International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Impact Factor (2012): 3.358

A Survey on Security Issues and Attacks in Cloud Environment

Varsha Narole[1], Anil Jaiswal[2], Narendra Narole[3]

[1] Research Scholar, GHRIETW, Nagpur, Maharashtra, India

[2]Assistant Professor, CSE, GHRIETW, Nagpur, Maharashtra, India

[3]Assistant Professor, ECE, PIET, Nagpur, Maharashtra, India

Abstract: ***Now a days Cloud Computing play an important role for provide the services and data storage in the internet. Cloud computing drive out the need of IT based companies to invest in high computing infrastructure and services used by them. In cloud, the data is dwell into set of networked resources that enable data to be accessed via virtual machines. These data canters are located in various parts of the world beyond the control and reach of the user, so there are multiple challenges and security issues that need to be addressed and understood. There are a number of different challenges to make safe cloud infrastructure from different types of attacks. This review paper aims to analyze and elaborate various security issues and attacks in cloud computing which is the base for our future roadmap.***

Keywords: Security architecture, privacy, cloud security

1. Introduction

The word 'cloud' makes buzz in distributed computing. It is one of the rapidly growing segments of IT industries because IT industry always wants : To increase the capabilities on the air without investing into the infrastructure, purchasing new software or training a new personnel. So the cloud computing comes into the existence. High convinience and low cost are the major benefits of cloud computing. “Cloud computing is a model for enabling ubiquitous, 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”[1]. Even though the concept of cloud computing is advancing now-a-days, the basic concept of resource sharing by multiple users is not new. The concept of cloud computing is emerged in 1950 with execution of mainframe computers, which were accessible via static machines. 1960s, was leading to the birth of IT Services industries and increased the demand for personal desktops. Evolution of client/server architecture, demand for high bandwidth was started in 1990s. Also, the telecommunication companies started offering virtual private network services. In 2000, the concept of virtualization was born and the IT infrastructure management started the concept of outsourcing, with hosted environment. Cloud computing is the result of these previous efforts. Beyond 2010, cloud computing as a service began and delivered IaaS, PaaS, SaaS, NaaS as shown in Fig. 1.

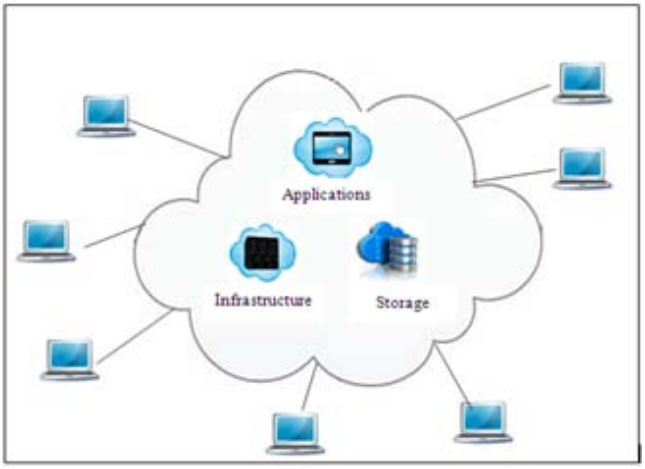

Figure 1: Scenario of Cloud Computing

A. Deployment Models

NIST classifies the deployment models based on accessability of clouds. Cloud can have Public access, Private access, Hybrid access and Community access.

- Public cloud : Service provider makes services and systems to be easily accessible to the public over the internet. but it may be less secure because of its openness.
- Private cloud : Service provider makes services and systems to be accessible whithin an organisation. It is highly secure because of its secure nature.
- Community Cloud : Service provider makes services and systems to be accessible by the group of organisations.
- Hybrid cloud : It is combination of two or more clouds of deployment models.

B. Service Models

NIST offered three types of services on cloud : Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Software as a Service (SaaS).

- Infrastructure as a Service (IaaS) : It provides several resources such as storage, virtual machines, network capacity except data centre infrastructure.

- Platform as a Service (PaaS) : It provides runtime environment for deployment, development , application on cloud server and allowed to use development tool to create their application
- Software as a Service (SaaS) : It allows the user to use deployed services on server.

C. Characteristics of Cloud Computing

As outlined by Mel and Grance [2], cloud computing has four major characteristics.

- On demand self service : Cloud computing allows the client to use resources and services at the time of their demand only.
- Pool of resources : Cloud service provider share the resources between multiple clients whenever they required.
- Broad network access : Cloud can be accessed from any where, any time.
- Rapid elasticity : Resources can be scale up or scale down at any time.

2. Attacks in Cloud based Environment

Considering the simplicity of cloud, most of the companies are moving towards the cloud environment. In order to gain trust in cloud computing, there is a need to assure the user of the security. Providing security is of atmost importance in cloud computing. The use of virtualization while implementing cloud infrastructure can provide security to the users or tenants. Virtualization is one of the important concept in cloud computing and it is a technique, which allows to share single physical instance of an application among multiple tenants or customers. This is done by assigning a logical name to a application/resource and providing a pointer to that physical application/resource when demanded.

There are different types of attacks made on the cloud infrastructure. The attackers aim at damaging the bandwidth, processing power and storage capacities of a cloud network. These different attacks can be: Denial of Service (DoS) attacks, cloud malware injection attack, authentication attack, attacks on the hypervisor, etc. We shall now discuss the attack on hypervisor which is known as VM escape.

A. VM escape

Virtual machines are encased and have a secluded environment. The operating system which is working in the virtual machine is completely unaware of their isolation. The virtual machine must be secured and protected, or else it can be breached by the attacker. There should be no way to breach out of the virtual machine and interact with the parent hypervisor. “VM escape”[10] is the process of breaking out of the virtual machine and interacting with the parent hypervisor as shown in Fig. 2. A hypervisor is also called as Virtual Machine Monitor. It is placed between the hardware and the guest operating system. The hypervisor manages the overall execution of the virtual machines.

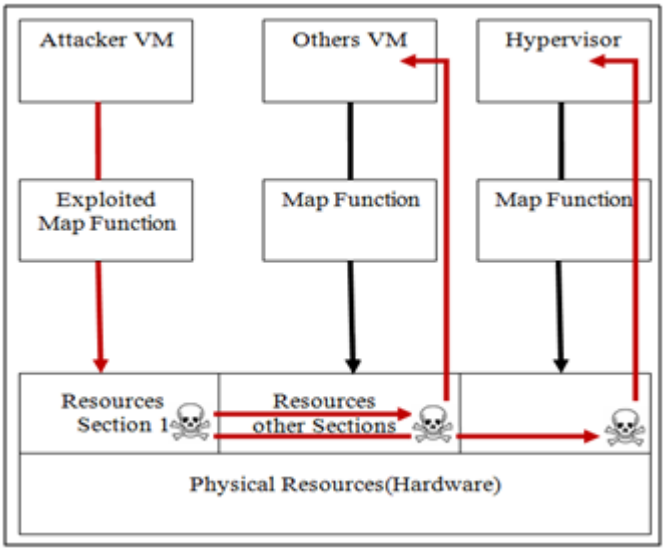

Figure 2: VM Escape

B. IP Spoofing

An intruder can use spoofing technique to break the security of the system. It tries to send data packets to the destination user while pretending the packets are sent from the original source. To make use of IP Spoofing[8], the attacker must first find a way to find the IP address of a trusted host and then spoof the packets, so that it appears as they are arriving from the host. The following figure illustrates a general scenario of IP Spoofing.

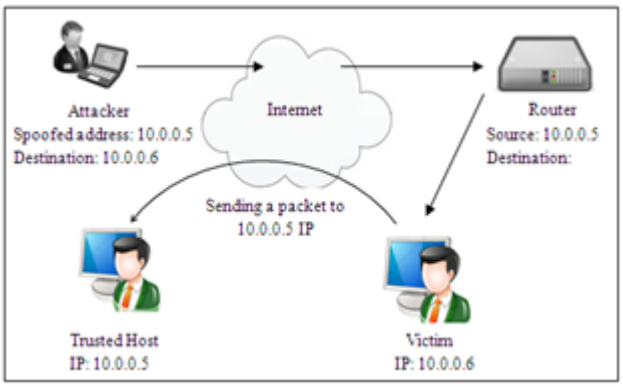

Figure 3: IP Spoofing

3. Related Work

Vijay Vardharajan , Udaya Tupakula[4] proposed Cloud Service provider provide the Infrastructure as a Service to the customer. Basically security of customer’s infrastructure is the responsibility of customer. In common the customer of cloud can run different applications and operating system in their virtual machine. The applications and operating system of the customers can be possibly enormous and complicated, so they may have some security vulnerabilities. This vulnerabilities possibly broken by an attacker and produce various types of attacks. These attacks targeted in opposition to the cloud infrastructure in addition to against other virtual machines belong to other customers. The Threat Model shown in Fig. 4 from[4]. These model shows the different types of attacks and attacker that can arise in the infrastructure as a service cloud environment.

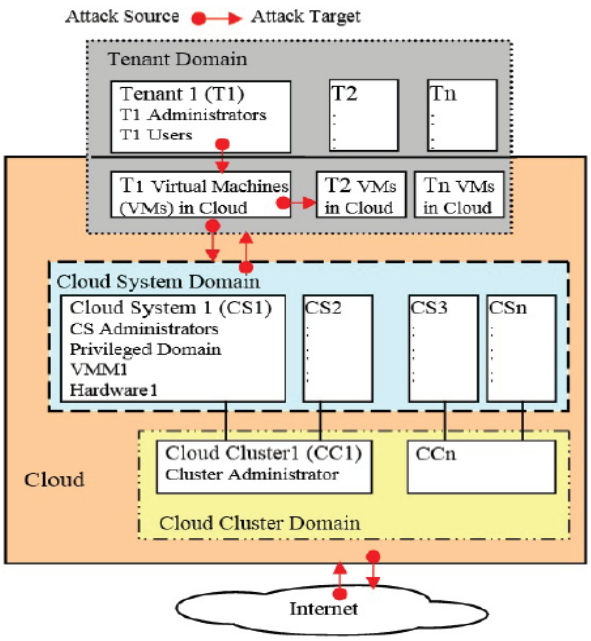

Figure 4: Threat Model

In fig 4 circle shows the source of the attack and target of attack shows by the arrow head. In this model there are three types of domains are used that is Tenant Domain, Cloud System Domain, and Cloud Cluster Domain. The tenant domain include tenant users and tenant administrators. The cloud system domain consist of virtual machine monitor platform and cloud system administrator. Then cloud cluster domain consist of cloud system domains that include the cloud infrastructure. The various types of attack can target on both the cloud infrastructure in addition to tenants. The paper introduced the Baseline Security service provide by the cloud provider to its customer to secure its infrastructure.

Deyan Chen, Hong Zhao [3] proposed that cloud computing has various prospective advantages and many enterprise applications and data are migrate to public or hybrid cloud. From the consumers' point of view cloud computing security relate, specially privacy protection and data security issues, stay behind the primary inhibitor for implementation of cloud computing services. Some issues are the openness of cloud and sharing virtualized resources by multi-tenant, user data may be accessed by unauthorized users.Accordingly the service delivery models of cloud computing, resources cloud services based on may be owned by multiple providers. As there is a variance of interest, it is complex to deploy a integrated security measures. The paper focused to design a set of united uniqueness management and privacy protection frameworks transversely cloud computing services or applications.

David Wetherall, Member,Anna Karlin, and Tom Anderson[5] proposed that IP Traceback technique is used for tracing unidentified packet flooding attack. Denial of service attacks expend the resources of network or remote host thereby corrupting or denying service to valid users. This attacks are difficult to prevent, simple to implement and difficult to trace. auther focused on Traceback problem it means basically identify the machines that produce attack traffic and the network path this traffic consequently follows.

Anat Bremler-barr ,Hanoch Levy[6] proposed that An intruder can use spoofing technique to break the security of the system. It tries to send data packets to the destination user while pretending the packets are sent from the original source. To make use of IP Spoofing, the attacker must first find a way to find the IP address of a trusted host and then spoof the packets, so that it appears as they are arriving from the host. Paper introduced a new approach called Spoofing Prevention Method is used for filtering spoofed IP packets. This method enable routers nearer to the destination of a packet to validate the accuracy of the source address of the packet.

Trieu C. Chieu, Ajay Mohindra, Alexei A. Karve and Alla Segal[7] proposed that Cloud computing provides a service to the users to access resources on-demand. But some attacks can show the way to increase of load on the customer virtual machine. In the proposed architecture the cloud provider monitors the active connections(load) on the customer web server and vigorously varies the number of virtual machines allocated to the customer. Paper used a scaling set-up to address the dynamic scalability of web applications on a virtualized Cloud Computing environment.

4. Comparative Analysis

There are various techniques which are proposed to avoid the attacks in cloud environment. Ingress filtering technique [4] proposed to deal with spoofing attack. Ingress filtering technique proposed to authenticate the source of IP packets. Additionally, Ingress filtering is not successful if the compromised host spoofs its source address with a valid address within the domain. We will propose egress filtering technique[6]. Along with egress filtering, the network operator makes setting to their routers to dribble any packet whose IP address is from unallocated address space . Reverse Path Forwarding feature [8], can be used to drop the packets whose source address is not mentioned in the forwarding table. Traceback security technique [5] also proposed for to avoid spoofing attack. This technique is used to determine the source of attacker traffic in the Internet. This feature can be added to the capabilities of the routers in two different ways. First is the way to involve stamping the traffic packets with a signature of the routers they pass through [9].

5. Conclusion

The rapid growth in cloud computing has also increased the security concerns related to cloud computing environment. Giving extra right for cloud service provider may also lead to security attack on tenant's data. So to provide best model to share and secure virtual machines over cloud is the need for secure cloud computing model. In this paper, we have discussed the basic concepts of cloud computing, different security and privacy issues in cloud environment, A survey on different cloud computing attacks is also described. We try to achieve a secure architecture for the cloud users as well as for cloud service providers, while benefiting both the entities.

References

[1] P. Mell and T. Grance, "The nist definition of cloud computing (draft)," NIST special publication, vol. 800, no. 145, p. 7, 2011.
[2] T. Grance and P. Mell, "The nist definition of cloud computing," National Institute of Standards and Technology (NIST), 2011.
[3] Deyan Chen, Hong Zhao'Data Security and Privacy Protection issues in Cloud Computing", International Conference on Computer Science and Electronics Engineering 2012.
[4] Vijay Vardharajan , Udaya Tupakula "Security as a Service Model for Cloud Environment" , IEEE TRANSACTIONS ON NETWORK AND SERVICE MANAGEMENT, VOL. 11, NO. 1, MARCH 2014.
[5] Stefan Savage, David Wetherall, Member, IEEE, Anna Karlin, and Tom Anderson "Network Support for IP Traceback", IEEE/ACM TRANSACTIONS ON NETWORKING, VOL. 9, NO. 3, JUNE 2001.
[6] Anat Bremler-barr , Hanoch Levy, "Spoofing Prevention method" , In Proc. IEEE INFOCOM 2005
[7] Trieu C. Chieu, Ajay Mohindra, Alexei A. Karve and Alla Segal, "Dynamic Scaling of Web Applications in a Virtualized Cloud Computing Environment". 2009 IEEE International Conference on e-Business Engineering.
[8] Cisco IOS, "Unicast reverse path forwarding," 1999.
[9] Stefan Savage, David Wetherall, Anna R. Karlin, and Tom Anderson, "Practical network support for IP traceback," in SIGCOMM, 2000, pp. 295–306.
[10] Wang Z, Jiang X, "HyperSafe: A Lightweight Approach to Provide Lifetime Hypervisor Control-Flow Integrity", proceedings of the IEEE symposium on Security and privacy. Washington, DC, USA: IEEE Computer Society. pp 380-395, 2010.