International Journal of Research Studies in Science, Engineering and Technology [IJRSSET]
Volume 1, Issue 4, July 2014, PP 29-35
ISSN 2349-4751 (Print) & ISSN 2349-476X (Online)

Security with Multiclouds

Ms. S. M. Bansode

Assistant Professor CSE department
SGGSIET, Nanded

Abstract: *cloud boon is on with Security fear in minds. Users are worried about attacks on the integrity, confidentiality and the availability of their important data in the cloud. Malicious insiders in the cloud and outsiders could also pose side channel attacks.[2,3,7].This paper focuses on the issues related to the data security and privacy aspects in cloud computing, such as data integrity, data intrusion, service availability as well as side channel attack. It describes a Multi-clouds Database Model (MCDB)[5] which is based on Multi-clouds service providers instead of using single cloud service provider. In addition, it will discuss and present the architecture of the proposed MCDB model and describe its components and layers and its use to mitigate the side channel attack on the virtual instance of user.*

Keywords: *Cloud computing, single cloud, multi-clouds, cloud storage, data integrity, side channel attack.*

1. INTRODUCTION

Use of computers and huge database is increasing day by day. Organizations are in need of huge storage and processing of this data which creates a need to have a hassle of maintaining the data in terms of time as well as money. Cloud as storage, service and infrastructure satisfy the requirement but pose security threats from outsiders as well as insiders of the cloud[2,3]. Security in cloud is considered to be the most critical issue in cloud computing environment due to the valuable stored information for users in the cloud. Cloud providers should address privacy and security issues. This paper proposes a new model MCDBDI with existing Multi-clouds Database Model (MCDB)[6] which uses Multi-clouds service providers instead of using single cloud and distributed instance(DI).

The purpose of the proposed new model MCDBDI is to address the security and the privacy risks challenges in cloud computing environment and the side channel attacks.

There are four security factors that will be examined in proposed model, namely data integrity, data intrusion, service availability and side channel attack.

The remainder of this paper is organized as follows. Section II discusses an example of single cloud service providers. Section III describes the security risks in cloud computing with the advice of moving towards multi-clouds. Section IV describes the MCDB model with a thorough data flow explanation and proposes MCDBDI. Section V concludes the paper.

2. RELATED WORK

This section presents an example of single cloud to compare it with MCDB model. In addition, it mentions about Shamir's secret sharing algorithm which have been used in this model.

A.**Cloud Computing:** Cloud computing consist of three components such as Infrastructure as a service(IaaS), platform as a service (PaaS), and software as a service (SaaS)[1]. Amazon web service is an example of IaaS, GoogleApps is an example of PaaS and the Salesforce.com CRM application is an example of SaaS.

B.**Single Cloud** Provider 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. Amazon produced the Amazon Elastic compute cloud (EC2) as a cloud service to allow users to purchase computational resources, without the need to have significant technical background to deal with the cloud computing environment. Users can focus on their own application instead of maintaining the cloud environment software and hardware. Amazon EC2 is a virtual machine that provides users with a super computer equivalent without the need to purchase it. The cost of renting the services of a cloud service provider

(as-you-go) is cheaper than purchasing a super computer for the same purpose. Because of Amazon EC2 instances are virtual machines, so they do not have the ability to backup the changes on disks, hence the changes on the virtual disk are lost when the instance is shut down. Therefore, in order to save modifications, the user should save them in Amazon Simple Storage Service (S3). Public cloud services for data storage, such as S3 in Amazon, provide customers with dynamic and scalable storage services. The public cloud protects the user from the cost of purchasing hardware and software for their storage infrastructure; instead, they pay a cloud service provider.

3. SECURITY IN CLOUD COMPUTING

This section discusses the security risks of cloud computing. Movement from single cloud towards multi-clouds [5] is discussed.

A. Security Risks

Cloud providers can offer benefits to users, but security risks is a major issue for users. Moving databases 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. Cloud itself is built on internet. The security issues in internet are greatly inherent to the public cloud than the private cloud. Encryption techniques and secure protocols are not sufficient to assist data transmission in the cloud. Data intrusion of the cloud through the Internet by hackers and cybercriminals needs to be addressed and the cloud environment needs to be secure and private for clients [5,8].

B. Multi-Clouds

Cloud security issues could be resolved to some extent by using multi-clouds.

4. PROPOSED MODEL

In this section, Multi-clouds Database (MCDB) is discussed [6]. MCDB ensures security and privacy in cloud computing environment and

is based on multi-clouds service providers and the secret sharing algorithm.

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, intrusion availability and side channel attack will be examined.

A.Multi-Clouds Database Model

Figure 1 illustrates the general overview [5] of cloud computing environment. Part A represents the client side, which sends data inquiries to server or instance such as in Amazon in cloud service provider (CSP) in part B. The data source in part B stores the data in the cloud side which is supposed to be a trusted cloud, additional to ensuring the privacy of any query that the client has made and for the security of the client stored data. A problem occurs when we cannot guarantee cloud is a trusted service.

Figure 2. Is General Overview of Multi-Clouds. MCDB provides cloud with database storage in multi-clouds service provider which is different than Amazon cloud service. MCDB model (see Figure 2)does not preserve security by single cloud; rather security and privacy of data will be preserved by applying multi shares technique [5] on multi-cloud providers. By doing so, it avoids the negative effects of single cloud, reduces the security risks from malicious insider in cloud computing environment, and reduces the negative impact of encryption techniques. MCDB preserves security and privacy of user's data by replicating data among several clouds and by using the secret sharing approach. It deals with the database management system DBMS (data source) to manage and control the operations between the clients and the cloud service providers (CSP). Table 1 describes each component in the proposed model. Dividing data depend on the number of CSP to store it is considerd the main factor in the secret sharing approach.

A.Multi-Clouds Database Model

MCDB preserves security and privacy of user's data by replicating data among several clouds by using secret sharing approach. It deals with database management system DBMS (data source) to manage and control the operations between the clients and the cloud service providers (CSP). Table 1 describes each component in the proposed model. Dividing data depend on the number of CSP to store it is considered

the main factor in the secret sharing approach. Amozon Ec2 offers its instance to users. Malicious attackers could use these instances to leak the information with side channel attack. Such side channel attack poses great threat to the users as these attacks are not noticeable to the users neither to the service providers. The attacks considered require two main [6] steps: placement and extraction. Placement refers to the adversary arranging to place their malicious VM on the same physical machine as that of a target customer. Using Amazon's EC2 as a case study, T. Ristenpart demonstrated that careful empirical "mapping" can reveal how to launch VMs in a way that maximizes likelihood of an advantageous placement.

Having managed to place a VM co-resident with the target, the next step is to extract confidential information via a cross-VM attack.

While there are a number of avenues for such an attack, in this paper focus is on side-channels: cross-VM information leakage due to the sharing of physical resources (e.g., the CPU's data caches).

Component	Description
Browser	End user's web browser is responsible for displaying user interface
HTTP Server	HTTP server is responsible for managing the communication between the application and the browser. The user interface is generated by the execution from the application for server side logic.
Servlet Engine	The Servlet Engine communicates with the data source through the JDBC protocol.
(Data Source) DBMS	DBMS is responsible for rewriting the user's query (one for each CSP), generating polynomial values (polynomial values are not stored at the data source but are generated at the data source at the beginning and end of query processing), handling the user's query to each CSP and then receiving the result from CSP.
CSP Data Storage	CSP is responsible for storing the data in its cloud storage (like S3 in Amazon), that is divided into n shares and then returning the relevant shares to the DBMS that consists of the user's query result.

B. The MCDB Layers MCDB contains three layers [5] (Table 2): the presentation layer, the application layer, and the data management layer. The presentation layer contains the end user's browser and HTTP server. The management layer consists of the Database Management System (DBMS) and the database service provider. DBMS communicates with the Servlet Engine through the JDBC protocol. Communication between components is through a secured private high speed network that uses secure protocols.

C. The MCDB Model Data Flow

This section will discuss the data flow for the MCDB model and shows the procedure of sending the data to the DBMS and how the users can run queries through the model in secure and private way. In addition, it describes how DBMS manages the data and divides them into shares and distributes shares into separate instances in different CSP.

Sending Data Procedure

As can be seen in Figure 2, a user sends a query by using a user interface and a web browser through an HTTP request. The HTTP server plays a major role in communication between the web browser and the application. After that, the user's query will be sent from the HTTP server to a Servlet Engine by an application request. Hereafter, the communication between the Servlet Engine and the DBMS is done by a JDBC protocol. When the query arrives at the data source, the DBMS will manage the query and send it to the CSP. After the result of the query is returned to the DBMS, the DBMS returns the query result to the

Engine and then the HTTP server return the result of the query to the user interface again. The benefit for the HTTP server is the communication between the two components: the user browser and the Servlet Engine.

• Procedure between DBMS and CSP

In this section, we describe the data flow from DBMS to the multi-cloud providers in model MCDB. DBMS divides the data into n shares and stores each share in a different CSP (see Figure 2). After that, the DBMS generates a random polynomials function in the same degree for each value of the valuable attribute that the client wants to hide from the un-trusted cloud provider.

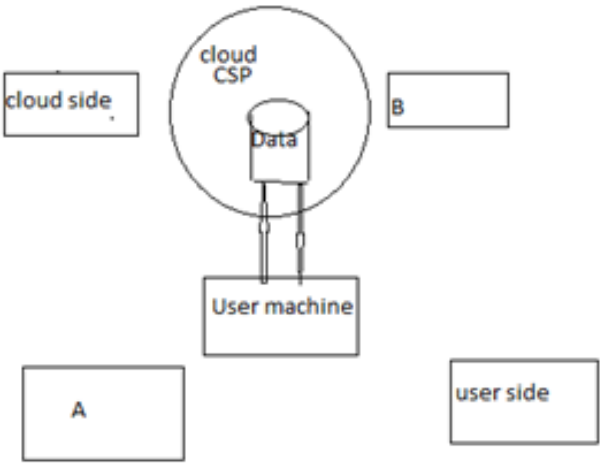

Fig 1. *Genaral overview of user/cloud Model*

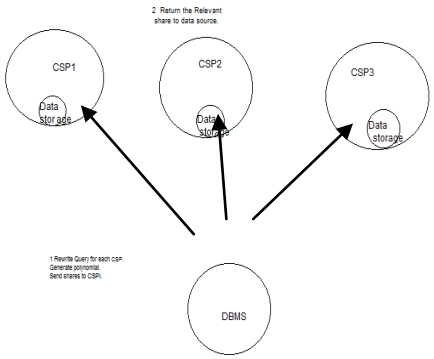

Figure 2. *General overview of multiclouds*

The polynomials are not stored at the data source but are generated at the front (when the query received from user at DBMS) and the end of the query processing (when the value is retrieved from CSP) at the data source. When a user's query arrives at the data source. When a user's query arrives at the DBMS, the DBMS To find share(2000,1), data source D first generates polynomials for the secret value salary 2000 and the position for the value in the share p2000(xi). After retrieving the relevant rewrites n queries one for each CSP and the relevant share will be retrieved from CSP. For example, the rewritten query for CSP1 retrieves

Table 2. *The MCDB Layers*

Layer Name	Component
Presentation	User
Application	HTTP servelet Engine server
Management	DBMS data source

all workers whose salary is share(2000,1) where the secret value is the salary 2000 and the cloud service provider is CSP1. To find share (2000,1), data source D first generates polynomials for the secret value salary 2000 and the position for the value in the share p2000(xi). After retrieving the relevant tuple from CSP, D computes the secret value to send to the client through the secured and private network. The secret sharing method can be applied to execute different types of query such as exact match, range, and aggregation query.

A.MCDB Scenario

In our proposed model, DBMS divides the data that the user wants to hide from the un-trusted Cloud provider into n shares or clusters. After dividing the data (assuming the data is a numeric value, for example, worker's salary) into 3 shares and storing them in different CSPs, the DBMS generates random polynomial functions with degree at the same level, one for each worker's salary in the WORKER table with the actual salary as the constant part of the function. These values will then be stored in different CSP. For this scenario, the value of n = 3 and k= 2. In addition, the DBMS uses the secret information X values (x1=3, x2=1, x3=2) to create the secret value. The polynomial for salaries {1000, 2500, 2900, 3000, and 3200} would be: q1000(x) = 100x +1000; q2500(x) =5x +2500; q2900(x) = x +2900; q3000(x) = 2x +3000; and q3200(x) = 4x +3200. If x1 is applied in polynomials, the value of salary 1000 will be stored as 1300 at CSP1 and stored as 1100 at CSP2 and stored as 1200 at CSP3. At this stage, the user's query should have arrived at the DBMS and DBMS should rewrite the query again to retrieve the result from the relevant share from CSP. Then, DBMS computes the secret value to send it to the client. The numeric attribute data type is considered in the secret sharing approach. Therefore, to represent a non-numeric attribute it is converted into a numeric attribute to apply a converted attribute to the schema. In other words, any word consists of 27 possible characters which are enumerated (*=0, A=1, B=2, C=3..., Z=26). In our scenario, if the user wants to query the suburb for a certain worker living in "Reservoir", the value of the address will be converted to a numeric value as (185195182215918) and will execute the polynomial functions on this value before it is stored in CSPs.

B Distributing the instance on multi clouds

It is discussed that the database is distributed over the number of clouds. Now we discuss the instance distribution. After the distribution of data on say three clouds user would have the VMs distributed on those clouds As in Figure. This would make the side channel attack difficult to the attacker. Attacker has to check where the user has got instance of VM. Even with this scheme if the attacker is able to get co-residence to the VM instance of user attacker may not be able to get access to whole data of the user instance as the user have three VM instances working together. Knowing the different clouds and the VM instance of user where this instance is located is a difficult task for the attacker. **What Makes MCDBDI Different?**

Our proposed MCDBDI model differs from Amazon cloud service in the following three security factors:

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. For example the data integrity has been recently compromised in Amazon S3 where users suffered from data corruption. Garfinkel argues that information privacy is not guaranteed in Amazon S3. Data authentication assures that the returned data is the same stored data is extremely important. Garfinkel claims that instead of following Amazon's advice that organizations encrypt data before storing them in Amazon S3, organizations should use HMAC technology or a digital signature to ensure data is not modified by Amazon S3. These technologies protect users from Amazon data modification and from hackers if they have stolen their email or password. However, as explained before, the proposed MCDB model used multi-clouds which is different from the Amazon cloud service. In addition, the use of Shamir's secret approach makes MCDB different. For example, the data will be distributed into three different cloud providers in MCDB model. In addition, the secret sharing algorithm will be applied on the stored data in the multiple cloud providers. If the intruder or malicious insider wants to know the hidden information inside the cloud, they should retrieve at least three values from three different cloud service providers to be able to know the real value which has been converted and hidden before it stored at the multiclouds providers. This depends on Shamir's secret sharing algorithm with a polynomial function technique which claim that, if there are 3 shares stored in 3 cloud providers (n=3, k=2), knowledge of the value of 2 shares or less makes the secret un-constructible whereas the knowledge of the value of more than two shares will enable the value to be reconstruct. Therefore, MCDB model is superior to Amazon cloud service in addressing the issue of data integrity.

• **Data Intrusion** According to Garfinkel, another security risk that may occur with a cloud provider, such as the Amazon cloud service, is a hacked password or data intrusion. If anyone gains access to an Amazon account 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 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 for a discussion of the potential risks of E-Mail), 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. However, MCDB model is different from the Amazon cloud service. MCDB replicates the data among three different cloud providers; hackers need to retrieve all the information from the three cloud providers to be able to reconstruct the real value of the data in the cloud. In other words, if the hacker hacked one cloud provider's password or even two cloud provider's passwords, they still need to hack the third cloud provider (in our case) to know the secret which is the worst and the hardest case scenario. Hence, replicating data into multi-clouds by using a multi share technique may reduce the risk of data intrusion such as in MCDB model and different than Amazon the single cloud.

• **Service Availability** Another major concern in cloud services 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 Amazon Company regarding this failure. 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. Garfinkel argues that information privacy is not guaranteed in Amazon S3. Data authentication assures that the returned data is the same stored data is extremely important. However, MCDB is different from Amazon cloud service in relation to service availability risk or loss of data. MCDB distributed the data into different cloud providers and therefore it could be argued that the data loss risk will be reduced.

If one cloud provider fails, users can still access their data live in other cloud providers. According to other research, to ensuring backup even if instances are down Garfinkel advices users to run their services on multiple instances in Amazon EC2 and storing data in multiple Amazon S3, then link different Amazon Web Services (AWS) to different email's addresses. But what will happen if Amazon decided to delete user's data for any reason from their all instances depend on their web service licensing agreement (WSLA). Therefore, using multiple cloud service providers in MCDB model may reduce the risk of loss of data.

As the data is spread on more than one cloud by using polynomial function malicious attacker will not be able to have the access to the instance. If the attacker is able to get the access to one of the instance as the data is spread over the number of clouds partial data available in one As a result of the three above arguments for data integrity, data intrusion, and service availability, MCDB model is better in addressing the three security factors than in Amazon cloud service and more secured in protecting user's data from untrusted cloud service providers and from the malicious insider especially when Amazon cloud service ask the users to encrypt their data before storing it in their instances, whereas, MCDB take responsibility of this task.

Side channel attack

As the data and the VM instance are distributed over number of clouds. Attacker may not be able to do any side channel attack.

5. 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. 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 propose a new model with existing MCDB system which use multi-clouds providers instead of single cloud. This model is helpful to cope with side channel attacks in addition to, dealing with other security issues of privacy, integrity.

REFERENCES

[1] Michael Armbrust,Armando Fox,Rean Griffith,Anthony D. Joseph,Randy H. Katz,Andrew Konwinski,Gunho Lee,David A. Patterson,riel RabkinIon Stoica, Matei Zaharia Above the

Clouds: A Berkeley View of Cloud Computing Technical Report No. UCB/EECS-2009-28 http://www.eecs.berkeley.edu/Pubs/TechRpts/2009/EECS-2009-28.html February 10, 2009

[2] L. M. Kaufman, Data security in the world of cloud computing, IEEE Security & Privacy (2009), pp.61-64.

[3] Bernd Grobauer, Tobias Walloschek, and Elmar Stöcker Siemens Understanding Cloud Computing Vulnerabilities IEEE COMPUTER AND RELIABILITY SOCIETIES 1540-7993/11/$26.00 © 2011 IEEE MARCH/APRIL 2011

[4] Alok Tripathi IT DivisionAbhinav Mishra Cloud Computing Security Considerations Guidelines on Security and Privacy in Public Cloud Computing Wayne Jansen Timothy GranceDraf t NIST Special Publication

[5] Amandeep Verma and Sakshi Kaushal Cloud Computing Security Issues and Challenges:A Survey ACC 2011, Part IV, CCIS 193, pp. 445–454, 2011

[6] Mohammed A. AlZain, Ben Soh and Eric Pardede Department of Computer Science and Computer Engineering, La Trobe University, Bundoora 3086, Australia. MCDB: Using Multi-Clouds to Ensure Security in Cloud Computing 2011 Ninth IEEE International Conference on Dependable, Autonomic and Secure Computing

[7] T. Ristenpart, E. Tromer, H. Shacham and S.Savage, Hey, you, get off of my cloud: exploring information leakage in third-party compute clouds,ACM, 2009, pp. 199-212.

[8] 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.

[9] H. Takabi, J. B. D. Joshi and G. Ahn, Security and Privacy Challenges in Cloud Computing Environments, Security & Privacy, IEEE, 8 (2010),pp. 24-31.