International Journal of Advance Research in Science and Engineering
Vol. No.4, Special Issue (01), September 2015
www.ijarse.com
IJARSE
ISSN 2319 - 8354

MULTILAYER INTRUSION DETECTION SYSTEM FOR INFRASTRUCTURE-AS-A-SERVICE PROVIDER ON CLOUD

Deepika Agrawal[1], Dr. Sudhakar Pandey[2], B Ramachandra Reddy[3]

[1]Research Scholar, [2]Head, [3]Faculty, Dept of Information Technology, NIT Raipur(India)

ABSTRACT

Cloud computing is a new boom to the IT industry and provides resources to the user as a service over the internet. Cloud computing provides three types of services to the user, SaaS, PaaS, IaaS. It has a unique feature "anytime, anywhere" which made it a latest technology. Cloud environment is shared by clients and they do not want the data to leak from one domain to another. Virtual machine attacks are at a higher risk. Intrusion Detection Systems can be used to monitor system activities for malicious activity. Given the distributed architecture for cloud computing, conventional IDS like host based or network based alone are not suitable, so a multilayer IDS at the cloud provider's site that takes a hybrid approach to suit cloud computing has been designed and implemented. DOS attack and VM compromise are two major attacks against the cloud services provider. These two attacks are mainly considered in this paper.

Keywords: Behaviour based IDS, Cloud, Cloud IaaS, IDS, DOS attack, Network based IDS, VM.

I. INTRODUCTION

Cloud Computing generates a lot of interest and competition in the industry. Cloud computing is a cost-effective, proven delivery and flexible platform for providing IT services over the Internet. Cloud resources can be easily scaled and rapidly deployed, with all processes, applications, and services provisioned "on demand", regardless of location of user or device. It offers "pay-per-use" service to the clients just like electricity bill. In electricity bill, the user pays only according to his usage. With the ease of these services, it also suffers from several significant vulnerabilities. When the data of an organization gets ready to move to a cloud computing environment, security measures should be there to prevent data from leakage, hacking, etc. Virtualization is one of the main components of a cloud. Virtual machines are dynamic in nature i.e. it can quickly be reverted to previous instances, paused and restarted.

Denial of Service and Virtual Machine Compromise are two major attacks against the cloud services provider. In first type of attack, the attackers flood the server with false requests resulting in legitimate users being denied service. If a guest VM is compromised, then attacker can pass infection to other guest VMs on the same host. Co-location of multiple VMs, which is common in cloud architecture, increases the surface and risk of this attack. Recent reports on such attack like the Distributed DoS attack on Ultra DNS affecting Amazon & Sales Force, play station network hack launched from Amazon EC2 shows the vulnerabilities in existing cloud

security. IDS are proactive mechanisms to monitor network/system activities for malicious activities or policy violations. But the question arises that, where does the IDS fit in?

Several research papers have been published for the deployment of IDS in cloud environment. Some are based on Network Based IDS and some are based on Host Based IDS. We are trying to combine these two IDS in cloud architecture in two different positions so that the user can get the benefits of cloud computing services.

The rest of the paper is organized as follows. Section 2 describes the cloud architecture in more detail. Further it presents the related works, which have done in the recent past and explains why the existing approaches cannot adequately solve the intrusion detection problem. Section 3 presents the proposed architecture and provides details of the implementation and results. The results are discussed in the Section 4. The conclusion and future work are mentioned in Section 5.

II. LITERATURE SURVEY

2.1 Cloud Computing

Cloud computing is a term generally used for anything that involves delivering of services over the Internet and it is pay per use services. These services are broadly divided into three categories:

- Infrastructure-as-a-Service (IaaS): IaaS provides application program interface. Customers use this to configure their storage and virtual servers and they can start, stop their virtual servers. These virtual server instances have unique IP addresses and blocks of storage on demand. It is referred as utility computing, as pay-for-what-you-use model resembles the way fuel, electricity and water are consumed.
- Platform-as-a-Service (PaaS): This is defined as a set of software and product development tools hosted on the provider's infrastructure. Users create applications on the provider's platform over the Internet.
- Software-as-a-Service (SaaS): The cloud provider supplies hardware infrastructure, software product and interacts with the user through a front end portal. The service provider hosts both application and the data, end user is free to use this service from anywhere [29].

A cloud services have three distinct characteristics that differentiate it from traditional hosting. They are:

- It is sold on demand, typically by the minute or the hour.
- Its elasticity, a user can have as much or as little of service as they want at any given time, and
- The service is fully managed by the provider.

There are two types of cloud:

a) Private: It is a data center that supplies services to a limited number of people or subscriber.

b) Public: It provides services to anyone on the Internet. Currently, Amazon Web Services is the largest public cloud provider.

When a service provider uses public cloud resources to create their private cloud, this method is called as a virtual private cloud. The major goal of cloud computing is to provide easy as well as scalable access to computing resources and IT services [29].

2.2 Cloud Architecture

Base architecture for our proposed model for application service scalability using multiple IaaS providers in cloud is illustrated in Fig.1. A user sends requests for using software applications offered by a SaaS provider,

which includes application layer and platform layer. These layers satisfy the user's request. All application services which a SaaS provider can offer to users are controlled by application layer. The platform layer respond to user's request and makes decision whether to accept or reject a request and includes admission control and scheduling policies. Also, the platform layer schedules the processing of requests on VMs from IaaS providers.

2.3 Related Work

Bamiah et al [3] describes that cloud computing depends on the internet as a medium for users to access the required service at anytime, anywhere and in pay per use pattern. They and also describe the possible threats and vulnerabilities in this technology. This paper also describes the risk associated when an organization is ready to shift their critical data to the cloud. Several risks included Session riding and hijacking, VM escape, insecure cryptography, data protection and portability are explained. Since cloud computing is dynamic in nature and is flexible, multi-shared and scalable and it gives an innovative shape of carrying out business. But besides this benefit there are threats and vulnerabilities that need to be taken care of. Also there is a need to develop in-depth security techniques and policies in terms of people, processes and technology.

Gruschka et al [6] presents one such taxonomy based on the notion of attack surfaces of the cloud computing scenario participants. This paper modeled cloud computing scenario using three different classes of participants such as service users, service instances and the cloud provider. Authors describes that the attackers do not always restrict themselves to only one attacking surfaces. Especially in cloud computing scenario, they may incorporate using several attack surfaces in combination for achieving the indented attack effects. This paper gives a first step towards classifying the attacks and thus making them concrete. Using this notation of attack surfaces, they illustrated the developed classification taxonomy by means of four up-to-date attack incidents of cloud computing.

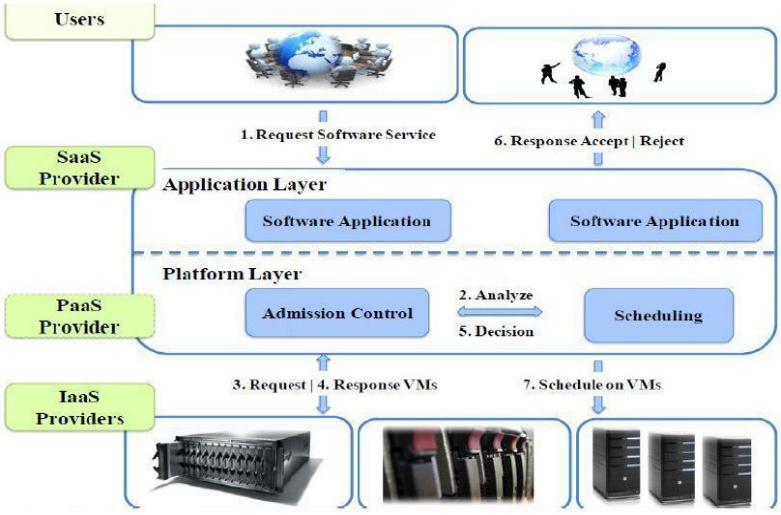

Figure 1. Architecture for Cloud

Roschke et al [13] describes several requirements for deploying IDS in the cloud are given and it also proposed an extensible IDS architecture for deployment in distributed cloud infrastructure. This architecture is an integration of VM management and IDS management. In this architecture, each virtual component should be secured by a separate IDS sensor, which is responsible for one virtual machine and can be configured by the

cloud user. In this paper, only basic UML based features for starting, restarting, stopping and recovering IDS VM's are implemented. This needs to be extended by generic methods for VM management, e.g., monitoring and controlling of Xen based VM's.

Dhage et al [14] describes an architecture in which mini IDS instances are deployed between each user of cloud and the cloud service provider. And this mini IDS instances will be able to work in an efficient way because the load on each IDS instance will be less than that on single IDS instances. Whenever any user wants to access any service that the cloud provider provides, then it is the duty of the IDS controller to provide IDS instance to that user. This model detects multiple threats that could occur in cloud environment but overhead of maintenance this mini IDS instances are high.

Marcos et al [15] describes the usage of virtual machine to improve the security of a computer system. Also proposed a new approach by applying intrusion detection techniques to systems which is based on virtual machines. This keeps the IDS out of reach from intruders. The main idea of this proposal is to encapsulate the system to monitor inside a virtual machine, which is monitored from outside. The IDS are implemented outside the virtual machine i.e., the proposal considers the type II VMM, so the system can be implemented as a host system processes. This system generates an access control list (ACL) which keeps track of the processes executing in the guest system and their respective users. If any system call is not found in the ACL then an anomalous situation is signaled and that process is declared suspect. The system has a drawback that if any user or process who is not anomaly and not found in the generated ACL are also declared suspect. Also the traffic generated by the virtual machine is not considered.

III. PROPOSED ARCHITECTURE AND IMPLEMENTATION

We propose a hybrid IDS in cloud using multilayer technique to improve security in cloud infrastructure. Our multilayer hybrid IDS is combination of two layers; one at the application layer and other at the infrastructure layer. HIDS at the application layer and NIDS at the infrastructure layer.

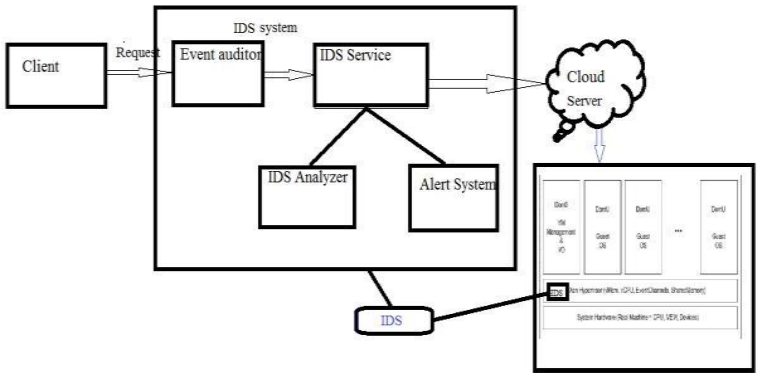

Figure 2. Proposed System Architecture

3.1 HIDS (Host Intrusion Detection System)

HIDS at server level is responsible for monitoring the user activities. The intrusion detection is detected on the basis of user behavior. User behavior in terms of what browser the user used to access the cloud [28], login IP of

the user. These features are stored in a database in terms of count of different browser of the user had used to access. If the user accesses the browser with count less than the threshold count then it is considered as an anomaly in the behavior. Similarly, the login IP user used to access the cloud is stored, we store the count of IP used to access the cloud. When the user logins, IP is checked, if the IP count is less than threshold then it is considered as an anomaly in behavior. If found any anomaly in both the cases, then an extra verification is done to authenticate the user. This is done by security questions which user had entered at the time of creation of profile. If this doesn't match then it is considered as an intruder and an alarm is generated.

3.2 Nids (Network Intrusion Detection System)

NIDS is at the infrastructure layer in cloud IaaS. When a user requests for a VM is allocated at the host, and IP is allocated to it. It is the property of cloud scheduler that VM gets nearby IP addresses therefore the risk of VM compromised is higher.

In general without NIDS, attacker checks for nearby IP address through network probing and find evidence of co-residence. Here co-resident refers to instances that are running on the same physical machine. Once the attacker knows the activated IP, attacker can compromise the VM by sending malicious packets.

In current scenario, proposals are been made to improve NIDS at the VM level i.e., implementing firewalls separately for each VM [14]. But this approach has a drawback that it takes lots of memory and implementing and maintaining firewall at VM level is not simple and there is a great risk that the attacker can destroy the firewall. So, NIDS at the global level is proposed i.e., IDS at the virtual network. This takes less memory, VM maintenance is not required. The benefit of this is the initialization and updation of the firewall rules can be done at any instance of time without making any changes to the VM's.

At the time of creation of VM, firewall rules are updated. User may change his VM firewall but this will not affect global firewall. When a user tries to send malicious packets to any other VM, then the packets are dropped or forwarded based on the NIDS rules. If the user does not have a permission to access other VM then packets are dropped. This restricts the user to access other users VM.

Global updating of firewall is needed because it may possible that user has two machines and he wants communication between the two. Since, firewall which is implemented prevents the user from communication between the VM's. So global updation is required for granting access rights.

When the user requests for a VM, it provides its specification to the server about the VM. This specification is then passed to the server. Converting an existing set of arguments into a guest description using libvirt Domain XML is provided by the virsh domxml and that can then be used by libvirt. This domain XML contains all the VM information like domain name, uuid,memory, vcpu, OS, OS type, OS boot dev, clock offset, on_poweroff, on_reboot, on_crash, devices, disk type etc.

3.2.1 Network Filters

Network filters act as firewall in cloud Infrastructure layer. For creating global filters, a parameterized network filters is created which takes MAC address of VM as an input. Each time VM is created, these filters are implemented in VM using parameters. The interface XML is used to reference a global filter. In the following example, the interface description references the filter clean-traffic:

All filters are implemented based on the MAC address of each VM. At the time of allocation of VM, only MAC address is specified. Internal IP is automatically assigned after creation of VM. Hence each filter is created with reference to MAC address of virtual machine.

<devices>

<interface type='bridge'>

<mac address='00:16:3e:5d:c7:9e'/> <filterref filter='no-icmp-spoofing'>

<parameter name='MAC' value=' 00:16:3e:5d:c7:9e'/>

</filterref> </interface> </devices>

All filters are implemented based on the MAC address of each VM. At the time of allocation of VM, only MAC address is specified. Internal IP is automatically assigned after creation of VM. Hence each filter is created with reference to MAC address of virtual machine.

IV. RESULTS

The results are analyzed with behavior analysis graph and simulation with NIDS and without NIDS. The behavior analysis graph is shown in the Fig. 3.

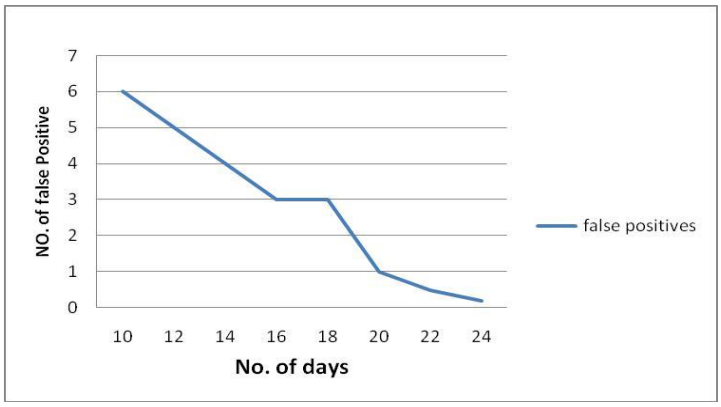

Figure 3. Behavior Analysis Graph

To measure IDS efficiency, we considered accuracy in terms of the system's ability to detect attacks and avoid false alarms. A system is imperfect if it accuses a legitimate action of being malicious. So, we measured accuracy using the number of false positives (legitimate actions marked as attacks) .We started the training with 24 days of simulation. The rate of false alarm in terms of false positive gradually decreased with days.

This is the first phase of our result. Secondly, we did simulation with NIDS and without NIDS. Since after allocation of VM, intruder who wants to hack or compromise other's VM tried to ping his nearby IP to find activated IP. Zenmap tool is used to scan other's IP and sends packets to activated IP in order to compromise other's VM. Through Zenmap tool, attacker finds the activated IP and starts sending packets to the VM of activated IP. Two scenarios is taken into account:

a. One is without NIDS: In this scenario, attacker easily finds activated IP and starts sending packets and compromised VM.

b. Other is with NIDS: In this scenario, 100% loss in packet results and thus intruder doesn't get the activated IP. NIDS inform of network filters will prevent the VM from being compromised.

V. CONCLUSION AND FUTURE WORK

In this paper, two security issues are taken into consideration. First is DoS attack at the server in the form of bogus requests and second is security issue of virtualization i.e., VM compromise attack. A new approach for this issues is introduced which is hybrid IDS, combines both NIDS and HIDS. The future work will be to implement the proposed architecture in a real environment. And also to explore methods by which we can characterize the goals and behavior of intruder, how well a IDS can deal with an attacker who is able to modify the guest operating system kernel and to further increase detection accuracy, how to configure IDS so that no symptoms are missed.

REFERENCES

[1] "Security Guidance for Critical Areas of Focus in Cloud Computing", http://www.cloudsecurityalliance.org/guidance/csaguide.v2.1.pdf, April 2009.

[2] G. Boss, P. Malladi, D. Quan, L. Legregni and H. Hall, Cloud Computing, Version 1.0, 8 October 2007.

[3] M. A. Bamiah and S. N. Brohi, Seven Deadly Threats and Vulnerabilities in Cloud Computing, International Journal Of Advanced Engineering Sciences And Technologies, 9(1), 2011, 087 -090.

[4] B. Grobauer, T. Walloschek, and E. Stocker, Understanding Cloud Computing Vulnerabilities, Security & Privacy, IEEE, 9(2), 2011, 50-57.

[5] S.N. Brohi and M.A. Bamiah, Challenges and Benefits for Adopting the Paradigm of Cloud Computing, International Journal of Advanced Engineering Sciences and Technologies (IJAEST), 8, 2011, 286-290.

[6] N. Gruschka and M. Jensen, Attack Surfaces: Taxonomy for Attacks on Cloud Services, Proc. 3rd IEEE Conf. on Cloud Computing, Miami, Florida, 2010, 276-279.

[7] B.R. Kandukuri, V.R. Paturi and A. Rakshit, Cloud Security Issues, Proc. IEEE Conf. on Services Computing, Bangalore, India, 2009, 517-520.

[8] C.P. Pfleeger and S.L Pfleeger, Security in Computing, Pearson Education, chapter 7. "Security in networks", 2002, 514-520.

[9] S. Subashini and V. Kavitha, A survey on security issues in service delivery models of cloud computing, Journal of Network and Computer Applications, 34, 2011, 1-11.

[10] K. Kajendran, J.J. Jeyaseelan, J.J. Joshi, An approach for secured data storage using cloud computing, International Journal of Computer Trends and Technology, 1(2), 2011, 91-101.

[11] C. Mazzariello, R. Bifulco and R. Canonico, Integrating a Network IDS into an Open Source Cloud Computing Environment, Proc. 6th IEEE Conf. on Information Assurance and Security (IAS) , Atlanta, GA, 2010, 265-270.

[12] K. Hwang and D. Li, Trusted cloud computing with secure resources and data coloring, IEEE Internet Computing, 14(5) 2010, 14-22.

[13] S. Roschke, F. Cheng and C. Meinel, Intrusion Detection in the Cloud, Proc. 8th IEEE Conf. on Dependable, Autonomic and Secure Computing, Chengdu ,China, 2009, 729-734.

[14] S.N. Dhage, B.B. Meshram, Intrusion Detection System in Cloud Computing Environment , International Journal of Cloud Computing, 1(2-3), 2012, 261-282.

[15] M. Laureano, C. Maziero and E. Jamhour, Intrusion Detection in Virtual Machine Environments, Proc. 30th IEEE Conf. on Euromicro Conference, 2004, 520-525.

[16] C.C. Lo, C.C. Huang and J. Ku, A Cooperative Intrusion Detection System Framework for Cloud Computing Networks, Proc. 39th IEEE Conf. on Parallel Processing Workshops, San Diego, CA, 2010, 280-284.

[17] N.K. Sehgal, S. Sohini, Y. Xiong, D. Fritz, W. Mulia and J.M. Acken, A Cross Section of the Issues and Research Activities Related to Both Information Security and Cloud Computing, IETE Technical review, 28(4), 2011, 279-291.

[18] T. Garfinkel and M. Rosenblum, A Virtual Machine Introspection Based Architecture for Intrusion Detection", Proc. of Conf. on Network and Distributed System Security Symposium (NDSS), 3, 2003,191-206.

[19] A. Chonka,Y. Xiang W. Zhou and A. Bonti, Cloud security defense to protect cloud computing against HTTP-DoS and XML- DoS attacks, Journal of Network and Computer Applications, 34(4), 2011, 1097-1107.

[20] T. Ristenpart, E. Tromer, H. Shacham and S. Savage, Hey, You, Get Off of My Cloud: Exploring Information Leakage in Third-Party Compute Clouds, Proc. 16th ACM Conf. on Computer and communications security, Chicago, Illinois, USA, 2009, 199-212.

[21] National Institute of Standards and Technology Special Publication , 800-94 Natl. Inst. Stand. Technol. Spec. Publ. 2007.

[22] M.B. Jadhav, V.J. Gaikwad, C.V. Patil and G.S. Deshpande, Cloud Computing Application in Computational Science, International Journal of Advanced Computer and Mathematical Sciences, 1(1) , 2010, 1-6.

[23] V.K. Reddy, Security Architecture of Cloud Computing, International Journal of Engineering Science and Technology, 3(9).2011.

[24] P. Porras, H. Saidi and V. Yogeswaran, An analysis of conficker's logic and rendezvous points, Technical report, SRI International, March 2009.

[25] D. Jamil et. Al.,"Security issues in cloud computing and countermeasures, International Journal of Engineering Science and Technology (IJEST), 3(4), 2011, 2672-2676.

[26] P. Schoo et al, Challenges for cloud networking security, Proc. Of Conf. In Mobile Networks and Management, 2011, 298-313.

[27] W. Dawoud, I. Takouna and C. Meinel, Infrastructure as a service Security: Challenges and solutions, Proc. 7th IEEE Conf. In Informatics and Systems (INFOS), 2010, 1-8.

[28] www.isecpartners.com

[29] G. Boss, P. Malladi, D. Quan, L. Legregni and H. Hall, Cloud Computing, Version 1.0, 2007.