A Survey on Infrastructure as Service Layer based Security Models for Cloud

Shalinee Jadon
UIT RGPV Bhopal

Sanjay Silakari, PhD
UIT RGPV Bhopal

Uday Chourasia
UIT RGPV Bhopal

ABSTRACT
Cloud security is been a center of attraction of all the researchers in the recent years. In this paper a survey is done on cloud security issues which are focused on Infrastructure as a Service (IaaS) layer. The virtualization in cloud is provided by infrastructure as a service layer and in this paper security issues related to virtualization is discussed.

Keywords
Cloud, VM isolation, VM migration, VM escape, VM image sharing, RSA.

1. INTRODUCTION
Cloud computing provides a pay per use service to large number of clients across the globe. There are many vendors for cloud service but there are many security concerns and performance constraints. In section II the major drivers of cloud computing are described. In section III barriers of cloud that is the issues which push cloud adaption backward are also discussed. The cloud computing service is distributed across the three layers of cloud namely Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS). The main concern of this paper is IaaS as all the virtualization and resource management is done by this layer's component.

2. DRIVERS OF CLOUD COMPUTING

Attribute	Description
Availability	The main aim of cloud computing is to provide service 24x7 without interruption.
Collaboration	Cloud provides users across different geographical locations to work on same data shared on cloud. Thus cloud support collaborative working with the help of community and public clouds.
Elasticity	Cloud provides large set of resources based on the user requirement. Thus if load is increased on user's paid resources then he can ask for more resources on pay per use basis.
Lower Infrastructure Costs	Cloud provides pay as per the use model. So client has to pay only for the resources he has used. There is no extra maintenance cost for the infrastructure.
Mobility	Users can access the cloud from any geographical location across the world.
Risk Reduction	Cloud saves the risk of investment as any organization can test a particular idea on cloud and then invest in the model. This saves the risk of investment.
Scalability	Each user can ask for resources according to requirement. Cloud resources scale from few resources to large number of resources.
Virtualization	Each user will have single view of all the resources he has registered irrespective of the geographical location of the physical machine located. A physical machine may host for a number of virtual machines for a number of users.

3. BARRIERS OF CLOUD COMPUTING

Concern	Description
Interoperability	There is no universal standard of cloud platform. So there might be a problem in migrating from one cloud service provider to another.
Latency	Access to cloud can be done via internet only. So there persists some delay in communication over internet termed as latency.
Platform or Language Constraints	All platform and languages are not supported by all cloud service provider. So these are constraints of cloud service.
Regulations	There are certain limitations for community cloud that are spread across international boundaries. So client must check regulations for data transfer and sensitive information over international boundaries.
Reliability	Cloud uses commodity hardware that is cheap and may fail unexpectedly.
Resource Control	The resource control to the user varies from vendors to vendors. So resource control is another major issue of cloud computing.
Security	Data and resource security is a major concern of cloud computing. In this paper IaaS is studied for virtualization security concerns.

4. LITERATURE REVIEW
As more companies are moving to cloud computing. Thus, hackers are also increasing in the same field. Some of the potential attack vectors that hacker may attempt include:

Denial of Service (DoS) attacks: A denial of service (DoS) attack is a malicious attempt to make a server or a network resource unavailable to users, usually by temporarily interrupting or suspending the services of a host connected to the Internet [8].

The cloud providers employ variety of strategies to partition resources in such a way that denial of services, whether accidental or deliberate are less likely to happen. Providers such as Amazon divide their cloud into "availability zones" that are designed to fail independently [9]. To maximize uptime, developers must replicate their applications in multiple zones and allow fail over between them.

Breach of confidentiality: With collocation-based breaches of confidentiality, attackers attempt to use collocation in order to compromise the confidentiality of a virtual machine (VM). Information about the data stored inside a VM can be inferred by noticing patterns of resource usage, particularly CPU usage. Such resource usage can be inferred through resource contention with a co-located attacker virtual machine [3].

Cloud Malware Injection Attack: A first considerable attack attempt aims at injecting a malicious service implementation or virtual machine into the cloud system. Such kind of cloud malware can serve any particular purpose the adversary is interested in, ranging from eavesdropping via subtle data modifications to full functionality changes or blockings [4].

Side Channel Attacks: An attacker could attempt to compromise the cloud by placing a malicious virtual machine in close proximity to a target cloud server and then launching a side channel attack [5].

5. SECURE CLOUD ARCHITECTURE

A. Secure VM image sharing

To initialize a VM, VM image is used by the broker. User itself can create his own VM image using VM repository to directly submit a VM [9]. Users can upload their created VM image in repository and may also download existing VM image from the repository [10]. But an attacker or malicious user can detect loopholes in the VM image code and can also upload a malicious VM image [11]. A VM which is initiated using a malicious VM image created by an attacker may behave suspiciously and may affect other VMs running on the same PM and may also harm the data stored on the PM [13]. The figure 1 shows normal VM creation using VM image. And Figure 2 shows secure VM creation method which uses encrypted VM image provided by the hypervisor with digital signature.

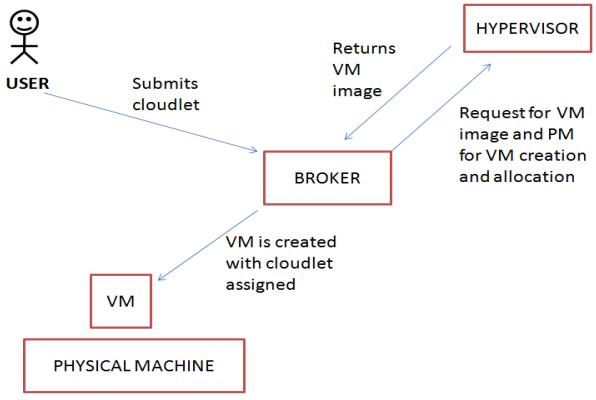

Fig 1: Figure showing VM image sharing concept in cloud

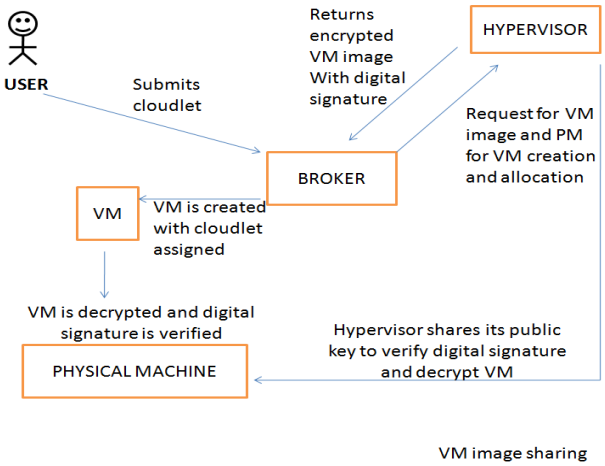

Fig 2: Digital signature approach for VM security

B. VM isolation and solution

All the VMs running on the same physical machine must be unaffected by the execution of other VMs present this concept is called isolation of VMs [3]. A malicious VM may breach data confidentiality of other VMs on that PM. Isolation violation may also include computational loss of other VMs also. To avoid this situation data for each VM can be encrypted using separate keys so that even if data confidentiality is compromised it can't be read by any other VM.

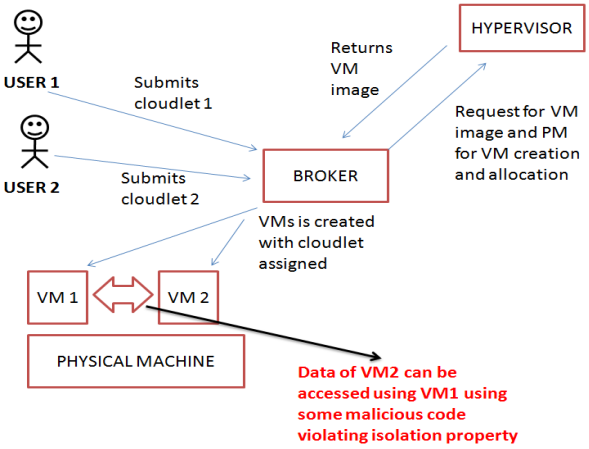

Fig 3: Figure showing data theft by VM1 on data of VM2.

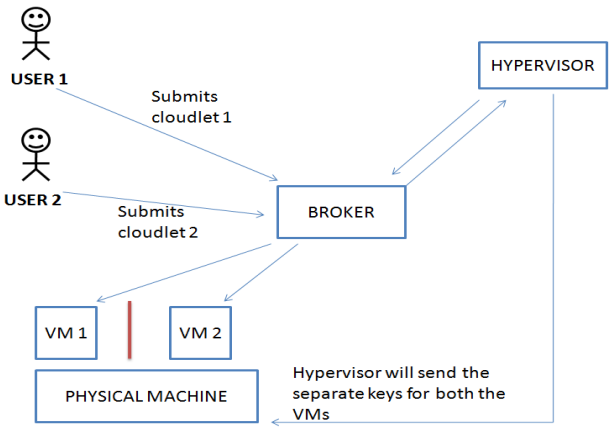

Fig 4: Figure showing proposed encryption scheme for maintaining VM isolation

C. Secure VM migration and VM escape protection

a. VM escape: Situation in which a malicious user or VM escapes from the control of hypervisor or virtual machine manager (VMM) is termed as VM escape. A VMM is a component of cloud information service that manages all the VMs and their access to the hardware. VM escape can affect the functioning of VMM or other VMs also. This situation can also result in breach in confidentiality of IaaS layer which can in turn affect functionality of other layers also.

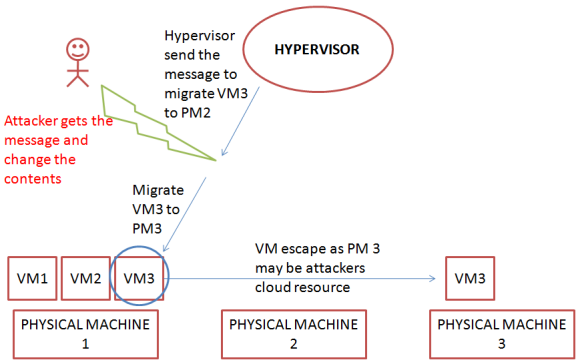

Fig 5: Figure showing VM escape by attacker.

b. VM migration: The process of transferring a VM running on a PM to another PM is termed as VM Migration. VM migration may occur to balance the load of the cloud and to reduce energy consumption by process of VM consolidation. VM migration is categorized into two type live VM migration and non live VM migration. But if attacker manages to migrate VM to a compromised PM then VM and associated data may be lost and result in SLA violation.

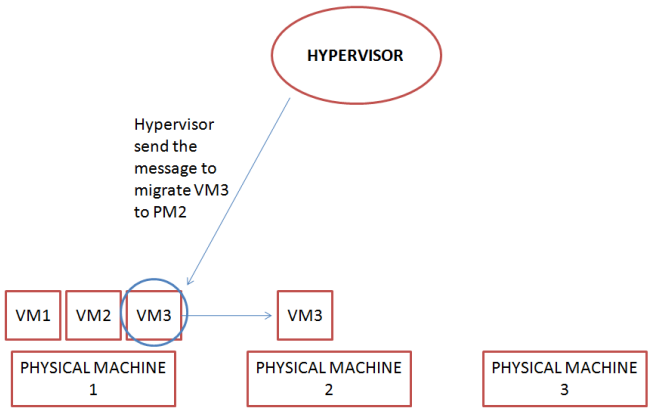

Fig 6: Figure showing normal VM migration from PM1 to PM2.

The above situation can be avoided using secure VM migration approach proposed in this thesis:

- Each message sent by the hypervisor will have digital signature of hypervisor and is encrypted also.
- So message content can't be altered and attacker can't pretend as hypervisor.
- All the data is encrypted and only its respective VM and PM has the key. So when Data and VM is migrated from one PM to another key is also changed and redistributed by hypervisor.

6. CONCLUSION

In this paper a survey on security issues related to virtualization are studied. And some security measures are proposed for security in case of VM creation, VM migration and to solve VM isolation problem and VM escape.

7. REFERENCES

[1] C. C. Basics, "Cloud Computing basics for non-experts", cloud weeks, pp. 1–8, May, 2015.

[2] Huth and J. Cebula, "The Basics of Cloud Computing", Carnegie Mellon University, Pp.1–4, February, 2011.

[3] M. Armbrust, A. D. Joseph, R. H. Katz and D. A. Patterson, "Above the Clouds: A Berkeley View of Cloud Computing," University of California at Berkeley pp. 14-19, February, 2009.

[4] T. Cloud and C. Stack, "The Cloud Computing Stack" Diversity Limited, pp. 1-9, October, 2013.

[5] URL:"http://www.thoughtsoncloud.com/2014/03/a-brief-history-of-cloud-computing", [last visited : May 30, 2015, 10:01:22 AM]

[6] URL: "https://www.salesforce.com/blog/2014/03/things-from-1999.html",[last visited : June 09, 2015, 2:06:47 AM].

[7] S. Home, "Rackspace Support Network Understanding the Cloud Computing Stack", Rackspace Support network, pp. 1–9, May, 2015.

[8] M. Sutton, "the Attacker within How Hackers Are Targeting Enterprise Networks from the Inside-Out", the Ohio State University, pp.1-9, November, 2009.

[9] Xiaofeng Chen, Jin Li, Willy Susilo, "Efficient Fair Conditional Payments for Outsourcing Computations, Transactions on Information Forensics and Security", IEEE, pp.1687-1694, March,2012.

[10] B. J. Brodkin, N. W. Cloud, S. Risks, C. Computing and G. A. Engine, "Gartner: Seven cloud-computing security risks," pp. 2–3, October, 2008.

[11] M. Armbrust, A. D. Joseph, R. H. Katz and D. A. Patterson, "Above the Clouds: A Berkeley View of Cloud Computing", University of California at Berkeley pp. 14-19, February 10, 2009.

[12] A. Shieh, S. Kandula, A. Greenberg and C. Kim, "Seawall: performance isolation for Cloud datacenter networks", in Proceedings of the 2nd USENIX conference on Hot topics in Cloud Computing, pp. 33-45,may,2010.

[13] S. Agarwal, J. Dunagan, N. Jain, S. Saroiu, A. Wolman and H. Bhogan, "Volley: Automated data placement for geo-distributed Cloud services," in Proceedings of the 7th USENIX conference on Networked systems design and implementation, pp.155-170, April, 2010.