Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 2, Issue. 10, October 2013, pg.57 – 61

RESEARCH ARTICLE

Cloud Computing Security from Single to Multi-Clouds

G. Sidharth[1], D. Baswaraj[2]

[1]M.Tech (CSE), CMR Institute of Technology, Hyderabad, India

[2]Head of the Department (CSE), CMR Institute of Technology, Hyderabad, India

[1] sidharthgoparapu@gmail.com; [2] braj5555@yahoo.co.in

Abstract— ***Cloud computing, in now days it is been playing a crucial role in terms of data storing and reducing the overall cost to entrepreneurs. But most of them worried about security; mostly they used to keep the data in single cloud. In this case if the data is lost or hacked in the sense entire data will be loose. To avoid these kinds of vulnerabilities and to achieve better security we are proposing of multicolour where the data will be stored in different databases means clouds. This paper surveys recent research related to single and multi-cloud security and addresses possible solutions. It is found that the research into the use of multicolour providers to maintain security has received less attention from the research community than has the use of single clouds. This work aims to promote the use of multi-clouds due to its ability to reduce security risks. In cloud data is been changing dynamically from user side in this case hacker may have a chance to hack the data through the network or attacking on the database.***

Keywords: -Security; Distributing Data; Storing Data in Cloud multi-clouds; Single-Cloud; Data Integrity; Data Intrusion; service availability

I. INTRODUCTION

Cloud computing, or something being in the cloud, is a colloquial expression used to describe a variety of different types of computing concepts that involve a large number of computers connected through a real-time communication network such as the Internet.

Cloud computing is a term without a commonly accepted unequivocal scientific or technical definition. In science, cloud computing is a synonym for distributed computing over a network and means the ability to run a program on many connected computers at the same time. The phrase is also more commonly used to refer to network-based services which appear to be provided by real server hardware, which in fact are served up by virtual hardware, simulated by software running on one or more real machines. Such virtual servers do not physically exist and can therefore be moved around and scaled up (or down) on the fly without affecting the end user—arguably, rather like a cloud.

The remainder of this paper is organized as follows. Section 2 describes the beginning of cloud computing and its components. In addition, it presents examples of cloud providers and the benefits of using their services. Section 3 discusses security risks in cloud computing. Section 4 analyses the new generation of cloud computing, that is, multi-clouds and recent solutions to address the security of cloud computing, as well as examining their limitations. Section 5 presents suggestions for future work. Section 6 will conclude the paper.

II. DATA INTEGRITY

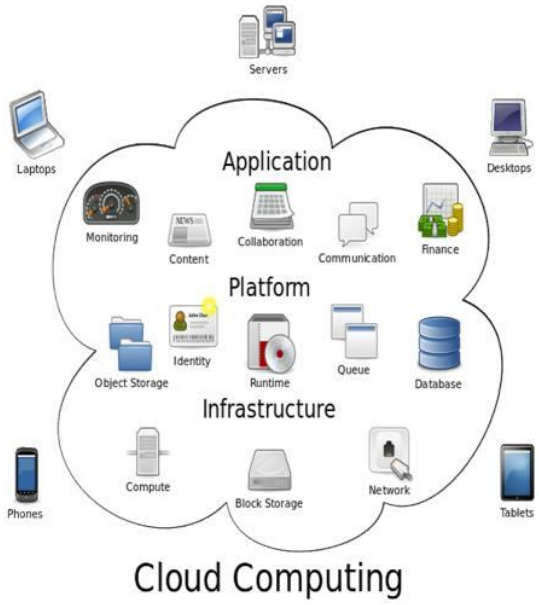
One of the most important issues related to cloud security risks is data integrity. The data stored in the cloud may suffer from damage during transition operations from or to the cloud storage provider. Cachinet al. gives examples of the risk of attacks from both inside and outside the cloud provider, such as the recently attacked Red Hat Linux.

Although this protocol solves the problem from a cloud storage perspective, Cachinet alargue that they remain concerned about the users' view, due to the fact that users trust the cloud as a single reliable domain or as a private cloud without being aware of the protection protocols used in the cloud provider's servers. As a solution, Cachinet al. suggests that using Byzantine fault-tolerant protocols across multiple clouds from different providers is a beneficial solution.

III. DATA INTRUSION

According to Garfinkel [19], another security risk that may occur with a cloud provider, such as the Amazon cloud service, is a hacked password or data intrusion. If someone gains access to an Amazon account password, they will be able to access all of the account's instances and resources. Thus the stolen password allows the hacker to erase all the information inside any virtual machine instance for the stolen user account, modify it, or even disable its services. Furthermore, there is a possibility for the user's email (Amazon user name) to be hacked (see [18] for a discussion of the potential risks of email), and since Amazon allows a lost password to be reset by email, the hacker may still be able to log in to the account after receiving the new reset password.

A. Service Availability



So many kinds services will be available through this cloud computing paradigm like as we seen in the picture in so many ways data will be accessed by the users in less cost and it has divided into categorise like SAS,PAS.

IV. MULTI-CLOUDS COMPUTING SECURITY

This section will discuss the migration of cloud computing from single to multi-clouds to ensure the security of the user's data.

4.1 Multi-Clouds: Preliminary

The term "multi-clouds" is similar to the terms "interclouds" or "cloud-of-clouds" that were introduced by Vukolic [54]. These terms suggest that cloud computing should not end with a single cloud. Using their

illustration, a cloudy sky incorporates different colors and shapes of clouds which leads to different implementations and administrative domains.

Recent research has focused on the multi-cloud environment [3],[8],[10],[11] which control several clouds and avoids dependency on any one individual cloud.

Cachin et al. [11] identify two layers in the multi- cloud environment: the bottom layer is the inner-cloud, while the second layer is the inter-cloud. In the inter- cloud, the Byzantine fault tolerance finds its place. We will first summarize the previous Byzantine protocols over the last three decades.

4.2 Introduction of Byzantine Protocols

In cloud computing, any faults in software or hardware are known as Byzantine faults that usually relate to inappropriate behavior and intrusion tolerance. In addition, it also includes arbitrary and crash faults [54]. Much research has been dedicated to Byzantine fault tolerance (BFT) since its first introduction [28], [38]. Although BFT research has received a great deal of attention, it still suffers from the limitations of practical adoption [27] and remains peripheral in distributed systems [54].

The relationship between BFT and cloud computing has been investigated, and many argue that in the last few years, it has been considered one of the major roles of the distributed system agenda. Furthermore, many describe BFT as being of only "purely academic interest" for a cloud service [9]. This lack of interest in BFT is quite different to the level of interest shown in the mechanisms for tolerating crash faults that are used in large-scale systems. Reasons that reduce the adoption of BFT are, for example Byzantine fault-tolerant data is being stolen from the cloud provider. 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. This fact has been discovered from this survey and we will explore dealing with different cloud provider interfaces and the network traffic between cloud providers.

4.3 DepSky Architecture

The DepSky architecture [8] 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 (Figure 2). 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.

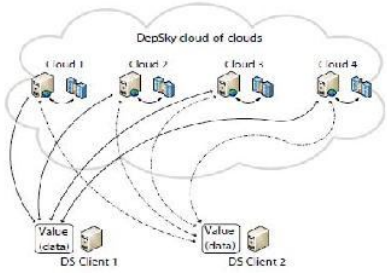


Figure 2:DepSky Architecture [8].

4.3.1 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.

4.3.2 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. Bessani etal.[8]explain the 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.

Coding

```
/*
* To change this template, choose Tools | Templates
* and open the template in the editor.
```



```
   */
   package DB;

   import java.sql.Connection;
   import java.sql.DriverManager;

   /**
   *
   * @author Raj
   */
   public class DBConn { Connection con;
   public Connection getConn(){
   try{
   Class.forName("com.mysql.jdbc.Driver");
   con=
DriverManager.getConnection("jdbc:mysql://localhost:33
06/eeits","root","root"); System.out.println("db connected..");
       }catch(Exception e){
                                    e.printStackTrace();

       }
       return con;
   }
   public static void main(String[] args) {
       new DBConn().getConn();
   }

}
```

V. CONCLUSION

We can conclude here that the data of enter pruners is very volatile to the enterprises.at the same time providing a security to that data is a big deal to cloud owners as well as firm maintainers. It is clear that although the use of cloud computing has rapidly increased, cloud computing security is still considered the major issue in the cloud computing environment. Customers do not want to lose their private information as a result of malicious insiders in the cloud. In addition, the loss of service availability has caused many problems for a large number of customers recently. Furthermore, data intrusion leads to many problems for the users of cloud computing. The purpose of this work is to survey the recent research on single clouds and multi-clouds to address the security risks and solutions. We have found that much research has been done to ensure the security of the single cloud and cloud storage whereas multi- clouds have received less attention in the area of security. We support the migration to multi-clouds due to its ability to decrease security risks that affect the cloud computing user.

REFERENCES

[1] (NIST), http://www.nist.gov/itl/cloud/.
[2] I. Abraham, G. Chockler, I. Keidar and D. Malkhi, "Byzantine disk paxos: optimal resilience with Byzantine shared memory", Distributed Computing, 18(5), 2006, pp. 387-408.
[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, 2010, pp. 229-240.
[4] D. Agrawal, A. El Abbadi, F. Emekci and A. Metwally, "Database Management as a Service: Challenges and Opportunities", ICDE'09:Proc.25thIntl. Conf. on Data Engineering, 2009, pp. 1709-1716.
[5] M.A. AlZain and E. Pardede, "Using Multi Shares for Ensuring Privacy in Database-as-a-Service", 44th Hawaii Intl. Conf. on System Sciences (HICSS), 2011, pp. 1-9.
[6] Amazon, Amazon Web Services. Web services licensing agreement, October3,2006.
[7] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson and D. Song, "Provable data possession at untrusted stores", Proc. 14th ACM

About the Authors:

Mr. G. Sidharth is pursuing M.Tech (CSE) in CMR Institute of Technology, JNTU Hyderabad. He has completed his B.Tech (CSE). His area of interests includes cloud computing and network security.

Mr. D. Baswaraj working as Head Of The Department (CSE) in CMR Institute of Technology, Hyderabad. He has completed his M.Tech (CSE) from JNTU Hyderabad and B.Tech (CSE) from JNTU. His interests are cloud computing and database systems.

