Virtualization and Cloud Computing

Yuping Xing and Yongzhao Zhan

School of Computer Science and Telecommunication Engineering, Jiangsu University, Zhenjiang, China
{xingyuping,yzzhan}@ujs.edu.cn

Abstract. Cloud Computing is the fundamental change happening in the field of Information Technology. It is a representation of a movement towards the intensive, large scale specialization. Virtualization is the key component of cloud computing. With the use of virtualization, cloud computing brings about not only convenience and efficiency benefits, but also great challenges in the field of data security and privacy protection. For example, it maybe bind different tenants' virtual resources to the same physical resource, then the user data will be accessed by other users. To solve this problem, the paper analyses and discusses several ways to improve the safety of cloud computing.

Keywords: Cloud Computing, Cloud Security, Virtualization.

1 Introduction

Cloud computing has improved computation's efficiency while reducing its cost for users[1].Virtualization is the key component of cloud computing for providing computing and storage services. Although most readers should be familiar with sharing CPU and storage facilities, the memory leak and hard disk leak have not been described as well. This paper introduces cloud computing, virtualization technologies, and discusses the relationship between them, and presents risk of security by the use of the virtualization technology and the ways to bring down the danger.

2 What Is Cloud Computing

Cloud computing is a technology that uses the internet and central remote servers to maintain data and applications. Cloud computing allows consumers and businesses to use applications without installation and access their personal files at any computer with internet access. This technology allows for much more efficient computing by centralizing storage, memory, process- sing and bandwidth.

2.1 The Background of Cloud Computing

The general idea behind the technology dates back to the 1960s, when John McCarthy wrote that "computation may someday be organized as a public utility." Then, grid computing originated in the early 1990s as an idea for making computer power as easy to access as an electric power grid also contributed to cloud computing. [2] The first

Y. Zhang (Ed.): Future Wireless Networks and Information Systems, LNEE 143, pp. 305–312.
springerlink.com

time the term “cloud computing” was used in its current context was in a 1997 lecture by Ramnath Chellappa.

One of the first movers in cloud computing was Salesforce.com, which in 1999 introduced the concept of delivering enterprise applications via a simple website. Amazon was next on the bandwagon, launching Amazon Web Service in 2002. Then came Google Docs[3] in 2006 which really brought cloud computing to the forefront of public consciousness. 2006 also saw the introduction of Amazon’s Elastic Compute cloud (EC2)[4] as a commercial web service that allowed small companies and individuals to rent computers on which to run their own computer applications.

This was soon followed by an industry-wide collaboration in 2007 between Google, IBM and a number of universities across the United States. Next came Eucalyptus in 2008, the first open source AWS API compatible platform for deploying private clouds, followed by Open Nebula, the first open source software for deploying private and hybrid clouds.

2009 saw Microsoft’s entry into cloud computing with the launch of Windows Azure[5] The latest entrants include Oracle, Dell, Fujitsu, Teradata, HP, and a host of other household names.

In China, the cloud is growing very fast. In 2008, The China's first and second cloud computing center, established by IBM, was put into operation in Wuxi and Beijing; In 2010, Shanghai is committed to create "Asia-Pacific Cloud Computing Centers" in the next 3 years; Currently, the "Cloud Computing Industry Base in Shanghai" has been settled in Shanghai.[6]

2.2 Cloud Computing Model

This cloud model promotes availability and is composed of five essential characteristics, three service models, and four deployment models[7].

Five essential characteristics:(1)On-demand self-service;(2)Ubiquitous network access: available through standard Internet-enabled devices;(3) Location independent resource pooling;(4)Rapid elasticity;(5)Pay per use.

Three service models defined by NIST (National institute of Standards and Technology, U.S. Department of Commerce): (1)SaaS (Software as a Service): The consumer is free of any worries and hassles related to the service. The Service Provider has very high administrative control on the application and is responsible for update, deployment, maintenance and security. The provider exercises final authority over the application. For example, Gmail, Salesforce’s CRM are SaaS; (2)PaaS(Platform as a Service): The entire life cycle of a software can be operated on a PaaS, like Google Apps Engine, Microsoft Windows Azure; (3)IaaS(Infrastructure as a Service): Providers rent virtual computers, cloud storage, network infrastructure components to consumers, and usage fees are calculated. Amazon is the pioneer of IaaS.

Four deployment models[9]:(1)Private cloud: The cloud infrastructure is operated solely for an organization; (2)Community cloud: It is shared by several organizations and supports a specific community that has shared concerns; (3)Public cloud: The cloud infrastructure is made available to the general public or a large industry group and is owned by an organization selling cloud services;(4)Hybrid cloud: The cloud infrastructure is a composition of two or more clouds (private, community, or public) that remain unique entities but are bound together by standardized or proprietary technology that enables data.

Although different deployment models cater to different kind of consumers, they have common cloud characteristics, such as massive scale, homogeneity, virtualization, resilient computing, low cost software, geographic distribution, service orientation and advanced security technologies. Virtualization technology is one key component of cloud computing. Fig. 1[10] shows the architecture of cloud computing from the point of virtualization.

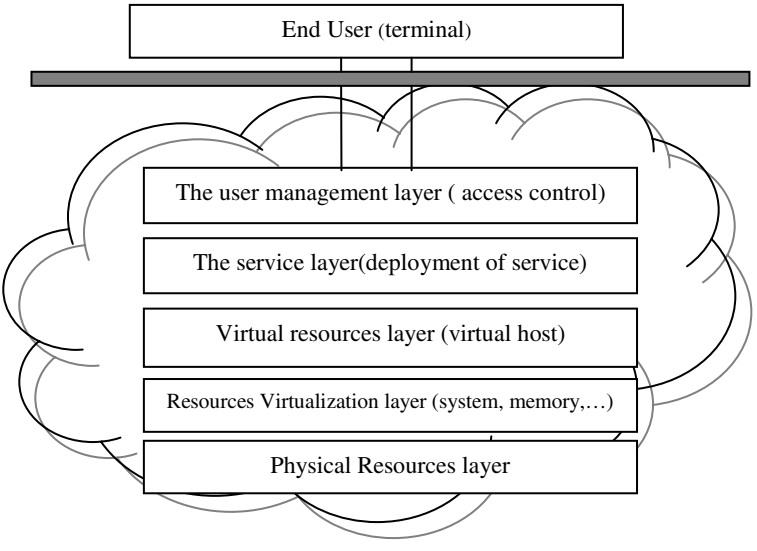

Fig. 1. Architecture of Cloud Computing

Cloud computing makes end users get service anywhere through different kinds of terminal. The resources it required come from cloud instead of visible entity. You can take your need through net service using a notebook pc or a mobile phone. Users can attain or share it safely through an easy way, anytime, anywhere. Users can complete a task that can't be completed in a single computer. The user management layer is the interaction entrance between user and cloud, and the user access "clouds" through it. The cloud computing service provides control the access to this layer. The service layer transforms various resources of the cloud into the corresponding services (such as storage, software as a service, platform and services) which will cater to end users. Virtual resources layer will integrate and manage the resources what have been virtualized, and then provide it for its upper layer. Resources Virtualization layer processes the virtualization of all kinds of the computing resources, and it makes sure that users do not have to deal with the problem such as real physical machine position, maintenance, and so on. In the bottom of the architecture is the physical resource layer, it is the foundation of the whole cloud computing platform, storage of real physical resources. By introducing virtualization, cloud computing allows users don't have to care about the maintenance of physical host, management and optimization problem.

3 Discussion about Virtualization

Virtualization is a foundation technology platform fostering cloud computing. The term virtualization refers to the abstraction of compute resources (CPU, storage, network, memory, application stack, and database) from applications and end users consuming the service. Virtualization technologies enable multi-tenancy cloud business models by providing a scalable, shared resource platform for all tenants.

3.1 Different Kinds of Virtualization

From an enterprise perspective, virtualization offers data center consolidation and improved IT operational efficiency. Today, enterprises have deployed virtualization technology within data centers in various forms, including OS virtualization (VMware[11], Xen), storage virtualization (NAS, SAN), database virtualization, and application or software virtualization (Apache Tomcat, JBoss, Oracle App Server, WebSphere).

IaaS providers including Amazon (EC2) and Sun Cloud employ OS virtualization, which enables customers to run instances of various operating system flavors in a public cloud. In addition to OS and storage virtualization, Saas and PaaS service providers are known to have implemented software and database resources. For example, Salesforce.com is known to have virtualized both the software and the database stack.

3.2 Relation between Virtualization and Cloud Computing

When an end-user uses a computer, what he/she directly interacts with is a view provided by the OS which abstracts all the physical components available. The user gets information that he is interested on from the view.

It can be described that what virtualization does is to build up a few different logic views from a physical machine, each of which can be used to interact with a user simultaneously.

Cloud computing requirements of dynamic cutting and distribution of computing resources are owing to Virtualization.

Virtualization involves the construction of an isomorphism that maps a virtual guest system to a real host. This isomorphism maps the guest state to the host state. From the angle of resource, virtualization creates plural subsets logically from the complete set of machine.

Each logic view may possess the similar architecture a physical view. When a user interacts with certain resources via a view, he/she doesn't need to know if the view is a drawing of physical resources or just a graph of a logic set of resources. The end users do not see the details of resources, but just pay attention and interact with the logic view provided by virtualization layer, or VMM (virtual machine monitor). These subsets that behave same as real machines are called VMs (virtual machine).

Therefore, on resource virtualization layer storage must be organized as a single logical pool of resources available to users, and on virtual resource layer , that software must package a set of computing resources and behaviors and present it as an

available computing environment is at the core of what it means to create a virtual machine. The service layer is built upon virtual organizations where the nodes are fully decentralized just like P2P systems.[12]

4 Risk of Data Virtualization and Solution

4.1 Risk of Virtualization

Despite the cloud's huge potential in reduced costs and improved productivity, and overwhelming enthusiasm from customers, security experts repeatedly warn that security problems could inhibit wide adoption of the cloud model [13].For example, in a typical cloud computing services platform, virtual resources are rented to needed users, according to the actual operations and physical resources. Because the cloud distribute logic resource to tenant, and it do not where the real resource address, so different tenants may be bound to the sharing resources, such as sharing memory ,the same hard disk and so on. Therefore, some tenants have a chance to read other tenant's data through the sharing real resource. If cloud platform exist security hole, it will face the risk of data leakage.

The security and integrity of virtualization layer are the foundation for the overall security of the cloud. We will face the following risks with the using of virtualization in the cloud [14]: (1) If the host were sabotaged, the client servers would be conquered which were controlled by it; (2) If the virtual network were sabotaged, the client will be damaged; (3) It is a must to safeguard the client sharing and the host sharing because these sharing may be holes which will be utilized by lawless users. (4) If the host has problem, all of the virtual machines will cause problems.

4.2 Some Ways to Improve the Security

With the wide application of cloud computing, any privacy information can be found in any equipment through the computers in the cloud. Safety management has become urgent need to resolve the problem. It will be the focus and challenge of the cloud infrastructure management that how to ensure that the user's information not be leaked out. Many scholars, researchers and engineers did a lot of theoretical research and engineering practices, and they had made some achievements.

Virtualization software and virtual server are most tools to reduce the risk of virtualization.

Sriya Santhanam and his partners put forward deploying virtual machines as sandboxes for the grid. Virtual machines provide a natural solution to the security and resource management issues that arise in sandboxing. They explore different designs for the VM-enabled sandbox and evaluate them with respect to various factors like structure, security guarantees, user convenience, feasibility and overheads in one such grid environment. And experiments indicate that the use of on-demand VMs imposes a constant startup overhead, with I/O-intensive applications incurring additional overheads depending on the design of the sandbox [15].

Raj H and his partners identify last level cache (LLC) sharing as one of the impediments to finer grain isolation required by a service, and advocate two resource management approaches to provide performance and security isolation in the shared cloud infrastructure - cache hierarchy aware core assignment and page coloring based cache partitioning. Experimental results demonstrate that these approaches are effective in isolating cache interference impacts a VM may have on another VM. They also incorporate these approaches in the resource management (RM) framework of their example cloud infrastructure, which enables the deployment of VMs with isolation enhanced SLAs.[16]

Jinpeng Wei and his partners propose an image management system that controls access to images, tracks the provenance of images, and provides users and administrators with efficient image filters and scanners that detect and repair security violations. Filters and scanners achieve efficiency by exploiting redundancy among images; an early implementation of the system shows that this approach scales better than a naive approach that treats each image independently. [17]

Many other ways have been proposed to improve the security of virtualization in cloud. From the point of my view, we should keep our minds on the following [14]:

(1) The security of virtualization software: Fig 1 shows that the virtualization software layer is deployed upon bare machine. It provides the ability to create, operate and destroy virtual server. We must strictly control any unauthorized users not to access it. Cloud service provider shall establish necessary safety control measures to control physical and logical access of the virtualization layer. The integrity and availability of virtualization layer should be the most important and the most critical element to guarantee the integrity and availability of the cloud which is constructed based on virtualization layer. A hole of virtualization software will expose all the business area to malicious intruders.

(2) The security of virtual server: Virtual server is located above the virtualization software. We should choose the physical server with the Trusted Platform (TPM) security Module. TPM refuse to start this virtual server with wrong password. Every virtual server should be assigned to an independent hard disk partition when install virtual server, then every virtual server can be isolated logically from each other. Virtual server system should install firewall, antivirus software, log records and recovery software based on the host to make up a multi-level protection system. Every virtual server should also be isolated logically through the VLAN and different IP network segment. In order to protect the security of different virtual servers, the network connection among them need through the VPN means. Every virtual server should implement backup strategy to backup important data.

From the point of view of the daily management of virtual server, we should reinforce its system security as a physical machine including system and application patches, allowable service, open ports, etc. It is important to control strictly the quantity of virtual service based on the physical host and prohibit the physical host running other network service. If the virtual server requires the link or share files with host, it should use VPN to prevent a breach of virtual server to influence the security of the physical host. We should pay attention to the safety and countermeasures of the host, eliminate the factors which will affect the stability and security of the host , and prevent attacks of spyware, Trojans, and hackers for that all virtual servers will be faced with security threats, or stop running when physical host are infringed.

5 Conclusion

Cloud computing has emerged as one of the most influential technologies in the IT industry and is rapidly revolutionizing the way IT resources are managed and utilized. Through clever use of virtualization technologies, the cloud offers customers the ability to start businesses without having to pay huge upfront capital expenses and the exhibition to scale the IT infrastructure up and down as a business evolves without worrying about over or under provisioning. However, many people and enterprise did not want to use cloud computing because the security holes in the cloud. Virtualization is the key component of cloud computing, so its safety is the urgent problems to be solved.

The paper cuts into cloud computing from the point of virtualization and made some discussion on the relationship between the two, presented the risk of security with the use of virtualization in cloud. Because to a great extent security service quality of the cloud computing platform was determined by the security of the virtual resources management, the paper analyses and discusses several methods to solve this problem with the help of virtualization in order to improve the safety of cloud computing, and proposed ways to improve the security.

It is no doubting that cloud computing is developing rapidly and has a promising prospect. However at the same time it will face challenges which never had met before. To some extent, it need IT sector and information security researcher jointly explore solutions. At the same time, the security of cloud computing is not only a technical problem, but it also involves standardization, supervising model, laws and regulations, and many other aspects. Therefore, from the only view of technology to solve the security of cloud computing is not enough, it also need to information security department, industrial community and the relevant government department joint efforts to achieve the goal.

References

1. Luo, Y.: Network I/O Virtualization for Cloud Computing in Plastics. IT Professional 12, 536–541 (2010)
2. A History of Cloud Computing, http://www.cloudtweaks.com/2011/02/a-history-of-cloud-computing
3. Google, http://code.google.com/intl/zh-CH/appengine/docs/
4. Amazon, http://docs.amazonwebservices.com/AWSEC2/lastest/DeveloperGuide/
5. Microsoft, http://www.microsoft.com/azure/whitepaper.mspx
6. Peng, L.: Cloud Computing. Publishing House of Electronic Industry, Beijing (2010) (in Chinese)
7. Peter, M., Timothy, G.: The NIST Definition of Cloud Computing (Draft).NIST Special Publication 800-145, 6–7
8. Shuai, Z.: Cloud Computing Research and Development Trend. In: 2010 Second International Conference on Future Networks, pp. 93–97. IEEE Computer Society, Piscataway (2010)

9. Shufen, Z.: Analysis and Research of Cloud Computing System Instance. In: 2010 Second International Conference on Future Networks, pp. 88–92. IEEE Computer Society, Piscataway (2010)
10. Xue, J.: The research of security mechanism in the cloud computing platform based on virtualization technology, Master's degree paper, vol. 2 (2010)
11. History of Virtualization, http://www.infobarrel.com/History_of_Virtualization
12. Hanfei, D.: Formal Discussion on Relationship between Virtualization and Cloud Computing. In: The 11th International Conference on Parallel and Distributed Computing Applications and Technologies, pp. 448–453. IEEE Computer Society, Piscataway (2010)
13. Feng, D.: Study on Cloud Computing Security. Journal of Software 1, 71–83 (2011) (in Chinese)
14. Communication World Web, http://www.cww.net.cn/cwwservice/
15. Sriya, S., Pradheep, E., Andrea, A., Miron, L.: Deploying virtual machines as sandboxes for the grid. In: Second Workshop on Real, Large Distributed Systems, pp. 7–12 (2005)
16. Raj, H., Nathuji, R., Singh, A., England, P.: Resource management for isolation enhanced cloud services. In: Sion, R. (ed.) Proc. of the 2009 ACM Workshop on Cloud Computing Security, CCSW 2009, Co-Located with the 16th ACM Computer and Communications Security Conf., CCS 2009, pp. 77–84. Association for Computing Machinery, New York (2009)
17. Wei, J., Zhang, X., Ammons, G., Bala, V., Ning, P.: Managing security of virtual machine images in a cloud environment. In: Sion, R. (ed.) Proc. of the 2009 ACM Workshop on Cloud Computing Security, CCSW 2009, Co-Located with the 16th ACM Computer and Communications Security Conf., CCS 2009, pp. 91–96. Association for Computing Machinery, New York (2009)