www.ijsrnsc.org

Available online at www.ijsrnsc.org

IJSRNSC

Volume-6, Issue-1, February 2018
Survey Paper

Int. J. Sc. Res. in Network Security and Communication

ISSN: 2321-3256

A Survey on Security Provided by Multi-Clouds in Cloud Computing

Sakshi kathuria

Computer Science, Starex University, Gurugram, India

**Corresponding Author: sakshi.bhatia@gmail.com*

Received: 16/Jan/2018, Revised: 29/Jan/2018, Accepted: 19/Feb/2018, Published: 28/Feb/2018

***Abstract*-**Many enterprises and other organizations store their data on clouds. When using cloud, the client is forced to blindly trust the service provider which is storing the complete data on a single cloud. But now a days single cloud concept is becoming less popular as there are risks of service availability failure, data integrity risks and the possibility of malicious insiders in the single cloud. Due to this the concept of "Cloud-of-Clouds "also known as "inter-clouds" or "multi-clouds" is becoming much popular.. Use of cloud-of-clouds provides a higher level of security to the confidential data. This is a survey paper related to research on the use of multi cloud and their security risks.

***Keywords*-** Cloud Computing, Cloud-of-Clouds, Inter-Clouds, Multi-Clouds, Security, Confidential Data, Data Integrity

I. INTRODUCTION

The increasing maturity of cloud computing technology is leading many organizations to migrate their IT infrastructure. Cloud computing provides many benefits in terms Of low cost and accessibility of data. Cloud computing offers limitless flexibility, better reliability, enhanced collaboration, portability, unlimited storage, ensuring the security of cloud computing is a major factor in the cloud computing environment. Users often store sensitive information with cloud storage providers but these providers may be un-trusted. Data stored in the cloud can be compromised or lost. Working with "single cloud" providers is becoming less popular with customers due to risks of service availability failure and the possibility of data leakage. A movement towards "cloud-of-clouds", or in other words "inter-clouds" or "multi-clouds" has emerged recently. This paper surveys recent research related to multi-cloud security It has been found that the research into the use of multi-cloud providers to maintain security has received less attention from the research community.

II. SECURITY RISKS IN CLOUD COMPUTING

Now days many organizations are using the cloud services to store their precious data on the cloud. These organizations also include defense agencies and international research companies. So it all sums up to the security provided by the cloud environment. In the single cloud storage all the data is stored at one centralized storage system. If someone tries to illegally access the data, the hacker ends up getting the entire information stored at a single location. Hence, the use of single cloud storage is not that reliable. Another possibility of losing the data is a server crash. In this case as well the user is not able to access his data. Although cloud service providers can offer benefits to users, security risks are a major problem in the cloud computing environment. As the cloud storage is an online service, any problem with the internet security will also affect the cloud services.

III. VARIOUS RESEARCH APPROACHES USED TO PROTECT THE DATA AND TO AVOID NETWORK CONGESTION USING MULTI CLOUDS

1. File replication on multi clouds:

This concept provides security in the multi-cloud environment. The data is distributed in different clouds. A unique key is generated by each cloud that is further given to the user. If user wants to access his data he can do so by using this key. In case, if a particular cloud crashes or is hacked, the user will not get the entire data. To overcome this issue, each of the distributed data unit is replicated and stored in another server and is recognized by the key generated for that unit by the original cloud. If any problem occurs in the clouds, this data can be retrieved from the server [1].Thus there is no loss of the user's data.

A. Registration & Authentication

It is a module where the login and registration of the users will be provided by the system. Their details will be stored in database or server.

B. File Distribution

In this module, all the files uploaded by the user are distributed on 3 cloud servers and simultaneously key will be generated from each cloud.

C. Key sharing

It is a module where unique and generalized key is generated from the system. The key will be encrypted and the key is stored by the server with their respective files allocated to it. This key will be used while retrieving the data again.

D. File Storage and Retrieval
This module is linked with key authenticating block, uploaded files are related to unique keys generated. The user enters the encrypted key and the encrypted key is then decrypted, once it's done they retrieve the required saved data from the different servers.

E. File Replication & Retrieval from Replicated Storage
The distributed files which are stored in 3 different clouds will be replicated/stored on another single server with three different files. The name of the files will be same as the three keys generated from the server. Further if there is difficulty in retrieving the files from the clouds then the file is searched in the replicated storage cloud with the help of key.

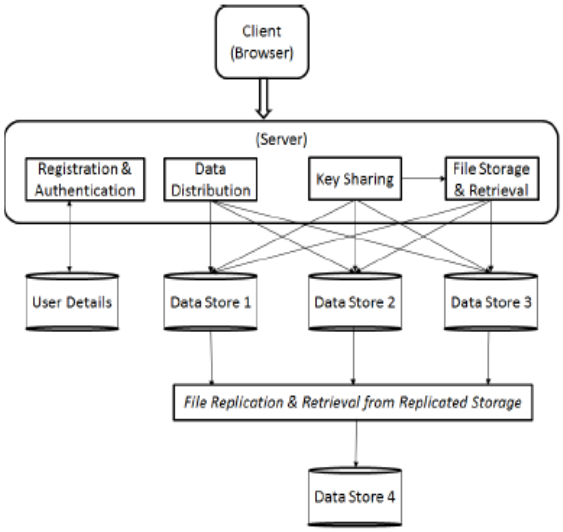

Fig1. File Replication on Multi-clouds

2. Replication of applications:
Multiple clouds executing multiple copies of the same application can be used. Instead of executing a particular application on one specific cloud, the same operation is executed by different clouds. After comparing the obtained results, the cloud user gets evidence on the integrity of the result. Instead of trusting one cloud service provider totally, the cloud user only needs to rely on the assumption that the cloud providers will not collaborate maliciously against the user[6].

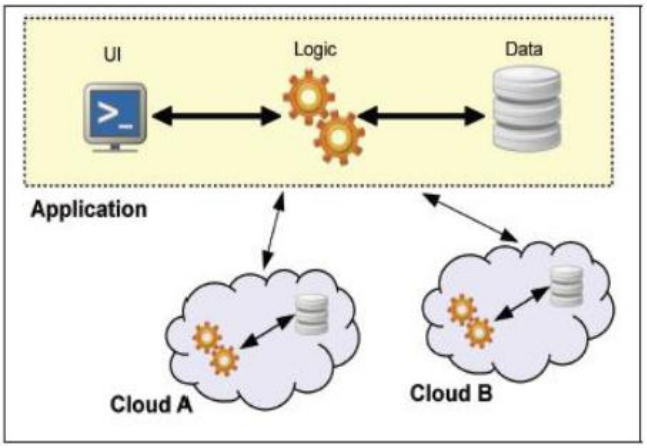

Fig2. Replication of Application Systems

3. Partition of application system into tiers:
It should be noted, that the security services provided by this architecture can only be fully exploited if the execution of the application logic on the data is performed on the cloud user's system. Only in this case, the application provider does not learn anything on the users' data. Besides the introduced overhead due to the additionally involved cloud, this architecture requires, moreover, standardized interfaces to couple applications with data services provided by distinct parties [12].

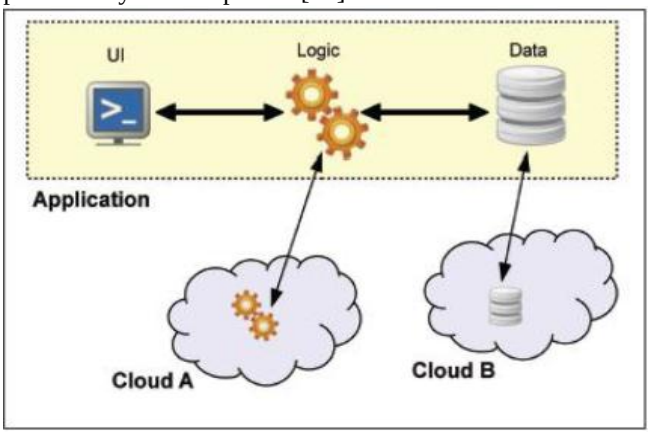

Fig3.Partitioning of application system into tiers

4. Partition of application logic into fragments:
The purpose of this architecture is that the application logic needs to be partitioned into fine-grained parts and these parts are distributed to different clouds. This approach can be incorporated in different ways depending on how the partitioning is performed. The clouds participating in the fragmented applications can be symmetric or asymmetric in terms of computing power and trust. Two concepts are common. The first involves a trusted private cloud that takes a small critical share of the computation, and a un-trusted public cloud that takes most of the computational load. The second distributes the computation among several

un-trusted public clouds, with the assumption that these clouds will not collaborate to break the security [6].

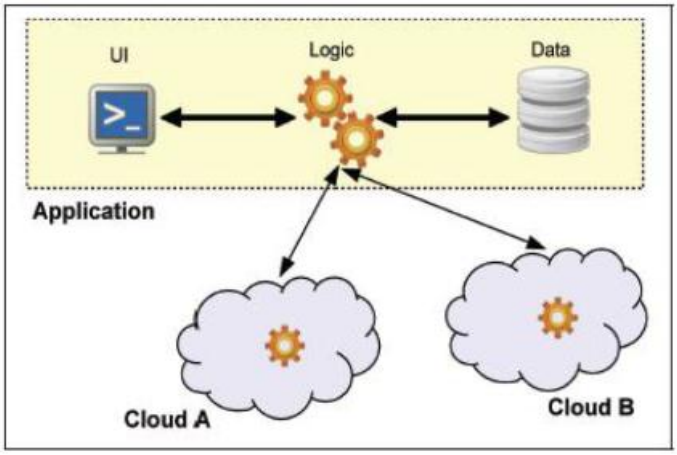

Fig4. Partitioning of application logic into fragments

5. Partition of application data into fragments:

The most common forms of data storage are files and databases. Files typically contain unstructured data and do not allow for easily splitting or exchanging parts of the data. This kind of data can only be partitioned using cryptographic methods. Databases contain data in structured form organized in columns and rows. Here, data partitioning can be performed by distributing different parts

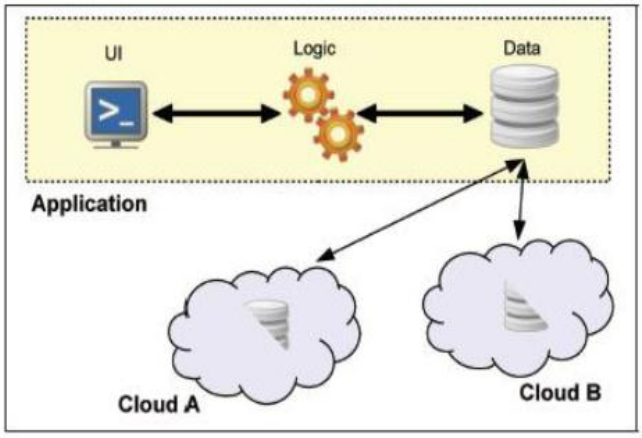

Fig5.Partition of application data into fragments

of the database to different cloud providers. Finally, files can also contain structured data. Here, the data can be splitted using similar approaches like for databases [12].

6. USE of Byzantine Protocols

In cloud computing, any faults in software or hardware are known as Byzantine faults, they usually relate to inappropriate behavior and intrusion tolerance. In addition, it also includes arbitrary crash and faults. Much research has been dedicated to Byzantine fault tolerance (BFT) since its first introduction. Regarding service availability risk or loss of data, if we replicate the data into different cloud providers, we could argue that the data loss risk will be reduced. If one cloud provider fails, we can still access our data live in other cloud providers [3].

7. Rain clouds system:

The term Rain Cloud System is a collection of several clouds. These clouds form a group of excess resources like rain drops and reduce the drought or lack of resources in a network. The condition of drought occurs mainly in private clouds. There could be several problems occurred in private clouds such as lacking of hardware and software resources, network, congestion of packets, data become bottleneck etc. These problems always either slow down the network, loss of packets or information. To resolve such kind of problems multi-clouds or rain clouds are introduced. The design architecture of Rain cloud consist of number of nodes (such as users) connected with the number of clouds within the network. Every node is connected to its owner cloud and also able to connect to its neighbor cloud whenever required. In the figure, there are four clouds and four clients that are interconnected through the communication links. The whole rain cloud system deals with different cloud providers but they exist in a particular organization as it is collection of several private clouds. The main point of rain cloud system is that it works only in the single or private organization. It is not reliable under public cloud system [7].The rain cloud system uses three Messages to communicate:

a) Service Request Message (SRQM)
b) Service Response Message (SRSM)
c) Service Level Agreement (SLA)

Suppose Client 4 sends SRM to the cloud 1 and waits for the acknowledgement. Cloud 1 also serves the client 2 and client 3 at that time. Client 4 repeatedly sends request messages to the cloud 1. At last cloud 1 is congested with the number of request messages and it temporarily fails down. In this case, a neighbor cloud provides the essential services to the client 4. The Service Level Agreement (SLA) messages are used to link the rain clouds with various public clouds that allow them to receive services, if all clouds are unable to serve, then send request to other public clouds. The following diagram shows the architecture design of a Rain-Cloud system.

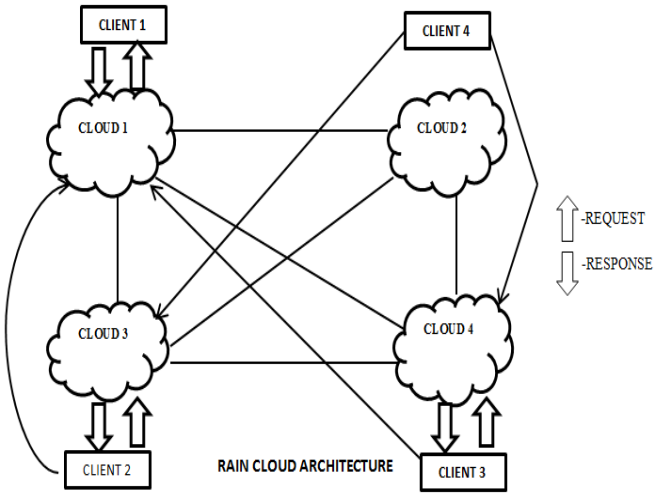

Fig6. Rain cloud Architecture

The rain cloud architecture always try to maintain the network congestion free because in small organizations the load of data traffic rapidly increases that causes severe problems.

8. DepSky Architecture:

The DepSky architecture consists of four clouds and each cloud uses its own particular interface. The DepSky algorithm exists in the clients' machines as a software library to communicate with each cloud as shown in figure. These four clouds are storage clouds, so there are no codes to be executed. The DepSky library permits reading and writing operations with the storage clouds [5].

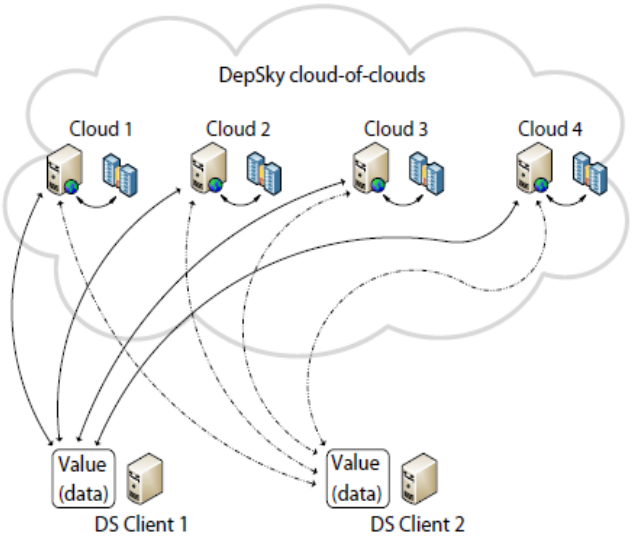

Fig7.Architecture of DEPSKY

1. DepSky Data Model: As the DepSky system deals with different cloud providers, the DepSky library deals with different cloud interface providers and consequently, the data format is accepted by each cloud. The DepSky data model consists of three abstraction levels: the conceptual data unit, a generic data unit, and the data unit implementation.

2. DepSKy System Model: The DepSky system model contains three parts: readers, writers, and four cloud storage providers, where readers and writers are the client's tasks. There is a difference between readers and writers for cloud storage. Readers can fail arbitrarily (for example, they can fail by crashing, they can fail from time to time and then display any behavior) whereas, writers only fail by crashing.

IV. CONCLUSION

It is clear that although the use of cloud computing is rapidly increasing; cloud computing security is still a major issue. Due to this, people or customers prefer storing the data in multiple clouds or cloud-of-clouds. In this paper, we discussed various secured cost-effective multicloud storage in cloud computing, which seeks to provide each customer with a better cloud data storage decision, In the next 2-3 years, the research approaches discussed in this paper will overcome the security issues in single cloud and promotes the use of multi clouds.

REFRENCES

[1]. Nikhil Shrivastva, Poorva Andurkar, Ajay Survase, Shubhada Bhandare,Sunil Kale," A New Approach For Cloud Data Security: From Single To Cloud-Of-Clouds" International Journal of Advances In Computer Science and Cloud Computing, Volume- 3, Issue- 1, May-2015.

[2]. Dr.K.Subramanian1, F. Leo John," Data Security in Single and Multi-Cloud Storage–An Overview", International Journal of Innovative Research in Computer and Communication Engineering" Vol. 4, Issue 11, November 2016.

[3]. 3.Mohammed A Alzain,Eric Pardede,Ben Soh,James A Thom," 45th Hawaii International Conference on System Sciences",2012.

[4]. Monjur Ahmed,Mohammad Ashraf Hossain," Cloud Computing and Security Issues in the Cloud", International Journal of Network Security & Its Applications (IJNSA),Vol.6, No.1, January 2014.

[5]. G. Sidharth, D. Baswaraj," Cloud Computing Security from Single to Multi-Clouds", International Journal of Computer Science and Mobile Computing, Vol. 2, Issue. 10, October 2013, pg.57 – 61.

[6]. A.Tulasi Ram, Anil Kumar Mahapatro," Security and Privacy-Enhancing Multi Cloud Architectures",International Journal & Magazine of Engineering, Technology,Management and Research,Vol.2,Issue. 10, November 2015.

[7]. Shaik.Aafreen Naaz, Pothireddygari.Ramya, P.Vishunu Vardhan Reddy," Cloud Computing: Use of Multi-Clouds".

[8]. Uma Maheswari. S," Security and Privacy Enhancing Multicloud Architectures", IJESE, vol. 6, Issue 5,2016.

[9]. N. R. Anitha Rani ,P. Prem Kumar," Security and Privacy Enhancing in Multi-Cloud Architecture with Data De-

Duplication" Global Research and Development Journal for Engineering, e-ISSN: 2455-5703,2016.

[10]. Akanksha Rana, Srinivas Arukonda," Multi-Tiered Security and Privacy-Enhancing Multi-cloud Environment", International Journal of Computer Trends and Technology, volume 23 Number 1 – May 2015.

[11]. Archana Waghmare, Rahul Patil, Pramod Mane, Shruti Bhosale," Data Storage in Secured Multi-Cloud Storage in Cloud Computing", International Journal of Computational Engineering Research, Vol, 04,Issue, 2, February 2014

[12]. R.Shobana, Dr.Dekson," Security And Privacy-Enhancing Multi Cloud Architectures",Elysium Journal", Volume-1, Special Issue-1,September 2014.

[13]. Yogita G. Patil,Pooja S. Deshmukh," A Review: Mobile Cloud Computing: Its Challenges and Security", International Journal of Scientific Research in Network Security and Communication, Volume-6, Issue-1, Jan 2018.

Authors Profile

Ms. Sakshi Kathuria has completed her B.Tech (Computer science) from Kurukshetra University and M.Tech (Computer Science) from Ch. Devi Lal University. She has various publications in reputed International Journals and various National and International Conferences. She has been a part of various organizational committees and institutional events. She is a life time member of IAENG (International association of engineers). Her main research work focuses on cloud computing. She is presently working as an Assistant Professor in Starex University. Ms.Sakshi has as an industrial and teaching experience of over 12 Years.

