RESEARCH REVIEW JOURNALS
Volume-04
Issue-01
January -2019

ISSN: 2455-3085 (Online)
RESEARCH REVIEW International Journal of Multidisciplinary
www.rrjournals.com [UGC Listed Journal]

A Study of Multilayered Security on Distributed Clouds

[1]Syed Azahad & [2]Dr. R. P. Singh

[1]*Research Scholar, Sri Satya Sai University ,Bhopal (India)*
[2]*Vice Chancellor, SSSUTMS, Bhopal (India)*

ARTICLE DETAILS

Article History
Published Online: 10 January 2019

Keywords
Security; Distributing Data; Storing Data in Cloud multi-clouds

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 multi clouds 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 multi clouds 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.

1. 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[1]. 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.[2]

2. 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. 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, 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, that using Byzantine fault-tolerant protocols across multiple clouds from different providers is a beneficial solution.[3]

3. Data Intrusion

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 to be hacked 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.[5]

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.

4. Multi-clouds computing security

The term "multi-clouds" is similar to the terms "interclouds" or "cloud-of-clouds" that. 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. the multi-cloud environment which control several clouds and avoids dependency on any one individual cloud.[6]

5. 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. Much research has been dedicated to Byzantine fault tolerance (BFT) since its first introduction. Although BFT research has received a great deal of attention, it still suffers from the limitations of practical adoption and remains peripheral in distributed systems. 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. 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.[7]

6. DEP Sky 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 (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.[8]

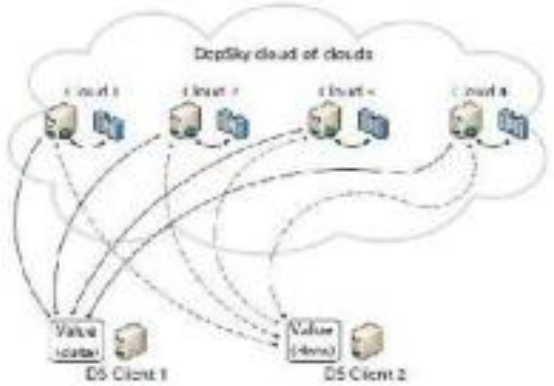

Figure: Dep Sky Architecture

7. 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.[9]

8. 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. 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.[10]

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();
}
}
```

9. SECURITY ISSUES IN CLOUD COMPUTING

we found that there are many issues in cloud computing but security is the major issue which is associated with cloud computing.

Top seven security issues in cloud computing environment as discovered by “Cloud Security Alliance” CSA are :

- Misuse and reprehensible Use of Cloud Computing.
- Insecure API.
- Wicked Insiders.
- Shared Technology issues/multi-tenancy nature.
- Data Crash.
- Account, Service & Traffic Hijacking.
- Unidentified Risk report.

Misuse and reprehensible Use of Cloud Computing

Hackers, spammers and other criminals take advantage of the suitable registration, simple procedures and comparatively unspecified access to cloud services to launch various attacks like key cracking or password .

Insecure Application Programming Interfaces (API)

Customers handle and interact with cloud services through interfaces or API's. Providers must ensure that security is integrated into their service models, while users must be aware of security risks .

Wicked Insiders

Malicious insiders create a larger threat in cloud computing environment, since consumers do not have a clear sight of provider policies and procedures. Malicious insiders can gain unauthorized access into organization and their assets .

Shared Technology issues/multi-tenancy nature

This is based on shared infrastructure, which is not designed to accommodate a multi-tenant architecture . Data Crash: Comprised data may include; deleted or altered data without making a backup; unlinking a record from a larger environment; loss of an encoding key; and illegal access of sensitive data .

Account, Service & Traffic hijacking

Account or service hijacking is usually carried out with stolen credentials. Such attacks include phishing, fraud and exploitation of software vulnerabilities. Attackers can access critical areas of cloud computing services like confidentiality, integrity and availability of services.

10. 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. "Security Guidance for Critical Areas of Focus in Cloud computing", April 2009, presented by Cloud Security Alliance (CSA).
2. Arijit Ukil, Debasish Jana and Ajanta De Sarkar" A SECURITY FRAMEWORK IN CLOUD COMPUTING INFRASTRUCTURE "International Journal of Network Security & Its Applications (IJNSA), Vol.5, No.5, September 2013 DOI: 10.5121/ijnsa.2013.5502 11.
3. Rabi Prasad Padhy, Manas Ranjan Patra and Suresh Chandra Satapathy ," Cloud Computing: Security Issues and Research Challenges", IRACST - International Journal of Computer Science and Information Technology & Security (IJCSITS) Vol. 1, No. 2, December 2011.
4. Kashif Munir and Prof Dr. Sellapan Palaniappan," FRAMEWORK FOR SECURE CLOUD COMPUTING ", International Journal on Cloud Computing: Services and Architecture (IJCCSA), Vol.3, No.2, April 2013.
5. (NIST), http://www.nist.gov/itl/cloud/.
6. 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.
7. 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.
8. 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.
9. 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.
10. Amazon, Amazon Web Services. Web services licensing agreement, October3,2006.
11. G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson and D. Song, "Provable data possession at untrusted stores", Proc. 14th AC

