ISSN: 2393-8528

IJICSE Open Access

Contents lists available at www.ijicse.in

International Journal of Innovative Computer Science & Engineering

Volume 1 Issue 3; Page No.27-29

A Survey on Secure the Cloud Environment using hypervisor-based virtualization technology

Urmila Jangid, Nidhi Sharma, Kalpana Rathi

Jyoti Vidyapeeth Women's, University, Jaipur, Rajasthan, India

ARTICLE INFO

Received 12 Oct. 2014
Accepted 30 Nov. 2014

Corresponding Author:

Urmila Jangid

1 Jyoti Vidyapeeth Women's, University, Jaipur, Rajasthan, India

Key words: Virtualization, cloud computing, security, hypervisor, cloud environment.

ABSTRACT

Cloud computing is one of today's most sensational technologies, because it can decrease the cost and complexity of applications, and it is flexible and accessible. These benefits changed cloud computing from a thoughtful idea into one of the fastest growing technologies today. For bright future of this technology we need to secure the cloud using virtualization technology. Virtualization is the core of cloud computing. Actually virtualization technology is an old technology and has had security issues that must be addressed before cloud technology is affected by them. The virtualization technology has limit security capabilities in order to secure wide area environment such as the cloud. This paper proposes new security architecture in a hypervisor-based virtualization technology in order to protect the cloud environment.

1. INTRODUCTION

When you store your photos online instead of on your home computer, or use webmail or a social networking site, you are using a "cloud computing" service. Cloud computing refers to the delivery of computing resources over the Internet. Basically a cloud computing is a network-based environment that focuses on sharing computations and resources. Cloud technology is built on Virtualization technology which has limited security capabilities in order to secure a wide area environment such as the cloud. Generally, Cloud providers use virtualization technologies and virtualization technology is to allow large expensive mainframes to be easily shared among different application environments.More recently, virtualization at all levels (system, storage, and network) became important again as a way to improve system reliability and availability, security, reduce costs, and provide greater flexibility. Because virtualization is not a new technology and it has not enough security capabilities for wide network such as cloud.

Hypervisor is a software program manages multiple operating systems in single computer system. The hypervisor manages the system's memory, processor, and other resources. A hypervisor allow to multiple operating systems, termed guests, to run concurrently on a host system, a feature called hardware virtualization.

2. CLOUD MODELS:

In the cloud computing distribution model services like infrastructure of software and hardware, networking, storage are provided to the clients. Cloud has three working models

1.1. Public cloud: A public cloud is maintained by the cloud provider and is open for public use. The infrastructure is provided to many clients and is managed by the third party. Users can simultaneously access the application equally. The main feature of public cloud is more than one user can access anywhere any time through internet. Example of a public cloud is Amazon, Google, Microsoft, Sales Force etc.

1.2. Private cloud: The services and infrastructure made offered to a specific customer, which is maintained and manage by the organization not share to other organization. In private hardware and software sharing is limited and security is provided by encryption. Private cloud provides the higher security, improved reliability and efficiency in cloud environment. Examples of a private cloud is HP data center, IBM, Sun, Oracle, 3tera etc.

1.3. Hybrid cloud: A hybrid cloud is an integrated cloud service utilizing both private and public clouds to perform various functions within the same organization. Simply a usage of both private and public cloud together is called hybrid cloud. Public cloud services are more cost effective and scalable than private clouds. Therefore, an organization can maximize their efficiencies by employing public cloud services for all non-responsive operations, only relying on a private cloud where they require it and ensuring that all of their platforms are seamlessly integrated.

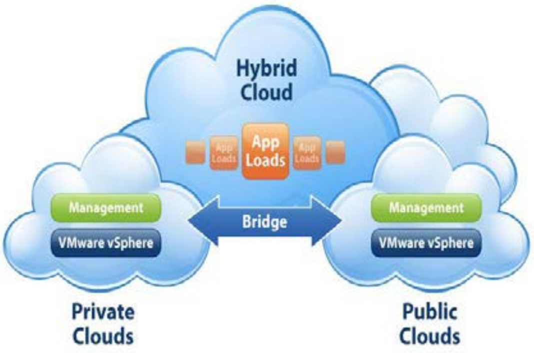

Figure 1: Types of cloud

3. VIRTULIZATION TECHNIQUE IN CLOUD ENVIRONMENT

Virtualization is a technology to create cloud computing platform.Virtualization is the strength of cloud computing. Virtualization is the concept of hardware or software system that lets applications run on top of the virtualized environment without the need of knowing the original resources available. Otherwise the virtualized environment is known as the virtual machine (VM). It lets you run multiple virtual machines on a single physical machine, with each virtual machine sharing the resources of single physical computer across multiple environments. Different virtual machines can run different operating systems and multiple applications on the same physical computer. Moreover, since because of this virtualization key technology, effective utilization of resources are more promising feature of cloud computing. Since many servers can run on a single server, many virtual machines can run on a single host machine with a help of a hypervisor which in turn saving power, which shows the way to green computing. Some of the key points to maintain security of the cloud.

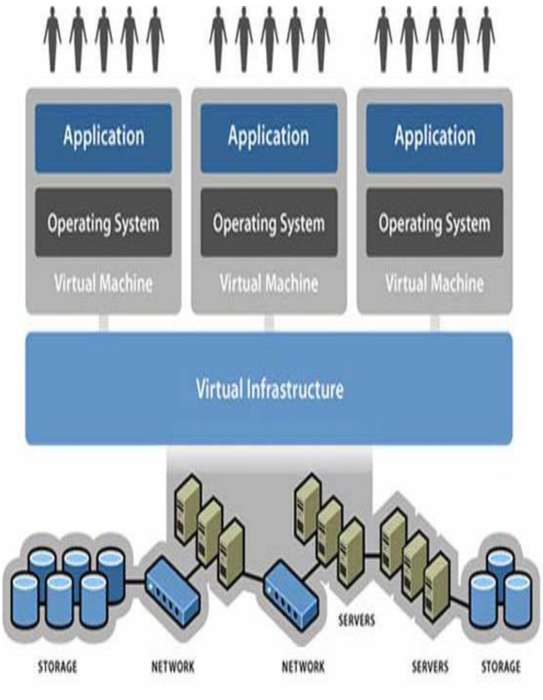

Figure 2: Virtualization mechanism

4. VIRTUALIZATION RELATED APPROACHES

There are several common approaches to virtualization with differences between how each controls the virtual machines. These are following approaches is

1.4. Operating system-based virtualization: In this approach ,Virtualization is enabled by a hosting operating system that supports multiple isolated and virtualized guest OS on a single physical server with this characteristic that all are on the same operating system kernel with has control on Hardware infrastructure Fully. The hosting operating system has visibility and control over the VMs. This approach is simple but it has vulnerabilities. For example, an attacker can inject kernel scripts in hosting operating system and this can cause all guest OS have to run their OS on this kernel. The result is attacker have control over all VMs that exist or will establish in future.

1.5. Application-based virtualization: An application-based virtualization is hosted on top of the hosting operating system. This virtualization method follows each VM which contains its own guest operating system and related applications. This virtualization architecture is not commonly used in commercial environments. Security issues of this approach are similar to Operating system-based.

1.6. Hypervisor-based virtualization: As mentioned before, a hypervisor is embedded in the hardware infrastructure or the hosting operating system kernel. The Hypervisor is available at the booting time of machine in order to control the sharing of system resources across multiple VMs. Some of these VMs are privileged partitions that they managed the virtualization platform and hosted VMs. In this architecture, the privileged partitions have visibility and control over the VMs. This approach establish most controllable environment and can perform additional security tools such as Intrusion detection systems. But it was vulnerable because of the hypervisor is single point of failure. If hypervisor crashed or attacker gets control over it then all VMs are on the attacker control. However, take control over hypervisor from VM level is difficult but not impossible.

5. BENEFITS OF HYPERVISOR TO PROVIDE THE SECURE ENVIRONMENT

- Hypervisor provides a narrow interface nearly similar to original hardware interface in traditional system to Guest OS. Actually Hypervisor teaches the hardware in favor of guest OS. This capability allows hypervisor-based virtualization to have a secure infrastructure. Hypervisor can performance as a firewall and will be able to prevent malicious users to from compromising the hardware infrastructure.
- Hypervisor is implemented below the guest OS in the cloud computing hierarchy, which means that if an attack passes the security systems in the guest OS, the hypervisor can detect it and it also, provides simplified transaction monitoring process.
- Some services take advantage of services provided by hypervisors. Like a service running below the operating system can fairly easily encapsulate the whole state of a virtual machine. The resulting capsule can then be used to migrate the virtual machine to another physical machine.

SECURITY RELATED ISSUES

In this technology a hypervisor is responsible for creation and management of virtual machines. By attacking on hypervisor, attacker can gain access to all guest machines that is running on host machine. Security can be related to the number of client-server domain. Basically work related to the following attack surface areas.

Service-to-User: This is the common server-to-client interface, thus enabling (and being vulnerable to) all kinds of attacks that are possible in common client-server-architectures as well such as man-in-the-middle, cloud malware injection attack.

User-to-Service: This is the common environment a client program provides to a server, e.g. browser-based attacks for an HTML based service attacks on browser caches and sessions.

- Single point of failure: if the hypervisor crashes or if is affected by attack then the virtualization system fails.
- Vulnerability: hypervisor are vulnerable to Buffer overflow, Format string attacks.
- In cloud various kinds of attacks like session attack, man-in-the-middle attack, flooding attack, cloud malware injection attack etc.

6. CONCLUSION:

Cloud computing is a new technology in field of information technology. This paper provides the basic knowledge of hypervisor and virtualization these models and security related issues. This paper showed some crucial and well known security attacks of different security notions that can be possible on hypervisor.

In the future, research should aim to provide new architectures, and techniques to maintain security on higher level for hypervisors. The concepts have discussed here will help to build a strong architecture for hypervisor security in the fields of cloud computing.

7. REFERENCES:

1. Nancy Arya , Mukesh Gidwani and Shailendra Kumar Gupta ,Hypervisor Security - A Major Concern, International Journal of Information and Computation Technology, ISSN 0974-2239 Volume 3, Number 6 (2013), pp. 533-538.
2. Lena AlMutair, Soha S. Zaghloul, A NEW VIRTUALIZATION-BASED SECURITY ARCHITECTURE IN A CLOUD COMPUTING ENVIRONMENT, ISBN: 978-0-9853483-3-5 (2013).
3. Farzad Sabahi, Member, IEEE, Secure Virtualization for Cloud Environment Using Hypervisor-based Technology, International Journal of Machine Learning and Computing, Vol. 2, No. 1, February 2012.
4. Farzad Sabahi, Secure Virtualization Technology, International Journal of Computer Theory and Engineering, Vol. 4, No. 5, October 2012.
5. Madhu Chauhan, Riidhei Malhotra, Mukul Pathak, Uday Pratap Singh, DIFFERENT ASPECTS OF CLOUD SECURITY , International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622. Vol. 2, Issue 2, Mar-Apr 2012, pp.864-869.
6. Krishna tej Koganti1, Eswar Patnala2, Sai Sagar Narasingu3, J.N. Chaitanya, Virtualization Technology in Cloud Computing Environment, International Journal of Emerging Technology and Advanced Engineering (ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 3, Issue 3, March 2013).
7. T.Swathi, K.Srikanth , S. Raghunath Reddy, VIRTUALIZATION IN CLOUD COMPUTING, International Journal of Computer Science and Mobile Computing, Vol.3 Issue.5, May- 2014(pg. 540-546) ISSN: 2320–088X