Security in Cloud Computing using Virtualization-Level

Vachana M S
8th Sem, Computer Science & Engineering Department
Coorg Institute of Technology
Ponnampet, South Kodagu
msvachana@gmail.com

Navile Nageshwara Naveen
Lecturer, Computer Science & Engineering Department
Coorg Institute of Technology
Ponnampet, South Kodagu
nnnaveen.nag@gmail.com

Abstract

Cloud computing is one of today's most exciting technology because of its cost-reducing, flexibility, and scalability. With the fast growing of cloud computing technology, Data security becomes more and more important in it. In evaluating whether to move to cloud computing, it is important to compare benefits and also risks of it. Thus, security and other existed issues in the cloud cause cloud clients need more time to think about moving to cloud environments. But Security-related topics is one of the most arguable issues in the cloud computing which caused several enterprises looks to this technology uncertainly and move toward it warily. In this paper I try to summarize cloud computing RAS (Reliability, Availability, and Security) issues and also clarify available solution for some of them. In this paper I try to summarize virtualization level of cloud computing security in detailed view.

I. INTRODUCTION

Cloud computing is a network-based environment that focuses on sharing computations and resources. Basically, clouds are Internet-based and try to disguise complexity for clients. Cloud providers use virtualization technologies combined with self-service abilities for computing resources via network infrastructure especially the Internet. In cloud environments multiple VMs (VM) hosted on the same physical server as infrastructure. In cloud, costumers only have to pay for what they use. Cloud computing refers to both the applications delivered as services over the Internet and the hardware and systems software in the datacenters that provide those services.

II. VIRTUALIZATION COMPONENTS

Virtualization is one of most important elements that makes Cloud computing. Virtualization is a technology to helping IT organizations optimize their application performance in a cost-effective manner, but it can also present its share of application delivery challenges that cause some security risks. Most of the current interest in virtualization revolves around virtual servers in part because virtualizing servers can result in significant cost savings. The phrase VM refers to a software computer that, like a physical computer, runs an operating system and applications. An operating system on a VM is called a guest operating system. A layer called a VM monitor or manager (VMM) creates and controls the VM's other virtual subsystems (see Figure 1).

A. Hypervisor

A hypervisor is one of many virtualization techniques which allow multiple operating systems, termed guests, to run concurrently on a host computer, a feature called hardware virtualization. It is so named because it is conceptually one level higher than a supervisor. 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. Generally, Hypervisor is installed on server hardware whose only task is to run guest operating systems (See Figure 3).

III. VIRTUALIZATION APPROACHES

In the traditional environments which consist of several physical servers that connected by a physical switch, IT organizations can get detailed management information about the traffic that transmits between the servers from the physical switch. Unfortunately, that level of information management is not provided typically by a virtual switch (The virtual switch has links from physical switch via physical NIC that attach to VMs). The resultant is lack of visibility into the traffic flows between and among the VMs on the same physical level that impacts security performance. There are several common approaches to virtualization with differences in how they have control over the VMs.

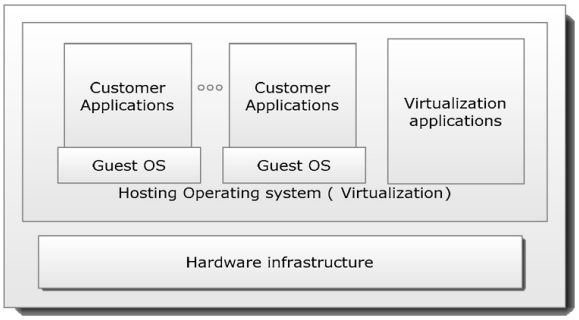

Figure 1. Operating system-based Virtualization

A. Operating system-based virtualization

In this approach (Figure1), 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 Exclusively. 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.

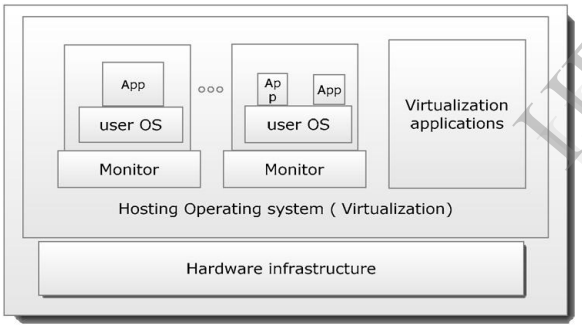

Figure 2. Application-based Virtualization

B. Application-based virtualization

An application-based virtualization is hosted on top of the hosting operating system (Figure 2). This virtualization method emulates 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].

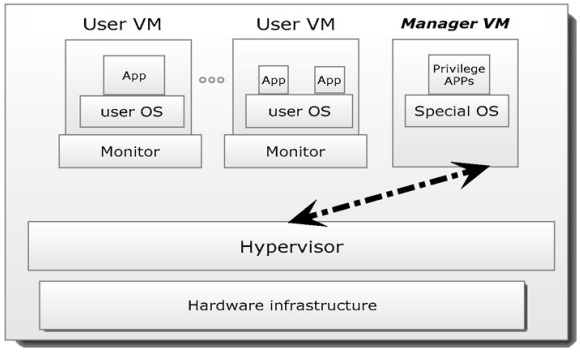

Figure 3. Hypervisor-based Virtualization

C. Hypervisor-based virtualization

As mentioned before, a hypervisor is embedded in the hardware infrastructure or the hosting operating system kernel (Figure 3). 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.

IV. CLOUD-BASED VIRTUALIZATION CONCERNS

The potential problem also exists for virtualization is provider combine too many VMs onto a physical server. This can result in performance problems caused by impact factors such as limited CPU cycles or 1/0 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 single physical server to multiple VMs that all of them competing 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 continuously monitor in real time the utilization of both physical servers and VMs. 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 [2].

Another challenge in Virtualization is that cloud organizations now have to manage VMs sprawl. With VM Sprawl, the number of VMs running in a virtualized environment increases because of creating new VMs, not because those VMs are necessary for the business. Worries with VM sprawl are the overuse of the infrastructure. To prevent VM sprawl, VM manager should analyze the need for all new VMs carefully and ensure that unnecessary VMs migrate to other physical server. In addition, an unnecessary VM will able to move from one physical server to another with high availability and energy efficiency. But be considering the VM destination can be challenging to ensure that the migrated VM keeps the same security, QoS configurations, and needed privacy policies. In the other hand, the destination must be assurance keeping all the required configurations of migrated VM.

A. VM security and threats

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

In the hypervisor, all the users see their systems as selfcontained computers isolated from other users, even though every user is served by the same machine. In this context, a VM is an operating system that is managed by an underlying control program. There are various threats and attacks in this level that major issues mentioned below:

• **VM level attacks**: Potential vulnerabilities are the hypervisor or VM technology used by cloud vendors are a potential problem in multi-tenant architecture [3]. These technologies involve "VMs" remote versions of traditional on-site computer systems, including the hardware and operating system. The number of these VMs can be expanded or contracted on the fly to meet demand, creating tremendous efficiencies [4].

• **Cloud provider vulnerabilities**: These could be platform-level, such as an SQL-injection or crosssite scripting vulnerability that exist in cloud service layer which cause insecure environment.

• **Expanded network attack surface**: 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 [8].

• **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**: VMs have to communicate and also share data with each other. If these communications didn't meet significant security parameters then they have potential of becoming attacks target.

B. Hypervisor Security

In a virtualization environment there are several VMs that may have their independent security zones which can't accessible from other VMs which have their own zones. In a virtualization environment a hypervisor has own security zone and it is the controlling agent for everything within the virtualization host. Hypervisor can touch and affect all acts of the VMs running within the virtualization host [7]. There are multiple security zones but these security zones exist within the same physical infrastructure that in more traditional senses generally only exists within a single security zone. This can cause a security issue when an attacker can take control over hypervisor then the attacker have full control on all works within hypervisor territory. Another major virtualization security concerns is "escaping the VM" or being able to reach the hypervisor from within the VM level. This will be even more of a concern issue as more APIs are created for the virtualization platforms [8]. As more APIs are created, so are undamaging controls to disable the functionality within a VM and 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 it a trust zone. Other available VMs are under probating of the hypervisor and they can rely on it as users are trusting on administrators will do what they can to do tasks properly. In security characteristic, there are three major levels in security management of hypervisor as mentioned below:

- **Authentication**: Users have to authenticate their account properly using the appropriate, standard, and available mechanisms.
- **Authorization**: users must authorize and they must have permission to do that they try to do.
- **Networking**: using mechanism that assurance secure connection to communicate with the management application that most likely lives in a different security zone of that 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 [I]. General belief is that networking is most important issues in transaction between users and hypervisor but there is much more to virtualization security than just networking. Networking plays a critical role in security but it is not significant for ensuring security achieving solely. But it is just as important to understand the APIs and basic concepts of available hypervisor and VMs and how those management tools work. 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 [9]. If cloud provider at Virtualization level does not or just depend on network security to do the tasks then the implemented virtual environment is at risk and has poor security ability. It is waste of money if a cloud provider only spent too much money for creating robust secure network and neglect from communication among VMs and hypervisor that can cause several problems.

C. Data Leakage

Basically, when moving to a cloud there is two changes for customers' data. First, the data will store away from the customer's locale machine. Second, the data is moving from a single-tenant to a multitenant environment. These changes can arise an important concern that 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

Nowadays, there has been interested in the use of data leakage prevention (DLP) applications to protect sensitive data. With the appearance of cloud computing for prevent from data leakage some companies think about DLP Products. But the DLP products existed before appearing cloud computing. These products aim to help with data confidentiality and detect the unauthorized reveal of data but these products are not intended to use for insuring the integrity or availability of data. As a result, there is not expectation to 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 stores in data centers that cloud provider diffuse them all over the globe within hundreds of server that communicate through Internet which have several well-known potential risks within it. Because of cloud services are using the Internet as communication infrastructure, cloud computing involve with several kinds of security risks [10]. Cloud providers, especially laaS 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 [9]. A service provider must implement security measures sufficiently to assurance 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 on query processing in clouds. Integration of data encryption with data is useful to protect user's data against outside malicious attacks and to limit the liability of the service provider.

It seems protection from malicious users who might access to the service provider's system is the final goal but this is not enough when clients will also

prefer privacy protection from provider's access to their data. Any data privacy solution will have to use particular encryption but this cause another availability issue that is data recovery. Assume user data encrypted with user-known key and user lost his/her key. So, how provider can recover his data when it doesn't know what is it the key? If user Put provider in authority to know the key then this makes the privacy by using user-known encryption key become useless. The Simple way for solve this problem is find a cloud provider which user can trust it. This way is acceptable when data stored in cloud is not very important. This method seems useful but for enterprises with maximum size of small companies which may be decides to find trustable providers rather than finding a solution for data recovery problem. For medium-sized companies to large-sized companies, it is more critical for Development of techniques and methods that enable query processing directly over encrypted data to ensure the privacy from cloud providers. If the service providers themselves are not trusted, the protecting the privacy of users' data is much more challenging issue. However, for those companies it seems using private cloud is wisely solution.

If data encryption is used as a wise solution to data privacy problem, 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 cause compromising the integrity of the users' data. When this happens and the client does not have any mechanism to analysis the integrity of the original data. Hence, new techniques have to be applied to provide methods to check the integrity of users' data hosted at the service provider side.

All encryption methods rely on secure and impressive key management architectures. One of the problems that can occur in encrypted environment is encryption key management in cloud. In cloud environment there are several users who may use their own encryption method and managing these keys is another issue to address in the context of encrypted data. For example, if cloud provides Database Service (DaaS), the cloud provider faces to more challenges on key management architectures such as generation, registration, storage, and update of encryption keys.

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]. 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. Basically, IT organizations which have their own servers and certainty have full control on their servers and for privacy purpose they use various available tools which give ability to them to destroy unwanted and important data safety. But when they are migrate to cloud environment they have virtual servers that controlled by third-party.

As a solution, IT governments must choice cloud which 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 is only one solution that is customers can encrypt their data with confidential key that prevent reconstruction data from residual data after erasing.

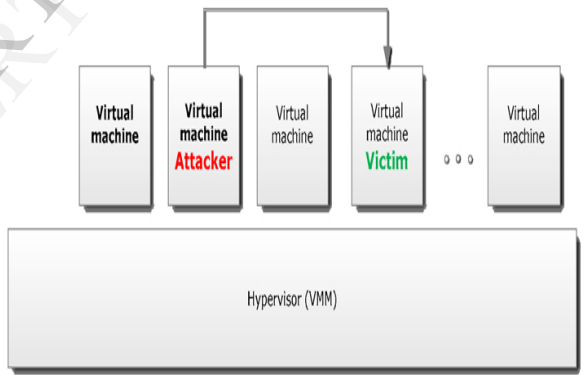

Figure 4. Attack scenario within cloud.

F. Attacks in Virtualization level

Nowadays, there are several attacks in the IT world. Basically, 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 which may be a Distribute Denial of Service (DdoS) attacks against cloud itself or arranging another user in the cloud. 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 this scenario that both attacker and victim are in same network but with this difference that they use VMs instead of physical network (Figure 4).

1) DDoS attacks

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 may be cause undesirable DDoS attacks. Solution for this event is a traditional solution that is increase number of such critical resources. It may be more accurate to say that DDoS protection is part of the Network Virtualization layer rather than Server Virtualization. For example, cloud systems use VMs can be overcome by ARP spoofing at the network layer and it is really about how to layer security across multivendor networks, firewalls and load balances [14].

2) Client to client attacks

One malicious VM could infect all VMs 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 VMs become easy to access, the attacker has to spend time attacking one VM, 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

Cloud computing is defined as a pool of virtualized computer resources. Based on this Virtualization the Cloud Computing paradigm allows workloads to be deployed and scaled-out quickly through the rapid provisioning of VMs or physical machines. A Cloud Computing platform supports redundant, self-recovering, highly scalable programming models that allow workloads to recover from many inevitable hardware/software failures. A virtual appliance relieve some of the notable management issues in enterprises because most of the maintenance, software updates, configuration and other management tasks that they are automated and centralized at the data center by cloud provider responsible for them. But this suggestive way for decentralized application and access every time and everywhere to data create their own set of challenges and security problems that must consider before transfer data to a cloud. Moving toward cloud computing require to consider several essential factors and most important of them is security.

REFERENCES

[1] t. Ristenpart and e. ai, "Hey, you, get off of my cloud: exploring information leakage in third-party compute clouds," 2009.

[2] "Virtualization: The next generation of application delivery challenges."

[3] R. Chow, et a!., "Controlling Data in the Cloud: Outsourcing Computation without Outsourcing Control," presented at the CCSW'09, Chicago, Illinois, USA., 2009.

[4] D. Talbot. (2009). Vulnerability Seen in Amazon's CloudComputing.Available:http://www.technologyreview.comlprinter jriendly arti cle.aspx?id=23792

[5] P. Sefton, "Privacy and data control in the era of cloud computing. "

[6] D. Rowe. (2011, The Impact of Cloud on Mid-size Businesses.Available:http://www.macquarietelecom.com/hosting/blogicloudcomputing/impact-cloudcomputing-zidsize-businesses

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

[8] D. E. Y. SAR NA, Implementing and Developing Cloud Computing Applications: Taylor and Francis Group, LLC, 2011.

[9] "Securing Virtualization in Real-World Environments," White paper2009.

[10] C. Almond, "A Practical Guide to Cloud Computing Security," 27 August 2009 2009.

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

[12] 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.

[13] P. R. Gallagher, A Guide to Understanding Data Remanence in Automated Information Systems: The Rainbow Books, 1991.