Cloud Computing and Virtualization Security: A Survey

V. A. Meshram¹, V. V. Meshram², P. V. Khandare³, Dr. S. R. Sakhare⁴

Vishwakarma Institute of Information Technology
Department of Computer Engineering, University of Pune-48, India

Abstract—Cloud computing is one important domain in nowadays, the meaning of cloud computing is computing in cloud. In this paper, we explained different term related with cloud computing like deployment model of cloud, service models of cloud, also we focuses on need of virtualization, different risk associated with the it and different solution for different risk associated with virtualization.

Keywords—cloud, cloud computing

I. INTRODUCTION

The term cloud computing comes from the telecommunication world. The meaning of term cloud computing is “computing is in the cloud”. This term is related with the computation, data access, software which can be easily accessed by the end user. In IT enterprises, the cloud is recent trends, i.e. it is ability to move computing and data away from desktop and portable PCs into large data centres. There are different terms given by different people, according to National Institute of Standard and Technology is “It is a model for permitting convenient, on demand network access to a shared pool of computing resources.” For example it may include networks, server, application etc., these can be easily provided and released with minimum management effort with minimum cost. The main goal of this technology is to make best utilization of distributed resources and achieve higher throughput and remove large scale computation problem. This term is associated with or has a characteristics scalability, virtualization, quality of service. Cloud computing provides services based on their several fundamental models, it include IaaS, PaaS, and SaaS. The IaaS stands for infrastructure as a service, this offers computers physical or virtual machine of other resources. It may offer extra resources like firewall, load balancers, VLAN etc. The platform as a service (PaaS) model provides a platform (for computing), basically it includes operating system, database, webserver. Developer can develop their own application and can easily run those applications on the cloud without buying and managing the required hardware and software (layer). The PaaS providers like Microsoft Azure and Google App Engine, provide a facility to end user that cloud user does not have demand to allocate resource manually. In SaaS, user has a privilege to access application software and databases. SaaS is sometime defined as the “On Demand Software” and it usually charge end user based on pay per use. The cloud model has different model like public cloud, private cloud and private cloud. Private cloud can be operated for the single organization, that can be managed by a third party and it may be operated internally or externally. To form a private cloud, it requires certain significant level and degree of commitment to virtualize the business environment. A cloud is called a public cloud when the services provided by the service provider over a network are open for the public use. If we look carefully by considering the architecture of public and private cloud there is no difference. Amazon AWS, Microsoft and Google are the example of public cloud and offer access only via internet i.e. direct connectivity is not provided. Hybrid cloud is another type of cloud; this is nothing but the combination of two or more cloud. It may include combination of private, community or public. Now we move toward the virtualization, it is nothing but the technology which provide or enables a single computer or server simultaneously run multiple sessions or multiple operating system of a single OS. A hypervisor provide a hardware device, a virtual machine for each virtual operating system. Organization of paper is as Page Layout follows: Section I provide introduction to cloud computing, section II describe the need of virtualization, Section III describe virtualization weakness and attacks, Section IV describe different solution for virtualization security risk and in section IV, we conclude the paper [1, 2, 3, 4, 5].

II. DEPLOYMENT MODEL AND CLOUD SERVICES

The main motto behind the deployment model is to know the nature of how cloud is located. As per the NIST definition there are basic four deployments model are as follows; public cloud, private cloud, hybrid cloud and community cloud.

Public cloud: In this cloud infrastructure is use in large amount i.e. it is available for the public use e.g. large industry group [4].

Private cloud: In this cloud infrastructure is not used in large area. It is used for only organization and it can be easily managed by the organization or third party. Private cloud may be either on –or off the premises.

Hybrid: Hybrid cloud is nothing but the combination of multiple cloud, it may be combination of private, community of public where those cloud retain their unique identities, but are not bound together as a unit.

Community cloud: A community cloud has been organized to serve a common function or purpose [4].
Public cloud (External)  
Private Cloud (internal)

Fig. 1: Deployment models

Deployment location is different; it is totally based upon the type of cloud. The following figure can illustrates deployment location for different cloud types.

Service Models:
In simple words, we can say that cloud is nothing but the boundary where a client network and responsibilities end and the work of service provider starts. There are the different vendors who offer clouds that have different services associated with them. The portfolio of services offered adds another set of definitions called the service model. Basically three types of services are accepted by the world, which are IaaS, PaaS, and SaaS.

IaaS(Infrastructure as a Service): It provide virtual machine, virtual storage, virtual structure and other thing as per the client requirement. In this type, service provider can manage the entire infrastructure. While the client is responsible for all other aspects like deployment which may include operating system, applications etc [4].

PaaS(Platform as a Service):This service provide virtual machine, operating system etc. The service user can easily deploy application on the cloud infrastructure, which is made up with help of programming languages. The client is totally responsible for installing and managing the application that it is deployed [4].

SaaS(Software as a Service) : It is complete operating environment with management, applications and the user interface[4].

III. NEED OF VIRTUALIZATION
In a simple word you can say that virtualization is way in which we divide the resources of a computer into multiple execution environments. This can be achieved with the help of technologies like hardware and time sharing. Following figure explain you basic architecture of virtualization.

With the help virtualization operating system considers overall control over the underlying hardware. This can be done with the help hypervisor /VMM. The hypervisor or VMM is a software layer which permits end user to run more operating system simultaneously over on a single computer system, also provide hardware abstraction to run end user OS and multiplexes underlying hardware resources. There are many differences between physical and virtual machine for example in terms of operating system, underlying hardware etc. When concern with the physical machine it has limited OS to access but in term of virtual machine OS is independent on the hardware. In physical machine, hardware and software are tightly coupled but in case of virtual machine OS is not under the hardware. There are different virtualization approaches, it has various types like operating system based virtualization, application based virtualization, and hypervisor based virtualization. In the first approach that is OS based approach virtualization can be enabled by hosting a OS and that can be easily support to multiple isolated guest OS on a single physical server. The second type of virtualization is hosted on top of the OS.

Hypervisor:
Hypervisor is software or low level program which handles all activities of Virtual Machine Manager. Basically, there are two types of hypervisor Type 1 Hypervisor and Type 2 Hypervisor. The Type 1 Hypervisor run on the bare system. It does not have any host operating system because they are installed on a bare system, e.g. LynxSecure, RTS Hypervisor, Oracle VM, Sun xVM Server. Type 2 hypervisor is a software interface that emulates the devices with which a system normally interacts. Containers, KVM, Microsoft Hyper V, VMware Fusion, Virtual Server 2005 R2, Windows Virtual PC and VMware workstation 6.0 are examples of Type 2 hypervisor.

IV. RISK ANALYSIS OF VIRTUALIZATION
Virtualization technology is not new, but if we apply it to cloud computing, it creates some security risk that may be exploited harmfully and cause major security incident. Basically there are two aspect of this technology, first safety of virtualization technology and second one is issue related
with virtualization technology. There are different risks like risk for access control, risk of DOS attack, risk of virtualization platform building network and risk of virtualization platform security.

![Virtualization Architecture Type 1](image)

**Fig. 3: virtualization architecture Type 1**

Risk (1): When we place resources into logical platform that we can use for storage or many purposes but there is not that much level of security. The user can only see logical storage location but don’t know the actual storage location of data. It may be in off-premises storage infrastructure, due to this it may cause leakage of secret information which may include infrastructure manager and control the infrastructure by using the vulnerability of virtualization platform might extract the secret information. When the platform is attacked, the policy of administrator may be stolen and used harmfully[3].

Risk (2): A virtualization service has a chance to slow or even stop when a large number of application and unlimited number of platform are used for processing. This is similar to our old network, when server gets requests more than its limit it may get slow processed, that means it reduces the speed of response. When we concern with large case, application layer DDoS (Distributed Denial of Service) are possible. It causes the server down and service may be stopped. Hence due to this reason we have more security for virtualization platform. The main purpose of virtual platform is to provide design facility to each end user with required service, when the lot of user is logged simultaneously then virtualization platform must try to provide that service in a better way to end user. Due to this type of scenario it will take up too many resources and virtualized platform will run in an effective way. The excessive number of users normally use virtualization platform. User can create or expand the virtualization platform and increase the resources to resolve it. Malicious application that has a number of services creates a lot of damage to the unlimited resources of service. This damage is not affordable to any kind of high performance virtualization platform as it can be destructive. Hence it may cause DOS attack [3].

Risk (3): The network can be established, which include the client and server. This network can be established with the help of software hub. Suppose there are two clients who are the member of some network, then they share same virtual interface. In this case, two clients can see the server and all traffic of the client end because the traffic of two networks can see the server and all traffic of the client end, this is possible because the traffic of two network are connected by a virtual switch machine through the same physical network card. All end client and server share the same software stack, hence sharing of software is a major problem of virtualization security, if the client end user and server share same software stack, the attacker can easily access entire stack only by attacking client’s computer [3].

Risk (4): When we build a cloud then there is separation between the physical source and the internet. Due to this library of Trojan and viruses for the virtualization cannot be updated rapidly, hence due to this vulnerabilities of virtualization, platform cannot be repaired in time. Due to internet environment there must be updating of viruses and Trojan. When the internet is concern with the business, they update their security mechanism. For a cloud environment there is “time poor” in updating the security mechanism of the virtualization platform. Due to this Trojan, viruses may cause disturbance in the cloud and it causes the security risk [3].

### Table 1: Security Priorities in Cloud Types

<table>
<thead>
<tr>
<th>Cloud Types</th>
<th>Security Priorities</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Low</td>
</tr>
<tr>
<td>Private</td>
<td>√</td>
</tr>
<tr>
<td>Public</td>
<td></td>
</tr>
<tr>
<td>Hybrid</td>
<td></td>
</tr>
<tr>
<td>Community</td>
<td></td>
</tr>
</tbody>
</table>

V. DIFFERENT SOLUTION FOR VIRTUALIZATION

As per the security point of virtualization, the proper technical measure can be used. It includes encryption and integrity checking of virtual memory image files, isolation and reinforcement of virtual machines, monitoring the virtual machine etc.

For the risk 1, we have to provide a different policy like policies that are applied to the networks like LAN (Local Area Network), WAN and internet. As per the virtualization concept, we can’t control the number of user; also user is not conducive to the maintenance. All the deployed application is deployed under certain standard. Whatever the data stored in to the virtualization platform is stored with the help of encryption technique. Directory services must be applied to manage identities and provide capability of access control. When the end user wants to access resource on cloud they have only onetime permission to access the resource and the entire remaining thing will be secret for that user, in this way we can resolve the problem [3].
For the risk 2, we have adopted workload equilibrium and migration strategy to move to other work area. At the same time we use the audit mechanisms for user end services. Each and every application must be reviewed to prevent the malicious user from applying lot of resources to the virtual platform. For the data protection we have to refer data protection and disaster recovery [3].

For the risk 3, we have to form a separate administrator. A process running in a secure area within the real time, involved in virus and Trojan killing, as well as bug fixes, while another process is an isolated area, communicate with the outside world, updating the virus and Trojan library and obtain the latest vulnerability information and download that patches stored in a separate isolated “box” the first process to obtain the information of the box and the area security is maintained [3].

VI. CONCLUSION
In this paper, we explain different deployment model as well as service model for cloud. Also we propose that, in virtualization we have to provide best security approach. So virtualization is important factor, as there is need to provide better security. Hence it is responsibility of service provider to provide service with proper or high level security.

REFERENCES