Secure Virtualization Technology

Farzad Sabahi

***Abstract*—Cloud is one of today's most interesting technologies because of it can reduce cost and make flexibility and scalability. Hence, cloud computing became a promising business from a pure idea in a few years. However, there are some issues in cloud about which IT organizations concern such as security. As a matter of fact, basis of cloud computing is virtual environments. Although, the virtualization is not a new technology, appearance of cloud computing caused raising new concerns about security that may be caused hesitation before moving to cloud environments. This paper tries to describe security problems in the virtualization in cloud-environment aspect of view.**

This article tries to review issues and solutions of virtualization technology which is used in the cloud computing. The paper begins which a discussion on virtualization technology. Then, it addresses the challenges and available solutions.

***Index Terms*—Virtualization, virtual machine, security.**

I. Introduction

Cloud computing is a network-based environment that focuses on sharing computations and resources; specially they are Internet-based and designed to reduce complexity from their users. Actually, cloud providers use virtualization technologies combined with some other abilities for increasing processing resources via network infrastructures such as the Internet. Moreover, the cloud environments according to several services that they have to serve to their users, several kinds of virtual machines are hosted on the same physical server in them. In fact, costumers only have to pay for what they use and do not have to spend money for local resources.

This paper is organized as follows:

- Section 2 provides a general overview of virtualization components.
- Section 3 describes the virtualization technology methods which are usable in cloud computing.
- Section 4 discuss deeply about issues of virtualization that are important in cloud and possibility of solutions.
- Finally, Section 5 concludes the paper.

II. Components of Virtualization

Virtualization is a technology in order to help IT organizations to optimize their application performance in a cost-effective manner. Nonetheless, it can also present challenges that cause some security difficulties that are, unfortunately, serious.

Manuscript received June 15, 2012; revised August 1, 2012.

F. Sabahi is with the Azad University, Zanjan, Iran (e-mail: f.sabahi@ieee.org).

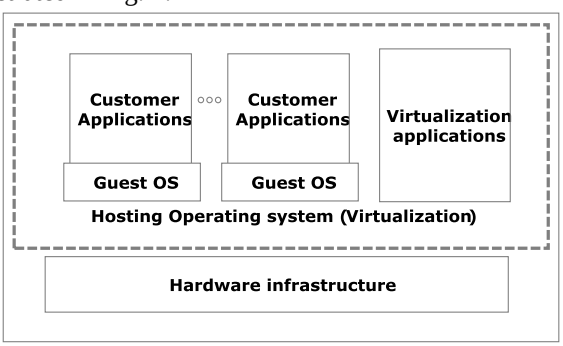
Most of the current interest in virtualization is virtual servers because virtualizing servers have a good potential to reduce cost of server-based services. In definition, the phrase virtual machine is a software that, similar to a physical computer, operates an operating system and desired applications. The main parts of a virtual system's controlling system are; GOS (Guest Operation System) which is a special operating system and a layer called a virtual machine monitor or manager (VMM) which creates and controls the virtual machine's other virtual subsystems.

In addition of two parts of controlling system, there a main part which are essential in typical virtual machine, which is called hypervisor. The hypervisor is one of many virtualization techniques that allow multiple operating systems, termed guests, to run concurrently on a host computer, a feature called hardware virtualization. It is named because it is conceptually one level higher than a supervisor is. The hypervisor presents to the guest operating systems a virtual operating platform and monitors the execution of the guest operating systems. Multiple instances of a variety of operating systems may share the virtualized hardware resources [1], [2]. Hypervisor installs on hardware server whose main task is to operate guest operating systems.

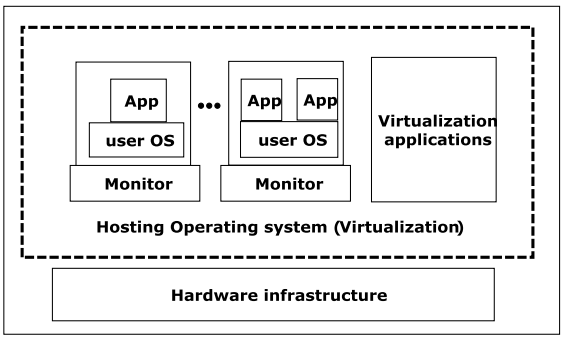
III. Virtualization Methods

In a traditional environment consisting of physical servers connected by a physical switch, IT organizations can get detailed management information about the traffic that goes between the servers from that switch. Unfortunately, that level of information management does not provide from a virtual switch which has some links from the physical switch that attaches to virtual machines. In addition, the lack of oversight of the traffic flows among the virtual machines on the same physical level affects security abilities and overall performance.

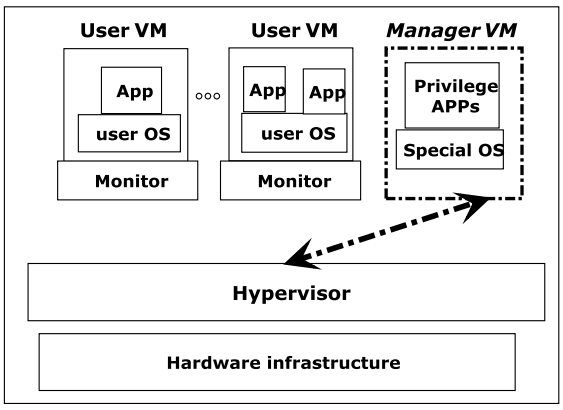
Generally, there are several common approaches to virtualization with differences between how each controls the virtual machines. The architecture of these approaches is illustrated in Fig. 1.



(a) Operating system-based virtualization



(b) Application-based virtualization



(c) Hypervisor-based virtualization

Fig. 1. Virtualization approaches.

A. Operating System-Based Virtualization

In this approach (Fig. 1.a), virtualization is enabled by a host operating system that supports multiple isolated and virtualized guest OS's on a single physical server with the characteristic that all are on the same operating system kernel with exclusive control over the hardware infrastructure. The host operating system can view and has control over the Virtual Machines. This approach is simple, but it has vulnerabilities, such as when an attacker injects controlling scripts into the host operating system that causes all guest OS's to gain control over the host OS on this kernel. The result is that the attacker will have control over all VMs that exist or will be established in the future.

B. Application-Based Virtualization

An application-based virtualization is hosted on top of the hosting operating system (Fig. 1.b). This virtualization application then emulates each VM containing 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.

C. Hypervisor-Based Virtualization

The hypervisor is available at the boot time of machine in order to control the sharing of system resources across multiple VMs. Some of these VMs are privileged partitions that manage the virtualization platform and hosted Virtual Machines. In this architecture, the privileged partitions view and control the Virtual Machines.

This approach establishes the most controllable environment and can utilize additional security tools such as intrusion detection systems. However, it is vulnerable because the hypervisor has a single point of failure. If the hypervisor crashes or the attacker gains control over it, then all VMs are under the attacker's control. However, taking control over the hypervisor from the virtual machine level is difficult, though not impossible.

IV. Virtualization Concerns

Another potential problem that exists for virtualization is that the provider may combine too many Virtual Machines onto a physical server. This can result in performance problems caused by impact factors such as limited CPU cycles or I/O bottlenecks. These problems can occur in a traditional physical server, but they are more likely to occur in a virtualized server because of the connection of a single physical server to multiple Virtual Machines such that they all compete 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 monitor continuously the utilization of both physical servers and Virtual Machines in real time. 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 implement policy-based remediation that helps the organization to ensure that service levels are being met [3].

Another challenge in Virtualization is that cloud organizations must now manage Virtual Machine sprawl. With Virtual Machine sprawl, the number of Virtual Machines running in a virtualized environment increases because of the creation of new Virtual Machines that are not necessary for business. Worries about Virtual Machine sprawl include the overuse of infrastructure. To prevent Virtual Machine sprawl, Virtual Machine managers should analyze the need for all new Virtual Machines carefully and ensure that unnecessary Virtual Machines migrate to other physical servers. In addition, an unnecessary virtual machine will able to move from one physical server to another with high availability and energy efficiency. However, consider that it can be challenging to ensure that the migrated Virtual Machine keeps the same security, QoS configurations, and needed privacy policies. It must be ensured that the destination maintains all the required configurations of migrated Virtual Machines.

A. Virtual Machine Security and Threats

As mentioned before, there are at least two levels of virtualization, Virtual Machines and the hypervisor. Virtualization is not as new a technology as cloud, but it contains several security issues that have now migrated to cloud technology. Also, there are other vulnerabilities and security issues which are unique to cloud environment or may have a more critical role in cloud.

In the hypervisor, all users see their systems as self-contained computers isolated from other users, even though the same machine serves every user. In this context, a Virtual Machine is an operating system that is managed by an underlying control program.

- Virtual machine level attacks: Potential vulnerabilities are the hypervisor or Virtual machine technology used by cloud vendors are a potential problem in multi-tenant architecture [1]. These technologies involve "virtual Machines" remote versions of traditional on-site computer systems, including the hardware and operating system. The number of these virtual Machines can be expanded or contracted on the fly to meet demand, creating tremendous efficiencies.
- Cloud provider vulnerabilities: These could be platform-level, such as an SQL-injection or cross-site scripting vulnerability that exist in cloud service layer which cause insecure environment.
- Expanded network attack surface: The 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 [4].
- 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.
- 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 [5].
- Data control in cloud: For midsize businesses used to having, complete visibility and control over their entire IT portfolio, moving even some components into the Cloud can create operational “blind spots”, with little advance warning of degraded or interrupted service [6].
- Communication in virtualization level: Virtual machines have to communicate and share data with each other. If these communications did not meet significant security parameters then they have potential of becoming attacks target.

B. Hypervisor Security

In a virtualization environment, several Virtual Machines may have independent security zones that are not accessible from other virtual machines that have their own zones. A hypervisor has its own security zone, and it is the controlling agent for everything within the virtualization host. Hypervisor can touch and affect all acts of the virtual machines running within the virtualization host [7].There are multiple security zones, but these security zones exist within the same physical infrastructure that, in a more traditional sense, only exists within a single security zone. This can cause a security issue when an attacker takes control over the hypervisor. Then the attacker has full control over all data within the hypervisor’s territory. Another major virtualization security concern is “escaping the Virtual Machine” or the ability to reach the hypervisor from within the Virtual Machine level. This will be even more of a concern as more APIs are created for virtualization platforms [8]. As more APIs are created, so are controls to disable the functionality within a Virtual Machine that can reduce performance and availability.

1) Confronting against hypervisor security problems

As mentioned before, hypervisors are management tools, and the main goal of creating this security zone is building a trust zone around them. Other available Virtual Machines are under the probation of the hypervisor, and they can rely on it, as users are trusting that administrators will do what they can to do provide security. There are three major levels in security management of hypervisor as mentioned below:

- Authentication: users must authenticate their account properly, using the appropriate, standard, and available mechanisms.
- Authorization: users must secure authorization and must have permission to do everything they try to do.
- Networking: the network must be designed using mechanisms that ensure secure connections with the management application, which is most likely located in a different security zone than the typical user.

Authentication and Authorization are some of the most interesting auditing aspects of management because there are so many methods available to manage a virtual host auditing purpose [9]. The general belief is that networking is the most important issue in the transaction between users and the hypervisor, but there is much more to virtualization security than just networking. Moreover, if security manager can address Authentication, Authorization, and Virtual Hardware and hypervisor security as well as networking security, cloud clients well on the way to a comprehensive security policy [4]. If a cloud provider at the virtualization level depends only on network security to perform these tasks, then the implemented virtual environment will be at risk. It is a waste of money if a cloud provider spends too much on creating a robust, secure network and neglects communication among virtual machines and the hypervisor.

C. Data Leakage

When moving to a cloud, there are two changes for customers’ data. First, the data will be stored away from the customer's locale machine. Second, the data will be moved from a single-tenant to a multi-tenant environment. These changes can raise an important concern called data leakage. Because of them has become one of the greatest organizational risks from security standpoint [10]. Virtually every government worldwide has regulations that mandate protections for certain data types [10]. The cloud provider should have the ability to map its policy to the security mandate user must comply with and discuss the issues.

1) DLP

Currently, there is interested in the use of data leakage prevention (DLP) applications to protect sensitive data. These products aim to help with data confidentiality and detect the unauthorized retrieval of data, but they are not intended for use in insuring the integrity or availability of data. As a result, there is no expectation of DLP products to address integrity or availability of data in any cloud model. Thus, DLP efficacy in cloud computing is fly-around confidentiality only.

D. Privacy

Cloud clients’ data is stored in data centers that cloud providers diffuse all over the globe within hundreds of servers that communicate through the Internet. This has several well-known risks. Because of cloud services are

using the Internet as communication infrastructure, cloud computing involve with several kinds of security risks [10]. Cloud providers, especially IaaS providers, offer their customers the illusion of unlimited compute, network, and storage capacity, often coupled with a frictionless registration process that allows anyone begin using cloud service [11]. The relative anonymity of these usage models encourages spammers, malicious code authors, and other hackers, who have been able to conduct their activities with relative impunity [12]. PaaS providers have traditionally suffered most from such attacks; however, recent evidence shows the hackers begun to target IaaS vendors as well [11].

In cloud-based services, user's data stores on the third-party's storage location [4]. A service provider must implement security measures sufficiently to ensure data privacy. Data encryption is a solution to ensure the privacy of the data in the databases against malicious attacks. Therefore, encryption methods have significant performance implications regarding query processing in clouds. Integration of data encryption with data is useful in protecting the user's data against outside malicious attacks and limiting the liability of the service provider.

It seems protection from malicious users who might access the service provider's system is the final goal, but this is not enough when clients also demand privacy protection from the provider himself. Any data privacy solution must use a particular encryption, but this causes another availability issue, which is data recovery. Imagine a user's data is encrypted with a user-known key and user loses his key. How can the provider recover his data if he does not know the key? If the user allows the provider in authority to know the key, then this makes the user-known encryption key useless. The simple way to solve this problem is to find a cloud provider whom the user can trust. This is acceptable when the data stored in cloud is not very important, and small companies may be decide to find trustable providers rather than a solution for data recovery problems. For medium-sized to large-sized companies, it is more critical to ensure privacy from cloud providers. If the service providers themselves are not trusted, the protection of the privacy of users' data is a much more challenging issue. However, for those companies it seems using private cloud is a wise solution.

If data encryption is used as a solution to data privacy problems, there are other issues in this context. One of the most important issues is ensuring the integrity of the data. Both malicious and non-malicious users can compromise the integrity of the users' data. When this happens, the client does not have any mechanism to analysis the integrity of the original data. Hence, new techniques must be applied in order to check the integrity of users' data hosted on the service provider's side.

All encryption methods rely on secure and impressive key management architectures. One of the problems that can occur in an encrypted environment is encryption key management in cloud. In cloud environments, there are several users who may use their own encryption methods, and the management of these keys is another issue to address in the context of encrypted data.

E. Data Remanence Issue in Virtualization

Data remanence is the residual physical representation of data that has been in some way erased. After storage media is erased there may be some physical characteristics that allow data to be reconstructed [13], [14]. After storage media is erased there may be some physical characteristics that allow data to be reconstructed. As a result, any critical data must not only be protected against unauthorized access, but also it is very important that securely erase at the end of data life cycle. Generally, IT organizations, which have their own servers and certainty, have full control on their servers and for privacy purpose; they use various available tools that give ability to them to destroy unwanted and important data safety. However, when they are migrate to cloud environment they have virtual servers that controlled by third party.

As a solution, IT governments must choice cloud that it can guarantee that all erased data by costumer are securely erased immediately. A traditional solution for securely deleting data is overwriting but this technique does not work without collaborate the cloud provider. In cloud environment customers can't access to the physical device and have access to data level. Thus, there seems to be only one considerable solution which is customers can encrypt their data in order to prevent rebuilding data from residual data after erasing.

F. Attacks in Virtualization Level

Nowadays, there are several attacks in the IT world. As the cloud can give service to legal users, it can also service to users that have malicious purposes. A hacker can use a cloud to host a malicious application for achieve his object that may be a DDoS attacks against cloud itself or arranging another user in the cloud [2]. For example, an attacker knew that his victim is using cloud vendor with name X, now attacker by using similar cloud provider can sketch an attack against his victim(s). This situation is similar to the scenario that both attacker and victim are in same network but with this difference that they use virtual machines instead of physical network (Fig. 2).

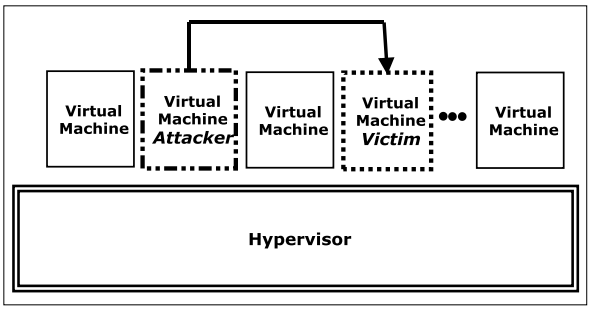


Fig. 2. Attack scenario within cloud.

1) DDoS attacks

Distributed Denial of Service (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. If cloud has not sufficient resource to provide services to its VMs then maybe cause undesirable DDoS attacks. Solution for this event is a traditional solution that is increase number

of such critical resources. Nevertheless, serious problem is when a malicious user deliberately done a DDoS attacks using bot-net.

It may be more accurate to say that DDoS protection is part of the Network Virtualization layer rather than Server Virtualization. For example, ARP spoofing at the network layer can overcome cloud systems use virtual machines and it is really about how to layer security across multivendor networks, firewalls and load balances.

2) Client to client attacks

One malicious virtual machine could infect all Virtual Machines 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 virtual machines become easy to access, the attacker has to spend time attacking one virtual machine, 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. Hence, the major security risk in virtualization environments is "client to client attacks". In this attack an attacker gets the administrator privileges on the infrastructure level of virtualization environment and then can access to all VMs. If the hacker could also get control of the hypervisor and he owns all data transmitting between the hypervisor and VMs and he can perform a spoofing attack.

V. Conclusion

Based on the virtualization, the Cloud computing paradigm allows workloads to be deployed and scaled-out quickly through the rapid provisioning of Virtual Machines or physical machines. A cloud-computing platform supports several considerable capabilities such as redundant, self-recovering, scalable programming models. Using all of these features, the cloud will be allowed to recover from many hardware/software failures. In addition, this technology are able to centralize and automate some of the considerable management issues such as maintenance, software updates, configuration. However, this way to decentralize applications and allow universal access to data creates its own set of challenges and security problems that must be considered before transferring data to a cloud. Moving toward cloud computing requires deeply consideration of several essential factors, and the most important of them is security.

References

[1] R. Chow, et al., "Controlling data in the cloud: Outsourcing computation without outsourcing control," Presented at the ACM Cloud Computing Security Workshop, Chicago, IL, November 13, 2009.

[2] F. Sabahi. (2011). Cloud computing RAS issues and challenges. *ICTer Journal*, 2011. [Online]. 4(2). pp. 12 – 23. Available: http://www.icter.org/journal/index.php/ICTer/article/view/128/19

[3] P. Dermond, "Virtualization: The next generation of application delivery challenges," December 2009.

[4] T. Ristenpart and e. al, "Hey, you, get off of my cloud: exploring information leakage in third-party compute clouds," in *Proc 16th ACM conference on Computer and communications security*, New York, NY, 2009, pp. 199-212.

[5] D. Talbot. (December 2009). Vulnerability Seen in Amazon's Cloud-Computing. [Online]. Available: http://www.technologyreview.com/printer_friendly_article.aspx?id=23792

[6] P. Sefton, Privacy and data control in the era of cloud computing. [Online]. Available: http:// brightline.com.au/external/cloudprivacypaper100326.pdf

[7] D. Rowe. (2011). The Impact of Cloud on Mid-size Businesses. [Online]. Available: http://www.macquarietelecom.com/hosting/blog/cloud-computing/impact-cloudcomputing-midsize-businesses

[8] Texiwill. (2009). Is Network Security the Major Component of Virtualization Security? [Online]. Available: http://www.virtualizationpractice.com/blog/?p=350

[9] *Taylor and Francis Group, LLC*, Implementing and Developing Cloud Computing Applications, 2011.

[10] "Securing Virtualization in real-world environments," White paper, 2009 [Online]. Available: http:// www.ibm.com/jm/download/SEW03016USEN.pdf.

[11] C. Almond, "A practical guide to cloud computing security," 2009.

[12] N. Mead, et al., "Security quality requirements engineering (SQUARE) methodology," *Carnegie Mellon Software Engineering Institute*.

[13] K. K. Fletcher, "Cloud security requirements analysis and security policy development using a high-order object-oriented modeling," *Master of Science, Computer Science, Missouri University of Science and Technology*, 2010.

[14] P. R. Gallagher, "A guide to understanding data remanence in automated information systems," *The Rainbow Books*, 1991.

Farzad Sabahi received Bachelor of Science and Master of Science degrees in Computer Engineering from Azad University in 2003 and 2007 respectively, specializing in the computer architecture. His research interests include computer architecture, distributed systems, cloud computing, hypervisor-based security and wireless network security. He is a lecturer in the Department of Electrical and Computer Engineering at the Azad University, Zanjan, Iran. He has published several papers in distributed systems, cloud computing, and wireless network security. He has been an invited reviewer for different international conferences. He has been member of The Institute of Electrical and Electronics Engineers (IEEE) since 2006.