# Various types of Virtual Machines Attacks in Cloud Computing: A Survey

**[1]S. Annapoorani, [2]Dr. B. Srinivasan**

[1]Ph.D Scholar, [2]Associate Professor
PG & Research Department of Computer Science
Gobi Arts & Science College, Tamil Nadu, India

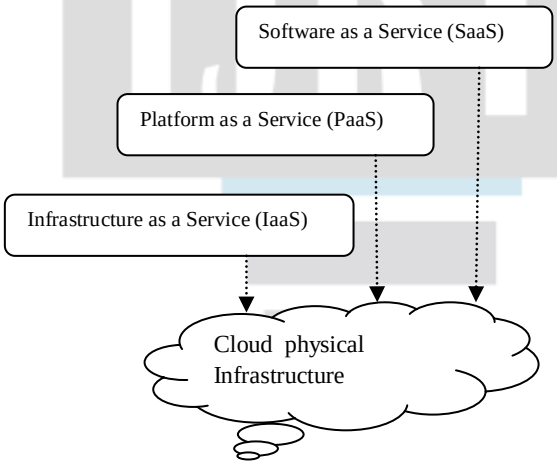
***ABSTRACT:*** **Cloud computing is advanced technology for resource sharing through network with less cost as compare to other technologies. Cloud infrastructure supports various models IaaS, SaaS, PaaS. Today the most important technique used in cloud computing is the concept of virtualization. By using virtualization, more than one operating system is supported with all resources on single hardware. In addition, the virtualization technology has limit security capabilities in order to secure wide area cloud environment. Sharing of one database to many tenants is known as Multi tenancy. Multi-tenancy is achieved by utilizing virtualization and allowing resource sharing where Multi-tenancy is seen differently from different service models.To secure cloud infrastructure a hypervisor based virtualization is used. This paper describes the various virtual machine security attacks and also hypervisor security in virtualization environment.**

**Index Terms: Virtual Machine, Multi tenancy, Hypervisor, VMs attacks**

## INTRODUCTION

Cloud computing supports multiple resources, including computing resources, to deliver an integrated service to the end user. In Cloud Computing, the IT and business resources such as servers, storage, network, applications, and processes that can be dynamically stipulated to the user needs and workload. Cloud computing means storing and accessing data and programs over the internet from a remote location. When we store data on or run a program from the local computer's hard drive, this is called local storage and computing. The formal definition of Cloud Computing comes from the NIST: "Cloud computing is a model of for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction". This is composed of five essential characteristics, three service models, and four deployment models.

Cloud computing products, also called cloud service delivery models, as in Below *Fig* shows, which are often roughly classified into a hierarchy of a service terms, presented here in order of increasing specialization:




**Infrastructure-as-a-service (IaaS):** where cloud providers deliver computation resources, storage and network as an internet-based services. This service model is based on the virtualization technology. Amazon EC2 is the most IaaS provider.

**Platform-as-a-service (PaaS):** where cloud providers deliver platforms, tools and other business services that enable customers to develop, deploy, and manage their own applications, without installing any of these platforms or support tools on their local be hosted on top of IaaS model or on top of the cloud infrastructures directly. Google Apps and Microsoft Windows Azure are the most known.

**Software-as-a-service (SaaS)** applications hosted on the cloud infrastructure as internet based service for end users, applications on the customers' computers be hosted on top of PaaS, IaaS or directly hosted on cloud infrastructure. SalesForce CRM is an example of the provider.

**Multi tenancy**

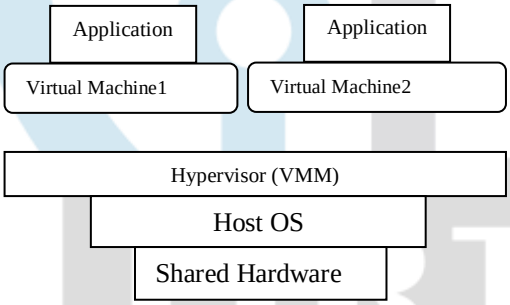
The requirements for cloud services such as multi tenancy, service life cycle management, security,.. Multi tenancy provides isolation of the different users of the cloud system (tenants) while maximizing resource sharing. To increase the resource utilization, the companies started using the technology called virtualization where a single physical infrastructure can be used to run multiple OS and applications.

## II. VIRTUALIZATION COMPONENTS

Virtualization is a technology that enables the single physical infrastructure to function as a multiple logical infrastructure or resources. The virtualization reduces the huge amount invested in buying additional resources. [2] Virtualization is a technique, which allows to share single physical instance of an application or resource among multiple organizations or tenants. Hardware virtualization is the abstraction of computing resources from the software that uses those resources. Hardware virtualization is also called server virtualization. Hardware virtualization installs a hypervisor or virtual machine manager (VMM), which creates an abstraction layer between the software and the underlying hardware. Virtual Machine Security becomes as important as physical machine security. Virtualized environments are vulnerable to all types of attacks for normal infrastructures. The virtual machine is managed by a software or firmware, which is known as hypervisor.

**Hypervisor**

Hypervisor is a firmware or low-level program that acts as a Virtual Machine Monitor (VMM)[2]. Hypervisors are the software tool sits in between Virtual Machines and physical infrastructure and provides the required virtual infrastructure for VMs. After the hypervisor gets compromised, the attacker can have the malicious activities such as (i) get the unauthorized access to the other VMs that share the physical hardware. (ii) Attacker can utilize the hardware resources fully to launch resource exhaustion attacks etc.




The goal of our work is to understand the concept of multitenancy and the various types of virtual machine attacks in cloud environment

## III. LITERATURE REVIEW

Several Researchers has been fine out that the Mutli-tenancy as s security issue in Cloud computing such as [1] who proposed a survey on security issues in service delivery models in clouds and also stated that Multi-tenancy is an important for Cloud Computing characteristics that leads to confidentiality contravention. [3] states that the Multi-tenancy is achieved by utilizing virtualization and allowing resource sharing where Multi-tenancy is seen differently from different service models. In Software-as-a-Service (SaaS), applications are provided as s service by the Cloud Service Provider (CSP) where the customer cannot monitor or control the underlying infrastructure.

### 3.1 Denial of Service (DoS) Attacks

[4] introduces a secure hypervisor-based Technology create a secure cloud environment. Basically, as the cloud gives services to legal users. It can also services to users that have malicious purposes. A hacker can use a cloud to host a malicious application to achieve the object which may be a DDoS attacks against the cloud itself, or targetting another user in the cloud. For example, an attacker knew that his victim is using a cloud vendor with name X, now attacker by using similar cloud provider can sketch an attack against the victims.

### 3.2 Co-Residential Attacks

[5] using Virtual Machine Allocation Policies to defend against Co-resident Attacks in Cloud Computing. The co-residential attack, where malicious users build side channels and extract private information from virtual machines co-located on the same server. The attacker is able to extract any private information from the victim, need to co-locate the VMs with the target VMs. This paper investigates VM allocation policies and practical counter measures against by developing a set of security metrics and a quantitative model. In this paper, discussed about all the aspects of security, workload balance and power consumption into consideration to make PSSF more applicable to existing commercial cloud platforms

[6] A virtual cloud resource allocation model is proposed. In this, the problem of virtual cloud resources allocation is abstracted as a utility-maximization problem, taking tradeoffs between the utility of the data center and the performance of the applications into account, and maximizing the utility on the premise of meet user's performance.

### 3.3 Cache-Based Side Channel Attacks

[7] Resource sharing in cloud computing raises a threat of Cache-Based Side Channel Attack (CSCA). It is proposed to detect and prevent guest virtual machines from CSCA. Cache miss patterns were analysed in this solution to detect side channel attack. CSCA is divided into two types and those are time driven cache attacks, and trace driven cache attacks. It is based on a cloud setting with two VMs installed on a same physical machine using bare-metal hypervisor sharing highest level cache.

## IV. HYPERVISOR SECURITY

In a virtualization environment, there are several Virtual Machines that may have independent security zones which are not accessible from other virtual machines that have their own zones. A hypervisor has its own security zone, and it is the controlling agent for everything within the virtualization host. Hypervisor can touch and affect all acts of the virtual machines running within the virtualization host. There are multiple security zones exist within the same physical infrastructure. This can cause a security issue when an attacker takes control over the hypervisor. [2] Another major virtualization security concern is "escaping the virtual machine" ot the ability to reach the hypervisor from within the virtual machine level. Even more, APIs are created for virtualization platforms.

## V. CONCLUSION

A survey shows that security is the most significant user's concerns in cloud computing. In this paper, we focussed on the various virtual machine security attacks in cloud environment. Attacks against the hypervisor becoming more popular among the attackers realm. In this paper, we highlighted Multi tenancy as vulnerability and provided in depth understanding related to different dimensions of Multi tenancy. And also discussed about the hypervisor security with in the virtual machine environment.

## REFERENCES

[1] S. Subashini, and V. Kavitha, "A Survey on security issues in service delivery models of cloud computing," Journal of Network and Computer Applications (2011).
[2] K. Sunitha " A Survey on Securing the Virtual Machines in Cloud Computing " International Journal of Innovative Science, Engineering & Technology, Vol. 1 Issue 4, June 2014.
[3] Hussian AlJahdali, Abdulaziz Albatli, Peter Garraghan, Paul Townend, Lydia Lau, "Multi-tenancy in Cloud Computing", International Symposium on Service Oriented Engineering (SOSE), April 2014.
[4] Rajesh Bose, Debabrata Sarddar, " A Secure Hypervisor-based Technology Create a Secure Cloud Environment", International Journal of Emerging Research in Management & Technology, Vol.4 Issue 2,Feb 2015.
[5] Yi Han, Jeffrey Chan, Tansu Alpcan, Christopher Keckie "Using Virtual Machine Allocation Policies to defense against Co-resident Attacks in Cloud Computing", IEEE Transactions on Dependable and Secure Computing, 2015.
[6] Zhu Jianrong , Li Jing and Zhuang Yi " Utility-based Virtual Cloud Resource Allocation Model and Algorithm in Cloud Computing" International Journal of Grid Distribution Computing Vol.8, No.2 (2015), pp.177-190.
[7] Munish Chouhan and Halabi Hasbullah "Defense against Cache-Based Side Channel Attacks for secure Cloud Computing" ARPN Journal of Engineering and Applied Sciences Vol.11 No.22, (2016), ISSN 1819-6608.
[8] Omar Abdel Wahab, Jarnal Bentahar, Hadi Otrok, and Azzam Mourad, " Optimal Load Distribution of VM-based DDoS Attacks in the Cloud", IEEE Transactions on Service Computing,2017.
[9] Manjinder Singh, Charanjit Singh, " Multi Tenancy Security in Cloud Computing", International Journal of Engineering Sciences & Research Technology, Vol.6 Issue 3, Mar 2017.
[10] Raghvendra Kumar, Arti Pandey, " A Survey on Security Issues in Cloud Computing", IJSRSET, Vol. 2 Issue 3, 2016