Data and Virtualization Security in Cloud

Khushbu Dixit[1], Amrit Suman[2], Sadhna K. Mishra[3]

CSE Dept., LNCTs, Bhopal, India

***Abstract* - Cloud computing is getting attention of the researchers these days. Large number of users are attached with cloud computing. But as there are several merits of cloud computing some demerits are also there. The one of the greatest threat in cloud computing is security. This security is concerned with data of the users that is present in cloud and is transferred across the clouds and the virtualization concept. In this paper several attacks on cloud are studied and solutions to those threats are compiled. In this paper a secure technique to handle data in cloud and secure virtualization is proposed in this paper. A secure VM migration technique which gives VM isolation guarantee and VM escape protection is proposed here. And it is shown that this security algorithm posses no considerable overhead**.

***Keyword* - Cloud, VM isolation, VM migration, VM escape, VM image sharing, RSA.**

I. INTRODUCTION

Some decades ago when Internet was not introduced, companies ran e-mail as an application where data was stored in the hardware or in a secure place only. All the files, documents, messages and other important information were stored in a protection on the company's premises only [1]. However, it was not possible to store the huge amount of data due to lake of storage space. By moving forward into the 20th century, when companies like Google started showing up and email system has been started [1]. Then it became easy, it would have been a great invention of Google, that cause more subscribers, however these companies choose to open their own servers to store e-mail information for customers. However, to access that data, user has to adopt their applications like Gmail, Yahoo Mail and so many others. Further to open own servers and access all these applications to store the information of customers, Internet arrived. Moving further, if describe practically about cloud computing, adopting other people's servers to run applications for the organization, remotely is called as cloud computing system. For example, with cloud computing, different applications and services can be accessed without ever buying an extra piece of hardware or software. Whenever user required any changes to the cloud data, there needs an Internet connection [1]. The cloud computing nature is shared resource, identity management, privacy and access control; these all parameters are the area of concern in cloud computing. Organizations are increasing day by day for computation of applications in the cloud, this is necessary to deal with cloud computing security issues.

II. 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].

III. CLOUD COMPUTING

The cloud computing is computing technique in which large groups of remote servers are networked to allow centralized data storage and online access to computer services or resources. It provides flexibility and different computing platform for organizations. The Pinterest is an example of cloud computing, it is a free website that requires registration to access, where users can upload, save, sort and manage

images known as pins and other media content such as videos and images, through collections known as pinboard. It is viewed by approximately 17 million people per month and has a great storage capacity. It is hosted on Amazon's cloud platform [2]. Initially, due to absence of cloud computing, maintaining security of the information had been very difficult task. However, introduction of the cloud computing has made life easy. The cloud consists of certain elements such as clients, servers and the main centre where all servers are managed [3]. Figure 1.1 shows the architecture of cloud computing system, where the data owner stores the data and applications to the cloud storage. Whenever user needed to access data and applications, the owner provide access to the user through the cloud.

IV. TYPES OF SERVICES

The cloud computing categories as follows [7].

- **Software as a service (SaaS)** applications are intended for end-users, delivered over the network.
- **Platform as a service (PaaS)** is the set of tools and services developed to perform coding and organizing the applications.
- **Infrastructure as a service (IaaS)** is the software and hardware that commands all servers, storage, networks and operating systems.

V. SECURE CLOUD ARCHITECTURE

A. *Secure VM image sharing*

A VM image is used to instantiate VMs. A user can create his/her own VM image or can use an image from the shared image repository [9]. The users are allowed to upload and download images from the repository. Sharing of VM images in the image repositories is a common practice and can evolve as a serious threat if it is used in malicious manner [10]. A malicious user can investigate the code of the image to look for probable attack point. On the other hand, a malicious user can upload an image that contains a malware [11]. The VM instantiated through the infected VM image will become

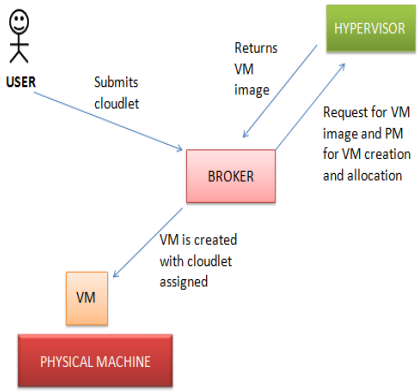

Fig 5.1: Figure showing VM image sharing concept in cloud

source of introducing malware in the cloud computing system. Moreover, an infected VM can be used to monitor the

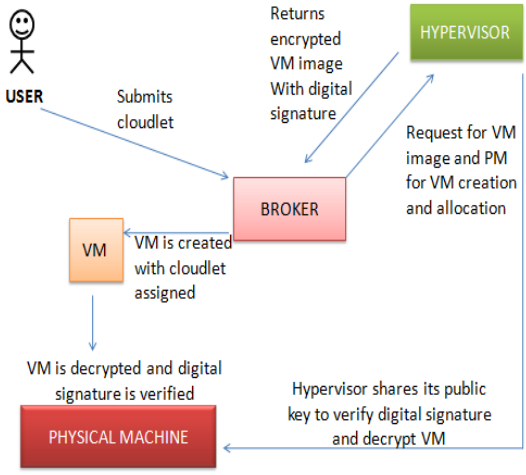

Fig 5.2: Attack on VM image through malicious activity by cloudlet

activities and data of other users resulting in privacy breach. Likewise, if the image is not properly cleaned, it can expose some confidential information of the user [13].

B. *VM isolation and solution*

VMs running on the same physical hardware need to be isolated from each other. Although logical isolation is present between different VMS, the access to same physical resources can lead to data breach and cross-VM attacks. Isolation is not only needed on storage devices but memory and computational hardware also needs fine grained isolation of VMs [3].

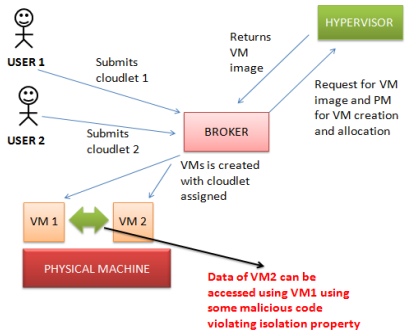

Fig 5.3: Figure showing data theft by VM1 on data of VM2.

C. *Secure VM migration and VM escape protection*

1) **VM escape:** VM escape is a situation in which a malicious user or VM escapes from the control of VMM or hypervisor. A VMM is a software component that manages all the VMs and their access to the hardware. The VM escape situation can provide attacker access to other VMs or can bring the VMM down. A successful VM escape attack can provide access to the computing and storage hardware. The IaaS service model is affected that can in turn effect other service models.

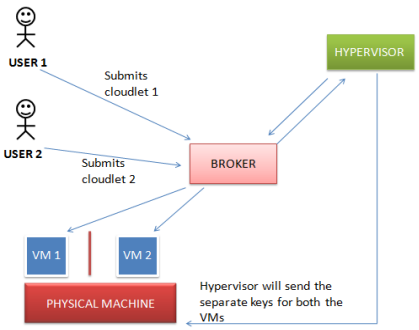

Fig 5.4: Figure showing proposed encryption scheme for maintaining VM isolation

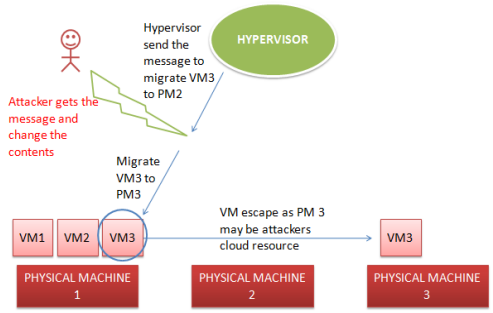

Fig 5.5: Figure showing VM escape by attacker.

2) **VM migration:** The VM migration is the process of relocating a VM to another physical machine without shutting down the VM. The VM migration is carried out for a number of reasons, such as load balancing, fault tolerance, and maintenance. During the migration phase, the contents of the VM are exposed to the network that might lead to data privacy and integrity concerns. Besides data, the code of VM also becomes vulnerable to attackers during migration. The migration module can be compromised by an attacker to relocate the VM to a compromised server or under the control of compromised VMM. The VM migration is a crucial phase and needs to be carried out in a secured manner.

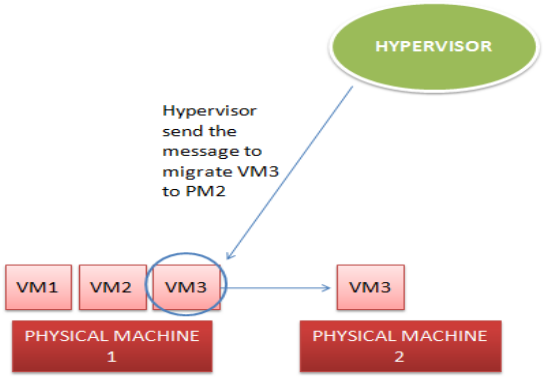

Fig 5.6: Figure showing normal VM migration from PM1 to PM2.

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.

VI. Comparative Analysis and Results

A. *Key generation by hyper visor for itself*

Key is generated using the same RSA algorithm. It involves following overhead

TABLE 6.1
KEY GENERATION AND DISTRIBUTION OVERHEAD

Key generation and distribution overhead	
Key generation time	312 msec.
Key distribution time	It depends on the number of physical machines. Public key is distributed to all physical machines and Broker for digital signature verification. In this thesis 5 VMs and 4 Physical machines are used in simulation and one broker is used in architecture. **Key distribution time: 916 msec.**

B. *VM image sharing process Vs Secure VM image sharing*

TABLE 6.2:
TABLE SHOWING SECURITY OVERHEAD IN SECURE VM IMAGE SHARING PROCESS.

	Normal VM image sharing	**Secure VM image sharing**
Key generation at hypervisor	NA	312 ms
Public key distribution to all PM (4 in this thesis)	NA	916 ms
VM image encryption at hypervisor	NA	411 ms
VM image transmission from hypervisor to Broker	272 ms	317 ms
VM image creation at PM	179 ms	183 ms
VM image decryption at PM	NA	398 ms
TOTAL TIME (ms)	451 ms	2537 ms

C. *Secure VM isolation*

Whole data of every VM is encrypted using VM secret key known only to PM. And data encryption time and decryption time depends on the data length as illustrated in table discussed.

TABLE 6.3
TABLE SHOWING SECURITY OVERHEAD IN SECURE VM ISOLATION.

	Time in milliseconds
Key generation for each VM by hypervisor (5 in this thesis)	1129 ms
Key distribution by Broker to all PM on which VMs are running	385 ms

D. Secure VM Migration

TABLE 6.4:
RESULTS FOR SECURE VM MIGRATION PROCESS.

	Time in milliseconds
Key generation to new PM on which it is to be migrated	254 ms
VM decryption using current PM key	119 ms
VM encryption using new PM key	224 ms

Using above secure VM migration technique ensures VM escape protection.

VII. CONCLUSION

In this paper all the virtualization concepts which include VM image sharing, VM migration, VM isolation and VM escape are studied. All the algorithms are implemented using CloudSim library with the help of Eclipse. It is proved that these security algorithms doesn't put any additional considerable overhead in terms of time. And will increase security and provide severe attacks on cloud.

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.