**Security Aspects of Virtualization in Cloud Computing**

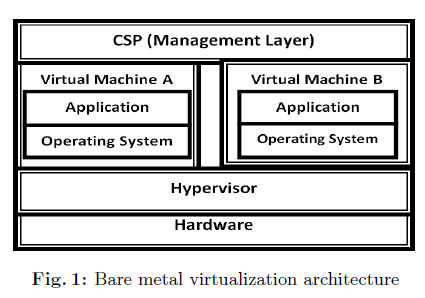
OULD SI BOUZIANE ABD EL NOUR

**1 - Abstract**

Abstract. In Cloud computing, virtualization is the basis of delivering Infrastructure as a Service (IaaS) that separates data, network, applica- tions and machines from hardware constraints. Although Cloud comput- ing has been a focused area of research in the last decade, research on Cloud virtualization security has not been extensive. In this paper, di er- ent aspects of Cloud virtualization security have been explored. Specif- ically, we have identi ed: i) security requirements for virtualization in Cloud computing which can be used as a step towards securing virtual infrastructure of Cloud, ii) attacks that can be launched on Cloud vir- tual infrastructure, and iii) security solutions to secure the virtualization environment by overcoming the possible threats and attacks.

**2 - Security Requirements of Virtualization**

Different virtualization approaches can be applied to various system layers in- cluding hardware, desktop, operating system, software, memory, storage, data and network. Full virtualization is a form of hardware virtualization that in- volves complete abstraction of underlying hardware and provides better oper- ational eciency by putting more work load on each physical system



The unique characteristics of virtualization along with their bene ts also have some drawbacks. Each component of virtualization needs to be secured from the possible threats. In general, before planning and implementing security of any system it is important to understand the security requirements of that environ- ment. This section presents general requirements to prevent virtualization layers attacks in Cloud.

In Security Requirements of Virtualization there is :

**Service Provider Requirements**

To secure the virtualization hardware, (Cloud) service provider must limit access of hardware resources to authorized person. Similarly, proper access control should be implemented in the management layer, so that each administrator has access only to its concerned data and software

**Hypervisor Requirements**

Programs that control the hypervisor must be secured using similar practices used for security of programs running on servers. Similarly access to the hyper- visor must be restricted

**Virtual Machine Requirements**

Limit on VM resource usage has to be assigned so that malicious VMs can be restricted from consuming extra resources of the system

**Guest Image Requirements**

Hypervisors use disk images (host les used as disk drive for guest OSs) to present guest OSs with virtual hard drives

**3 - Attacks on Virtualization**

Each component of virtualization layer can act as an attack vector to launch multiple attacks on the system. Attacks that target di erent components of virtualization environment may result in security issues such as compromise of complete Cloud infrastructure, stealing of customer data and system hacking. This section discusses di erent attack scenarios at virtualization environment in Cloud. We can see that in this partie there is

**Service Provider Attacks , Hypervisor Attacks , Virtual Machine Attacks , Guest Image Attacks**

**4- Security Solutions for Virtualization**

To cater the attacks on virtualization environment di erent security solutions have been proposed in literature. This section discusses those security solutions.

For each component of virtualization architecture. By implementing these secu- rity solutions the attacks discussed in section 3 can be mitigated or at least the impact of those attacks on virtualization environment can be minimized.

We can see that in this partie there is :

**Service Provider Security, Hypervisor Security , Virtual Machine Security, Guest Image Security**

**5 - Conclusion**

The security of cloud cannot be maintained unless its virtualization environ- ment is secured. Although di erent virtualization approaches exist, bare metal virtualization approach is commonly used in large computing systems such as Cloud for server virtualization. This paper presents general architecture of bare metal virtualization and covers security aspects of its di erent components. Cloud virtualization environment can be compromised by di erent attacks at service provider, hypervisor, virtual machines, guest operating system and disk images. The attack scenarios at these components are discussed in the paper. To provide security to the virtualization environment, general requirements for vir- tualization security and di erent existing security schemes that provide security to virtualization environment have also been discussed. Therefore, the holistic picture of virtualization security in Cloud is provided through structured anal- ysis in which security requirements, attacks and solutions correspond to each other.