various hackers, this paper helps you to choose the good cloud storage providers to store the data in cloud.

The figure2 shows the best three cloud storage providers in public cloud such as Dropbox, Google Drive and

Revised Manuscript Received on April 05, 2019.

E. Srimathi, Research Scholar, Saveetha School of Engineering, Saveetha Institute of Medical and Technical Sciences.

SP.Chokkalingam, Professor, Department of CSE, Saveetha School of Engineering, Saveetha Institute of Medical and Technical Sciences.

OneDrive. Now in trend; different public cloud storage providers are available, but this three are most commonly used public cloud storage among organisation, business and for a single users too. Data which are stored in this clouds are very reliable and easy to access the file from anywhere with all type of devices such as computers, labtops, tablets and mobiles.

Figure 2: Public Cloud Storage Providers

2.1 Dropbox

Dropbox is one of the most common public cloud storage used by the web user to store their information such as audio, video, text, picture and any format of data. Dropbox is extremely convenient to user, information stored in cloud can be access easily and the stored files can be shared easily. Dropbox provides 2GB of free space; this free space can be increase to 16 GB by referring dropbox to the other user. Speed limit of file uploading and downloading depends upon the broadband user choice.

Verification process in dropbox:

Step l: Password protection (Two step authentication process)

Step 2: Additionally it use the extra text send to the personal phone number of the user at the time of Dropbox account creation.

Step 3: Encryption done at the time of uploading the file in cloud (256 bit AES key encryption)

Encryption technique is used in dropbox to store the data in public cloud, encryption mean transferring the original text into human unreadable text to secure the data over cloud; data can be decrypt when user require to read the file from the cloud. Dropbox use 256 bit Advanced Encryption Standard (AES) to secure the data from hackers in the cloud. It uses Secure Socket layer with transport layer to transfer the information in secure manner in cloud, it creates the secure tunnel protector by 128 bit AES.

2.2 Google Drive

Google Drive is also one of the most common public cloud storage used by the web user to store their information in cloud. In Google drive it is easy to make manipulation in the cloud file and it can be access from various devices. It offers 15GB of space for the Google drive users to store the data in cloud, it supports in all types of devices. The files which are stored in drive can be shared easily among the web user.

Verification process in Google Drive:

Step l: Password protection (Two step authentication process)

Step 2: Additionally it create one Google folder in Boxcryptor (creates a virtual drive on system) for encryption.

Step 3: End-to-End encryption with zero knowledge standard.

Google drive supports multiple uploads simultaneously. Uploading the file or downloading the file is done as quickly as possible. Boxcryptor is used for encryption in the Google drive cloud. It supports End - to - End encryption with zero knowledge standard (no one can hack the data). Boxcryptor create one Google folder to encrypt the file which are uploaded by the user, it creates the virtual drive on device.

2.3 OneDrive

OneDrive has a close collaboration with office on social network; it is also one of the public cloud storage used among the web user. OneDrive provides 15GB of free space to store the data in cloud; it is very easy to organize the file in cloud. It supports 256 bit encryption technique while uploading the file but after that no encryptions are provided on storage.

Verification process in OneDrive:

Step l: Password protection (Two step authentication process)

Step 2: Sharing choices (Default permission to share files with different user)

Step 3: Encryption done at the time of syncing the file in cloud (256 bit encryption)

The speed limit of uploading and downloading file in cloud can be done in “kilobytes-per-second” but at the same time we can change the speed manually also.

3. RESULTS

Storage Providers	Free usage	1TB cost	Encryption	Speed Limit
Dropbox	2GB but user can use 16 GB by referring.	736.25	AES,256-bit encrytion	Depends upon the broadband user choice

Google Drive	15 GB	736.25 but we can use till 2TB	Boxcryptor (Chunk key & Wrapping key)	Upload the file as quick as possible
OneDrive	Scaled down from 5GB to 15GB	589	256-bit encryption	Kilobytes per second but speed can change manually

Comparison table between public cloud storage providers

CONCLUSION

Cloud storage plays an important role in cloud computing because we can access the data from cloud at anytime from anywhere on the internet. Public cloud offers the user to store their data in free of cost at certain limitations, all the three cloud storage providers are user friendly to store the data in cloud but it has some cons also such as Dropbox details can be access by the administrators or developers who maintain it; Google Drive speed become low at the time of millions user access; in OneDrive no encryption after uploading the files. Among these three providers Google drive is good to store the data on public cloud on secure manner.

REFERENCE

1. H. Takabi, J. B. Joshi, and G.-J. Ahn, “Security and privacy challenges in cloud computing environments,” IEEE Security & Privacy, no. 6, pp. 24–31, 2010
2. K. Ren, C. Wang, and Q. Wang, “Security challenges for the public cloud,” IEEE Internet Computing, no. 1, pp. 69–73, 2012
3. Wen, X., et al, Comparison of open-source cloud management platforms: "OpenStack and OpenNebula. Fuzzy Systems and Knowledge Discovery (FSKD)," 2012 9th International Conference on. IEEE
4. E.Srimathi and Dr. SP.Chokkalingam, ”OpenKey-Generation for Enabling Cloud Storage Security in Open Source Cloud Computing”,JARDCS,Vol.9.Sp-17/2017.
5. Yang Luo, Wu Luo, Tian Puyang, Qingni Shen, Anbang Ruan†, Zhonghai Wu, "OpenStack Security Modules: a Least-Invasive Access Control Framework for the Cloud,"2016 IEEE 9th International Conference on Cloud Computing
6. Kui Ren, Cong Wang, and Qian Wang • Illinois Institute of Technology, "Security Challenges for the Public Cloud"
7. Suryadipta Majumdar, Taous Madi, Yushun Wang, Yosr Jarraya, Makan Pourzandi, Lingyu Wang and Mourad Debbabi, "Security Compliance Auditing of Identity and Access
8. Secured Data Communication in Cloud Computing using Channel API with MD5 Hashing, ISSN: 2320-1363, journal of International Journal of Merging Technology and Advanced Research in Computing
9. Management in the Cloud: Application to OpenStack," 2015 IEEE 7th International Conference on Cloud Computing Technology and Science