ijournals International Journal of Software & Hardware Research in Engineering
ISSN No: 2347-4890 Volume 2 Issue 3, March 2014

Security challenges and antivirus layer role in cloud

Pooja V. Bhokare[1]; Chitra J. Patil[2];

Assistant Professor, SSBT COET Bambhori, Jalgaon[1];

Assistant Professor, SSBT COET Bambhori, Jalgaon[2];

ABSTRACT

As we know, Cloud is an emerging era in the field of Information Technology. The cloud computing resolves biggest issues regarding Information Technology. But the cloud itself can also be not secure. There are various issues that can create biggest problem in cloud environment. This paper mainly focuses on problems regarding cloud environment and how these security issues can be resolved in the cloud.

Keywords

Virtualization, Virtual Machine, Security, Integrity

1. INTRODUCTION

Generally, a cloud computing is a large-scale distributed network system implemented based on a number of servers in data centers. The cloud services are generally classified based on a layer concept. In the upper layers of this paradigm, Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS) are stacked. Data centers layer: This layer provides the hardware facility and infrastructure for clouds. In data center layer, a number of servers are linked with high-speed networks to provide services for customers. Typically, data centers are built in less populated places, with high power supply stability and a low risk of disaster. Infrastructure as a Service (IaaS): IaaS is built on top of the data center layer. IaaS enables the provision of storage, hardware, servers and networking components. The client typically pays on a per-use basis. Thus, clients can save cost as the payment is only based on how much resource they really use. Infrastructure can be expanded or shrunk dynamically as needed. The examples of IaaS are Amazon EC2 (Elastic Cloud Computing) and S3 (Simple Storage Service). Platform as a Service (PaaS): PaaS offers an advanced integrated environment for building, testing and deploying custom applications. The examples of PaaS are Google App Engine, Microsoft Azure, and Amazon Map Reduce/Simple Storage Service. Software as a Service (SaaS): SaaS supports a software distribution with specific requirements. In this layer, the users can access an application and information remotely via the Internet and pay only for that they use. Sales force is one of the pioneers in providing this service model. Microsoft's Live Mesh also allows sharing files and folders across multiple devices simultaneously .Although the cloud computing architecture can be divided into four layers shown in Fig 1.6. It does not mean that the top layer must be built on the layer directly below it. For example, the SaaS application can be deployed directly on IaaS, instead of PaaS. Also, some services can be considered as a part of more than one layer. For example, data storage service can be viewed as either in IaaS or PaaS. Given this architectural model, the users can use the services flexibly and efficiently. Now, we see how cloud security belongs to authentication, authorization, confidentiality and non repudiation.

2. CLOUD SECURITY

As we know, Cloud computing is an emerging area in the field of Information Technology. The cloud can easily solves various problems regarding Information Technology such as security problems, storage problems, globalization problems and cost problems. Thus all these problems are easily overcome by the cloud. The most important topic here is Resource pool i.e. the virtualization. The cloud is divided into two parts i.e. classic data center and virtual data center and the most important step towards the cloud is virtualization machine. The virtual machine is a logical machine which behaves and acts like a physical machine. This virtual machine consists of files as logical files that are stored on the physical machine. The security of these files is an important aspect. The authentication, authorization, data integrity, confidentiality and non repudiation are main goals of security. Coming towards virtualization, the virtualization creates file system either in VMFS or NFS. The VMFS and NFS are two file systems which

work over the virtualization. So it must be important to keep these file systems very secure. In case of cloud computing, as we all know that cloud can be public, private and hybrid. This can be shown in figure 1.1

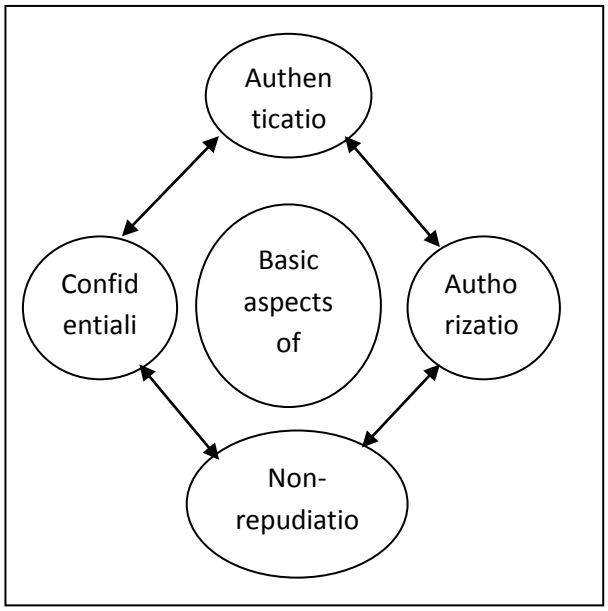


Figure 1.1. Basic aspects of security

The private cloud is less vulnerable because it contains data regarding to only one domain and it keep that data accessible to only that domain. Others can't accept that data. The public clouds are more vulnerable because they contain the various data from different domain around the world. The main distributors of the public cloud are mainly responsible for the providing the services to the cloud.

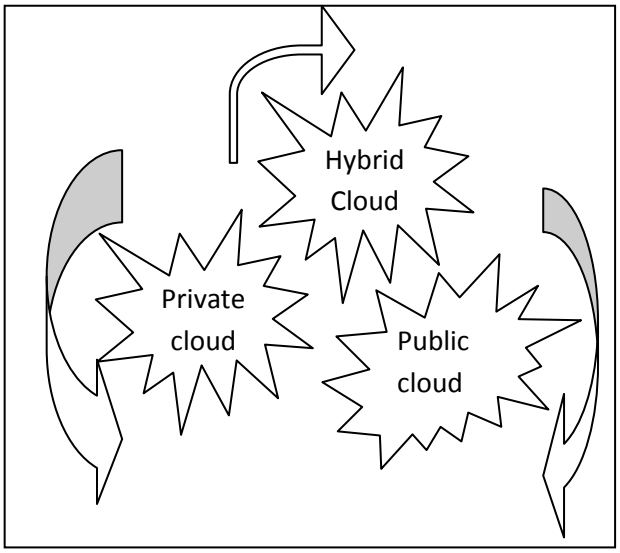


Figure 1.2. The cloud system

3. PROBLEM DOMAIN

The main vulnerability of cloud computing which causes cloud more vulnerable is shown in following figure. Basically, it consists of bad operating system services, software maintenance, password and access control, malicious service, dangerous services and application services. These vulnerabilities are connected in such a way that they all causes cloud to be vulnerable. The interconnection between them is shown in following figure The main various vulnerability which can cause problem, this vulnerability can destroy the applications the main problem which can occur if operating system do not work properly is about the operating system not configured properly, the virtualization layer i.e. Hypervisor which mainly allows the many operating system to run simultaneously on the physical machine, the main vulnerability can create problem for the system. The malware can easily exploit the property of machine they can be categorized into two form either required a host program and other one is independent.

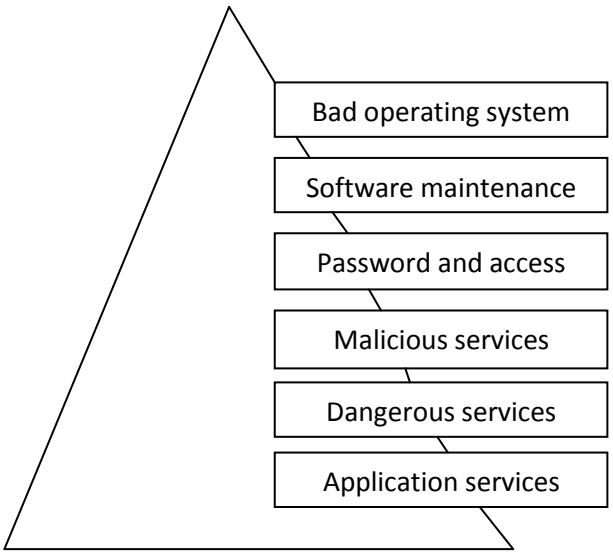


Figure.1.3. Cloud vulnerabilities

Trapdoor, logic bomb, virus and Trojan horse are malware which always required an host program. They always required a file to support while worm and zombie perform independently. The virtual machine consist of applications and operating system, the virtualization layer mainly works between physical machine and virtual machine these virtual file runs over the physical machine. When the machine start booting at that instant if the boot sector virus can easily exploit the booting problem does not allow the machine to boot, while memory resident virus can exploit the memory of system.

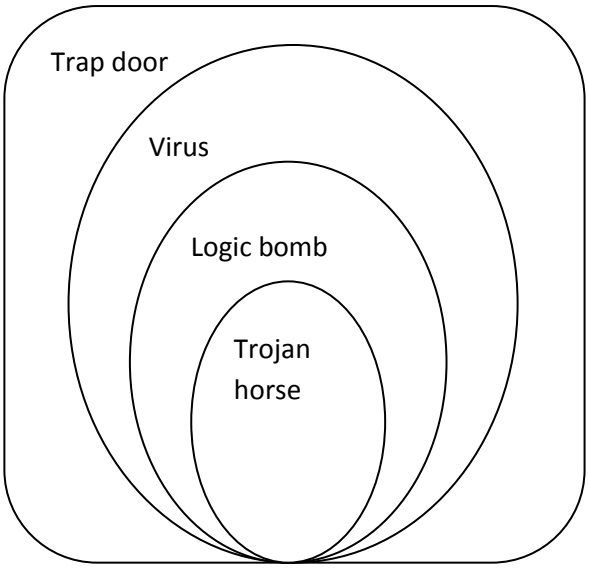
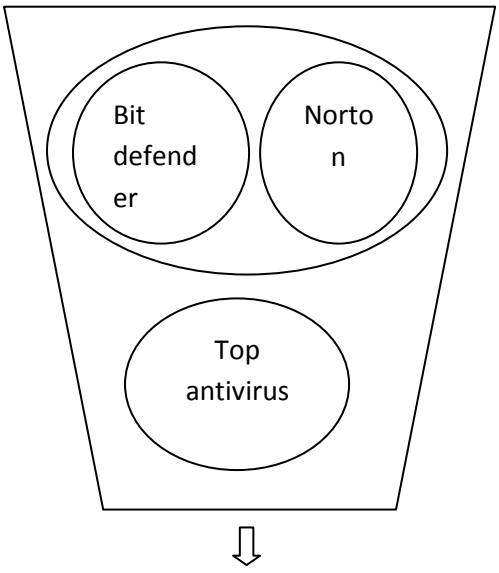


Figure 1.4. Various Malware

The virtualization can easily suffer by these malware, so there should be an antivirus between the physical machines, virtual machine. Above the hypervisor layer the antivirus layer should work. These will prevent the physical machine from various threats and various problems regarding virtualization can also be solved the antivirus which should be placed in cloud, it should be cloud antivirus, mainly combine the best antivirus system: cloud antivirus should combine all the best features of top antivirus such as Norton, Bit defender, kaspersky , MacAfee, Avast, and so on : Following figure 1.5 shows the concept of cloud antivirus which mainly combine all top antivirus services and new antivirus which is cloud antivirus is used these antivirus mainly work between the physical machine and virtual machine



Cloud antivirus

Figure 1.5. The cloud antivirus

4 .LAYERS OF CLOUD COMPUTING

The cloud computing is composed of several layers, all of which can be accessed by users connected to it. Understanding what each layer comprises of, the functions of each layer, how these layers interact with each other, including the need for diverse technological skills to make the elements work together, are all essential.

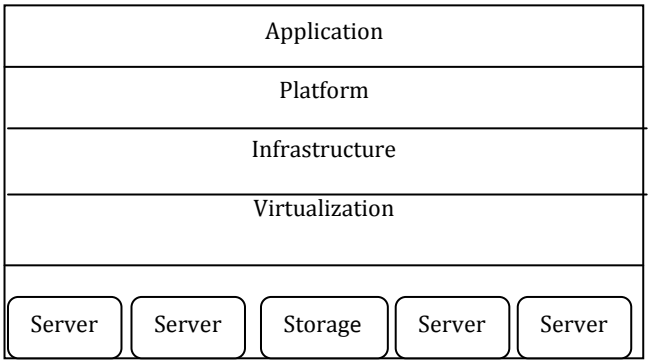


Figure 1.6. Layers of cloud computing

Cloud computing demands a mix of technology skills, negotiating skills, and people skills and business acumen. By simplifying the cloud computing concept into layers, it is easier to define the roles and skills needed within the overall structure to see where your business fits into the model. There are the four key layers of a cloud environment and the technological skills required to better understand the aspects of cloud computing as shown in figure 1.6.

4.1. THE VIRTUALIZATION LAYER

This layer forms the foundation of cloud technology. This enables user request for computing resources by accessing appropriate resources and deploy large numbers of virtual machines (VMs) on hardware. The most important skill needed is that understanding virtualization management principles, such as load balancing. Other necessary skills are having knowledge of the virtualization platform, storage, connecting storage to a virtualization host, and allocating storage properly. Networking knowledge is also needed to configure hosts properly.

4.2. THE NETWORKING LAYER

It is in this layer that solid understanding of network protocols such as TCP/IP and domain name server, including switching and routing principles are needed.

4.3. THE OS LAYER

The core skills required are ensuring that the system is properly tuned for its role, setting up a server with correct applications and settings, and maintaining optimal performance settings. To ensure that cloud services are optimally deployed, delivered and maintained, networking skills are also vital in this layer.

4.4. .THE APPLICATION LAYER

This is the most utilized layer of cloud computing. The cloud provided needs responsibility in the management of the software and databases, including installation, updates and removal. Cloud developers should have knowledge in JavaScript, XML and Perl languages.

5. ANTIVIRUS LAYER

The problem of virtualization is to maintain the data integrity and Confidentiality. Integrity in the virtualization mainly focus on data content, problem of virtual machine loss, data leakage loss and virtual machine theft loss can be controlled if the cloud AV can be used between the Hypervisor and virtual machine. So the theft problem can be controlled and data leakage problem can be avoided. Cloud antivirus mainly provide the protection against various malware, as various malware spread in different forms and these virus can destroy the various applications in various modes several virus such as Boot sector virus, memory resident virus, polymorphic virus, stealth virus , parasitic virus. These viruses mainly work in four different phases they can be dormant phase, propagation phase, triggered phase and last execution phase. These different viruses can destroy various cloud application running on classic data center. So the protection of these is quite necessary. The antivirus layer mainly avoids these malware from spreading into the system. So according to our paper [cloud service utilization] the antivirus layer mainly lies in between physical machine and virtual machine. The antivirus layer is shown in figure 1.6.

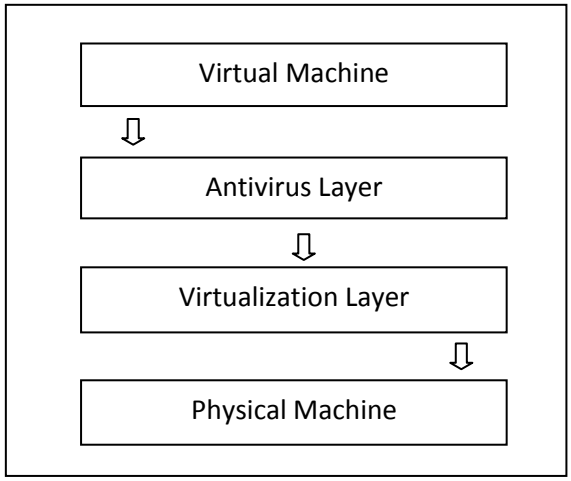


Fig.1.7. Antivirus layer

6. CLOUD FRAMEWORK DESIGN

This paper described a flexible approach to manage autonomically cloud resource isolation between different layers, reconciling computing and network views. The corresponding framework overcomes fragmentation of security components and automates their administration by orchestrating different autonomic loops, vertically and horizontally. Going beyond the presented architecture requires several modules in different views, currently under implementation. HTTP Web servers included into physical equipments need specific APIs and a wrapper in the AVM. At the hypervisor layer, the libvirt API uses a library named netcf to enforce new network rules via XML. Although the frontend is clearly defined, the back end is OS-dependent. We thus have to fully translate netcf's XML configuration files and to implement commands for interface creation, modification and deletion. In the VM layer, we have chosen to use ClamAV as a flexible antivirus with Python support for remote control as source code is available. Real time production is missing but we are implementing a kernel module to scan files when they are loaded in memory and control their execution. This example underlines what can be achieved in the VM layer:

7. CONCLUSION

Cloud computing an emerging area and various vendors providing various services to cloud. These services can be secure at client end. If the antivirus layer mainly works between the physical layer and virtual machine, various viruses can be avoided before they execute in the system. The vulnerability

such as bad operating system configuration, malware services etc can be easily avoided in the system. The system can be safe and secure.

8. REFERENCES

[1]http://india.emc.com/microsites/cloud/cloud.htm ?p Id=home-small-cloudtransformsit-230212

[2]http://www.iprodeveloper.com/article/security/c lou D-security-698789,.

[3].http://www.computerworlduk.com/news/securit y/3297764/dropbox-fixes-three-major-cloudvulnerabilities/

[4].http://en.wikipedia.org/wiki/Cloud computing

[5]...http://www.ibm.com/developerworks/websphe re/techjournal/0904_amrhein/0904_amrhein.html

[6].http://india.emc.com/index.htm?fromGlobalSiteS elect

[7].http://www.businessweek.com/technology/conte nt/Aug2008/tc2008082_445669_page_3.htm

[8] http://en.wikipedia.org/wiki/Cloud_computing