ISSN 22773061

Virutalized Cloud Environment : A Survey

Er.Gursimran Singh[1] , Dr.Gurjit Singh Bhathal[2]
E-mail: gursimran51@gmail.com, gurjit.bhathal@gmail.com
[1]Student , Computer Engineering Department, University College of Engineering,
Punjabi University, Patiala
[2]Assistant Professor in Computer Engineering Department,
University College of Engineering
Punjabi University, Patiala

Abstract:

Cloud computing is one of today's most exciting technology because of its cost-reducing, flexibility, and scalability. With the fast growing of cloud computing technology, Data security becomes more and more important in it. In evaluating whether to move to cloud computing, it is important to compare benefits and also risks of it. Thus, security and other existed issues in the cloud cause cloud clients need more time to think about moving to cloud environments. But Security-related topics is one of the most arguable issues in the cloud computing which caused several enterprises looks to this technology uncertainly and move toward it warily[2]. A Virtualization Security framework is presented which contains two parts: virtual system security and virtualization security management.[1] The paper is devoted to the mechanism of monitoring of virtual machines aimed at guaranteeing increased security to cloud resources. Furthermore, the requirements for this mechanism are enumerated.[3]

Keywords- Virtualization; Cloud computing; Security.

ISSN 22773061

1. INTRODUCTION

In recent years, cloud computing has emerged as one of the fastest-growing section of the IT industry and more and more businesses have gone to the cloud. It changes the delivery model which provides on-demand self-service access to a shared pool of physical and virtual computing resources via broad network access. Providing secure virtualization is a

major component of this model. Cloud computing already leverages virtualization for load balancing via dynamic provisioning and migration of virtual machines among physical resources [3]. Cloud computing is primarily altering the expectations for how and when computing, storage and networking resources should be allocated, managed and consumed. End-users are gradually more sensitive to the latency of services they consume. Service Developers want the Service Providers to ensure or provide the capability to dynamically allocate and manage resources in response to changing demand patterns in real-time. Ultimately, Service Providers are under pressure to architect their infrastructure to enable real-time end to- end visibility and dynamic resource management with fine-grained control to reduce total cost of ownership while also improving agility [4]. Cloud computing is a network-based environment that focuses on sharing computations and resources. Basically, clouds are Internet-based and try to mask complexity for clients. Cloud providers use virtualization technologies combined with self-service abilities for computing resources via network infrastructure particularly the Internet. In cloud environments multiple VMs (VM) hosted on the same physical server as infrastructure. In cloud, costumers only have to pay for what they use. Cloud computing refers to both the applications delivered as services over the Internet and the hardware and systems software in the datacenters that provide those services.[2]. Security of clouds has many facets. A number of researchers discuss cloud security from their own viewpoints. We can observe that many of them work under cloud security Alliance and continue publishing strategy on security [1].

2. SERVICE LAYERS OF CLOUD COMPUTING

These are services that are offered in a conventional IT data center. In a cloud value chain, they are virtualized and delivered on demand. The three major layers in the cloud computing value chain are as follows and shown in figure:

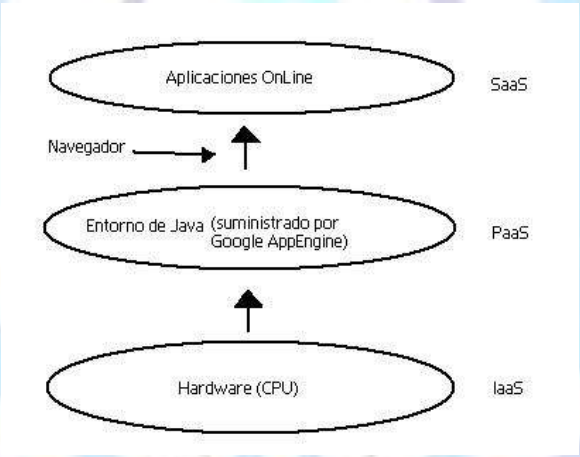

Figure 1: Service Layers of Cloud Computing

● Software as a Service (SaaS) is where application services are delivered over the network on a subscription and on-demand basis. Cisco, Sales force, Microsoft, and Google are a few providers in this layer.

● Platform as a Service (PaaS) consists of run-time environments and software development frameworks and components delivered over the network on a pay-as-you-go basis. PaaS offerings are classically presented as API to consumers. Examples of this are: Google Apps Engine, Amazon Web Services, force.com, and Cisco WebEx Connect.

● Infrastructure as a Service (IaaS) is where compute, network, and storage are delivered over the network on a pay-as-you-go basis. Amazon pioneered this with AWS (Amazon Web Service), and now IBM and HP are entrants here also. The approach that Cisco is taking is to enable service providers to move into this area.

3. BENEFITS OF THE CLOUD

Clouds computing fundamentally changes the way that IT services are delivered to organizations. Instead of both owning and administration IT services for themselves, or using an outsourcing approach built around dedicated hardware, software, and support services, organizations can use cloud computing to meet their IT requirements using a

flexible, on-demand, and quickly scalable model that requires neither ownership on their part, nor provision of dedicated resources. Some of the benefits that cloud computing brings are as follows:

a) **Reduced Cost:** Cost is a clear benefit of cloud computing, both in terms of CapEx and OpEx. The reduction in CapEx is understandable because an organization can spend in increments of required capacity and does not need to build infrastructure for maximum (or burst) capacity. For most enterprises, OpEx constitutes the majority of spending; therefore, by utilizing a cloud provider or adopting cloud paradigms within, organizations can save operational and maintenance budgets.
b) **Flexibility**: Flexibility benefits derive from rapid provisioning of new capacity and rapid relocation or migration of workloads. In public sector settings, cloud computing provides agility in terms of procurement and acquisition process and timelines.
c) **Improved Automation**: Cloud computing is based on the premise that services can not only be provisioned, but also de-provisioned in a highly automated fashion. This specific attribute offers significant efficiencies to enterprises.
d) **Focus on Core Competency**: Government agencies can reap the benefits of cloud computing in order to focus on its core mission and core objectives and leverage IT resources as a means to provide services to citizens.
e) **Sustainability**: The poor energy efficiency of most existing data centers, due to poor design or poor asset utilization, is now understood to be environmentally and economically unsustainable. Through leveraging economies of scale and the capacity to manage assets more efficiently, cloud computing consumes far less energy and other resources than a traditional IT data center.

4. CLOUD-BASED VIRTUALIZATION

The potential problem also exists for virtualization is

provider combine too many VMs onto a physical server. This can result in performance problems caused by impact factors such as limited CPU cycles or 1/0 bottlenecks. These problems can take place in a traditional physical server, but they are more likely to occur in a virtualized server because of the connection single physical server to multiple VMs that all of them challenging for critical resources. Thereby, management tasks such as performance management and capacity planning management are more critical in a virtualized environment than in a similar physical environment. This means that IT organizations must be able to constantly monitor in real time the utilization of both physical servers and VMs. This capability allows IT organizations to avoid both over- and underutilization of server resources such as CPU and memory and to allocate and reallocate resources based on changing business requirements. This capability also enables IT organizations to execute policy-based remediation that helps the organization to ensure that service levels are being met. In addition, an unnecessary VM will able to move from one physical server to another

with high availability and energy efficiency. But be considering the VM destination can be demanding to ensure that the migrated VM keeps the same security, QoS configurations, and needed privacy policies. In the other hand, the destination must be assurance keeping all the required configurations of migrated VM[2].

5. CLOUD SECURITY ISSUES

Security is one of the most important issues which reduces the growth of cloud computing and complications with data privacy and data protection continue to plague the market. One of the key issues of cloud computing is loss of control. As a first example, the user does not know where accurately its data is processed and stored in the cloud. A second example of loss of control is that the cloud provider gets paid for running a service he does not know the details of some of the other security issues of a cloud are:

• Recovery

• Privileged user access

• Data segregation

• Bug exploitation

• Privacy

Privacy is exposure of sensitive information stored on the platforms implies legal liability and loss of reputation. It is one of the main issues which depends on virtualization security. The core set of requirements to be met by a security system for clouds are the following [2]:

• Effectiveness

• Precision

• Transparency

• Non-subvert ability[3]

5.1. ATTACKS IN VIRTUALIZATION LEVEL

Nowadays, there are several attacks in the IT world. Basically, as the cloud can give service to legal users it can also service to users that have malicious purposes.

a) **DDoS attacks:** DDoS attacks typically focus high quantity of IP packets at specific network entry elements; usually any form of hardware that operates on a Blacklist pattern is quickly overrun. In cloud computing where infrastructure is shared by large number of VM clients, DDoS attacks make have the potential of having much greater impact than against single tenanted architectures.

b) **Client to client attacks**: One malicious VM could infect all VMs that exist in physical server. An attack on one client VM can escape to other VM's that hosted in the same physical, this is the biggest security risk in a virtualized environment. When malicious user puts the focus on VMs become easy to access, the attacker has to spend time attacking one VM, which can lead to infecting other VMs, and thereby escaping the hypervisor and accessing the environment level that officially it can't accessible from VM level.

5.2. VM SECURITY AND THREATS

Virtualization is not as new technology as cloud but in it there are several security issues that now migrated to cloud technology. Also, there are other vulnerabilities and security issues which exclusive in cloud environment or may have more critical role in cloud. There are various threats and attacks in this level that major issues mentioned below:

a) **VM level attacks**: Potential vulnerabilities are the hypervisor or VM technology used by cloud vendors are a potential problem in multi-tenant.

b) **Cloud provider vulnerabilities**: These could be platform-level, such as an SQL-injection or cross site scripting susceptibility that exist in cloud service layer which cause insecure environment.

c) **Expanded network attack surface**: Cloud user must protect the infrastructure used to connect and interact with the cloud, a task complicated by the cloud being outside the firewall in many cases [8]

d) **Authentication and Authorization:** The enterprise authentication and authorization framework does not naturally extend into the cloud. Enterprises have to merge cloud security policies with their own security metrics and policies.

e) **Lock-in**: It seems to be a lot of angst about lock-in in cloud computing. The cloud provider can encrypt user data in particular format and if user decides to migrate to another vendor or something like.

6. CONCLUSION

Cloud computing is distinct as a pool of virtualized computer resources. Based on this Virtualization the Cloud Computing paradigm allows workloads to be deployed and scaled-out quickly through the rapid provisioning of VMs or physical machines. A Cloud Computing platform supports redundant, self-recovering, highly scalable programming models that allow workloads to recover from many inevitable hardware/software failures [2]. Virtual Machine Monitor for cloud protection that can observe both guest and middleware integrity and protect them from most kinds of attack while remaining fully transparent to service users. VM system architecture can solve the problem of virtualization security effectively, and virtualization security management settles the question that various VM managements bring.

7. REFERENCES

1. Shengmei Luo, Zhaoji Lin, Xiaohua Chen," Virtualization security for cloud computing service", 2011 International Conference on Cloud and Service Computing,pp-174-176

2. Farzad Sabahi," Virtualization-Level Security in Cloud Computing", 2011 IEEE,pp-250-254

3. Artem Volokyta, Igor Kokhanevych, Dmytro Ivanov," Secure Virtualization in Cloud Computing", TCSET'2012, February 21-24,2012,

4.http://www.cisco.com/web/strategy/docs/gov/CiscoCloudComputing_WP.pdf