INTERNATIONAL JOURNAL OF RESEARCH IN COMPUTER APPLICATIONS AND ROBOTICS
ISSN 2320-7345

A REVIEW ON CLOUD COMPUTING ISSUES AND CHALLENGES

Simran Kaur[1], P S Mann[2]

[1]Assistant Professor, Department of Electrical Engineering, DAVIET, Jalandhar,simran347@gmail.com
[2]Assistant Professor, Department of Information Technology, DAVIET, Jalandhar, psmaan@hotmail.com

Abstract

Cloud computing is one of the most exciting technologies because of its ability to reduce costs associated with computing while increasing flexibility and scalability for the user's processes. Cloud Computing generally incorporates combination of IaaS, SaaS and PaaS. With cloud computing, the users do not need to require all the applications, resources, and hardware or software platform to run its processes. Though there are enormous benefits, at the same time there are certain security risks associated with this technology. Some of the possible security attacks on clouds include: Denial of Service attack, Access control, Malware-Injection attacks, Flooding attacks etc. Providing Security to the Cloud is a major concern.

In this paper we have discussed various characteristics, system and deployment models along with the benefits of implementing cloud computing. Several solutions have been proposed to provide security to the users over cloud system, in accordance with the type of problem or the threat encountered.

Keywords: *Cloud Computing, IaaS, SaaS, PaaS.*

1. Introduction

According to National Institute of Standards and Technology's (NIST) Information Technology Laboratory [4] recognizes that cloud computing is an "evolving paradigm." As such, its definition attributes, and characteristics are still being debated by the public and private sectors, and are certain to continue to evolve in the near future. Nevertheless, initial steps have been taken toward constructing a universally accepted explanation of cloud computing key characteristics, as well as definitions for the various deployment and service models. These definitions have been widely reported but are worth repeating, particularly in a field that is still rapidly developing.

2. Cloud Characteristics

On-demand self service: A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service's provider.

Broad network access: Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, laptops, and PDAs).

Resource pooling: The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. There is a sense of location independence in that the customer generally has no control about location of the provided resources but may be able to specify location at a higher level of abstraction Examples of resources include storage, processing, memory etc.

Rapid elasticity: Capabilities can be rapidly and elastically provisioned, in some cases automatically, to quickly scale out, and rapidly released to quickly scale in. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be purchased in any quantity at any time.

Measured service: Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled, and reported providing transparency for both the provider and consumer of the utilized service.

3. Service Models

Cloud computing models [7] can be broken into three basic designs, which are shown here and described below.

Infrastructure as a service (IaaS)

The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, deployed applications, and possibly limited control of select networking components (e.g., host firewalls).

Software as a service (SaaS)

The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through a thin client interface such as a web browser (e.g., web based email). The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user specific application configuration settings. Factored Operating Systems (FOS) are designed to address the challenges found in systems, such as cloud computing and many core systems. Instead of simple exploitation of parallelism between servers, fos seeks to distribute and parallelize within a server for a single high level function In a cloud, the OS at the customer end is considered as the Virtual Machine (VM) and the application with a specific job or request is running as an instance in the provider's end.

Cloud Platform as a Service (PaaS)

The capability provided to the consumer is to deploy onto the cloud infrastructure consumer- created or acquired applications created using programming languages and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly application hosting environment configurations.

4. Deployment Models

Private cloud: The cloud infrastructure is operated solely for an organization. It may be managed by the organization or a third party and may exist on premise or off premise.

Community cloud: The cloud infrastructure is shared by several organizations and supports a specific community that has shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be managed by the organizations or a third party and may exist on premise or off premise.

Public cloud: The cloud infrastructure is made available to the general public or a large industry group and is owned by an organization selling cloud services.

Hybrid cloud: The cloud infrastructure is a composition of two or more clouds (private, community, or public) that remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load-balancing between clouds).

5. Issues and Challenges

Though cloud computing is on the verge of becoming a reality, there are several issues and challenges [1]. Some of the issues are given below:

- The data or knowledge Analytic servers may be processed outside the client's premises. So one needs to ensure the privacy of the data.
- Most of the Relational databases uses row based indexing however the analytics over cloud which accesses data on column at a time motivate one to opt for column oriented databases in place of row oriented databases.
- Even in case of failure at any node or server, Cloud should have capability to recover and progress in the event of one or more node failures.
- In many of the systems, the output of a query is most of the times incomplete due to poor quality of data. After adopting Cloud System, the data residing on multiple and highly distributed processing units creates poor data quality that may not be suitable for analytics.
- While working in the Cloud System, there should be more recent data on which the model built might stay invalid. Cloud can tackle this problem by reducing the cycle time between data availability and model generation.

Knowledge process can move from one active node in the cloud to the other, extracting enough knowledge from it. These knowledge instances learned need to be consolidated from time to time to infer Knowledge on the cloud.

6. Problems and Possible Solutions

The cloud system is running in the internet and the security problems[3] in the internet also can be found in the cloud system. The cloud system is not different the traditional system in the PC and it can meet other special and new security problems. The biggest concerns about cloud computing are security and privacy.

1. Data Leakage:

Innately, when moving to a cloud there is two changes for customer's data. First, the data will store away from the customer's local machine. Second, the data is moving from a single- tenant to a multi-tenant environment. These changes can raise an important concern that called data leakage. Data leakage[5] has become one of the greatest organizational risks from security standpoint.

Possible Solution: For mitigate effects of such problem there has been interested in the use of data leakage prevention (DLP) applications to protect sensitive data. Inherently, in SaaS and PaaS discovery of client's data with DLP agents is impossible except when the provider put ability of it to its service. However, it is possible embedding DLP agents into virtual. In private clouds, costumer has direct control over the whole infrastructure; it is not a policy issue whether DLP agents are deployed in connection with SaaS, PaaS,or IaaS services. But if data stored in a public cloud because of nature of it, using DLP products is valueless to protect the confidentiality of that data in all types of cloud.

2. Malware-Injection Attacks:

In a malware-injection attack, a malicious user attempts to inject malicious service or code, which appears as one of the valid instance services running in the cloud. If the attacker is successful, then the cloud service will suffer from eavesdropping. This can be accomplished via subtle data modifications to change the functionality, or causing deadlocks, which forces a legitimate user to wait until the completion of a job which was not generated by the user. The attacker takes his first step by implementing his malicious service in such a way that it will run in Iaas or SaaS of the cloud servers. This type of attack is also known as a meta-data spoofing attack.

Possible Solution

Usually when a customer opens an account in the cloud, the provider creates an image of the customer's

Virtual Machine in the image repository system of the cloud. The applications that the customer will run are considered with high efficiency and integrity. The Cloud system utilizes the File Allocation Table (FAT) system architecture, since its straightforward technique is supported by virtually all existing operating systems. From the File Allocation Table, the system know about the code or application that a customer is going to run by checking with the previous instances that had been already executed from the customer's machine to determine the validity and integrity of the new instance. So it is very difficult for an attacker to intrude in the IaaS level. For this purpose, we need to deploy a Hypervisor in the provider's end. This Hypervisor will be considered the most secured and sophisticated part of the cloud system whose security cannot be breached by any means. The Hypervisor is responsible for scheduling all the instances, but before scheduling it will check the integrity of the instance from the FAT table of the customer's VM.

3. Ddos Attacks Against Cloud/Flooding Attack Problem

Distributed Denial of Service (DDoS) attacks typically focus high quantity of IP packets at specific network entry elements. In cloud computing where infrastructure is shared by large number of clients, DDoS attacks make have the potential of having much greater impact than against single tenanted architectures. If cloud has not plenty resource to provide services to its costumers then this is may be cause undesirable DDoS attacks. Solution for this event is a traditional solution that is increase number of such critical resources. But serious problem is when a malicious user deliberately done a DDoS attacks using bot-net.

Possible Solution

To prevent from the DDoS attacks, there is a purposed system in which organize all the servers in the cloud system as a group of fleet of servers. Each fleet of servers will be designated for specific type of job, for e.g, One will perform the function of Memory Management and other will handle file Systems another for core computation related jobs, etc. In this approach, all the servers in the fleet will have internal communication among themselves through message passing. So when a server is overloaded, a new server will be deployed in the fleet and the name server, which has the complete records of the current states of the servers, will update the destination for the requests with the newly included server. a Hypervisor can also be utilized for the scheduling among these fleets, determining the authenticity of the requests and preventing the fleets from being overloaded with bogus requests from an adversary. In this way the DDoS or flooding attack can be mitigated to an extent. Also, a PID can be appended in the messaging, which will justify the identity of the legitimate customer's request and be checked by the Hypervisor in the assignment of instances to the fleet of servers. This PID can be encrypted with the help of various approaches, such as implementing hash values.

4. Problem of Wrapping Attack:

When a user makes a request from his Virtual Machine through the browser; the request is directed to the web server. In web server, a SOAP message is generated which contains the structural information to be exchanged b/w the browser and server during the message passing. Before message passing occurs, the XML document needs to be signed. Also, the signature values should be appended with the document. Finally, the SOAP header should contain all the necessary information for the destination after computation is done. For a wrapping attack, the malicious user does its deception during the translation of the SOAP message in the TLS (Transport Layer Service) layer. Thus the body of the message is duplicated by the malicious user and sent to the server as a authenticated user. The server checks the authentication by the Signature Value (which is also duplicated) and integrity checking for the message is done. As a result, the adversary is able to intrude in the cloud and can run malicious code to interrupt the usual functioning of the cloud servers.

Possible Solution

In the purposed Solution, the security during the message passing from the web server to a web browser is achieved by using the SOAP message. Specifically, as the signature value is appended, by adding an redundant bit (STAMP bit) with the SOAP header. This bit will be toggled when the message is interfered with by a third party during the transfer. When it is received in the destination, the STAMP bit is checked first and if it is found toggled, then a new signature value is generated in the browser end and the new value sent back to the server as recorded to modify the authenticity checking.

5. Access Control Problem:

This is the most traditional and common approach to breach a user account. The user account and password are stolen by any means[6]. As a result, the stealing of confidential or private data or even the destroying of data can hamper the storage integrity and security of the cloud. The providers face the first strike of such kind of problem.

Possible Solutions

a) Digital ID: There must be a strong authentications and ID Management for both the cloud provider and the client. One of the ideas of access monitoring is to implement of Key Management for both client and the cloud service provider. A Digital ID, sometimes called a digital certificate, is a file on your computer that identifies who you are. Some software applications use this file to prove your identity to another person or computer. For Example, when we bank online, our bank must be sure that we are the correct person to get account information. Like a driver's license or passport, a Digital ID confirms your identity to the online bank. Applying it to cloud computing, it is very useful as far as the authenticity of the data is concern.

b) Temporary sessions: This is the concept, where a key pair is used to verify the authenticity of the customer, but this approach only needs the special number appended with the Username. There will be an overhead for sending e-Mail to all the customers with a randomly generated number when their session will expire within a specified limited time.

6. Illegal Update Problems:

The data stored in the cloud system can meet the problem of stolen and modified unlawfully. The confidential data will be treated outer people of company and the other people can access the data. Traditional techniques can protect user data privacy and security in cloud the environment to some extent. These technologies include encryption mechanism, security authentication mechanism and access control policy the data can be encrypted before stored in the cloud system. But when in case there is large amount of data it will difficult to encrypt whole data due to the more time need to compute the data which lowers the performance to a large extend.

Possible Solution

Once the data is stored in the cloud, the cloud provider is responsible for security but the monitoring and auditing for them become important problem. The cloud provider can transmit the customer data from the server to another server [2] and the user can not know the data storage place. The data storage and manipulation are related to the resources of cloud centre in cloud computing environment. The cloud computing services provided for customers are difficult to achieve full transparency. Customers do not understand internal processes of cloud computing and data storage location information. The communication of worms, virus and Trojan in cloud computing platform within the network of internal and external must be controlled. Malicious programs must be isolated promptly. Damage to the system must be repaired immediately. The data traffic in the cloud system and cloud computing system running status should be monitored in real time. The abnormal action of network and system must be detected and fixed timely. The network attack detection and defence system must be deployed in the cloud network.
Problem with this solution is that Customers should have the right of the supervision and audit of cloud computing services in order to fully ensure the security of customer data. The customers do not know what kind of situation data will meet if an accident occurs.

REFERENCES

1. Dean, J. and Ghemawat S., MapReduce, "Simplified Data Processing On Large Clusters", Communications Of The ACM - 50th Anniversary Issue, 2008, Volume 51, p107-113.
2. Liu W., "Research On Cloud Computing Security Problem And Strategy", 2nd International Conference, 2012, April 21-23, page-1216-1219.
3. Meena B., Challa K A, "Cloud Computing Security Issues With Possible Solutions", International Journal on Computer Science and Technology, 2012, Vol. 3, Issue 1, Jan- March, page 340-344.
4. Peter Mell,Timothy Grance, "The NIST Definition of Cloud Computing", NIST Special Publication, October 25, 2011, page 800-145.
5. Sabahi, F., "Cloud Computing Security Threats And Responses", Communication Software and

Networks (ICCSN), 2011, IEEE 3rd International Conference, May 27-29, page 245-249.

6. SeungHwan J.,Gelogo E. Y., Park B., International Journal of Control and Automation, 2012, Vol. 5, No. 1, March, page 63-70.

7. Shaikh F. B., Haider S, "Security Threats In Cloud Computing", 6th International Conference On Internet Technology And Secured Transactions, 2011, December, page 214-219.