A Literature Survey on Virtualization Security Threats in Cloud Computing

Brona Shah[1], Jignesh Vania[2]

[1,2] Department of Computer Engineering, Gujarat Technological University, Gujarat, India

Abstract: ***Cloud Computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources, (for example networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. But it has many security issues they are Lack of trust, loss of control and multitenency. In cloud computing at IaaS Infrastructure is provided so Virtual machines are running in this level and service has been provided. SO there is one security threat is VM Migration. So for preventing this VM Migration problem one protocol is used so through that protocol this problem becomes less. At this level different VMs of different users are running on the same physical server. So another problem at this level is risk of co-resident attack, in which user of one VM can get information from another VM. So for reducing this co-resident Attack different policies are there which perform the best when servers are properly configured but if not then there is a risk of co-resident attack so for reduce the risk of this new policy is there in which Previously selected server First is used that is for allocating the server for user. But still there is problem so that another policy in which one agent is there which checks the user and authenticate them and if there is any malicious VM then it discard it so that possibility of co-resident attack is becoming less and efficiency will be improve and secure services are being provided. So in this paper survey on virtual machine threats mainly VM Migration and Co-resident Attack is discussed***.

Keywords*:* Cloud Computing, Cloud Security, Infrastructure as A Service, Virtualization, VM Migration, Co-resident Attack

1. Introduction

Cloud Computing is an on demand service model for IT provision based on Virtualization and distributed computing technologies.[1] In the current era, It is a wide field. It provides different services and platforms. It provides multi-tenency, Massive scalability, elasticity, self provisioning of resources. In cloud resources are shared so it is easy to use them whenever we want.

It provides different service delivery models. They are software As A Service (Saas), Platform As A service (Paas), and Infrastructure As A Service (Iaas). Saas rents software on a subscription basis. User can access the service through authorized device. In short Saas is a software distribution model in which Application resides on cloud service provider(CSP) and are available for its clients via a web browser (e.g Google docs) [2]. Paas offers development environment to application developers. So it refers to the delivery of operating systems, associated tools, toolkits, building blocks over the internet. A Client deploys his application on the cloud service provider without installing any tool or platform on their local machines. In Iaas, CSP outsource the processing power, Storage, network and all other computing resources in the form of Virtual Machines. Hypervisor is provided at this level.

Cloud computing provide different deployment models. They are Public cloud, Private cloud and Hybrid cloud. Public clouds are hosted, operated and managed by third party vendor. Their security and day to day management is also done by vendors. So It is available for all the consumers. While private clouds are restricted to any firm or organization. In which networks, infrastructures and data centres are owned by the organization. Hybrid cloud is a combination of both in which sensitive applications are provided by private cloud while non-sensitive applicators are provided by public cloud.

Data Center
Public Cloud
Data Center
Internet
Personal Cloud
Laptop
NFC
Desktop
Handheld

Figure 1: Cloud Usage Enterprise Environment

2. Background

As Cloud infrastructure consist of large scale virtualized resources, traditional security mechanisms are not enough. There are some security issues that need to be consider. Main security issues are loss of control, lack of trust and multi-tenancy. Apart from that at different level like network, host and application layer Security should be considered. In Saas customer has vey less control over resources, therefore CSP is responsible for the required security mechanism. Whereas the PaaS offers greater custom control as compare to SaaS so CSP and customer are responsible for security mechanism.While IaaS offers greater custome control over security as compare to SaaS and PaaS. The PaaS and SaaS models are dependent on IaaS so any breach in Iaas model will affect the security of PaaS and Saas.

Virtualization is key at IaaS Model. So at Iaas Virtualization is provided. Different instances running on the same physical machine are isolated from each other is a major task of virtualization. Therefore this dynamic nature makes it difficult to achieve and maintain consistence security. The hypervisor manages and allocates the physical resources among the VMs.[5]

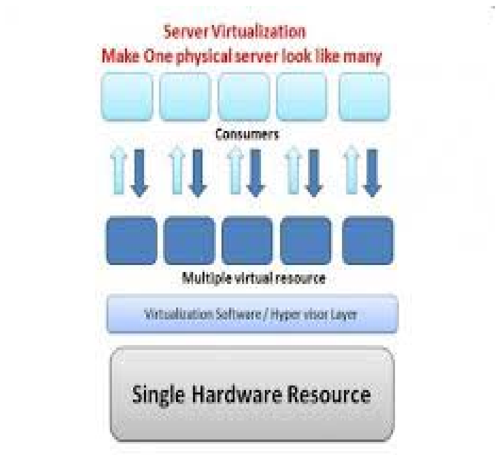
Server Virtualization
Make One physical server look like many
Consumers
Multiple virtual resource
Virtualization Software / Hyper visor Layer
Single Hardware Resource

Figure 2: Virtualization

In virtualization some Vulnerability are: VM hooping, VM Diversity, VM Denial of Service and VM Mobility. [4]

- **VM hooping (co-resident Attack)**: an attacker on one VM gains access to another VMs. The attacker can monitor any VM's resource usage, delete stored data and modify its configuration.
- **VM Mobility/Migration**: content can be moved or copied from one host to another.
- **VM Diversity**: Security management is done.
- **VM Denial of Service**: when multiple VMs share resources at a single time then VM denial of service is also one issue.

In virtualization Full Virtualization and Para Virtualization are two kinds of virtualization provided in cloud computing. For that Virtual Machine Monitor (VMM) is used which abstracts the physical resources used by the multiple virtual machine.[6]VMM provides a virtual processor. VMs are running at a one time so VM Lunch, VM authentication, VM Migration, VM license all things should need to be consider.

In cloud computing IaaS user can not verify the provider promised cloud platform integrity so it is a security risk. To prevent this issue one VM Lunch is introduced which allows the cloud user to securely bind the VM to a trusted computer.[7] Main issue is VM migration. VM live migration is done still there are some security issues that need to be consider.[11,12]

VM Migration

VM Migration is a process in which running VM is migrated from one platform to another. Virtualization can provide significant benefits by enabling virtual machine migration to balance load across data centre. It enables highly responsive and robust provisioning in data centre. It provides hardware/system maintenance, transparent mobility, work load balancing, consolidated management and high availability services. It is a administration tool which deals with situations like performing platform hardware maintenance without disrupting provisioned services, optimization of workload with provider resource pool. Xen and VMware have implemented "live" migration of VMs that involves short downtimes ranging from tens of millisecond to a second.[8] The major benefit is, it avoid hotspots, still it has some issue. That is detecting workload hotspot and initiating a migration lacks the agility to respond to sudden workload changes. And in memory state should be transferred consistently with integrated consideration of resources for application and physical servers. In Xen an attacker can gain control over guest OS or VMM due to vulnerabilities in migration module and similarly VMware exposes the sensitive information of guest OS during the VM migration.[3] So Live VM migration without security features become single point of failure for cloud environment.

Co-resident Attack

In cloud computing environments, in order to maximize the utilization rate of hardware platforms, it is common practice that the virtual machines (VMs) of different users run on the same physical server (i.e., these VMs are co-resident), and are logically isolated from each other. However, malicious users can circumvent the logical isolation, and obtain sensitive information from co-resident VMs [12]. If cloud providers cannot ensure data confidentiality and hence lose the basic trust from users, the future of cloud computing will be jeopardised. Therefore, it is crucial to find effective and practical countermeasures against this kind of threat.

Although, in principle, programs running on co-resident VMs should not be able to influence each other, there are a variety of ways this can occur in practice. For example, the cache utilisation rate has a major influence on the execution time of cache read operations. Therefore, the attacker is able to estimate the victim's cache usage by performing extensive cache read operations and comparing the execution time on a co-resident VM [10]. With similar approaches, attackers can also infer other private statistics, such as the traffic rate of a website.

In addition, co-resident VMs share the instruction cache and other hardware resources. This can also be exploited by malicious users to extract private information, such as cryptographic keys [13], although it requires overcoming several major challenges.

One way to encounter this kind of threat is to fundamentally eliminate the side channels between VMs. [14]. However, the proposed methods require substantial changes to be made to existing commercial platforms, and hence are impractical and not suitable for immediate deployment.

3. Related Work

VM Migration

The Importance of secure VM migration solution for IaaS clouds have earlier been identified. In that platforms within the CSP network could be malicious and untrusted which could result in security threats during VM migration. To overcome this problem Trusted Cloud Computing Platforms (TCCP) which are register with a Trusted Third Party (TTP) called External Trust Entity (ETE) are introduced which define trustworthiness of the platform during VM Launch and Migration.[3] In Migration following requirements are analyzed

1) **Security:** That is the user VM must be protected against any unauthorized migration on vulnerable platforms, either unintentionally or intentionally so that the user can trust the complete cloud service provider's infrastructure.
2) **Transparency:** In this main goal is to keep VM migration transparent from the user without compromising on the trustworthiness of the destination cloud platform.
3) **Scalability:** There are many cloud deployment models and each can have different VM migration requirements so the secure migration solution should scale well to high number of simultaneous VM migration.
4) **Scheduling Flexibility:** For the IaaS provider to implement efficient load balancing, it must be possible for the provider to introduce scheduling mechanisms within the provide network.

To overcome these requirements in VM migration one protocol is introduced that is Trust_Token which certifies the trust worthiness of a platform up to a certain level.

It is important to ensure that cloud platform can present Trust_Token as a proof of trustworthiness only if it has the same software and hardware configuration for which the Platform Trust Assurance Authority (PTAA) assigned and evaluated the Trust Assurance Level- Value (TAL-Value) to it.[3]

Because of the bind key provided in this protocol it ensures high level of security and trust by allowing only the intended destination platform and in a good known integrity state to decrypt the user VM.It binds the trust level of a cloud platform with a TPM-based bind key which can used only if the platform meets the assigned trust level. So because of this protocol security, scalability, flexibility and transparency are provided. In short Trust_Token is used for the migration which ensures that the user VM is never migrated to the untrusted platform.[3] So that it can be secure.

Co-Resident Attack

Now, for co-resident attack which is also known as side channel attack or VM Hopping. For preventing side channel attack there are different technique used.

In VM side channel attack requires two things they are placement and extraction. Placement refers to the adversary or attacker arranging to place their malicious VM on the same physical machine. Extraction means after successfully placement of the malicious VM to the targeted VM extract the confidential information, file and documents on the targeted VM. So for that it might be accomplished by the combination of firewall and random encryption decryption. That is for preventing placement the virtual firewall appliance in the backend of the cloud computing and for preventing extraction random encryption decryption is used. [15] But problem with this things are sometimes someone gets key of encryption/decryption somehow. So this technique is used but it is not so efficient.

Now another thing is for preventing inter-VM Traffic. Virtualization is the fundamental of the cloud computing, security and availability are critical for cloud environments because their massive amount of resources, simplifies several attacks to the cloud services. So for inter-VM traffic one new approach that gives an identity to particular traffic, this identity is about the where and the who sends the request. So for that one approach which propose a frame called frame tag that holds the proper credentials which are the tenent and the application that sends the IP packet, providing data origin authentication and integrity and also proposing an agent which is abale to generate, caputure and analyze particular frame and respond to it by automated acceptance or rejection and security mechanisms in order to ensure the security and integrity of the frame tag.[16] Through this inter-VM traffic is being avoided but still there is risk of co-resident attack. For allocating VMs different policies are defined they are:

(1)/(2) Least VM/Most VM policy. For every new VM request, the policy selects one server randomly from those that host the least/most number of VMs, and have enough resources left. (3) Random policy. For every new VM request, the policy randomly selects one server from those with enough resources.

In least VM Allocation policy there is less number of VMs so chance of co-resident attack is become less. But problem with this policy is someone thinks its not reliable that's why there is less number of VMs.

In Most VM Allocation policy there are more number of VMs allocated on a single host so it is more trustworthy then other servers. But problem is that in this more VMs are allocated on a single server so there are more chances of co-resident attack. SO they propose a new policy in which They merge the three policies (Least VM, Most VM, and Random) with the following change: when a user *L* requests to start a VM, the servers that already host the VMs from the user, Servers will be considered first. If such servers do not exist, or do not have enough resources left, the allocation process still follows the original policy. It is called Previously Selected Server First (PSSF). [17] Under this policy, the best strategy for the attacker is to use multiple accounts, each of which starts only one VM at a time. But it is not implemented yet they only propose so still we cannot assure that it is efficient.

4. Conclusion

Virtualization is provided at IaaS level in cloud computing so it is one important thing. In cloud at a time so many requests are being handled so for providing it properly virtualization is necessary. But in virtualization there are some security threats which are need to be considered. So in this paper we have discussed about that threats but in them there are main two threats they are VM \migration/mobility and VM Hooping/co-resident attack. So In this paper some techniques which are used for preventing these two problems are discussed. So that using them one can avoid the problem of VM Migration and Co-resident attack and CSP provide more efficient and secure services to its users.

References

[1] Zhang, Qi, Lu Cheng, and Raouf Boutaba. "Cloud computing: state-of-the-art and research challenges." *Journal of internet services and applications* 1.1 (2010): 7-18.

[2] Bhadauria, Rohit, et al. "A survey on security issues in cloud computing." *arXiv preprint arXiv: 1109.5388* (2011).

[3] Aslam, Mudassar, Christian Gehrmann, and Mats Bjorkman. "Security and Trust Preserving VM Migrations in Public Clouds." *Trust, Security and Privacy in Computing and Communications (TrustCom), 2012 IEEE 11th International Conference on*. IEEE, 2012.

[4] Tsai, Hsin-Yi, et al. "Threat as a Service?: Virtualization's Impact on Cloud Security." *IT Professional* 14.1 (2012): 32-37.

[5] Nurmi, Daniel, et al. "The eucalyptus open-source cloud-computing system."*Cluster Computing and the Grid, 2009. CCGRID'09. 9th IEEE/ACM International Symposium on*. IEEE, 2009.

[6] Garfinkel, Tal, and Mendel Rosenblum. "A Virtual Machine Introspection Based Architecture for Intrusion Detection." *NDSS*. Vol. 3. 2003.

[7] Aslam, Mudassar, et al. "Securely launching virtual machines on trustworthy platforms in a public cloud." (2012).

[8] Clark, Christopher, et al. "Live migration of virtual machines." *Proceedings of the 2nd conference on Symposium on Networked Systems Design & Implementation-Volume 2*. USENIX Association, 2005.

[9] Ristenpart, T., Tromer, E., Shacham, H., and Savage, S.: "Hey, You, Get Off of My Cloud: Exploring Information Leakage in Third-Party Compute Clouds," Proc. 16th ACM Conference on Computer and Communications Security (CCS 2009), 2009, pp. 199-212

[10] K. Hashizume, D. G. Rosado, E. Fernández-Medina, and E. B. Fernandez, “An analysis of security issues for cloud computing,”Journal of Internet Services and Applications 2013.

[11] P. Mell, T. Grance, 'The NIST definition of cloud computing". NIST,Special Publication 800–145, Gaithersburg, MD.

[12] Zhang, Y., Juels, A., Reiter, M., and Ristenpart, T.: "Cross-VM Side Channels and Their Use to Extract Private Keys," Proc. 2012 ACM Conference on Computer and Communications Security - CCS '12, 2012, pp. 305-316

[13] Jin, S., Ahn, J., Cha, S., and Huh, J.: "Architectural Support for Se-cure Virtualization under a Vulnerable Hypervisor," Proc. 44th Annu-al IEEE/ACM International Symposium on Microarchitecture - MICRO '11, 2011, pp. 272-283

[14] International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 – 8958, Volume-2, Issue-2, December 2012 “**Security against Side Channel Attack in Cloud Computing**” by Bhrugu Sevak

[15] Benzidane, Karim, Sad Khoudali, and Abderrahim Sekkaki. "**Secured architecture for inter-VM traffic in a Cloud environment.**" *Cloud Computing and Communications (LatinCloud), 2nd IEEE Latin American Conference on*. IEEE, 2013.

[16] Han, Yi, et al. "**Virtual machine allocation policies against co-resident attacks in cloud computing.**" *Communications (ICC), 2014 IEEE International Conference on*. IEEE, 2014.