ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Special Issue 4, March 2017

Monitoring and Securing Virtualized Environment

J.PALANIVEL, M.C.A., M.Phil., B.Ed., M.Sc., R.PRABAKARAN, M.C.A., M.Phil., M.Tech, Ph.D.,
Assistant Professor, Assistant Professor & Head
PG Department of Computer Applications,
Arignar Anna Institute of Management Studies & Computer Applications,
Pennalur, Sriperumbudur, Kanchipuram District – 602 105.

Abstrract – Most of the organizations are currently focusing on reducing the cost of investment in establishing the infrastructure to their project(s) as well as product development. The emerging trends in computing like virtualization and cloud computing would minimizes the resources in the concept of reducing space and operating cost. Moreover, cloud computing has an added level of risk because of the essential services are outsourced to a third party tools, which is harder to maintain privacy, data security, service availability and compliance violation. It is also difficult to monitor the traffic flow from machines present under cloud. We will discuss about how to monitor the traffic flow, identifying the security concerns and how to resolve the vulnerabilities and threats with minimal solutions in the areas of cloud computing and virtualized environment.

Keywords: Cloud computing, Virtualization, Vulnerabilities, Threats, Security, Traffic Monitoring.

1. INTRODUCTION

Cloud computing technologies became the first among the top 10 technologies which provide better prospect in successive years for the companies and organizations, revealed by a study done by Gartner[1]. Cloud computing provides the organization with secure, quick, convenient data storage and net computing service with a vision of services delivered across the internet. The services rendered by cloud computing combines virtualization, Service Oriented Architecture (SOA), Web 2.0 and other technologies like providing business applications through online to fulfill the needs of users where their data are present in a server[2].

The major risk areas in cloud computing includes external data storage, data sharing across "public internet", lack of control, multi-tenancy and integration with internal security. The resources belonging to the cloud computing service providers are distributed, virtualized and heterogeneous. The security mechanisms followed in traditional ways are identity, authentication and authorization which are not exists in current cloud platform [3]. It is difficult to integrate the security solutions for cloud services based on their services rendered, technologies used and mode of operations.

1.2 Challenges in cloud computing

The common challenges faced by organizations which implemented cloud services in it are secured data storage, high speed across internet and standardization. To protect the data before storing data from users present in cloud computing environment concerns about the privacy, identity and application specific preferences. Compared with many other countries in Europe and Asia, United States became far behind in broadband speed which provides untenable high speed connections on wired as well as wireless communications. Cloud computing environment is possible with high speed internet connectivity. Finally, the standardization procedure used for implementation of different computer systems is not defined, publically reviewed and ratified.

Some of the common issues present in the cloud concept based on historical context are internet cloud's evolutionary development and its challenges to overcome fell into two primary areas

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Special Issue 4, March 2017

hardware and software.

1.3 Server Virtualization

The method of running multiple independent virtual operating systems in a single physical computer is called as server virtualization. The creation and management of virtual machine is called as *platform virtualization*. Also virtualization is reducing the majority of hardware acquisition and maintenance costs. The hardware component used to enable platform virtualization is called *control program,* which is used for simulate the virtual environment.

1.4 Security issues in cloud

In every organization the usage of cloud differ from variety of service models (SaaS, PaaS, IaaS, DaaS, NaaS) and deployment models (Private, Public, Hybrid and Community). Based on the above cloud model the security issues are classified in 2 categories namely *security issues faced by cloud providers*and*security issues faced by their customers* [4]. Cloud solution provider (CSP) is the one who must ensure that customers will continue to have the same security and privacy controls over applications and their services. They will also provide an evidence for the customers that they should meet the security-level standards and agreements which will prove compliance to the auditors.

The misuse of information or resources from external sites is referred as a *threat* and if the system allows an attack with the help of flaws at the time implementing the system to be efficient is referred as *vulnerability.*

1.5 Security in SPI Model

The diagrammatic representation of Cloud computing providers are as follows:

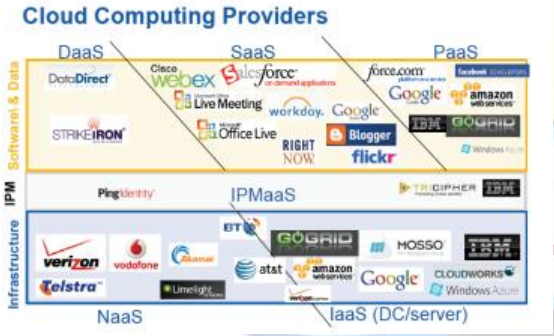

Figure1: Cloud computing providers

Based on the cloud providers the security provisions are described as follows :

Service	Description	Security Provision
Software as a Service (SaaS)	Consumer is allowed to use the provider's applications which is running on cloud infrastructure	Cloud provider has to minimize the accessibility based on customer control or extensibility
Platform as a Service (PaaS)	Allow the consumer to deploy their applications without installing base platform or tools in their local machines. This provides support of operating system and software development framework.	Depends on two software layers : security of the PaaS platform itself and security of customer applications deployed on platform.[5]
Infrastructure as a Service (IaaS)	Consumer is provided to access data storage, networks and other computing resources to deploy and run arbitrary software.	Minimize the threats at time of creation, communication, monitoring, modification and mobility of the systems.

2. Virtualization

Virtualization is the option of allowing the users to create copy, share, and migrate also rollback virtual machines for running a variety of applications [6]. The virtual machine (VM) security is most important one compared to the

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Special Issue 4, March 2017

physical machines since the VMs are more vulnerable to all types of attacks for the normal infrastructure. Unlike physical servers VMs have two boundaries: *physical and virtual*[7].

The virtualization providers for the creation, maintenance and monitoring the VMs are as follows:

Company Name	Virtualization Software
VMWare	vCenter / vSphere (Server/Client)
Microsoft	Hyper-V
Citrix	Xen
Redhat	RHEV
Amazon	Elastic Compute Cloud (EC2)
Google	Google Ganeti
Huawei	FusionSphere

Table1: Virtualization Software providers

In this paper, we are focusing on VMWare's vSphere Client for the creation, monitoring, and providing security of the VMs deployed.

2.1 Virtual Machine Manager (VMM)

Hypervisor otherwise called as virtual machine manager which is responsible for sharing the physical resources for administrator to create multiple operating systems. VMM is low level software that controls and monitors its virtual machines, keeping this as simple and small would reduce the risk of security vulnerabilities, so as to find and fix it easily. VMs located on same server can share CPU, memory, I/O and others. This will reduce the security of each VM.

2.2 Virtual Machines on VmWare

VMWare Inc, an American software company providing virtualization software and services and also specializing in virtualizing the x86 architecture family. VMware's desktop software runs on Microsoft Windows, Linux, and Mac OS X, while its enterprise softwarehypervisors for servers, VMware ESX and VMware ESXi, are bare-metal hypervisors that run directly on server hardware without requiring an additional underlying operating system.[8]

VMWare provides their own Java based Application Programming Interface (API) for accessing their VMs lying under their own hypervisor. Basically a bare-metal hypervisor of a Xen Server or HP Blade Server can be converted into an hardware providers for using vSphere client software. VMWare also provide Command Line Interface (CLI) commands over the ESX/ESXi hypervisor models for collecting the details of VMs which reside on the hypervisor server. On each VM's present under ESX/ESXi hypervisor on VMWare is supported by special cluster file system (CFS) called Virtual Machine File System (VMFS) [9].

The below diagram shows how multiple vSphere hosts with several virtual machines running on them can use VMFS to share a common clustered pool of storage.

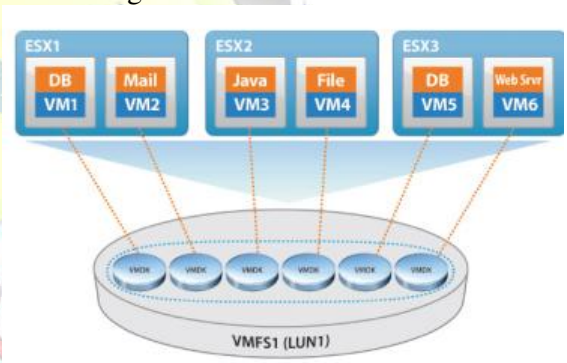

Figure 2: Virtual Machine File System overview

2.3 Monitoring the VMs

VMware provides several tools to help you monitor your virtual environment and to locate the source ofpotential issues and current problems[10].

a. **Performance Monitoring:**Allow you to see performance data on a variety of system resources includingCPU, Memory, Storage, and so on.
b. **Host health:**Allows you to quickly identify which hosts are healthy and which areexperiencing problems.
c. **Events, alerts, andalarms :**Allow you to configure alerts and alarms and to specify

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Special Issue 4, March 2017

the actions the systemshould take when they are triggered.

The performance monitoring of VMs and its server (hypervisor) ESX/ESXi has been done using the tools provided by the vCenter, which contains the following categories of performance monitoring.

1. **Monitoring the inventory objects:** contains the details of VMs, vNICs collected with the help of vSphere statistics collected from vCenter at frequent intervals.

2. **Monitoring Guest Operating System:** the performance of virtual machines which runs on Windows Operating system by installing vmware tools on it.

3. **Monitoring Host health status:** Used to collect the state of information of host hardware components such as CPU, Memory and other virtual components.

4. **Monitoring Events , Alarms and Automated Actions:** a set of user-configurable events and alarms of the sub-system helps in tracking vSphere client performance.

5. **Monitoring the network devices:**vSphere system runs SNMP agents on ESX(i) hosts to collect management information of both physical/virtual network devices using their enterprise MIBs.

3 Securing the Virtual environment

VMWare provides VIX API for accessing the guest operations, mainly authenticate on two security domains namely: vSphere Host, credentials for accessing the guest operating system.[11]

VMWare also ensures security in the ESX(i) environment from its system architecture, as a security perspective ESX consists of three major components: the virtualization layer, the virtual machines and the virtual networking layer.

The ESX architecture on security perspective can be present in VMWare as follows: [12]

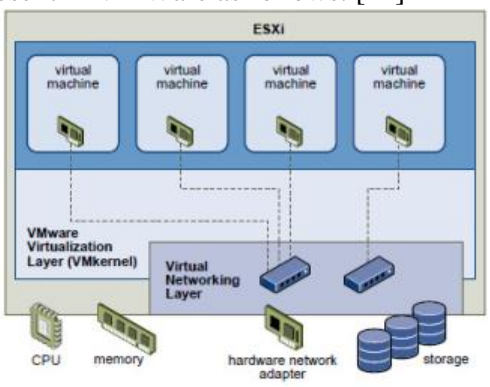

Figure2: ESXi Architecture

From the above diagram, the system administrator configured a host into three distinct virtual machine zones: FTP Server, internal virtual machines and DMZ. To reduce the risk of Denial of Service (DoS) and Distributed DoS (DDoS) the system administrator can configure certain limits of resource reservation for each and every virtual machine.

VMs can be secured by the use of firewalls components to safeguard the network and selected components in the network from any other intrusion to be configured by the system administrators. Securing the virtual management interface is difficult in protecting against unauthorized intrusion and misuse. The default recommendations are used for evaluating the host security and administration of the same: Limiting the user access, Use vSphere client to administer the ESX hosts and use only VMWare resources for upgrading the ESXi components.

The list of vulnerabilities and threats arise in cloud computing with appropriate measure to be taken to protect them are as follows:

Sl. No.	Vulnerabilities / Threats	Description	Measures to be taken
1	Data Related	a. Data backup taken by un-trusted providers[13] b. Incomplete data deletion (cannot be completely removed) c. Information	Specific Service Level Agreements to be provided by the Network Operations Center Administrator or system

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Special Issue 4, March 2017

		about data storage can be secured and made unavailable to un-trusted users. [14]	administrator
2	Vulnerabilities in Hypervisors	a. Complex Hypervisor Code[15] b. Flexible configuration of VMs	Configuring the Hypersafe [15], Trusted cloud computing platform (TCCP) and also a trusted virtual data center (TVDc) by admin can helps in protection
3.	Vulnerabilities in Virtual Machines	a. Unrestricted allocation and reallocation of resources in VMs.[13] b. Uncontrolled Snapshots – VMs cannot be copied [16] c. VMs IP address can be visualized to each & every user in the cloud [17]. d. Uncontrolled Migrations – VMs cannot be moved from one host to another [18].	Digital signatures, Encryption and FRS techniques to be provided.
4.	Vulnerabilities in Virtual Networks	Sharing of virtual bridges by several virtual machines [19].	Adopting the virtual network framework based on Xen servers to be bridged and routed.
5.	Vulnerabilities in Virtual Machine Images	a. Uncontrolled placement of VM Images in public repositories [7] b. VM images should not be patched because of their dormant artifacts	Mirage
6.	Data Leakage	The transfer of data to un-trusted users should be protected [20]	Encrypting the data at the time of transfer with the help of digital signature.
7.	Denial of Service	The resources should be protected from malicious user attacks which may downgrade the performance of application runs on Guest OS.	Provide a list of policies for protecting the computational resources.
8.	VM escape	Designed to exploit the hypervisor to control the infrastructure.[7]	Hypersafe configuration
9.	Sniffing / Spoofing virtual networks	A malicious or un-trusted VM must listen to the virtual network and also use ARP spoofing to redirect the packets from each other [19].	Adopting the virtual network framework.

Web services are the largest implementation technology in cloud environments which may also lead to several challenges need to be addressed. The security web services standards describe how the communication between applications could be done and also checks the integrity, confidentiality, authentication and authorization of the data. By adopting the security standard specifications like Security Assertion Markup Language (SAML), WS-Security and XML digital signature.

4Conclusion

Cloud computing is relatively provides a vide range of benefits for their users across various levels. Using the cloud computing technology the organizations can reduce or leverage the administrative costs for implementing the hardware resources for running the applications over cloud environment. Traditional web applications, data hosting and virtualization

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Special Issue 4, March 2017

security are discussed in the above sample vulnerabilities and threats.

The cloud service provider models are expressed to understand the sharing of resources and application without installing or changing the resources. Many surveys discussed the vulnerabilities and threats which are common in cloud among those the important issues are taken for discussion in this area.

In future we are focused on the comparison of various virtual environment providers from different organizations like Google, Microsoft and Redhat etc., In that we are focusing on the application provision and usage of hardware resources by individual software providers. Also, able to compare the security concerns in the API level and tools provided by hypervisor software.

REFERENCES

[1] Gartner Inc. Gasrtner identifies the Top 10 strategic technologies for 2011. Online available: http://gartner.com/it/page.jsp?id=145221. Accessed: 15-Jul-2011.

[2] Marinos A, Briscose G (2009) Community Cloud Computing. In: 1st International conference on cloud computing (CloudCom), Beijing, China. Springer-Verlag Berlin, Heidelberg

[3] Li W, Ping L (2009) Trust model to enhance Security and interoperability of cloud environment. In: Proceedings of the 1st International conference on cloud computing. Springer Berlin, Heidelberg, Beijing, China, pp 69-79.

[4] Cloud computing Wiki page

[5] Mather T, Kumarasamy S, Latif S (2009), Cloud security and privacy. O'Relilly Media, Inc, Sebastopol, CA

[6] Garfinkel T, Rosenblum M (2005) When virtual is harder than real: Security challenges in virtual machine based computing environments, In: Proceedings of the 10th conference on Hot topics in operating systems, Santa Fe,NM. Volume 10. USENIX Association Berkley, CA, USA, pp 227-229.

[7] Morsy MA, Grundy J, Muller I (2010) An analysis of the cloud computing security problem In: Proceedings of APSEC 2010 Cloud Workshop APSEC, Sydney, Australia

[8] *"ESX Server Architecture". Vmware.com. Archived from the original on January 31, 2009. Retrieved 2009-10-22.*

[9] *"vSphere 5.0 Storage Features Part 1 - VMFS5". VMware. 2011-07-12. Retrieved 2012-01-05.*

[10] vSphere Monitoring and perfromance, Revision 000799-02, VMWare Inc, 2010-2013 published.

[11] https://www.vmware.com/support/developer/vix-api/vix111_reference/security.html

[12] http://pubs.vmware.com/vsphere-51/topic/com.vmware.ICbase/PDF/vsphere-esxi-vcenter-server-511-security-guide.pdf

[13] Winkler V (2011) Securing the Cloud: Cloud computer Security techniques and tactics. Elsevier Inc, Waltham, MA

[14] Jansen WA (2011) Cloud Hooks: Security and Privacy Issues in CloudComputing. In: Proceedings of the 44th Hawaii International Conference onSystem Sciences, Koloa, Kauai, HI. IEEE Computer Society, Washington, DC,USA, pp 1–10.

[15] Wang Z, Jiang X (2010) HyperSafe: a lightweight approach to providelifetime hypervisor control-flow integrity. In: Proceedings of the IEEEsymposium on Security and privacy. IEEE Computer Society, Washington,DC, USA, pp 380–395

[16] Rittinghouse JW, Ransome JF (2009) Security in the Cloud. In: CloudComputing. Implementation, Management, and Security, CRC Press

[17] Ristenpart T, Tromer E, Shacham H, Savage S (2009) Hey, you, get off of mycloud: exploring information leakage in third-party compute clouds. In:Proceedings of the 16th ACM conference on Computer andcommunications security, Chicago, Illinois, USA. ACM New York, NY, USA,pp 199–212

[18] Dawoud W, Takouna I, Meinel C (2010) Infrastructure as a service security:Challenges

and solutions. In: the 7th International Conference onInformatics and Systems (INFOS), Potsdam, Germany. IEEE ComputerSociety, Washington, DC, USA, pp 1–8

[19] Wu H, Ding Y, Winer C, Yao L (2010) Network Security for virtual machine inCloud Computing. In: 5th International conference on computer sciencesand convergence information technology (ICCIT). IEEE Computer SocietyWashington, DC, USA, pp 18–21

[20] Keiko Hashizume, David G, Eduardo F, (2013) An analysis of security issues for cloud computing. In : International journal of internet services and applications, 4:5, Pg. 6-9.