HCTL Open Int. J. of Technology Innovations and Research
HCTL Open IJTIR, Volume 7, January 2014
e-ISSN: 2321-1814
ISBN (Print): 978-1-62951-250-1

Security in Cloud Computing

***Mahipal Singh*[*], Gaurav Mohan Singh[†], Ajay Kumar[‡] and Dr. Sanjay Bhargava[§]**
mahiditdun@gmail.com

Abstract

Cloud computing has developed into growing interest for organizations seeking to reduce their IT costs by offloading software costs onto alternative party organizations who offer software-as-a-service, platform-as-a-service, Security is the vital thing for that Cloud success. Cloud computing can be a long awaited and after this implemented desire having interactive services and software applications, at reduced operational cost inside the IT market, at highly automated and a system based on performance, an on-demand services and these are just a some of the advantages that what cloud computing bring back us and what all features and services cloud computing provide us.There's two such technologies Multi-tenancy, Virtualization which provides security about cloud computing. The paper proposes a burglar alarm Model and in addition standards based on Monitor based security protocol to the security of the clouds vendors to efficiently store data around the clouds and prevent data from threats.

[*] M.Tech. Student, DIT University, Dehradun, India
[†] M.Tech. Student, DIT University, Dehradun, India. Email: gauravmohan096@gmail.com
[‡] Assistant Professor, DIT University, Dehradun, India. Email: kumarajay7th@gmail.com
[§] Professor, DIT University, Dehradun, India. Email: sanjaybhargava78@gmail.com

Keywords

Cloud Computing, Network Security, Multi-tenancy, Cloud Security.

Introduction

The formative years of computing services that are based on cloud, there were uncertainties about the amount of data and information security offered by these facilities. Infrastructure-as-a-service (IaaS) within the cloud services are largely dependent on virtualization technology, which is known for providing security and process segregation required by a buyer. Multi-tenancy and virtualization enable a competent computing model. Multi-tenancy allows multiple tenants to coexist from the same physical machine sharing its resources (CPU, memory, network...) and, as well, creates an isolated environment to each one. Virtualization would be the means helpful to obtain multi-tenancy. Virtualization allows multiple operating systems (OS) running on a single physical device at the same time frame. This makes the possibility of several users to access their applications on the same physical environment, but cut off from one another. This paper will summarize in the region of cloud security that has a concentrate on virtualization security.

Virtualization

Virtualization has developed in the IT world for a long period. IBM was the first that introduced the thought in the early 1960s with all the term `Time Sharing`. Virtualization technology is already recognized in IT industry and being successfully deployed in several other related infrastructures. Virtualization of systems, also referred to as server virtualization, pertains to "a means of creating an actual computer be when it were a couple of computers where each non-physical or virtualized Computer will get the same basic architecture as those of a plain physical computer. Therefore virtualization technology allows the installation of an operating system on hardware that does not really exist." virtualization, resources may be divided or shared through multiple environments, where those environments may be aware about not on the others. These environments are classified as virtual machines (VMs), and sometimes host an OS, which can be usually referred as guest Oss.

In line with Velte et al., there's two virtualization types that concern cloud computing:

1. `Full Virtualization`: On this style of virtualization, an entire installing of one machine is run on another.

2. `Para-virtualization`: This type of virtualization allows multiple modified OSs running about the same hardware device while doing so by well using system resources.

The real difference totally is that in full virtualization the whole system must be emulated (BIOS, drive...); but also in para-virtualization, the OSs continues to be modified to function more proficiently with all the hypervisor. The application of para-virtualization reduces flexibility since OSs should be properly modified to operate, which means that probably new OSs will need some time before being available for this type of virtualization. Also, there's an increased security impact because modified OSs convey more control within the underlying hardware which could impact on additional virtualized systems and also the host OS.

Additionally, there are two main sorts of virtualization architectures:

1. Hosted Architecture: On this approach, the host OS includes a virtualization platform (hypervisor) installed into which or maybe more VMs run.

2. Hypervisor Architecture: Using this approach, by exporting the virtual machine abstraction, virtualization layer sits on top of the hardware.

Virtual Machines

A virtual machine (VM) can be considered as a virtualized representation of physical machines operated and maintained by the virtualization software. VM can be a self-contained operation environment. VM is often a self-contained operation environment. This environment behaves as a distinguished computer, emulating the processor, memory, and all other peripheral devices. VMs provide some benefits over physical machines. VMs are often compromised by way of single or list of files which might be read and executed by the virtualization platform. Because of this they could be easily migrated from a single system to a new, copied, or stored.

Virtual Appliance

A virtual appliance (VA) is termed "a pre-packaged software image built to run within a virtual machine". Types of VAs would be the virtualized kinds of physical network devices for example routers, or switches. Special kind of

VAs called virtual security appliance (VSA). A VSA includes a hardened OS and a single security application, and therefore are usually assigned a larger a higher level trust gain access to the hypervisor along with resources like virtual networks running in the hypervisor. This higher privilege allows the VSA to do system and management functions. Samples of VSAs are firewalls, anti-virus, or IDS/IPS.

Virtualization Security

Cloud computing, virtualization security is again for the mouth of security practitioners. To be a recent study by Gartner indicates, in 2012 around 60% on the virtualized servers is going to be less secure versus the physical servers they replace, hopefully dropping to 30% by 2015. The security of your VM relies on the OS in use; therefore, it ought to keep to the security practices as if the VM would be a physical host. From your security standpoint, a VM plus a physical server do not differ. There are two possible ways to access a Virtual Machine. The first is through the hypervisor, and also the other is via the network connections. A compromised VM enable you to affect the host servers along with other VMs from the same virtual or physical network. Attacks could possibly be launched against these VMs or perhaps a DoS attack could be performed from the host server. In Cloud environments, the chances of the danger increase since an attacker need not to compromise a Virtual Machine in order to attack other Virtual Machines within the network. The attacker just has to buy a cloud service and, being a consumer, start the attack avoiding the regular security network devices.

An interesting approach by Lindstrom provides listing of five unchangeable laws of virtualization security:

1. `Law 1`: All existing OS-level attacks be employed in the exact same way.
2. `Law 2`: The hypervisor attack surface is additive with a system's risk profile.
3. `Law 3`: Separating functionality and the contents into Virtual Machines can reduce risk.
4. `Law 4`: Aggregating functions and resources onto a physical platform raises risk.
5. `Law 5`: A system containing a reliable VM when using untrusted host has a the upper chances level compared to a system containing a dependable host with the untrusted VM.

Lindstrom continues and explains that, within a broad sense, the vulnerability degree of a system is usually a measure of the attack surface. Panic or anxiety attack surface can be defined as the type and extent of resources on the system which have been exposed and, therefore, attackable. Virtualization improves the vulnerability by having the attack surface of the hypervisor and the VMM. In cloud computing, virtualization technologies still share exactly the same security issues, but those are increased through the multi-tenant architecture plus the erosion with the perimeter. CSA is primarily worry about the impact that virtualization is wearing network security. Because VMs is now able to communicate throughout the hypervisor as an alternative to with the physical network, the more common network security controls become useless; and express the requirement of these controls to look at a fresh form in the virtual environment.

Another essential facet of the protection will be the sharing of resources between VMs with assorted sensitivities, security, and owners. Unless a whole new security architecture is developed it doesn't require any network dependency for protection, this risk will almost always be present.

A directory of security challenges of virtualization within the Cloud that summarize just about all the down sides:

1. `Inter-VM Attacks`: The new channel created between VMs can't be monitored using traditional network security controls.

2. `Instant-on gaps`: Provide up-to-date security to dormant VMs becomes a painful task. A compromised picture of a VM may potentially produce a security breach when instanced.

3. `Mixed Trust level VMs`: Several VMs with some other security levels may potentially be designed into the identical host machine. Many of the concerning when coexisting with unknown tenants.

4. `Resource contention`: Accidental or unauthorized by using shared resources could very well resulted in a denial of service.

5. `Complexity of management`: Management of the VMs becomes harder than before, requiring more technical patching and configuration policies.

6. `Multi-tenancy`: VMs coexist with other unidentified and potentially malicious Virtual Machines.

7. `Lack of audit trail`: The process of monitoring and log VMs activities grows more difficult on virtualization environments.

In cloud environments, several issues arise from using virtualization, but this can also become beneficial for organisations. The absence of a security measures and the highly sensitive nature of VMs will make organisations to implement robust security processes which can create a high-security infrastructure in computing.

Multi-Tenancy

"Multi-tenancy in cloud service models implies any excuses for policy-driven enforcement, segmentation, isolation, governance, service levels, and chargeback/billing models for several consumer constituencies" - as per CSA. There are many differences from a SaaS and an IaaS multi-tenant architecture. Based on the different deployment models, a multi-tenant environment will give you different security concerns. As outlined by IBM, the idea of multi-tenant means to be able to provide computing services to multiple customers simply using a common infrastructure and code base. Within a multi-tenant environment, tenants might have a non-public space and also a common space shared amongst all tenants. Multi-tenancy uses virtualization technologies to enhance resource utilization, load balancing, scalability, and reliability; and the usage of automation reduces complexity, decrease operation costs, and increase provisioning speed.

Multi-tenancy may be used on different levels. With respect to the level, the multi-tenancy architecture will cause different concerns. According to IBM these levels may include:

1. `Application level`: Multiple tenants make use of an application gives logical separation between users, access controls, and customization.

2. `Middleware level`: Multiple applications operate the same middleware which gives logical separation, access controls, and resources.

3. `Operating system (OS) level`: Multiple middleware runs beneath same OS which gives access controls, logical separation, and resources on the middleware.

4. `Hardware level`: The hardware provides the benefits of logical separation, access control and resource allocation to individual OS instance. Within this level, each OS is considered a tenant.

The commonest components that may be shared across multiple tenants are - Storage, CPU processing, Memory, Network bandwidth, Management, Provisioning, Complexity, Power Usage, Billing or chargeback. Virtualization technology is the key to solve these problems.

Multi-Tenancy Security

A key factor for cloud computing is the capacity of multi-tenancy to share resources. However, multi-tenancy is additionally one of the primary security concerns in accordance with CSA and ENISA. Virtualization will be the means helpful to achieve multi-tenant environments, in order that they share most of security risks. From a high viewpoint thinking about sharing resources and the coexistence of various tenants that are unknown to one another, enables each of the security risks. To counteract tenants affecting 1 another's operations when running on a single host machine, it is crucial to engage a substantial compartmentalization; and it's the most importance that consumers cannot access other consumer's data, network traffic, or other information related Multi-tenancy architectures allow servers that have been under used until now to get efficiently were able to reallocate the spare resources. Multiple tenants can coexist from the same host machine increasing their CPU, memory, as well as networking capabilities. Publicly clouds, organisations put vulnerable their data and operations sharing houses along with other unknown tenants, that may perfectly be malicious attackers with thirst of acquire some rewards.

Conclusion

Cloud computing is concerning gracefully losing control while keeping accountability whether or not the operational responsibility falls upon a number any other companies. Cloud computing several technologies and architectures needs to be mixed to further improve the characteristics, specifically multi-tenancy and virtualization; nonetheless they bring their particular security concerns to the already big list of cloud computing. As multi-tenancy, virtualization comes with a unique issues. The hypervisor provides a new attack surface to be compromised; and also the virtual network enables a malicious VM to accomplish attacks on other VMs avoiding traditional network security controls. This implies a whole new form to approach network security like using privileged VMs; but and also this generates new security risks if being compromised. CSA accurately states that "the minimum common denominator of security will likely be shared by all tenants from the multi-tenant virtual environment unless a whole new security architecture can be carried out that does not "wire straight into" any network dependency for protection". The movement to the Cloud could mean a noticeable difference in security to several organisations.

References

[1] Cloud Computing, The 2011 IBM Tech Trends Report, 2011, pp.8

[2] Cloud Computing from Wikipedia. http://upload.wikimedia.org/wikipedia/commons/3/3c/Cloud_computing_layers.png

[3] Jacobo Ros, Security in the Cloud: The threat of coexist with an unknown tenant on a public environment, MSc in Information Security at Royal Holloway, University of London. http://www.ma.rhul.ac.uk/static/techrep/2012/Dissertation-100692179-1.pdf

[4] Ankur Mishra, Ruchita Mathur, Shishir Jain, Jitendra Singh Rathore, Cloud Computing Security, International Journal on Recent and Innovation Trends in Computing and Communication, Vol. 1, Issue 1, Jan 2013. http://www.scribd.com/doc/191703409/Cloud-Computing-Security

[5] Amazon EC2, http://aws.amazon.com/ec2/

[6] Google App Engine, http://code.google.com/appengine/

[7] Google Apps, http://docs.google.com/

[8] Nessus, http://www.nessus.org/

[9] Amazon Web Services, Zeus Botnet Controller, Accessed on Jan 2014, http://aws.amazon.com/es/security/zeus-botnet-controller/

[10] A. Cargile, Hypervisor Security Concerns, December 2009, http://thecoffeedesk.com/news/index.php/2009/12/01/hypervisor-security-concerns/

[11] Cloud Security Alliance, Security Guidance for Critical Areas of Focus in Cloud Computing V2.1, December 2009, https://cloudsecurityalliance.org/wp-content/uploads/2011/07/csaguide.v2.1.pdf

[12] Cloud Security Alliance, Top Threats to Cloud Computing V1.0, March 2010, https://cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf

[13] Common Vulnerabilities and Exposures, CVE-2007-1744, Accessed on July 2011, http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-1744

[14] Gartner, 2011 CIO Agenda Findings, Accessed on July 2011, http://www.gartner.com/technology/cio/cioagenda_findings.jsp

[15] Amrit Suman, Mahesh Gour and Raksha Mehra, Cloud Computing: A Modern Art and its Research Challenges, Edition on Cloud and Distributed Computing: Advances and Applications, Volume 2 - August 2013 of HCTL Open Science and Technology Letters (STL), ISSN: 2321-6980, ISBN: 978-1-62840-833-1.

[16] Aman Sagar, Bineet Kumar Joshi and Nishant Mathur, A Study of Distributed Denial of Service Attack in Cloud Computing (DDoS), Edition on Cloud and Distributed Computing: Advances and Applications, Volume 2 - August 2013 of HCTL Open Science and Technology Letters (STL), ISSN: 2321-6980, ISBN: 978-1-62840-833-1.

[17] Shakti Dhar Tiwari, Mahesh Kumar and Preeti Mishra, Cloud Computing: Implementation of Software as a Service (SaaS) Multitenancy, Edition on Cloud and Distributed Computing: Advances and Applications, Volume 2 - August 2013 of HCTL Open Science and Technology Letters (STL), ISSN: 2321-6980, ISBN: 978-1-62840-833-1.

[18] Mahesh Kumar and Shakti Dhar Tiwari, Cloud Computing: Various Aspects of Cloud Security, Edition on Cloud and Distributed Computing: Advances and Applications, Volume 2 - August 2013 of HCTL Open Science and Technology Letters (STL), ISSN: 2321-6980, ISBN: 978-1-62840-833-1.

[19] Gaurav Mohan Singh, Mahipal Singh Kohli and Manoj Diwakar, A Review of Image Enhancement Techniques in Image Processing, HCTL Open International Journal of Technology Innovations and Research, Volume 5, Sept 2013, ISSN: 2321-1814, ISBN: 978-1-62840-986-4.