INTERNATIONAL JOURNAL OF PURE AND APPLIED RESEARCH IN ENGINEERING AND TECHNOLOGY

A PATH FOR HORIZING YOUR INNOVATIVE WORK

IMPROVE AVAILABILITY AND CONFIDENTIALITY FOR DATA STORAGE ON MULTI-CLOUD

TEJASWI. R. KARIYA[1], DR. V. M. THAKRE[2], DR. VARSHA. S. TONDRE[3]

1. Department of computer Science, SMT. N. Wadhawani College, SGB Amravati University, Yavatmal. MS. India.
2. Department of computer Science, SGB Amravati University, Amravati. MS. India.
3. Department of computer Science, Brijlal Biyani Science College, SGB Amravati University, Amravati , MS. India.

Accepted Date: 05/03/2015; Published Date: 01/05/2015

Abstract: Cloud computing has become part of IT enterprise because of its different internet services. The most useful service of cloud is cloud storage. In recent year, multi cloud computing has become popular due to its ability to handle security risks in cloud environment that effect on cloud users. However, security issues like service unavailability, data intrusion are still remaining concerns in cloud storage. To address these issues, this paper have discussed about two architectural approaches which are both utilizes secrete sharing technique but different ways to improve availability and confidentiality of data in multi cloud.

Keywords: Multi cloud, Availability, Confidentiality, CloudStash, A file distribution approach, Secrete sharing scheme, SLA.

Corresponding Author: MS. TEJASWI. R. KARIYA

PAPER-QR CODE

Access Online On:

www.ijpret.com

How to Cite This Article:

Tejaswi R. Kariya, IJPRET, 2015; Volume 3 (9): 347-356

INTRODUCTION

As the cloud services have been built over the internet, any issue that is related to internet security will affect cloud services. Cloud resources are accessed through the internet, still user data also transmitted through the internet which may be insecure. As result, internet security problem affect the cloud. Cloud user's worried about the security of critical data that has been stored in cloud.

In cloud computing, cloud services suffered a problem in terms of confidentiality if there is un-trusted cloud service provider. In previous research, to keep user data confidential against un-trusted cloud provider, encryption technique is used. But this technique leads key management issues like key generation, key distribution, and key regeneration among multi-users. To overcome these problem, multi cloud environment is used with secrete sharing approach. With this technique, data store separately on each cloud provider which is difficult for hacker to get stored data.

Multi cloud computing is also called cloud-of-clouds or inter cloud proposed by Vukolic [2]. In multi cloud user data store in distributed manners means store data in multiple cloud providers rather than on single cloud provider.

In addition, there are also issues of availability in cloud service. It is possible that the service might be unavailable from time to time. If any damage occurs in web then service may fails. Sometimes user's services may terminate for any reason at any time. To protect from these failures companies take backups or use multiple providers.

This paper will discuss a file distribution approach [5] and CloudStash approach [6] to achieve high availability and confidentiality for data storage on multi cloud. Both approaches provides confidentiality by applying secrete sharing scheme.

In a file distribution approach, multiple clouds for storage are dynamically evaluated in agreement with each file and cloud SLA (Service Level Agreement). Therefore, characteristics of each cloud are referred from the cloud's SLA and user requests for services are determined on the basis of confidentiality and availability. Each cloud with its own SLA, it is converted to items, which one-to-one maps with the requests and parameters in secrete sharing scheme. It is possible to determine best cloud services to each file by converted items and the requests [5].

Second approach is CloudStash which distributing multi-shares over the multiple clouds, not depending on a single cloud's availability. CloudStash provides performance by using multi-

threading to manage multi-shares into multi-clouds in parallel. CloudStash provides integrity and fault tolerance by hashing and signing each share and then distributing these signed multi-shares into multi-clouds. When the downloaded share is corrupted, CloudStash can regenerate a new share from different cloud [6].

II. ANALYSIS OF SECURITY AREAS

A. Data Confidentiality

It should be maintained while data is transmitted over the cloud. For these various techniques like checksum, encryption, hash functions are used. Also Byzantine fault tolerant replication protocol within the cloud is intended to be implemented to maintain confidentiality [7]. Cloud service provider's password hacking and data intrusion indicates security risk. If attacker gains access to account password, then they will be able to access all instances and resources. In addition, stolen password allows hacker to delete all information inside the instances, alter it, or even disable its services [8].

To provide confidentiality, multi cloud schemes such as Depsky [1] and Intercloud [2] uses symmetric encryption technique and distributes encrypted data over multiple clouds. In this distribution, each cloud stored part of encrypted data provides a high level of confidentiality. "DEPSKY" is a virtual cloud system, presented by Bessani et al. DEPSKY is a system that improves the availability, integrity and confidentiality of data stored in clouds forming a cloud-of-clouds. DepSky used DepSky-CA protocol to encrypt the data with random secret key. They encoded the encrypted data and shared key, then distributed them into four clouds where each cloud stored block of data along with key share. Intercloud also performed symmetric encryption on the data, and split the key into shares using the secret-sharing scheme, then they combined key shares to piece of data in order to distribute them to clouds.

B. Service Availability

Another major concern in cloud services is service availability. Data is continuously available in any situation either normal or disastrous. Availability is also a security issue in cloud because the data should be available to the user all the time and there should be no loss in data. Cloud providers such as Amazon, Microsoft and Google mention in their licensing agreement that the unavailability of their services may occur [8]. Thus, the user's service may crash without any prior notice at any time.

Multi-cloud schemes such as DepSky, HAIL [3], and RACS [4] provided high level of availability by dividing data over multiple clouds. HAIL (High-Availability and Integrity Layer) is a

distributed cryptographic system that offers a software layer to address availability and integrity of the stored data in multi cloud. DepSky used four commercial clouds and distributed data over four clouds where each cloud stored half of the data. RACS (Redundant Array of Cloud Storage) uses RAID like techniques that are utilized by disk and file system. Therefore, storage load will be divided into several cloud providers, which also avoids vendor lock-in. RAID techniques implements high-availability and storage-efficiency data replication on various clouds.

III. METHODOLOGY

A. A File Distribution Approach

This approach proposed by Yuuki Kajiura at el. [5], explained the different definition of multi cloud on the basis of cloud services. Multiple cloud services are divided into “homo-cloud” and “hetero-cloud” according to the difference between the types of cloud services. Homo-cloud is a multiple-cloud-service architecture combined the same type of cloud service environments. Second, hetero-cloud are used to provide different multiple cloud services. This usage is very similar to that of cloud-of-clouds, intercloud, multi-clouds, and Hybrid cloud. The concept of these two usages (homo- and hetero-) of cloud services is explained in Figure 1.

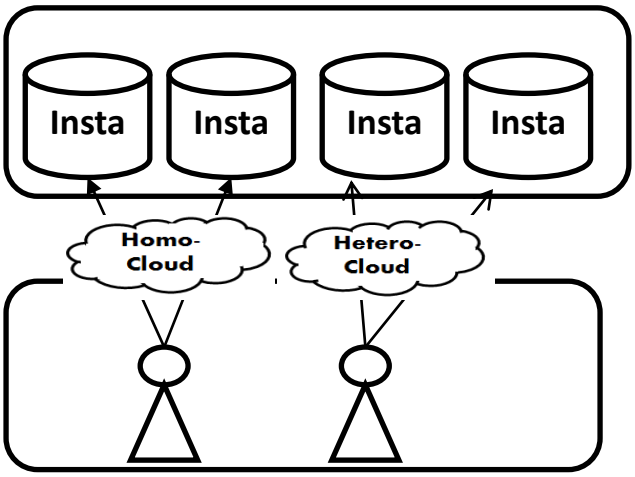

Figure 1: The definition of Homo-cloud and Hetero-cloud.

This approach which accomplish high availability and confidentiality at reasonable cost by using secrete sharing scheme technology and user find out best cloud storage using cloud SLA who maintain all information about cloud.

1) Cloud SLA:

Each user handles its own cloud SLA, and when user requires it then cloud sends SLA to use. The user matches the requests for a cloud and SLA. At last, the optimal cloud services for the user are determined. Figure 2 shows this condition. Currently cloud providers offer a wide range of services (machine sizes, availability modes, storage etc.) with complex pricing schemes (spot pricing, reservation pricing, etc.). At the same time, customers require distributed deployments in order to meet their own SLA commitments. The cloud provider forwards their pricing schemes along with their SLAs to the Cost Optimizer

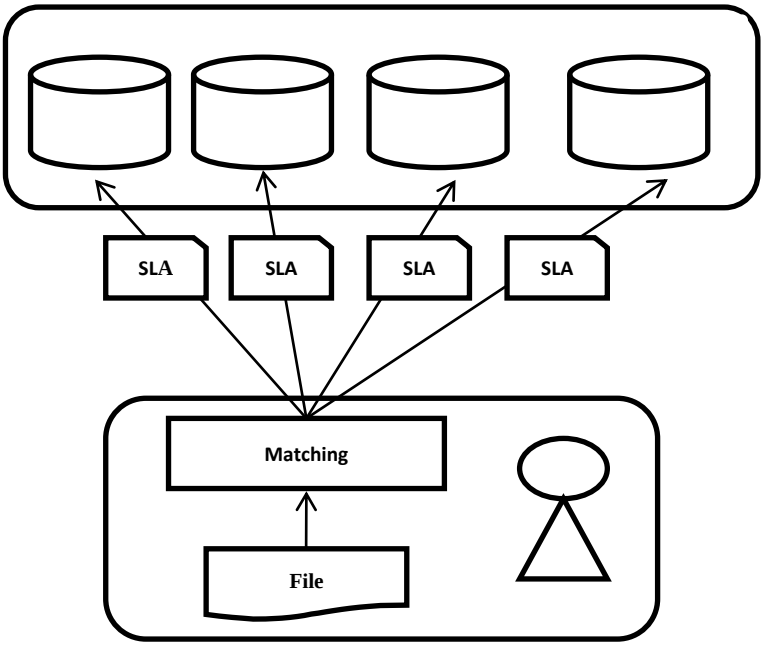

Figure 2: Overview of proposed technique.

When user wants to store data in cloud then the user prepares the data with requests-level of availability, confidentiality, cost, and performance. These requests are matched to the values calculated from the each cloud SLA with one-to-one correspondence with use requests. As a result, user gets best cloud services as per requests.

2) Secrete Sharing Scheme:

A secret sharing scheme is a method that generates “shares or secrete” from an original data, and it can recreate the original data if the number of shares is greater than or equal to a certain threshold. Out of number of shares n, k number of shares needed to recreate the original data [9]. A draft of the secret sharing scheme which is called “(k, n)-threshold scheme”. This method

is information-theoretic secure. Therefore, the size of each share is equal to that of the original data.

In [10], the "(k, L, n)- threshold scheme" was proposed by Yamamota. The two parameters used in this scheme are same as (k, n) of previous method plus one more additional parameter is L. In previous secrete sharing method the size of share is equal to original data but in these the size of share is 1/L of the size of original data. In this case, meaning of parameter k, L, and n of threshold scheme as follows:

k: it is required number of shares when an original file is recreate.

L: data size of user file that stored in each cloud service.

n: it is required number of cloud services when shares are distributed.

The security of the method is information-theoretic secure

When the number of shares is less than or equal to k-L,

When the number of shares is equal to k-t (1<=t<=L-1), t/L of the amount of the original data is specified, and

When the number of shares is equal to k or greater than k, the original data is completely recreated.

In this proposed technique, when user saving own file, user prepare data with request of availability and confidentiality. The user matches the requests and get best cloud service through cloud's SLA. Then shares are generated from original data by using threshold scheme-(k, L, n). This shares are manages in cloud service and distribute them in multiple clouds. Figure 3 shows this situation of share distributing in multiple clouds. At the time of data retrieval, the user collects shares from cloud services, and data is recreated. The original file is recovered as shown in figure 4.

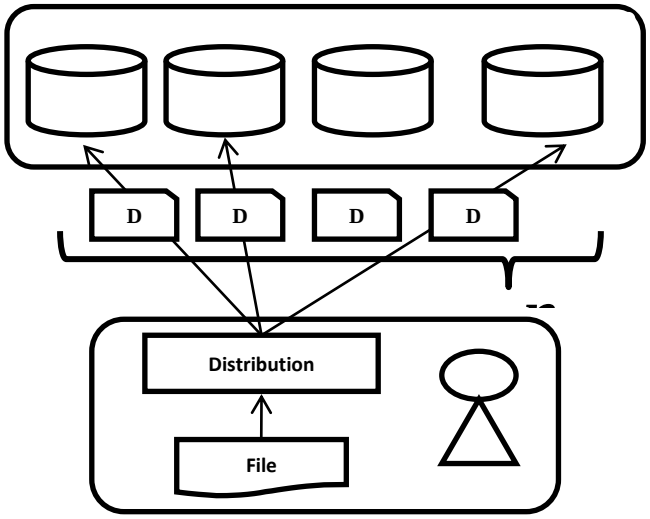

Figure 3: Uploading phase.

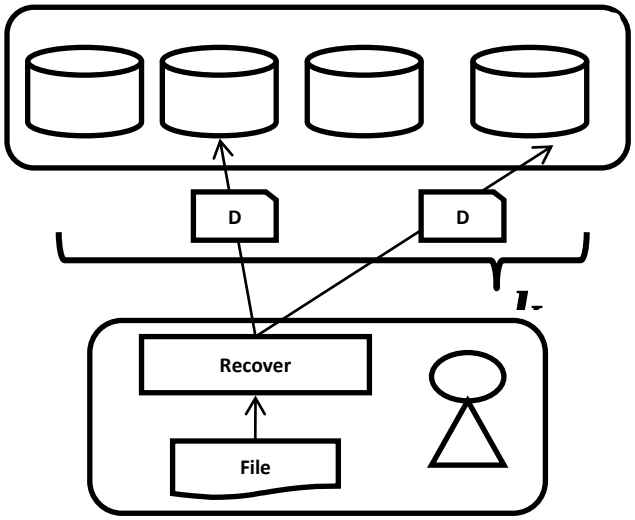

Figure 4: Downloading phase.

B) CloudStash Scheme

This scheme proposed by F. Alsolami [6]. CloudStash uses the secret-sharing approach and low cost cloud storages to provide confidentiality. Cloud-Stash divides a file into multi-shares and distributes these multi-shares (N) over multi-clouds. An attacker cannot break the confidentiality of CloudStash unless he hacks M cloud where M is secret sharing threshold M which subset of shares N. It means attacker must hack at least M cloud to obtain file which is very difficult.

When one cloud-storage is unavailable or attacked, client can retrieve their data from the other available clouds by reconstructing threshold shares. CloudStash also uses multi-threading in uploading and downloading operations in order to provide high performance. CloudStash provides integrity and fault tolerance by signing each share and distributing each share into a different cloud storage.

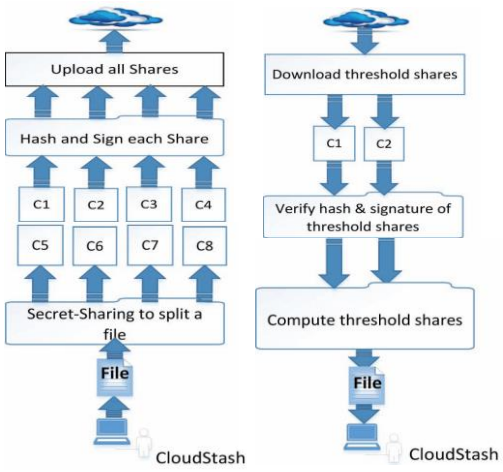

Figure 4: Architecture of CloudStash

The architecture of CloudStash is as shown in figure 4, which indicates operations of file uploading and downloading. At the time of file uploading, multi-threading program was used to upload the multi-shares in parallel into eight cloud storages, where each cloud storage store one share of the file. During a download operation, multithreading was used to download two shares from two cloud storages that the threshold shares, and then computed two shares to reconstruct the file back.

IV. CONCLUSION

This paper discussed two approaches based on multi cloud environment and used secrete sharing scheme by splitting data into several chunks and storing parts of it on multiple cloud providers in a manner that preserves data confidentiality, integrity and ensure availability. Also addresses key management issues that are occurred on other schemes.

In file distribution approach, through the SLA user determined best cloud service. Because of the SLA it is possible to provide convenient data storage service. This approach also used secrete sharing scheme with extra threshold parameters. In second approach CloudStash, while uploading file in cloud, it apply the secrete Shamir scheme on the file and split it into shares and

calculating the hash and signature for each file while uploading file and verifying hash and signature at the time of downloading file.

Both approaches uses secrete sharing approach but used in different ways, one file distribution approach used one extra parameter which reduces share computation while reconstructing share and second approach calculate and verify hash and signature for each share for more data protection.

REFERENCES

A. Bessani, M. Correia, B. Quaresma, F. André and P. Sousa, "DepSky: dependable and secure storage in a cloud-of-clouds", EuroSys'11:Proc. 6thConf. On Computer systems, pp. 31-46, 2011.

1. M. Vukolic, "The Byzantine empire in the intercloud", ACM SIGACT News, 41, pp. 105-111, 2010.

2. K.D. Bowers, A. Juels and A. Oprea, "HAIL: A high-availability and integrity layer for cloud storage", CCS'09: Proc.16th ACM Conf. on Computer and communications security, pp.187-198, 2009.

3. H. Abu-Libdeh, L. Princehouse and H. Weatherspoon, "RACS: a case for cloud storage diversity", SoCC'10:Proc. 1st ACM symposium on Cloud computing, pp. 229-240, 2010.

4. Yuuki Kajiura, Atsushi Kanai, Shigeaki Tanimoto, Hiroyuki Sato, “A File-distribution Approach to Achieve High Availability and Confidentiality for Data Storage on Multi-cloud”, IEEE 37th Annual Computer Software and Applications Conference Workshops, pp. 212-217, 2013.

5. Fahad Alsolami and Terrance Boult, “CloudStash: Using Secret-Sharing Scheme to Secure Data, Not Keys, in Multi-Clouds”, 11th International Conference on Information Technology: New Generations, pp. 315-320, 2014.

6. Richa Chowdhary Satyakshma Rawat, “One Time Password for Multi-Cloud Environment”, International Journal of Advanced Research in Computer Science and Software Engineering Volume 3, Issue 3, March 2013.

7. S. B. Shivakumar, Ramesh B. E., Kavitha G. M., Mala M., “Multi Cloud Architecture for Improved User Experience”, International Journal of Inventive Engineering and Sciences, Volume-1, Issue-7, June 2013.

8. Md Kausar Alam, Sharmila Banu K, "An Approach Secret Sharing Algorithm in Cloud Computing Security over Single to Multi Clouds", International Journal of Scientific and Research Publications, Volume 3, Issue 4, April 2013.

9. H. Yamamoto, "Secret Sharing System using (k, L, n) threshold scheme," Electron. Commun. Jpn. (Part I: Commun.), vol. 69, no. 9, pp.46-54, 1986.

10. Prof. V. N. Dhawas, Pranali Juikar, Neha Patekar, Neha Lendghar, Sushant Vartak, "A Secured Cost Effective Multi-Cloud Storage in Cloud Computing", International Journal of Scientific & Engineering Research, Volume 4, Issue 5, May-2013.