International Journal of Computer and Internet Security.
ISSN 0974-2247 Volume 5, Number 2 (2013), pp. 31-41

http://www.irphouse.com

Security Issues in Cloud Computing

Dr. M. Manimegalai and Shri R. Raghuraman

Director, Department of MCA,
Shrimati Indira Gandhi College, Tiruchirappalli- 620002
Research Scholar, Shrimati Indira Gandhi College, Tiruchirappalli- 620002.

"Cloud computing, in particular, continues to increase compared with previous years, driven by economic conditions and a shift from capital expenditure to operational expenditure, as well as potentially more important factors such as faster deployment and reduced risk, The demand is strongest in government agencies with more decentralised staff and those that have a large field workforce".[1]

Christine Arcaris, Research Director, Gartner

Abstract

Cloud computing is an emerging computing paradigm that offers the concept of time shared remote services with attractive technological and financial advantages. The infrastructure uses new technology and services which have not been fully evaluated with respect to security.

A few of the concerns include data security, expectations, trust, regulations and performance issues.

Cloud computing environments are multi-domain in which each domain can use different security, privacy and trust requirements and potentially employ various mechanisms, interfaces and semantics. The domain may represent individually enabled services or other infrastructural or application components. Service Oriented Architecture facilitates such multi domain formation through service composition and orchestration.

As the shape of the cloud computing is emerging and rapidly developing conceptually and in reality, the issues such as contractual, service quality, interoperability, security and privacy issues pose serious challenges. In this paper an attempt is made to identify the challenges and suggest technological solutions to mitigate these challenges and facilitate ubiquitous adoption of this technology.

1.0 Introduction

Cloud Computing is an IT based model where processing, storage and delivery are done with a shared pool of resources and the availability of physical resources is driven by clients demand. It can be termed on par with a 'Rent–a-car' scheme, wherein the physical resources like Servers, storage device, networking equipment are leased by a cloud provider as an outsourced service.

Cloud computing enables convenient and on demand network access to a pool of computing resources with provisioning for rapid release based on minimum interaction of service provider or management effort.

The use of internet infrastructure is envisaged to allow communication between client side and server side services/applications.

A key issue which comes to focus during adoption of cloud services is the security and it becomes a mandated responsibility of the cloud service provider to build sufficient controls as part of the system and guarantee control on network access, data loss/leakage, metered services based on usage, vulnerabilities and nefarious use.

2.0 Key Security Issues

2.1 Virtualization

The concept of cloud computing has lot of complexities and also offers a plethora of advantages. However it would require understanding about hypervisor which is an important component and much more complex than simple virtualization. According to NIST, a cloud may have the following characteristics:

- Self-service
- Broad network access
- Elasticity
- Chargeback
- Resource pooling

The need for virtualization in a cloud environment needs to be understood first. A virtual machine will be a commodity operating system instance that forms part of a configured and running OS image. The OS image serves as a snapshot of a server and includes space for virtual disk storage. The technology used to support the virtual machines may be in the form of a hypervisor. The Hypervisor presents to the VM the hardware environment with which it works with.

Most commonly there are two standard types of virtualization platforms in use today:

- Type-1 hypervisors which run directly on bare hardware. Guest operating systems run on top of the hypervisor. Examples : Microsoft Hyper-V and VMware ESX.[2]
- Type-2 hypervisors also known as "hosted hypervisors" where the hypervisor runs as a program in the host OS and the VMs run on top of the Type- 2 hypervisor. Examples: Oracle Virtual Box, Parallels, Virtual PC, VMware Fusion, VMware Server, Xen, and Xen Server [3]

It does demand a focus on key security issues related to hypervisors and more so when virtualization has been implemented in the cloud. Some of the concerns include:

- The need for each operating system running in a virtual environment be patched, maintained, and monitored as per the intended use like any non-virtual operating system in any network.
- An awareness that methods used to monitor traffic between VMs may need to use alternative methods and even forego network based intrusion detection system and move the attempt back to the host.
- When virtual machines are moved from one physical server to another, the systems may not know be aware that the services have moved and thus generate false alarms. This may get pronounced when clustering is implemented along with virtualization.
- It would devolve to pay attention to desired configuration management (DCM), VM mobility and capacity planning issues when applications and services have been run in a virtualized environment.

2.2 Virtualization Platform Security

In a traditional data center, automation may not be attempted unless the number of client or server operating systems required would force the same. However in a cloud environment, the OS has to be automated to support some of the considerations of cloud itself.

We need to consider critical security concerns about the role of virtualization in cloud computing. The foremost among them may be the chance that hypervisor itself is compromised. The hypervisor may have access to all the guest workloads running within cloud infrastructure. Under cloud deployment options where literally thousands of virtual machines can run, compromise on the security functions of hypervisor could have devastating role if not prevented by using network isolation strategies.

A hypervisor may be a compact unit than an operating system designed to provide an interface and development canvas for applications. It may be ensured that external network ports which are prone to attack are disabled in a hypervisor. The hypervisor may need to be updated with patches, invisible on the network and no guest operating systems should have access to it.

There may be a need to take control of the storage and memory on a public cloud and a private cloud too. This may be done by clearing the data manually and through defined policies for deleting or securing sensitive data

There are several possible solutions to detect network attacks. It may be possible to invoke OS-based traffic filtering or firewall or by resorting to virtual instances of network management and monitoring solutions like Cisco 1000V.[4]

Some of the hypervisors may have virtual switches positioned between the server's physical NICs and the virtual NICs used by the VMs. The cloud fabric must synchronise with changes being made to VM locations and may oversee allowable and disallowable communication paths feasible between them.

There thus emerges a need to manage risk in virtualized cloud environments by designing, planning and exercising control. The right step in the form of management automation would enable the virtualized cloud environment to have better security

and provide a total solution.

2.3 Security in Private Cloud Scenario

It is likely that a scenario may emerge that private cloud is different from what is known and infer it to be just a virtualized data center.

In a true sense, a cloud (private or public) must provide for the following five essential characteristics:

- On demand self service
- Broad network access
- Sharing of common resources
- Rapid elasticity
- Metered services

The concern for security in a private cloud is on par with security issues in a traditional data center. Yet it does need a lot of concern towards network security, authorization and auditing, identity management and authentication at every layer of the network and computing stack. It may be true that private cloud would require addressing priorities in identified areas.

2.4 Impact of On-Demand Service on Cloud Security

The services offered in a private cloud solution on demand basis include compute, network, storage and memory resources based on the customer's ability to pay for utilising these resources. In addition, under PaaS or SaaS, as a deployment model, the consumers get the facility of development platform and finished services also.

In private cloud environment, the consumers have the choice to deploy new operating systems, create any kind of applications, and run them based on the service adopted by them. In such an environment, it is very likely that there would be no control on what the customers do with the resources allotted to them.

There would be a stronger need for an alert system on possible misuse and a comprehensive reporting facility for detailed trend analysis to keep a check on the resources allotted and its utilisation pattern. The tools used should be capable to pin point new work load without any manual intervention.

2.5 Other Security Considerations

Some of them include:

- Basis of assigning rights and privileges to consume cloud services.
- Type of service - umbrella or granular
- Automated security responses to denial of service situations in situation of over-subscription to facilities offered.
- Control on the clients operating system and services
- Customers with stolen credentials.

Automation may serve to be the only arrangement to identify such risks and prevent misuse of the facilities.

2.5.1 Broad Network Access

The next key issue of concern is "Broad Network Access" which means that the resources hosted on the cloud would be available to any device through Internet. Based on the common deployment model that may be adopted, it would mean that private cloud has to be always accessible to the front-end components hosted on the cloud.

The relevant issues related to broad network access include the following:

- Perimeter network role and location
- Identity and Access Management (IdAM)
- Authentication
- Authorization
- Role-based access control (RBAC)
- Federation
- Logging and Auditing
- Public network connectivity
- Endpoint protection Client security

These factors are discussed below:-

2.5.2 Perimeter network role and location

Handling inbound connections to the resources on a private cloud would require a need to support a DMZ [5] between the cloud services and the Internet.

This would mean hosting a DMZ and firewalls in a virtualized environment. However, it may have to be ensured that all these services are not hosted on the same server which houses the production workloads also. This would help to overcome a situation of an attacker taking over the entire private cloud infrastructure when the gateway virtual machines are compromised.

2.5.3 Identity and Access Management (IdAM)

Identity and Access management requires to take into consideration the users and also the managers of the private cloud. It should facilitate them to only manage the pieces for which they are responsible within the cloud infrastructure.

2.5.4 Role-based access control (RBAC)

Access to most of the components of private cloud should be based on the role defined to a person including multiple roles. This needs more efforts considering that all components are integrated into a central infrastructure in cloud environment,

Networking, computing, and storage functions need to be delegated to specific people with responsibility through a central console.

Access to the end users of the cloud should be limited to components of the services they require. This would mean that the control set up provides them with the desired services access to controls that manages the functionality and performance of the defined work load.

a

2.5.5 Federation

Federation of authentication and authorization infrastructure is critical because of the number of systems present in a private cloud environment. There may not be a centralized authentication repository as the components of cloud may exist in private or public or vice versa or a mix of both. It is likely that there may not be knowledge of the client systems in advance and therefore a dire need to support a decentralized approach. Federation would allow this by facilitating private cloud to consume claims generated by trusted authentication repositories.

2.5.6 Logging and Auditing

The Cloud may require comprehensive log and report on all activities taking place in view of multiple user environment and varying workloads. This may be considered to be a complex phenomenon as the administrators extend services on an automated basis and enable their clients to connect to these resources without any definite understanding.

Logging and auditing may facilitate study on trends and patterns over the broad network access to study the usage pattern, demographic distribution of clients, potential threats etc and enable creation of automated responses to solve them.

2.5.7 Public network connectivity

Broad network access would pre-define the need for good internet connectivity, reliable ISP and adequate bandwidth to host the services on demand. It may also stress the importance of Quality of Service parameters to identify potential threats that may storm or flood the requests and slow down the services.

2.5.8 Endpoint protection and Client Security

In a broad network access the vital point of concern may be the endpoint protection and client security. This would mean enabling secure behaviour from all the devices connected to the workloads.

This would essentially require the use of gateway devices to assess the security configuration of the devices connected to the workload and provide a level of access to each of the device based on its current security posture.

3.0Resource Pooling

Resource pooling would enable the hypervisor to reassign tenants to different locations in the cloud for optimized resource usage. (e.g) VMware DRS and Hyper-V PRO. The virtualization set up planned should provide for scrubbing resources such as storage and RAM, before reassigning them to another virtual process or user. This function may be provided through automation which would undertake the clearing and allocation of resources to clients and protect the sensitive data from being exposed to other clients.

3.1.1 Security Implications

Resource pooling may affect the security design of a private cloud in many ways.

They may include such issues concerned with:

- Re-use of resources by different clients/processes.
- co-locating services that belong to different users on the same server
- automated processes to handle allocation/ de-allocation of resources

The private cloud arrangement may result in the same machine hosting applications and services that belong to different security zones and the applications and services themselves may include different security capabilities such as authentication and authorization.

3.1.2 Escalation of Privilege Issues

The proposed design shall envisage that a low business impact service may be compromised and gain leverage to attack higher business impact services. The attack may lead to a high value service being unavailable by creating a denial of service on a lower business impact service.

Network traffic monitoring and IDS/IPS [6] may be capable of identifying unusual traffic which can lead to a cloud service being compromised.

3.1.3 Network Abstraction and Virtualization

The Hypervisors are designed to support virtualization in the network and enable separation of logical and physical network traffic. This may lead to network traffic not being passed through a physical switch device and introduce the risk of network analysis tools not monitoring the traffic. Such a situation can be overcome by adopting any one of the solutions given below :

- Routing the network traffic through physical network devices
- Enabling monitoring functionality to each server by using network software analogues of physical monitoring devices.
- Deployment of a virtualization solution like extensible virtual switch to be included in the next version of Windows server.

The use of IPsec to provide authentication without encryption as included in Windows Server 2008 R2 is worthy of being adopted.

3.1.4 Disk Encryption

The relative advantages and disadvantages of security vs. performance are to be assessed before adopting any encryption technique. Different encryption algorithms [7] provide different performance impacts and enable different levels of protection. Low business impact data might require only authentication without encryption whereas. High business impact data would require encryption over the wire and authentication and authorization at the network level.

3.1.5 Core Infrastructure Security

Separation or isolation of resources can be done under different approaches. For (e.g) Hyper-V provides isolation between memory and compute resources of all VMs running on the same host operating system and flexibility to define isolated virtual

switches and allow each virtual machine to use its own virtual hard disks without affecting the other VMs. In case multiple tenant applications that are hosted on different virtual machines require access to a shared resource, it would permit only authorized applications to have access through monitoring.

The possible controls are:

- The host-based firewalls being configured to block network attacks.
- The configuration may allow inbound and outbound traffic from and to specific machines only.

3.1.6 Security Issues in Software

The responsibility to enforce security features in design may be entrusted only to the Application designers. They may work with the cloud service provider (CSP) and consciously be aware of the data protection services and security features available under cloud infrastructure.

The adopted encryption technologies may require a private key to perform encryption and decryption in the symmetric encryption algorithm [8] scenario, or decryption in the asymmetric algorithm scenario. Encryption techniques used by tenant applications for data protection may be rugged to work under both options.

Automated processes may ensure that the cryptographic keys used to protect application data are made available to applications and services as and when needed and may even provide for transfer of keys between locations through an e automated processes under secure environment.

4.0Rapid Elasticity

The concept of rapid elasticity is a key characteristic which differentiates cloud computing from traditional datacenter computing. Under cloud environment, multiple users may share components of a shared resource pool and return them to the pool when they no longer need these assets. The environment would provide facility for augmented services, if needed at times. The acquisition and release of assets from and to the shared pool may be automated and synchronised to meet the service demands driven by an intelligence policy.

Such a rapid, policy based acquisition and release system of shared pool resources defines the concept of rapid elasticity.

4.1 Security Concerns related to Rapid Elasticity

Rapid elasticity would facilitate optimized use of shared resource pool. This policy driven mechanism may include minimum guarantees and maximum caps. This would also help to avoid overprovision the cloud based infrastructure as the resources would be continuously released into the shared pool.

However some of the security concerns associated with rapid elasticity include:

- Authentication, authorization, and access controls (AAA) that govern the use and release of shared resources.
- Monitoring and auditing requests to acquire and release resources based on quota defined and maintenance of service viability.

- Release of all data remnants from the shared data pool.

4.2 Securing the Cloud Infrastructure

The cloud should provide a perception of infinite capacity to the tenants and as a repository of a fixed size pool of shared resources where quality of service needs to be monitored from the service provider's point of view.

This would require fixing a limit on the sizes of virtual machines, for example, 5% of virtual machines as large, 75% as medium, and 20% as small or under a different proportion.

The service provider would be required to define policies that describe quotas to control the use of resource allotted. This would help to overcome situations with excess provisioning requests.

It would also require determining the level of granularity for the shared resources and defining how the quotas will be adjusted. The quota may be defined per application or based on the resource intensive need of the tenant with matching cost consideration. The cloud service provider should also eliminate delays in allocation of resources.

The use of hybrid cloud deployment and extension of private cloud to a third party may be advisable if the demand is too elastic. This would however demand reviewing the security controls employed by the hosting party vis-a-vis security requirements. Some of the requirements may include:

- Cloud bursting issues to support rapid elasticity.
- Legal requirements related to data governance and location of tenants
- SLAs which govern the security requirements offered to cloud tenants
- Private cloud infrastructures should facilitate to move virtual machines between servers within the data center or between the corporate and hosting company's datacenters.

5.0Management Process in an Elastic Environment

The integrated cloud management system should provide for acquisition and release of resources through intuitive and programmatic interfaces. The use of role-based access control (RBAC) would enforce quota checks on resource allocation.

5.1.1 Metered Services

This generally refers to limitations and restrictions on usage. The terminology reminds users of "old model" of Internet connectivity, where usage charges were reckoned at hourly basis or the "new model" of capped bandwidth.

5.1.2 Need for metered services

Metered services most often would mean "pay per use". This would refer to the utility aspect of cloud computing.

It would be essential for a service provider to be transparent about usage pattern of the shared infrastructure by a tenant and charge him based on the level of usage.

The resources to be charge based on usage include the shared pool of compute,

networking and storage. A clear understanding of the policies would enable the tenant to plan the usage of resources and avoid wastage.

The concept of metered services would enable the tenant to assess the required level of availability, the increase in costs proportionately and the strain on the shared pool of resources. This would also enable them to plan for a lower level of availability based on the functional requirements.

5.1.3 Metered services in the Cloud

The charging principle under Cloud may be either in the form of accounting for all chargeable use of the services and billing the tenants or adopt the "show back" principle wherein reports of cloud service usage and service costs may be provided which makes the tenants accountable for the amount of resource used by them.

The security provisions may have to enforce that the tenants will not be bypass the monitoring systems in any way with a malafide intention to reduce their liability by tampering with the data which would indicate their real usage. This may lead not only to loss of monetary benefits but more to a potentially denial of service situation due to utilisation of increasing amount of cloud resources and lead to a pint of exhaustion of resource pool which would in turn affect the interests of other tenants.

There may also be a risk of someone trying to use the cloud resources for undesired purposes and lead to security breaches. In some situation it may often lead to a few individuals using the resources for personal gain by running a private web server in the corporate cloud environment. Such a risk may lead to loss of reputation for the cloud entrepreneur and adverse publicity.

It is also likely that an attacker may gain access to a private cloud to run a mail server and use it as a launch pad for e-mail based attacks or run a mail server without paying any attendant costs. This may be possible either through bypassing the monitoring and billing systems or to arrange for his unauthorised use to be paid by a legitimate client(s).

The system of metered service would provide for motivating tenants to release the resources to the pool from the moment they don't require them. This would enable the service provider to overcome inadvertent denial of service and running out of cloud services which would reduce the overall availability of the resource pool.

5.1.4 Record keeping

In view of the utmost importance for monitoring and logging facilities to measure the usage and report on the resource allocation, the metered services have become critical for upkeep of cloud infrastructure.

The tenants would require the facility of billing information which would also enable them to verify possible unauthorised usage of resources and find out inconsistencies in billing. The metered services would also encourage the cloud users to monitor their usage of resources based on need.

6.0 Conclusion

The security considerations discussed above highlight the key issue that both known

and unknown users may connect to the tenant services running on the cloud. The broad network access feature may apply to all private cloud services.

The other feature namely rapid elasticity has potential for repeated requests for resources and may impact the availability of shared resources forming a pool. If proper monitoring mechanisms are not put in place, it may lead to integrity issues and lead to risk of availability of tenant services.

The software security feature would require addressing the security issues affecting applications in the cloud.

The research paper would indeed bring in a rethink on the focus and emphasis for the cloud providers and users and provide a platform for better insight on the plan and design security for a private cloud.

References:

[1] Gartner pegs Govts' IT spend at $450bn."The Indian Express" dated 19.06.13.

[2] Doug Dinley, Paul Ferrill , "Virtualization showdown: Microsoft Hyper-V 2012 vs. VMware vSphere 5.1", published in April 2013, InfoWorld Home/Virtualisation/Test Centre.

[3] Lydia Leong, "Whitepaper on Citrix cloud solutions", April 2012, http://blogs.gartner.com/lydia_leong/2012/04/03/citrix-cloudstack-openstack-and-the-war-for-open-source-clouds.

[4] Bob Laliberte, "Cisco Nexus 1000V and Virtual Network Overlays", July 2012, The Enterprise Strategy Group. www.cisco.com

[5] Charu Chaubal, 'Security Hardening", VMware Infrastructure 3 Security Hardening, July 2008, http://www.vmware.com/files/pdf/vi35_security_hardening_wp.pdf.

[6] Asmaa Shaker Ashoor, Sharad Gore, "Differences between IDS and IPS", Communications in Computer and Information Science, Volume 196, 2011, pp 497-501, Advances in Network Security and Applications.

[7] Padmapriya, Subasri, "Cloud computing : security challenges & Encryption Practices", March 2013, International journal of Advanced Research in Computer Science and Software Engineering. www.ijarcsse.com

[8] Diaa Salama Abd Elminaam, Hatem Mohamed Abdual Kader, Mohiy Mohamed Hadhoud, "Evaluating The Performance of Symmetric Encryption Algorithms", International Journal of Network Security, Vol.10, No.3, PP.216–222, May 2010