Volume 4, Issue 4, April 2014 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Three Major Security Issues in Single Cloud Environment

Dr. Atul Patel
Principal, C.M.P.I.C.A., CHARUSAT, India

Kalpit Soni
Ph.D. Research Scholar, CMPICA, CHARUSAT, India

Abstract: ***Security is considered to be one of the most critical aspects in a cloud computing environment due to the sensitive and important information stored in the cloud for users. Users are wondering about attacks on the integrity and the availability of their data in the cloud from malicious insiders and outsiders, and from any collateral damage of cloud services. These issue are extremely significant but there is still much room for security research in cloud computing. This paper focuses more on the issues related to the data security and privacy aspects in cloud computing, such as data integrity, data intrusion, service availability. It proposes a Multi-clouds Database Model (MCDB) which is based on Multi-clouds service providers instead of using single cloud service provider.***

Keywords: ***Cloud computing, single cloud, multi-clouds, cloud storage, data integrity, Data intrusion, Service availability, Database as a service.***

I. INTRODUCTION

The need for Data outsourcing or database as a service (DaaS) is extremely important for any organization. In addition, data storage or data retrieval cost high specially for small companies.[1] Economic computing resources and advanced network technology is referred to as cloud computing. The use of cloud computing has increased rapidly in many organizations. The fast access to applications or the decreasing of the infrastructure costs are provided by cloud computing services.[2] The security of cloud computing is considered to be the most critical issue in cloud computing environment due to the valuable stored information for users in the cloud as shown in a survey conducted by the IDC enterprise panel.

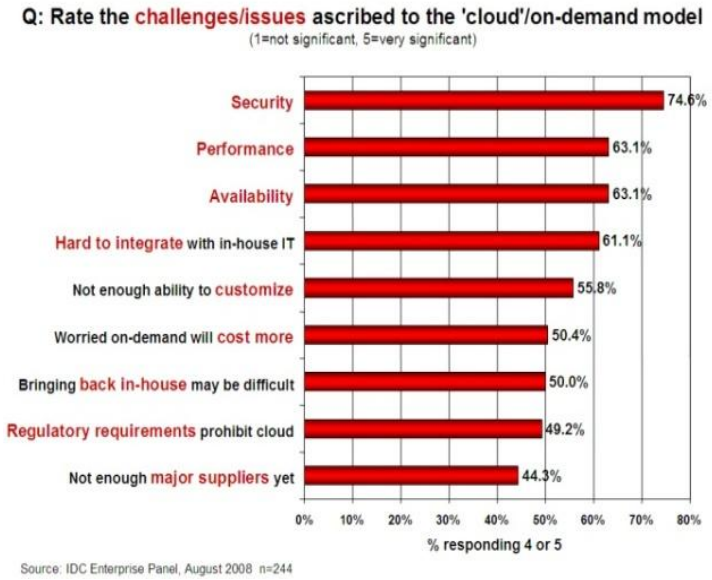

Figure 1. Rate the challenges in Cloud Model

As a result of the importance of data security in cloud computing, this paper focuses more on the issues related to the data security aspect in single cloud environment. It proposes a Multi-clouds Database Model (MCDB) which uses Multi-clouds service providers instead of using single cloud service provider such as in Amazon cloud service.[3]

II. RELATED WORK

This section presents security issue arise in single cloud environment and comparison between single cloud and multi-cloud database server.

2.1 Background:

Cloud computing is the delivery of computing as a service rather than a product, whereby shared resources, software and information are provided to computers and other devices as a leased or otherwise metered service over the Internet. In a

recent report, McKinsey pointed that there were "at least 22 different cloud definitions in common use".[4] In an October 2009 presentation titled "Effectively and Securely Using the Cloud Computing Paradigm"[5] by Peter Mell and Time Grance of the National Institute of Standards and Technology (NIST) Information Technology Laboratory, Cloud computing is defined as follows. "Cloud Computing is a model for enabling, convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal, management effort or service provider interaction".[6] The cloud computing model consists of five characteristics, three delivery models and four deployment models. The five key characteristics of cloud computing are on-demand self service, Broad network access, Resource pooling, Rapid elasticity and Measured service. Three cloud delivery models are infrastructure as a service, Platform as a service and Software as a service. Four deployment models are Private cloud, Public cloud, Community cloud and Hybrid cloud.

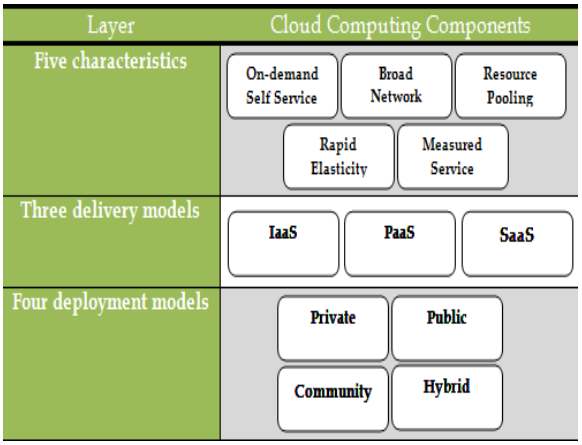

Figure 2. Cloud Computing Architecture

2.2 Single cloud Provider:

One of the first cloud computing implementations to deliver project services through a website was introduced by Salesforce.com in 1999.[7] Amazon Web Services in 2002 provided customers with advantages such as storage and computation services. In 2006, Amazon provided their customers with the Elastic Compute Cloud (EC2) service to allow them to use their instance for data processing and computing.[8] The drawback of single cloud provider is that it can be easily hacked by any attacker. In multiple cloud service provider model gives better security and availability of user private data.

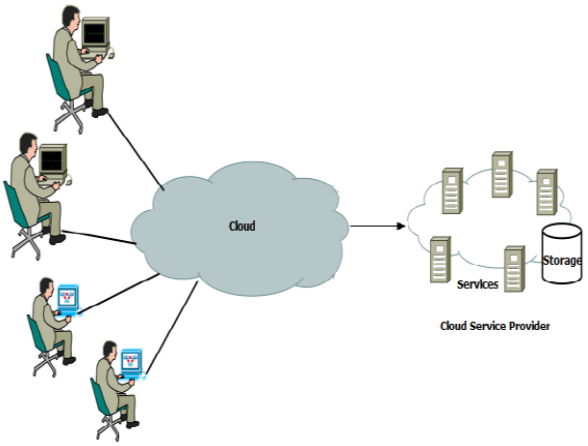

Figure 3. Single-Cloud Storage in Cloud Computing

III. CLOUD COMPUTING SECURITIES

3.1 Security Risks:

Cloud service providers can offers benefits to users, but security risks play a major role in the cloud computing environment.[9] Users who use online data sharing or network facilities are aware of the potential loss of privacy.[10] According to a recent IDCI survey, the top challenge for 74% of IT execution on CIO's of cloud computing adoption is related to security matters.[11] Protecting private and important information from attackers or malicious insiders is of critical importance. Moving database to a large data centre involves many security challenges such as Virtualization vulnerability, accessibility vulnerability, privacy and control issues related to data accessed from a third party, integrity, confidentiality, and data loss or theft. In different cloud service models, the security responsibility between users and providers is different. The impact of security issues in the public cloud is greater than the impact in the private cloud. As the cloud services have been built over the internet, any issue that is related to internet security will also affect the cloud services. Resources in the cloud are accessed through the internet; consequently even if the cloud provider focuses on

security in the cloud infrastructures, the data is still transmitted to the users through the internet network which may be insecure. As a result, the impact of internet security problems will affect the cloud. The technology used in the cloud is similar to technology used in the Internet. Encryption techniques and secure protocols are not sufficient to assist data transmission in the cloud.

3.2 Security Issues in Single Cloud:

Data Integrity:

One of the most important issues related to cloud security risks is data integrity. The stored data in the cloud storage may suffer from any damage occur during transition operations from or to the cloud storage provider. The risk of attacks from both inside and outside the cloud provider exists and should be considered. Data authentication assures that the returned data is the same stored data is extremely important.

Data Intrusion:

Another issues related to cloud security risks is data intrusion. If anyone gains access to a password, then they will be able to access all of the account's instances and resources. In addition, the stolen password allows the hacker to erase all the information inside the instance for the stole user account, modify it or even disable its services. There is a possibility for the user's email to be hacked and hacker may still be able to log in to the account after receiving the new reset password.

Service Availability:

Another major concern in cloud service is service availability. Amazon mentions in its licensing agreement that the unavailability of the service may occur in the Amazon Company. The user's web service may terminate for any reason at any time if any user's files break the cloud storage policy. In addition, if any damage occurs to any Amazon's web service and the service fails, in this case there will be no compensation from the company regarding this failure. Garfinkel argues that information privacy is not guaranteed in Amazon S3. Companies seek to protect their services from system failure to avoid the unavailability of any related service to the cloud providers such as backups or disconnection to any dependent cloud providers.[12]

IV. WHY MOVING TO MULTI-CLOUDS

The migration of cloud computing from single toward multi-clouds to ensure the security of user's data is extremely important. The term "multi-clouds" is similar to the terms "intercloud" or "cloud-of-clouds" that were introduced by Vukolic.[13] Moving from single cloud to multi-clouds is reasonable and important for many reasons. According to Cachin et al.[14] "Services of single cloud are still subject to outage". Vukolic assumes that the main purpose of moving to multi-clouds is to improve what was offered in single cloud by distributing the realibitiy, trust and the security among multiple cloud providers.

Table 1: Comparison between Single cloud / Multi cloud

	Data Integrity	**Data Intrusion**	**Service Availability**	**Data Status**	
				Safe	**Lost**
Single cloud	If data hacked?	If password hacked?	If system down?	No	Yes
Multi cloud	If data hacked from one Cloud service provider?	If password hacked from one Cloud service provider?	If one cloud down?	Yes	No

V. PROPOSED MODEL

We propose a new model called Multi-clouds Database (MCDB). Multi-clouds Database Model ensures security and privacy in cloud computing environment and is based on multi-clouds service providers and the secret sharing algorithm. MCDB provides "cloud database" which permit customers with different types of database queries such as aggregation and exact match and range query with the ability to store any different types of data such as video, pictures or documents. The purpose of the proposed new model is to avoid the risk of malicious insider in the cloud and to avoid the failing of cloud services. The security risks such as data integrity, data intrusion and service availability will be examined in the model.

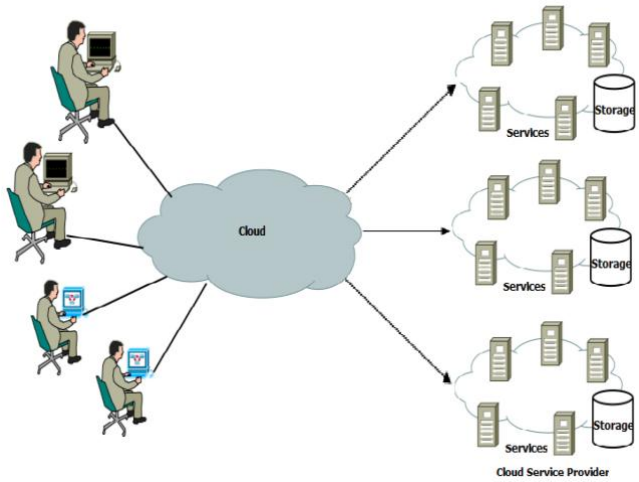

Figure 4. Multi-Cloud Storage in Cloud Computing

As a result of the three above arguments for data integrity, data intrusion and service availability, our newly proposed MCDB model is better in addressing the three security factors than in Single cloud service and more secured in protecting user's data from untrusted cloud service providers and from the malicious insider especially when single cloud service ask the users to encrypt their data before storing it in their instance, whereas, MCDB take responsibility of this task. Table 3 summarize the differences between Single Cloud and Multi-cloud Database Model in terms of the three security factors that may occur in cloud computing environment.

VI. CONCLUSION

It is clear that although the use of cloud computing has increased rapidly; cloud computing security is 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. The loss of service availability has caused many problems for a large number of customers recently. Data intrusion leads to many problems for the users of cloud computing. The purpose of this work is to propose a new model called Multi-Cloud Database Model (MCDB) instead of single cloud. The aim of this model is to reduce the security risks occurs in cloud computing environment.

ACKNOWLEDGEMENT:

The making of the paper needed co-operation and guidance of a number of people. We therefore consider it our prime duty to thank all those who had helped us for making it successful. It is our immense pleasure to express our gratitude to Dr. Atul Patel (Principal of CMPICA, CHARUSAT) as a guide who provided us constructive and positive feedback during the preparation of this paper. Last but not least, we are thankful to our friends and library staff members whose encouragement and suggestion helped us to complete our seminar. We are also thankful to our parents.

REFERENCES:

[1] B.I.Hacig, C.Li and S.Mehrotra, Executing SQL over encrypted data in the database-service-provider model, Procedings of the 2002 ACMSIGMOD international conference on Management of data, ACM, Madison, Wisconsin 2002, pp. 216-227
[2] S. Subashini and V.Kavitha, A survey on security issues in service delivery models of cloud computing, Journal of Network and Computer Applications (2011), pp-1-11.
[3] Amazon, Amazon Web Services. Web services licensing agreement, (2010)
[4] "The Internet Cloud". The Standard. Retrieved 2010-08-22.
[5] Csrc.nist.gov/groups/SNS/cloud-computing/cloud-computing-v25.ppt
[6] (http://csrc.nist.gov/groups/SNS/cloud-computing/cloud-def-v15.doc)
[7] S. Akioka and Y. Muraoka, HPC benchmarks on Amazon EC2, IEEE, 2010, PP. 1029-1034
[8] L.M.Kaufman, Data security in the world of cloud computing, IEEE security & Privacy(2009), pp. 61-64
[9] M. Vukolic The Byzantine empire in the intercloud, ACM SIGACT News, 41 (2010), pp. 105-111.
[10] C. Cachin, I. Keidar and A. Shraer, Trusting the cloud, ACM SIGACT News, 40(2009), pp. 81-86
[11] H. Mei, J. Dawei, L. Guoliang and Z. Yuan, Supporting Database Applications as a Service, Data Engineering, 2009 ICDE '09. IEEE 25th International Conference on, 2009, pp. 832-843.
[12] S.L. Garfinkel, Email-based identification and authentication: An alternative to PKI?, IEEE Security and Privacy (2003), pp. 20-26
[13] M. Vukolic The Byzantine empire in the intercloud, ACM SIGACT News, 41 (2010), pp. 105-111.
[14] C. Cachin, I. Keidar and A. Shraer, Trusting the cloud, ACM SIGACT News, 40 (2009), pp. 81-86

