ORIGINAL RESEARCH PAPER

Engineering

KEY WORDS: Cloud services; Virtual machine manager (VMM); security; vulnerability; virtual resource;

Multi-level Security for Virtualization in Cloud services

N.L.Udaya Kumar Research Scholar, Jain University, Bengaluru

Dr.M.Siddappa Professor and Head, Dept of CSE, SSIT, Tumkur

ABSTRACT

Cloud computing is the way of computing, where all the computing resources are available as a service over the internet based on requirements of the users. Virtualization is the concept which plays very important role in reducing the cost of investment and increases utilization and allows multi-tenancy. This concept helps to create virtual resources out of existing physical resources. When the virtual resources are created, they may face the problems due to various reasons and may not work properly. Providing the protection to these virtual resources and make them to work without any problem is the important. Here we introduce an approach to provide the security at different levels to make Virtual resources secure.

INTRODUCTION

Computational power, server capacity, applications, platforms, softwares etc are the IT resources, which are available to customers whenever they need, from cloud service providers through the internet. The virtualization logically partition these resources to create a pool of logical resources to reduce the investment and to increase the utilization.

Cloud models are available in two types. Deployment and Service models. There are three forms in Deployment models, Public, Private and Hybrid cloud. We have three basic service models, Infrastructure as a service (IaaS), Platform as a service (PaaS) and Software as a service (SaaS). Iaas is the base, over which PaaS will run and above that SaaS will run. Virtual Machine Manager (VMM) plays very important role in Cloud computing services. Cloud computing becomes a new way of computing, which plays an important role in providing services in the form of Computing resources to both IT companies and academia. To make services possible in cloud computing, it requires some promising techniques such as Service Oriented Architecture (SOA), Service Oriented Modelling and Architecture (SOMA) and other open architectures to develop the cloud applications that are platform independent, portable and easily usable. Though the use of virtualization in cloud computing has many benefits, it is suffering from security problems, when sharing the logical resources. In addition data security is the biggest issue of cloud computing. It is necessary to have the suitable security mechanisms to protect both logical and physical resources.

VMM allows provision of resources based on customer demand and to share resources among many customers, this enables cloud computing to have the property called multi-tenancy, there by reduces cost of using those resources. Current security systems may not provide the required security to virtual resources in cloud computing. In this paper we focus on challenges of virtualization security, vulnerabilities, impact of virtualization on cloud services and propose an approach to overcome them.

VIRTUALIZATION

Virtualization is the process of creating the virtual resources from the existing physical resources to make full utilization of them and there by satisfy many users concurrently. This reduces the overall investment on computing resources so that cloud service providers may provide services to multiple customers with minimum investment.

Benefits of virtualization:

- Increased availability
- Maximized hardware resources
- Reduces administration and labour costs
- Efficient application and desktop software deployment and maintenance
- Reduced time for server provisioning
- Server consolidation
- Green IT – reduced power and cooling
- Reduced hardware costs

A VMM is a piece of software, whose main function is to create the partitions over the existing physical resources. For example, several virtual machines can be created out of one existing physical machine, virtual machines are also called as instances or virtual instances. After creating the machines or instances, it is the responsibility of the VMM to take care of those machines. It has to allocate the resources such as computing power, storage, server capacity, bandwidth, application, data etc.., required by the machines to make them work according to user requirements. VMM is also called as Virtual machine manager or Hypervisor. It is the responsibility of the hypervisor to de-allocate the resources from that virtual machine after the work is over and release the virtual machine. The important factor is, the creation of required number virtual resources depends on the capacity of the physical resource. There are two types of hypervisors, Type1 and Type2 hypervisors. Type1 is also called as Bare metal or Native hypervisor, Type2 is also called as Hosted hypervisor. Virtual machines are called as Guest machines and physical machines are called as Host machines. The Operating system running in guest machines are called as Guest operating systems and operating systems running in host machines are called as Host operating systems. Type1 hypervisor directly runs on the physical hardware but Type2 hypervisor runs on host operating system. Type1 has direct control of hardware whereas Type2 has to interact with hardware via host operating system. Bare metal hypervisor uses high-level resource management policies to compute a target memory allocation for each virtual machine based on the current infrastructure load and parameter settings for each of the virtual machines.

PROBLEMS IN CLOUD VIRTUALIZATION

The machine where the VMM is running is the one, who acts as central control point for the purpose of allocating the resources to the virtual instances and de-allocating the same resources from those instances after the processing is over, there by releases the virtual machines. Since it is in the position of creating, allocating and de-allocating of resources, it may be vulnerable to attacks. In addition most of the times virtual machines are also vulnerable to attacks of malwares which leads to non-functioning of virtual machines.

Performance reduction: Surely this is one of the main issue of virtualization technology in cloud services. If the number of virtual resources created out of physical resource increases, it automatically reduces the performance of the virtual machines with increased latency. This can be experienced by the users. It is very essential to know the capacity of the existing physical resources and how many virtual resources can be created out of it.

Predicting future demands: This is one of the main concern with respect to cloud services. When the virtual machines are created out of physical resources and allocate the required amount of resources like computing power, storage, memory etc., to the virtual machines, it is very essential to have the knowledge of

predicting the future requests which may come from cloud service users based on their previous transactions history. So it is necessary to reserve some resources which are required by cloud service users in the future.

Authorised users and accesses[3]: The authorised users have more rights than the other users. The chances of injecting the attacks and involving in problematic access to the resources are usually more with the authorized users only, because the ordinary users are usually avoided at the basic level of security thereby avoiding the serious attacks at the initial stage itself. The main problem is identifying the authorized users who are involving in problematic activities, because they have authorization to access the resources and enter into the virtual environment and easily involve in such activities, which is one of the main issue.

Protection[3]: Service on request and Dynamic elasticity are two important characteristics of cloud computing. When there is a request from customers for computing resources, the same has to be provisioned by the cloud service providers without fail. These resources are provided with some level of protection mechanisms, whenever the customers requests for the resources which are different from previous requests, the protection mechanisms must identify these changes in the requests and intimate the cloud service providers and try to provide the required level protection to changed requests. These requests dynamically changes according to the needs of the users. As cloud computing gaining importance day by day, the quality and level of service and protection should be increased so that the customer safely and securely use resources which may lead to increase in the cloud business and help providers to involve in implementing high level of protection and security systems to satisfy more customers. This is one of the issues of cloud computing.

Resource availability[3]: This is one of the benefits facilitated by the concept virtualization. It also helps to track and leverage the resource pool under the same umbrella of resource units. Availability is not just a technology issue, it is a business issue as well. When it is working, you don't know it is there, so it is easy for management to assume it always will be. Achieving very high level of resource availability usually requires substantial investment by the cloud owners on infrastructure and other resources and virtualization concept to make logical resources with adequate security mechanisms to protect both physical and logical resources.

Service Secrecy[3]: The cloud service users requests for the required resources such as softwares, applications, infrastructures, platforms or storage from the cloud service providers. In this scenario the customer has to interact with the cloud service provider and their cloud services. During this interaction, exchange of data and confidential information with respect to cloud services will be happened using network transactions. In this situation, it is necessary to maintain customers information and their status safely and securely. The restricted users can try to hack customer's confidential information. This may create serious problems to customers. In addition, when many customers are sharing the common resources among them, it is necessary to avoid each customer from using or knowing the usage or status of other customers to avoid the problems. This is one of the issues of cloud computing.

Migrating instances[3]: Generally the virtual machines or instances which are created from the physical machines are available in the form of files. These files can go from one physical machine to another physical machine. During this movement of instances, they may vulnerable to attacks and problems. When they affected by the malwares or viruses they can create the problems to other virtual instances and also to physical machines by changing their settings, configurations and corrupting the files and folders of other virtual instances. This may tend leakage of data and information and in turn virtual instances may behave improperly. Sometimes this may create the problems to the operating systems running in physical machines. When these physical machine's operating systems are corrupted, these corrupted operating systems can create the problems to virtual instances. They may not allocate the required resources to the virtual instances, or they may de-allocate the resources from the virtual instances early before they complete the processing. It is the responsibility of OS to allocate and de-allocate the resources required by the virtual instances after their creation. This is also one of the serious issue.

Service Level Agreement[3]: It is the agreement or contract made between cloud service provider and service user before resources are provisioned to the user after their request. It plays very important role in cloud service business. It is very essential to make the cloud service business possible. It defines the level of service availability, response time, how reliable the resource components are, responsibilities of both customer and service user and other warranties with respect to service components. It specifies how the service user has to utilize the resources without breaching the SLA by maintaining the resources in the proper condition and specifies how the service provider has to provision the resources to the user, quality of services, replacement of resources when something happens, maintaining the uptime and backups, providing the quality of service, decreasing the response times etc. Tailoring the separate SLA for each and every customer is one of the biggest issue of cloud service business. When virtual instances created from physical machines, usually different operating systems are installed on virtual instances to make them to run compatible applications. After creation of instances, managing, maintaining and providing protection to those instances is the tedious task. Since they have different operating systems and applications running, it should be mentioned in agreement so that both service provider's and service user's responsibility in taking care of instances or virtual machines. The provider must neatly configure and settings should be made to those instances and attach security mechanisms. The service user must maintain this virtual instance by proper handling with proper updates and compatible patches which are received from service provider. This is the reason, we say that stitching a separate SLA for every customer is the tedious task.

In addition, virtual instances which are created from same physical machine must be isolated properly to make them run independently to process by running the compatible applications without any dependency. But sometimes it is possible that the virtual instances that are malicious, may attack neighbour instances or disrupt their normal routines by stealing the resources from them or by corrupting the data required to process by them or by injecting the malwares to the guest operating systems so that the guest operating systems should not work properly to handle the processing required by the customers. This leads to the serious problem to the virtual machine resources such as network bandwidth, memory, computational power that are shared among multiple users. This is one more situation where Service Level Agreement has to define the clear cut isolation policies among the virtual instances created from the same physical machine, which is a serious issue.

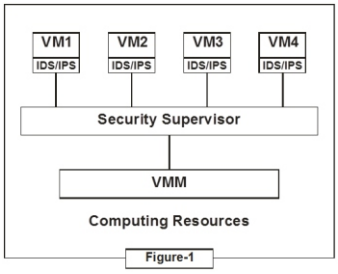
PROPOSED APPROACH

We are proposing two approaches.

In the first approach, we are introducing two levels of security mechanism to make virtual machines more secure and work according to the requirements of the users. Here we introduce Intrusion detection and Intrusion prevention system directly into the virtual system itself, so that any intrusions can be easily detected and prevented in these machines, which is shown in figure-1. This is second layer of security. In the first layer, we have security supervisor. The security supervisor checks the entering virtual machines details and its characteristics for validation. This provides the result in distinguishing malicious machine identification from non-malicious one. If the entering virtual machine does not satisfy the security supervisor, then it will be treated as attack or malicious software and it will be disconnected from system. It will not get the permission of access to the

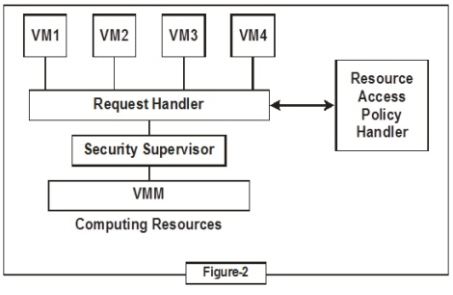
resources. If it is recognized as a valid virtual machine, then it will be registered and allow it to access the resources based on the control policy. This method will provide security to virtualization environment by avoiding invalid virtual machines resource requests, and allows only valid virtual machines to access the resources.

Figure-1



In the second approach, a virtual machine with various intentions enters virtualization environment and sends requests for receiving the virtual resources to the VMM. That request has to be delivered to the component called Request handler and in turn that request delivered to the Resource access policy handler which is shown in figure-2. When the requests are made by the virtual machines for resources, it is given to the Resource access policy handler through Request handler, where the requests are tested for authentication and authorization to decide whether they are valid or not. If they are valid and authorized requests for authenticated resources, then those requests are fulfilled otherwise those requests are ignored. Resource access policy handler in virtual environment refers to the practice of restricting entrance to a resource to authorized VM. A well designed Resource access policy handler will make the physical resources being used properly and communication between Virtual machines and between VM and VMM more reliable.

Figure-2



The function of Security supervisor is explained in the form of algorithm given below.

Algorithm (shows the function of Security Supervisor) [3]:

1. Virtual machine enters to the pool of virtual resources.
2. Sending request to Virtual Machine Manager.
3. That request pass through the Security supervisor.
4. Check for Authentication and validity.
5. If Invalid, disconnect from the environment.
6. If valid, check for access control policy.
7. Allow it to access resources.

Different types of security mechanisms, problem identification functions, problem correction methods, avoiding restricted users and accesses, process of hiding the originality of data mechanisms, methods of identifying and avoiding intruders, attackers, malwares, viruses should be included in Security supervisors.

In addition it may contain some updates and patches required by the virtual machines and softwares. It should have the flexibility of including the latest techniques and other solutions which may work very well in future. It should have the routine of redesigning its methods and solutions and keep updating at regular intervals so that it should always contain latest, adequate and effective security solutions.

It may given the flexibility that, some security solutions can directly injected to the virtual machines itself.

Performance issues may exist when implementing such type of security solutions inside the Security supervisor.

CONCLUSION

In this work, a set of security problems are discussed in cloud virtualization. Then we propose two approaches to overcome the vulnerabilities of VMs. Performance of the proposed approach in management of virtual machine resources facilitates security of performed operations on the platform. It distinguishes between valid and invalid (malicious) virtual machines. It is advisable to the IT infrastructures that, they mainly concentrate on investing on secured virtualization mechanisms since similar type of security challenges exists between both virtual and physical execution environments. Adopting the combined approach with security software provides required level of protection, immediate application of solutions and make sure that minimum level of security to all the virtual instances with no more overheads and problems. Here we have two levels of security mechanism in first approach. This truely helps to avoid any type of attacks and problems, but the problem is cost of implementation may be more and continuous supervision of security mechanism is very essential.

REFERENCES

[1] N.L.Udayakumar and Dr M.Siddappa, 2010, "Security issues and solutions for Virtualization in Cloud computing service", In International Journal for Engineering Research & Technology (IJERT), 2015.pp.55-57
[2] N.L.Udayakumar and Dr M.Siddappa, "Meeting the challenge of Virtualization impact on Cloud services", In International Journal of Computer Science and Information Technologies (IJCSIT) Vol. 7(1), 2016, 457-461.
[3] N.L.Udayakumar and Dr M.Siddappa, 2016, "Ensuring security for virtualization in Cloud services", In International conference on Electrical, Electronics, Communication, Computer Technologies and Optimization techniques (ICEECCOT-2016) in association with IEEE Bangalore at GSSSIET, Mysore.