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

SURVEY ON THREATS ATTACKS AND IMPLEMENTATION OF SECURITY IN CLOUD INFRASTRUCTURE

[1]Diksha Nagpal, [2]Dr. Deepti Sharma

[1]Advanced Institute of Technology &Management, Palwal
[2]Associate Professor & Head, Advanced Institute of Technology &Management, Palwal,
Email: nagpal43@gmail.com, Email: deeptiguria@gmail.com
Author's Correspondence: C-3, 103, Gulmohar Enclave, Ghaziabad,(U.P) Pin-201001, Phone Number: 9873242710

Abstract: - Cloud computing is the buzz word of today. Many of the organizations are using cloud infrastructure due to which there is better utilization of resources and cost is also less. Cloud data centers are keeping this huge information making it reliable and scalable. Emergence of cloud computing helps in reducing the cost of implementation and improves better utilization of resources, which attracts many organizations to redesign their infrastructure to make compatible with cloud environment. To achieve security in cloud environment is a biggest challenge because many of the solutions are vulnerable. Security includes confidentiality, integrity and availability. This paper summarizes the various methods which are being followed for the security in cloud infrastructure which includes public key infrastructure, encryption and Shamir's secret sharing approach. Also, this paper focuses on use of Intrusion Detection Systems and challenges, various attacks on cloud .

Keywords: Cloud Computing, IDS, Attacks, Firewall, Encryption

1. INTRODUCTION

Cloud computing is trying to remove the problems of maintaining current infrastructures and operations so that companies can spend more time making them at success. It is also saving the companies tons of money, which will enable the employers to pay employees more, and it is having 100% up time so that the electricity never go out. It is also providing security that companies do not have to worry about security anymore because the cloud service providers are concerned about that.

Cloud computing has three basic abstraction layers i.e system layer (which is a virtual machine abstraction of a server), the platform layer (a virtualized operating system of a server) and application layer (that includes web applications) Hardware layer is not included as it does not directly offer to users. Cloud computing also has three

service models namely Platform as a Service (PaaS), Infrastructure as a Service (IaaS) and Software as a Service (SaaS) models. PaaS model facilitates users by providing platform on which applications can be developed and run.

IaaS deliver services to users by maintaining large infrastructures like hosting servers, managing networks and other resources for clients. SaaS model makes user worry free of installing and running software services on its own machines. Presently, Salesforce.com, Google and Amazon are the leading cloud service providers who extend their services for storage, application and computation on pay as per use basis. Since Cloud computing supports distributed service oriented paradigm, multi-domain and multi-users administrative infrastructure, it is more prone to security threats and vulnerabilities.

Currently the biggest hurdle in cloud adoption by most of the corporate organizations is its security. Due to its distributed nature, cloud environment has high intrusion prospects and suspect of security infringements.
Data, application and services non-availability can be imposed through Denial of Service (DOS) or Distributed Denial of Service (DDOS) attacks and both cloud service provider and users become handicap to provide or receive cloud services. For such type of attacks Intrusion Detection System (IDS) can be emplaced as a strong defensive mechanism.
This paper describes the various types of attacks threats and vulnerabilities that exist in the cloud world. Also, it aims at describing the security techniques that are applied in Cloud Infrastructure.

2.1 CLOUD COMPUTING ATTACKS

As more companies are moving to cloud computing, hackers also follow. Some of the potential attack vectors criminals may attempt include:

2.1.1 Denial of Service (DoS) attacks

When the Cloud Computing operating system notices the high workload on the flooded service, it will start to provide more computational power (more virtual machines, more service instances to cope with the additional workload. Thus, the server hardware boundaries for maximum workload to process do no longer hold.

2.1.2 Cloud Malware Injection Attack

This attack requires the adversary to create its own malicious service implementation module (SaaS orPaaS) or virtual machine instance (IaaS), and add it to the Cloud system. Then, the adversary has to trick the Cloud system so that it treats the new service implementation instance as one of the valid instances for the particular service attacked by the adversary. If this If this succeeds, theCloud system automatically redirects valid user requests to the malicious service implementation, and the adversary's code is executed. A promising countermeasure approach to this threat consists in the Cloud system performing a service.

2.1.3 Side Channel Attacks

An attacker could attempt to compromise the cloud by placing a malicious virtual machine in close proximity to a target cloud server and then launching a side channel attack. Side-channel attacks have emerged as a kind of effective security threat targeting system implementation of cryptographic algorithms.

2.1.4 Authentication Attacks

Authentication is a weak point in hosted and virtual services and is frequently targeted. There are many different ways to authenticate users; for example, based on what a person knows, has, or is. The mechanisms used to secure the authentication process and the methods used are a frequent target of attackers. Currently, regarding the architecture of SaaS, IaaS, and Paas, there is only IaaS offering this kind of information protection and data encryption. If the transmitted data is categorized to high confidential for any enterprise, the

cloud computing service based on IaaS architecture will be the most suitable solution for secure data communication.

2.2 SECURITY TECHNIQUES IN CLOUD

Cloud computing security or, more simply, cloud security is an evolving sub-domain of computer security, network security, and, more broadly, information security. It refers to a broad set of policies, technologies, and controls deployed to protect data, applications, and the associated infrastructure of cloud computing.

2.2.1 FIREWALLS

i. Scalability: Cloud-based firewall providers deliver services to multiple customers and at the core of their service they use firewalls designed to scale to meet ever-increasing demand. From the enterprise perspective this scalability comes into play when bandwidth increases. Unlike an on-premise firewall that needs replacement when bandwidth exceeds firewall throughput, cloud-based firewalls are designed to scale as customer bandwidth increases—or at least any hardware upgrade has to be made transparent to customers.

ii. Availability: Cloud-based firewall providers offer extremely high availability (> 99.99%) through an infrastructure with fully redundant power, HVAC, and network services, as well as backup strategies in the event of a site failure.

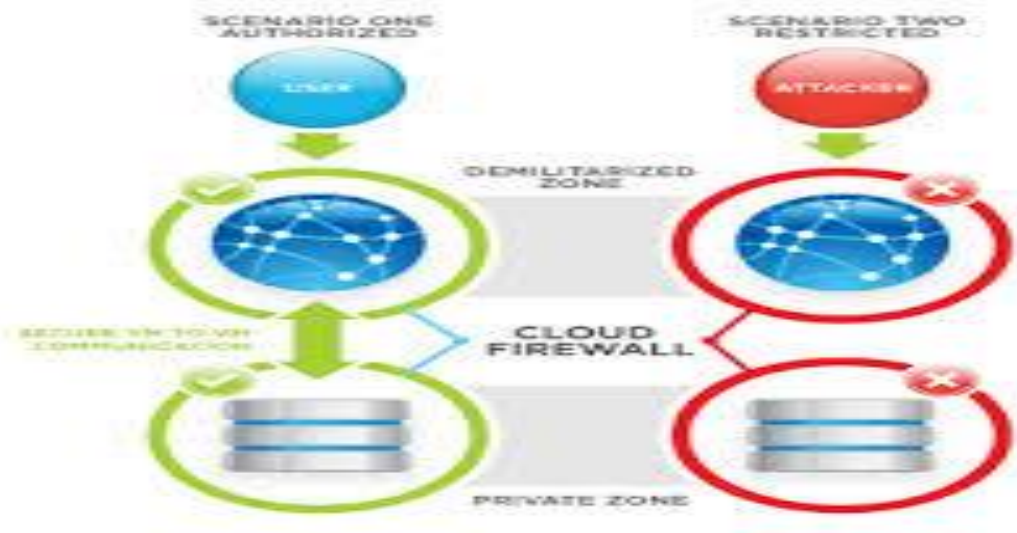
High availability is certainly possible but depending on the manufacturer, high-availability can double the cost of hardware and make operations more complex.

iii. Extensibility: Cloud-based firewalls are available anywhere the network manager can provide a protected communications path. Given interconnection agreements between network providers, the footprint of service may extend well beyond the boundaries of any single service provider's network.

iv. **Accessibility** – The cloud-based firewall model is structured on one internet connection, despite the number of locations. Traditional models require internet connections at a number of locations, which may mean multiple ISP contracts.

v. **Maintainability** – In this model, the service provider has the responsibility to maintain and support the firewall. With traditional models, setups, maintenance and support may require the redirection of internal resources.

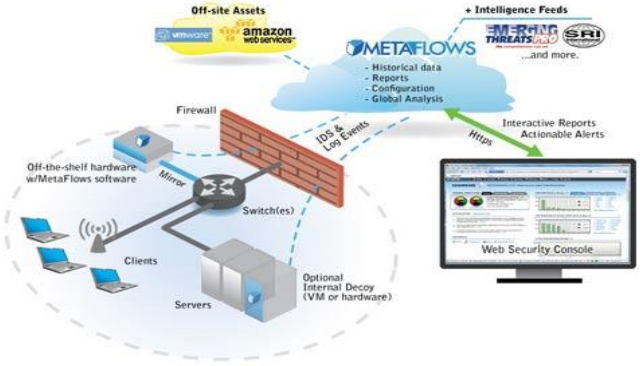
Figure 1 Cloud Firewall



2.2.2 INTRUSION DETECTION SYSTEMS

Intrusion detection systems (IDS) are an essential component of defensive measures protecting computer systems and network against harm abuse. It becomes crucial part in the Cloud computing environment. The main aim of IDS is to detect computer attacks and provide the proper response. An IDS is defined as the technique that is used to detect and respond to intrusion activities from malicious host or network. There are mainly two categories of IDSs, network based and host based. In addition, the IDS can be defined as a defense system, which detects hostile activities in a network. The key is to detect and possibly prevent activities that may Compromise system security or some hacking attempt in progress including reconnaissance/data collection phases that Involve for example, port scans. One key feature of intrusion detection systems is their ability to provide a view of unusual activity and to issue alerts notifying administrators and/or blocking a suspected connection.

Figure 2 Intrusion Detection System In Cloud



2.2.3 ENCRYPTION

Bring Your Own Encryption (BYOE)—also called Bring Your Own Key (BYOK) — refers to a cloud computing security model to help cloud service customers to use their own encryption software and manage their own encryption keys. BYOE allows cloud service customers to use a virtualized example of their own encryption software together with the business applications they are hosting in the cloud, in order to encrypt their data.BYOE is a cloud computing security model that enables organizations to use their own encryption software and manage their own encryption keys. This is done by deploying a virtualized instance of the encryption software alongside applications hosted in the cloud to securely encrypt data.

Figure 3 Encryption in Cloud

Table 3.2.1 lists all the vulnerabilities in cloud computing.

Table 3.2.1

Vulnerabilities in cloud computing

ID	Vulnerabilities	Description
V01	Insecure interfaces and APIs	Cloud providers offer services that can be accessed through APIs (SOAP, REST, or HTTP with XML/JSON) .The security of the cloud depends upon the security of these interfaces. Some problems are:
		a) Weak credentials
		b) Insufficient authorization checks
		c) Insufficient input-data validation
		Also, cloud APIs are still immature which means that are frequently updated. A fixed bug can introduce another security hole in the application.
V02	Unlimited allocation of resources	Inaccurate modeling of resource usage can lead to overbooking or over-provisioning.
V03	Data-related vulnerabilities	a) Data can be colocated with the data of unknown owners (competitors, or intruders) with a weak separation.
		b) Data may be located in different jurisdictions which have different laws.
		c) Incomplete data deletion – data cannot be completely removed.
		d) Data backup done by untrusted third-party providers.
		e) Information about the location of the data usually is unavailable or not disclosed to users.
		f) Data is often stored, processed, and transferred in clear plain text
V04	Vulnerabilities in Virtual Machines	a) Possible covert channels in the colocation of VMs.
		b) Unrestricted allocation and de-allocation of resources with VMs.
		c) Uncontrolled Migration - VMs can be migrated from one server to another server due to fault tolerance, load balance, or hardware maintenance.
		d) Uncontrolled snapshots – VMs can be copied in order to provide flexibility, which may lead to data leakage
		e) Uncontrolled rollback could lead to reset vulnerabilities - VMs can be backed up to a previous state for restoration, but patches applied after the previous state disappear
		f) VMs have IP addresses that are visible to anyone within the cloud - attackers can map where the target VM is located within the cloud (Cloud cartography)
V05	Vulnerabilities in Virtual Machine Images	a) Uncontrolled placement of VM images in public repositories.
		b) VM images are not able to be patched since they are dormant artifacts.
V06	Vulnerabilities in Hypervisors	a) Complex hypervisor code.
		b) Flexible configuration of VMs or hypervisors to meet organization needs can be exploited
V07	Vulnerabilities in Virtual Networks	Sharing of virtual bridges by several virtual machines.

Table 3.2.2 lists all the Threats in cloud computing.

Table 3.2.2

Threats in cloud computing

ID	Threats	Description
T01	Account or service hijacking	An account theft can be performed by different ways such as social engineering and weak credentials. If an attacker gains access to a user's credential, he can perform malicious activities such as access sensitive data, manipulate data, and redirect any transaction.
T02	Data scavenging	Since data cannot be completely removed from unless the device is destroyed, attackers may be able to recover this data
T03	Data leakage	Data leakage happens when the data gets into the wrong hands while it is being transferred, stored, audited or processed.
T04	Denial of Service	It is possible that a malicious user will take all the possible resources. Thus, the system cannot satisfy any request from other legitimate users due to resources being unavailable.
T05	Customer-data manipulation	Users attack web applications by manipulating data sent from their application component to the server's application For example, SQL injection, command injection, insecure direct object references, and cross-site scripting.
T06	VM escape	It is designed to exploit the hypervisor in order to take control of the underlying infrastructure.
T07	VM hopping	It happens when a VM is able to gain access to another VM (i.e. by exploting some hypervisor vulnerability)
T08	Malicious VM creation	An attacker who creates a valid account can create a VM image containing malicious code such as a Trojan horse and store it in the provider repository
T09	Insecure VM migration	Live migration of virtual machines exposes the contents of the VM state files to the network. An attacker can do the following actions:
		a) Access data illegally during migration.
		b) Transfer a VM to an untrusted host .
		c) Create and migrate several VM causing disruptions or DoS
T10	Sniffing/Spoofing virtual networks	A malicious VM can listen to the virtual network or even use ARP spoofing to redirect packets from/to other VMs .

4. CONCLUSION

According to the survey of the research papers ,it states that although the cloud computing is very secure but also it faces many types of attacks that have been listed above. Not only the attacks but also there are many threats and vulnerabilities that are existing in cloud infrastructure due to which many company servers have faced different types of attacks like mostly the DOS(denial of service) or DDOS(Distributed Denial Of Service).Also, the virtualization is very popular in cloud infrastructure so they are also susceptible to attacks. As, the vulnerabilities are there in cloud infrastructure, so also it is not secure. So, after identifying the threats and vulnerabilities there are various ways to secure the cloud infrastructure. The encryption methods and various devices are being used for the security like firewalls and intrusion detection systems which can further protect the cloud system.

Along with, these devices like Unified Threat Management (UTM) can also be implemented as the future work for the security of the Cloud system. So, all the threats, risks and vulnerabilities can be avoided and attacks can also be prevented.

REFERENCES

[1] Yasir mehmood,Umme Habiba, "Intrusion Detection System in Cloud Computing: Challenges and Opportunities" 2013, 2nd National Conference on Information Assurance (NCIA) .
[2] Sadia Syed, M. Ussenaiah ,"The Rise of Bring Your Own Encryption (BYOE) for Secure Data Storage in Cloud Databases" 2015,InternationalConference on Green Computing and Internet of Things (ICGCIoT).
[3] Patil Madhubala R, "Survey on Security Concerns in Cloud Computing" 2015, InternationalConference on Green Computing and Internet of Things (ICGCIoT).
[4] M.SenthilKumar, "A Secured Cloud Storage Technique To Improve Security In Cloud Infrastructure" 2013, International Conference on Recent Trends in Information Technology (ICRTIT).
[5] Vijay Varadharajan, "Trust Enhanced Security for Cloud Environments" 2012, IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications.

A Brief Author Biography

Diksha Nagpal : She is an efficient, sincere and hardworking individual. She has completed MCA and pursuing M.tech and has a keen interest in area of Cloud Computing, security and implementation of security especially the network security. She has an experience in the field of Security of 5 years and is looking forward for the research areas of the Cloud infrastructure. She is an Oracle Certified Associate and has teaching experience of 8 years.

Dr. Deepti Sharma: She is very dynamic personality and is working as an Associate Professor and Head Of Department in Advance Institute Of Technology and Management ,Palwal .She is an eminent mentor and has guided and is guiding many students a lot in their research work .She has already completed Ph.D. from Computer Science and Engineering.