A Secure Strategy using Weighted Active Monitoring Load Balancing Algorithm for Maintaining Privacy in Multi-Cloud Environments

Ms. T. Sivasankari
PG Student
Department of Computer Applications
IFET College Of Engineering

Mr. S. Sivasankaran
Senior Assistant Professor
Department of Computer Applications
IFET College Of Engineering

Abstract

Cloud Computing is the latest technology that is used by any organizations in this competitive world. As many organizations are using cloud computing, the major issue that has risen is security. In single cloud there are many security issues and the possibility of malicious insiders is also high. But in multi clouds the security issues has become less for the users and for the people in the research group. As the multi clouds provide the solutions rose in the security of a Single cloud the movement towards multi clouds is increased. The multi cloud deals with the security issues like data integrity, data intrusion and service availability in the cloud. Even though we cannot assure complete security in the multi-clouds. This is because if the hacker attacks the server which is related to the multi cloud environment he can easily hack our valuable information. In this Paper concentrate public cloud and also achieve the Load Balancing using WAM (Weighted Active Load Monitoring)Load Balancer Algorithm. The multi -cloud motivates the need for effective cloud security counter measures. The basic underlying is to use multiple distinct clouds at same time to mitigate the risk of malicious data manipulation, disclosure and process tempering. a typical way of database splitting is pseudonymization , one provider receives the data with some key fields(typical personal identification data link, address) replaced by a random identifier, and the second provider receives the mapping of the identifier to the original information. This work aims to promote the use of multi-clouds due to its ability to reduce security risks that affect the cloud computing user.

Keywords: Cloud computing, single cloud, multi cloud, public cloud, cloud storage, data integrity, data intrusion, service availability

I. INTRODUCTION

The use of cloud computing has increased rapidly in many organizations. As many organizations are using cloud computing, the major issue that has risen is security.

Dealing with "Single cloud" providers is becoming less popular with customers due to potential problems such as service availability failure and the possibility that there are malicious insiders in the single cloud. In recent years, there has been a move towards "Multi-clouds", "inter-cloud" or "cloud-of-clouds".

This paper focuses on the issues related to the data security aspect of cloud computing. As data and information will be store in different database and protected the information from attackers or malicious insiders.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 discusses proposed weighted active monitoring load balancing algorithm. Section 5 analysis 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 6 current solutions of security risks. Section 7 will conclude the paper. Section 8 presents suggestions for future work.

A. Cloud Computing Phases:

Definitions of cloud is defined by many expert, but the National Institute of Standards and Technology (NIST) definition is a generally accepted standard: "Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (such as networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction."4 More simply, a cloud can be

considered to be a collection of hardware, software and other resources that can be accessed over the Internet, and used to assemble a solution on demand (that is, at the time of the request) to provide a set of services back to the requester.

When analyzed the definitions, there is a consensus on few key points; (1) Cloud Computing ensure on-demand access to a pool of computing resources, (2) dynamically scalable services, (3) device and media independency, and (4) easier maintenance of applications due to do not need to be installed on users' computers. Cloud computing should be elasticity and scalability. Figure (1) [5], adapted [4] shows six phases of computing paradigms, from dummy terminals/mainframes, to PCs, networking computing, to grid and cloud computing.

1) In phase 1, many users shared powerful mainframes using dummy terminals.
2) In phase 2, stand-alone PCs became powerful enough to meet the majority of users' needs.
3) In phase 3, PCs, laptops, and servers were connected together through local networks to share resources and increase performance.
4) In phase 4, local networks were connected to other local networks forming a global network such as the Internet to utilize remote applications and resources.
5) In phase 5, grid computing provided shared computing power and storage through a distributed computing.

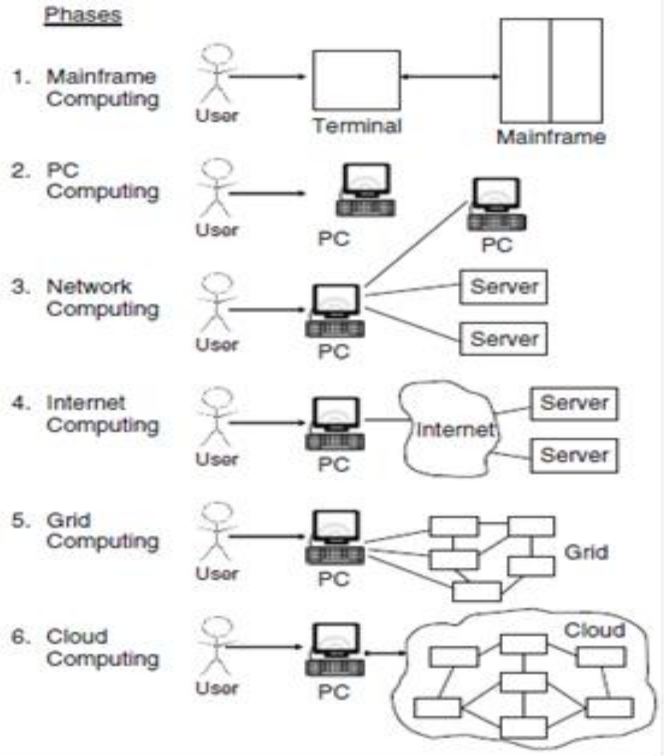

Fig. 1: Six computing paradigms

II. BACKGROUND

Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. Cloud Computing is "a model for enabling convenient, on demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services).

A. Cloud Computing Components:

There are five characteristics, three delivery models and four deployment models in cloud environment architecture. The five characteristics are On-demand self-service, Location independent resource pooling, Broad network access, Rapid Elasticity and Measured service.

The three delivery models are infrastructure as a service (IaaS), platform as a service (PaaS), and software as a service (SaaS). The deployment models are public, private, hybrid and community models.

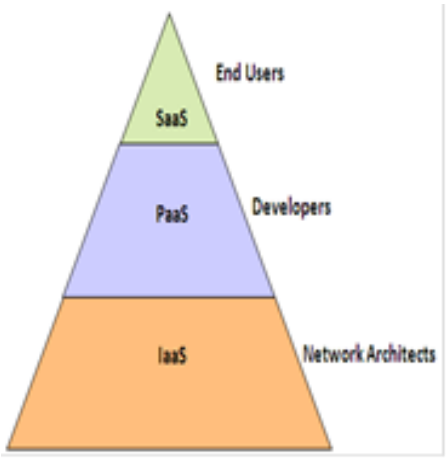

Fig. 2: Cloud computing service models

To understand the importance of cloud computing and its adoption, we must understand its principal characteristics, its delivery and deployment models, how customers use these services, and how to safeguard them. The five key characteristics of cloud computing include on-demand self-service, ubiquitous network access, location-independent resource pooling, rapid elasticity, and measured service, all of which are geared toward using clouds seamlessly and transparently.

In multiple unrelated cloud architecture we can find different servers which have their own authentication and proprietary services. The architecture consists of different cloud service providers which have their own domain. They constitute to form a multi cloud where multiple users can access their data at the same time. The drawbacks in a single cloud like data intrusion, service availability and data integrity can get overcome by using this architecture. Several clients can access their information stored in the cloud at any time without any time delay.

B. Cloud Service Providers Examples:

In the commercial world, various computing needs are provided as a service. The service providers take care of the customer's needs by, for example, maintaining software or purchasing expensive hardware. For instance, the service EC2, created by Amazon, provides customers with scalable servers. As another example, under the CLuE program, NSF joined with Google and IBM to offer academic institutions access to a large-scale distributed infrastructure.

There are many features of cloud computing. First, cloud storages, such as Amazon S3, Microsoft SkyDrive, or NirvanixCLoudNAS, permit consumers to access online data. Second, it provides computation resources for users such as Amazon EC2. Third, Google Apps or versioning repositories for source code are examples of online collaboration tools.

Cloud service providers should ensure the security of their customers' data and should be responsible if any security risk affects their Customers service infrastructure. A cloud provider offers many services that can benefit its customers, such as fast access to their data from any location, scalability, pay-for-use, data storage, and data recovery, protection against hackers, on-demand security controls, and use of the network and infrastructure facilities.

Reliability and availability are other benefits of the public cloud, in addition to low cost. However, there are also concerning issues for public cloud computing, most notably, issues surrounding data integrity and data confidentiality. Any customer will be worried about the security of sensitive information.

III. SECURITY RISKS IN CLOUD COMPUTING

Although cloud service providers can offer benefits to users, security risks play a major role in the cloud computing environment. Users of online data sharing or network facilities are aware of the potential loss of privacy. 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.

In SaaS, cloud providers are more responsible for the security and privacy of application services than the users. This responsibility is more relevant to the public than the private cloud environment because the clients need more strict security requirements in the public cloud.In addition, the path for the transmitted data can be also affected, especially when the data is transmitted to many third-party infrastructure devices.

As the cloud services have been built over the Internet, any issue that is related to internet security will also affect cloud services. Resources in the cloud are accessed through the Internet; consequently even if the cloud provider focuses on security in the cloud infrastructure, the data is still transmitted to the users through networks which may be insecure. As a result, internet security problems will affect the cloud, with greater risks due to valuable resources stored within the cloud and cloud vulnerability. The technology used in the cloud is similar to the technology used in the Internet. Encryption techniques and

secure protocols are not sufficient to protect 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.

We will address three security factors that particularly affect single clouds, namely data integrity, data intrusion, and service availability.

A. 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.

B. Data Intrusion:

Another security risk that may occur with a cloud provider, such as the cloud service, is a hacked password or data intrusion. If someone gains access to an 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.

C. Service Availability:

Another major concern in cloud services is service availability. The user's web service may terminate for any reason at any time if any user's files break the cloud storage policy.

IV. PROPOSED –WEIGHTED ACTIVE MONITORING LOAD BALANCING ALGORITHM

The 'Weighted Active Monitoring Load Algorithm' is implemented; modifying the Active Monitoring Load Balancer by assigning a weight to each VM as discussed in Weighted Round Robin Algorithm of cloud computing in order to achieve better response time and processing time. In this proposed Load balancing algorithm using the concept of weights in active monitoring, the VM are assigned varying (different) amount of the available processing power of server/ physical host to the individual application services. To these VMs of different processing powers; the tasks/requests (application services) are assigned or allocated to the most powerful VM and then to the lowest and so on according to its weight and its availability. Hence optimizing the given performance parameters.

A. Weighted Active Monitoring Load Balancer (Algorithm):

1) *Step 1:*

Create VM's of different Datacenter according to computing power of host/physical server in terms of its core processor, processing speed, memory, storage etc.

2) *Step 2:*

Allocate weighted count according to the computing power of the VM's in Datacenter. If one VM is capable of having twice as much load as the other, the powerful server gets a weight of '2' or if it can take four times load then server gets a weight of '4' and so on.
For example

- Host server with single core processor, 1GB of memory, 1TB of Storage space, 1000000 bandwidth will have weighted count=1
- Host server with 2 core processor, 4GB of memory, 2TB of Storage space and 1000000 bandwidth will have weighted count=2
- Host server with quard core processor, 8GB of memory 4TB of Storage space and 1000000 bandwidth will have weighted count=4 and so on..

3) *Step 3:*

Weighted Active VM Load Balancer maintains an index table of VMs, associated weighted count and the number of requests currently allocated to the VM. At start all VM's have 0 allocations.

4) *Step 4:*

When a request to allocate a new VM from the Data Centre Controller arrives, it parses the table and identifies the least loaded VM.

5) *Step 5:*

After identifying the least loaded VM's in different datacentres, it allocate requests to the most powerful VM according to the weight assigned. If there are more than one, the first identified is selected.

6) *Step 6:*

WeightedActiveVmLoadBalancer returns the VM id to the Datacenter Controller.

7) *Step 7:*

The Datacenter Controller sends the request to the VM identified by that id.

8) *Step 8:*

Datacenter Controller notifies the WeightedActiveVmLoadBalancer of the new allocation.

9) *Step 9:*

WeightedActiveVmLoadBalancer updates the allocation table increasing the allocations count for that VM.

10) *Step 10:*

When the VM finishes processing the request, and the Datacenter Controller receives the response cloudlet, it notifies the WeightedActiveVmLoadBalancer of the VM de-allocation.

11) *Step 11:*

The WeightedActiveVmLoadBalancer updates the allocation table by decreasing the allocation count for the VM by one.

12) *Step 12:*

Continue from step 4. The purpose of algorithm is to find the expected Response Time of each Virtual Machine because virtual machine are of heterogeneous capacity with regard to its processing performance, the expected response time can be found with the help of the following formulas:

Response Time = Fint - Arrt + TDelay (1) Where, Arrt is the arrival time of user request and Fint is the finish time of user request and the transmission delay can be determined by using the following formulas:

TDelay = T + T(2)latencytransfer Where, TDelay is the transmission delay Tlatency is the network latency and T transfer is the time taken to transfer the size of data of a single request (D) from source location to destination.

Ttransfer = D / Bwperuser (3) Bwperuser = Bwtotal / Nr (4) Where, Bwtotal is the total available bandwidth and Nr is the number of user requests currently in transmission. The Internet Characteristics also keeps track of the number of user requests in-flight between two regions for the value of Nr.

V. 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.

A. Multi-Clouds: Preliminary:

The term "multi-clouds" is similar to the terms "inter clouds" or "cloud-of-clouds" that were introduced by Vukolic. These terms suggest that cloud computing should not end with a single cloud. Recent research has focused on the multi-cloud environment which control several clouds and avoids dependency on any one individual cloud.

B. Analysis of Multi-Cloud Research:

Moving from single clouds or inner-clouds to multi-clouds is reasonable and important for many reasons; the main purpose of moving to inter clouds is to improve what was offered in single clouds by distributing reliability, trust, and security among multiple cloud providers.

C. Limitation of Multi-Cloud:

The multi cloud deals with the security issues like data integrity, data intrusion and service availability in the cloud. Even though we cannot assure complete security in the multi clouds. This is because if the hacker attacks the server which is related to the multi cloud environment he can easily hack our valuable information.

VI. CURRENT SOLUTION OF SECURITY RISKS

In my Project concentrate public cloud. The multi -cloud motivates the need for effective cloud security counter measures. The basic underlying is to use multiple distinct clouds at same time to mitigate the risk of malicious data manipulation, disclosure and process tempering. A typical way of database splitting is pseudonymization, and stored the database in different cloud location. one provider receives the data with some key fields(typical personal identification data link, address) replaced by a random identifier, and the second provider receives the mapping of the identifier to the original information. In order to reduce the risk in cloud storage, using cryptographic methods to protect the stored data in the cloud.

VII. CONCLUSION

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 my work is to the security risks and solutions. To ensure the security of the single cloud and cloud storage whereas multi-clouds have received less attention in the area of Security and Load Balancing.

VIII. FUTURE ENHANCEMENT

The use of computing resources as a delivered service is an important development in the world. At present Cloud Computing is a promising paradigm for delivering IT services as computing utilities. People around the world are making use of different cloud services provided by many companies. Security is the important factor that everyone thinks before choosing a cloud provider. The security issues can be solved by using multiple unrelated cloud architecture. Many users are provided with data security so that it may leads to the integration of many companies to form big cloud storage.

REFERENCES

[1] http://en.wikipedia.org/wiki/Cloud_computing
[2] NIST, http://www.nist.gov/itl/cloud/
[3] D. Agrawal, A. El Abbadi, F. Emekci and A Metwally, "Database Management as a Service: Challenges and Opportunities"
[4] H. Takabi, J.B.D. Joshi and G.-J.Ahn, "Security and Privacy Challenges in Cloud Computing Environment", http://ieeexplore.ieee.org
[5] C. Wang, Q. Wang, K. Ren and W. Lou, "Ensuring data security in cloud computing ARTCOM'10: Proc. Intl. Conf. on Advances in Recent Technologies in Communication and Computing, 2010.