Volume 1, Issue 8, November 2016 ISSN: 2456-0006
International Journal of Science Technology Management and Research
Available online at: www.ijstmr.com

A Review on Secured Data Storage and Retrieval in Multicloud Computing

Ashvini Deore[1]
Department of Computer
Gangamai College of Engineering,Nagaon,
Maharashtra, India

Jyoti Vadje[2]
Department of Computer
Gangamai College of Engineering,Nagaon,
Maharashtra, India

Umesh Shimpi[3]
Department of Computer
Gangamai College of Engineering, Nagaon,
Maharashtra, India

G.M.Poddar[4]
Prof. Department of Computer
Gangamai College of Engineering,Nagaon,
Maharashtra, India

Abstract: ***Now days, the Cloud Computing is a very popular technology for storing and retrieving of data. Cloud computing delivers the on demand services to its customers (users). As a result, many organizations makes use of cloud computing for processing their data. Cloud computing is also known as pay per service business model. In cloud computing, cloud stores sensitive and important information for its users. So, this information must be secure, but security is a big challenge in cloud computing environment. Privacy and security are the main issues in cloud computing. Therefore, cloud providers has to give high as well as urgent priority for solving these issues. This paper reviews some of the related work which will be useful for developing the multiclouds system in proposed work. For this, proposed system uses a multi-cloud secret sharp model which aims to provide good economical distribution as well as retrieval of data among the cloud service providers. This model will provide customers with the data availability and secure data storage.***

Keywords: **- Cloud Computing, Cloud Security, Data Integrity, Service Availability, Multi Cloud.**

I. INTRODUCTION

In the present era, with the wide adoption of technology the cloud computing has increasing its attention towards the organizations. The very important service that cloud computing offers, is cloud data storage. It allows subscribers to store the data on cloud servers instead of their own local server, so that the subscriber can store, manage and retrieve the data efficiently. The service providers are responsible for managing the cloud service in the cloud environment. For data storage service, subscriber has to pay to service providers. Flexibility and scalability are the key benefits of using the cloud service. Along with these, it also provide the advantage of paying only the amount of data the customer wants to store for a particular period of time. Cloud service does not concerns for effective storage mechanisms and maintainability issues even with the big amount of data storage. There is no geographical limitation, customers can easily access the data if the CSP's network and Internet is available. The data stored in the cloud may be vulnerable to attacks of integrity and availability from malicious insiders and outsiders as well as subsidiary damage of cloud services [1]. Users are worrying about such attacks. Therefore, security is an important but critical aspect in cloud environment as the information stored in the cloud is sensitive and

important for users [1]. The security problem is very significant, still there is scope for security research in cloud computing. Let us introduce the data security risks. Those are

1) Data Integrity

Data integrity is one of the most important issue in cloud security risks. The cloud data may suffer from damage during transition operation from or to the cloud storage provider. Data integrity ensures that the data in the cloud is supposed to be there, and is protected against accidental alteration without authorization.

2) Data Intrusion

Another security risk with the cloud service provider is a hacked password or data intrusion [7].

3) Service Availability

The most problematic issue is service availability. The cloud service should be access anytime and anywhere without any problem. The availability of cloud can be increase through widespread internet-enabled access. But some of the client is dependent on the timely and robust provision of resources. Availability is dependent on the capacity building and good architecture provided by the service provider, as well as the defined contract between user and the service provider.

To solve the issue of data security we are providing a framework that will guarantee to prevent security risks in cloud computing. The framework contains multi-clouds and secret sharing algorithm to secure cloud database. This will lessen the risk of data intrusion and the loss of service availability in the cloud as well as ensures data integrity.

The rest of the paper is as follows: Section II presents the literature survey over the related work. In section III, proposed system is presented. Finally, the section IV concludes the survey paper.

II. LITERATURE REVIEW

In this section, we have studied some data as well as previous research papers related to securing the cloud data storage in cloud computing.

Data security is a major challenge in cloud computing. To solve this, there are various methods and algorithms for data encryption and data security. The encryption algorithms for security implementation are RSA, DES and Blowfish algorithm etc. These algorithms have some drawbacks if used in cloud computing. Hence, we will be using AES algorithm. Storage outsourcing is an increasing trend which suggests a number of security problems, among them many are largely searched in the past. Provable Data Possession (PDP) is one of the recent topic in the research literature. The cloud storage server is assumed to be untrusted entity when considering the security and reliability aspects of data storage. It is important to frequent, effective and secure verification of clients outsourced data by the storage server. Let us see some of the papers view related to cloud security as well as multicloud concept.

Bowers and Juels [2] proposed a HAIL protocol i.e. High Availability and Integrity Layer. It is a protocol for controlling multiple clouds. As HAIL is a distributed cryptographic system it ensures the client's data retrievability and data integrity. To address the data availability and integrity of stored data, a software layer is provided by the HAIL in an intercloud [2]. But the drawbacks of HAIL are, it does not guarantee about data confidentiality and it needs code execution on their servers. Also, it does not deal with multiple versions of data.

A. Bessani [3] develops a DepSky system, which does not have limitations like HAIL. H. Weatherspoon [4] proposed a RACS system which differs from the DepSky system. RACS system deals with "economic failures" and vendor lock-in. But it does not address the cloud storage security issues. Also, it does not ensures data confidentiality and updates of the stored data. To address the data retrievability issue, Bessani uses a Byzantine fault-tolerant replication for storing the data on cloud servers. Because of this, the data is able to retrieve correctly even if the cloud provider is damaged. Also, to address the loss of data privacy issue, Bessani uses data encryption as a solution [3]. They suggest that the data should be encrypted before it is stored on the cloud, so that the stored data can get protected from the malicious insider. To achieve this, DepSky system uses secret sharing algorithm and to hide the key value from malicious insider, the system stores the cryptographic security keys in the cloud.

The limitation of DepSky is, it is only a storage service like Amazon S3 and does not offer a IaaS cloud model [5]. Further, this system provides a safe storage cloud, but does not provide security of data in the IaaS cloud model. Because it uses data encryption and stores the encrypted key in the clouds using a secret sharing technique, it is unsuitable for the IaaS cloud model [5].

Cachin et al. [6] presents two layers in the multicloud environment 1)Bottom layer (inner cloud) 2)Inter cloud layer one is the bottom layer is the inner-cloud. Intercloud layer has the Byzantine fault tolerance method. Author primarily outline the previous Byzantine protocols across the last three decades. Cachin et al. [6] proposed a framework for intercloud storage (ICStore), the framework is finer than RACS and HAIL as a dependable service in multiple clouds. He also develop theories as well as protocols to address the attributes like confidentiality, integrity, reliability and consistency of the data stored in clouds in cloud environment.

III. PROPOSED SYSTEM

Proposed system uses multi cloud architecture as shown in Fig. 1. Multicloud concept will be implement using Shamir's Secret Sharing algorithm. It will reduce the risk of data intrusion and loss of service availability for ensuring data.

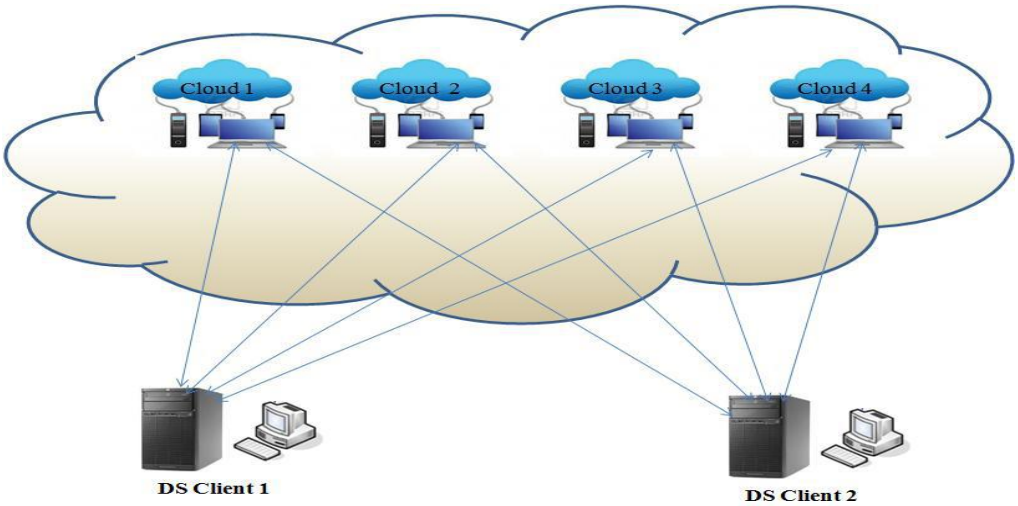

Figure 1: Multicloud Architecture

Using multicloud concept, a multi-cloud secret sharp model will be proposed in cloud computing. It holds an economical distribution and retrieval of data key among the available CSPs in the market and provide customers with data availability and secure data storage.

Proposed model is illustrated with an example in Fig. 2. In this, we assume that there are five Cloud Service Providers (CSP's) i.e. CSP1, CSP2, CSP3, CSP4 and CSP5. Customer (C1) encrypts his own data, after this the available encoded key is split and wishes to store on some servers into five pieces of encoded data key.

Let us assume that a customer (C1) has encrypt his own data then the available encoded key is split and store on some CSP's servers into five pieces of encoded data key. To reconstruct and get the full information a customer requires at least three pieces of encoded data key from different service providers. In our example, the CSP's that will participate in the encoded data key retrieval are CSP1, CSP3 and CSP5.

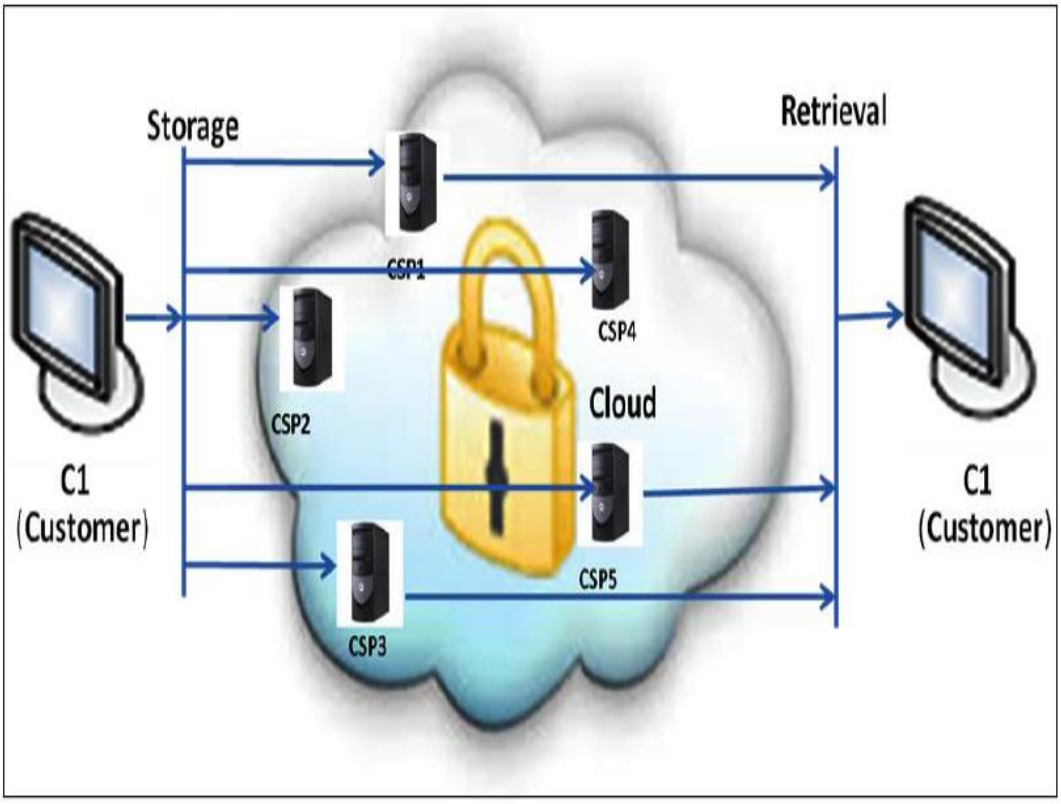

Figure 2: Data Storage and Retrieval in proposed system

The proposed system has two phases 1) Data Storage and 2) Data Retrieval.

Secured data storage in proposed system involves data distribution from the data source to different cloud providers. This is done after executing the polynomial functions on the data.

The data retrieval process in the multi-cloud secret sharp model starts from six various cloud providers. For this three number of shares are required, one for each CSP. Once, the three shares are retrieved they have to reconstruct using Lagrange functions. After the file decoding, the user can download the original file.Increasing the number of shares will also increase the security level of data.

We have compare the three cloud security models (Amazon, DepSky, Multicoud Secret Sharp (proposed model)) as shown in following Table .

Security Issues / Cloud Security Architectures		Data Integrity	Data Intrusion	Service Availability	Malicious Insiders
Amazon		If data hacked?	If password hacked?	If system down?	If malicious insider is present?
Data Status	Safe				
	Lost	√	√	√	√
Depsky		If data hacked from one CSP?	If password hacked from one CSP?	If one cloud down?	If malicious insider is present?
Data Status	Safe	√	√	√	
	Lost				√
Multi-Cloud Secret Sharp		If data hacked from one CSP?	If password hacked from one CSP?	If one cloud down?	If malicious insider is present?
Data Status	Safe	√	√	√	√
	Lost				

Table 1: Comparison between Amezon, Depsky and Multi-Cloud Secret Sharp Models

In the table, the models are compared considering the three characteristics i.e. data integrity, data intrusion, and service availability. It reveals that, our newly proposed Multi-Coud Secret Sharp model is superior in achieving the three security factors than in Amazon and Depsky cloud service model. Also, the proposed model is more secure to protect users data from untrusted CSP's and malicious threats whereas the Amazon cloud service ask the users to encrypt their data before storing it in their instances. In this way, multi cloud secret sharp model supports data integrity, data intrusion, service availability in a well manner than other cloud service model and also protects the cloud data from malicious insiders.

CONCLUSION

Thus, we have studied the research papers on single and multicloud system. It is clear that the security is a major issue in cloud computing environment. Customer wants their data to be keep confidential and available at any cost. They want surety of not losing their sensitive data to malicious threats as well as saving of data in case of any sudden damage of cloud services. To avoid this, proposed work will present a new model called Multi-Cloud Secret Sharp and uses Shamir's secret sharing algorithm. It uses multicloud model instead of single cloud model. The multicloud model is compared with Amazon, Depsky cloud service model. The result of comparison reveals that multicoud model is better than single cloud model in addressing the security problems in cloud computing. Both the secret sharing algorithm and Shamir's Secret Sharing algorithm generates its own secret sharing schemes and uses secure channels to distribute shares among themselves. It provides an excellent

framework for not only proofs but also applications. We provide a secure computation platform based on a simple secret sharing scheme than Shamir's scheme. The migration facility to multicloud decrease the security risks and thus, relax the cloud computing users.

ACKNOWLEDGMENT

We would like express our sentiments of gratitude to all who rendered their valuable guidance to us. We would like to express our appreciation and thanks to the Principal of our college. We are also thankful to the Head of Department. We are thankful to the anonymous reviewers for their valuable comments.

REFERENCES

1. Mohammed A. AlZain , Eric Pardede , Ben Soh , James A. Thom, "Cloud Computing Security: From Single to Multi-Clouds", 2012 45th Hawaii International Conference on System Sciences, 2012, pp. 5490-5499.

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, 2009, pp. 187-198.

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

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

5. F. Rocha and M. Correia, "Lucy in the Sky without Diamonds: Stealing Confidential Data in the Cloud", Proc.1stIntl. Workshop of Dependability of Clouds, Data Centers and Virtual Computing Environments, 2011, pp. 1-6.

6. C. Cachin, R. Haas and M. Vukolic, "Dependable storage in the Intercloud", Research Report RZ, 3783, 2010.

7. S. L. Garfinkel, An evaluation of amazon's grid computing services: EC2, S3, and SQS, Citeseer, 2007, pp. 1-15