ISSN 22773061

History Aware Anomaly Based IDS for Cloud IaaS

Punit Gupta[1], Pallavi Kaliyar[2]
[1]Department of Computer Science Engineering, JUIT
Himachal Pradesh, India
punitg07@gmail.com

[2]Department of Computer Science & Engineering
JECRC UDML College of Engineering, Jaipur, India
pallavi.kaliyar@gmail.com

ABSTRACT

Cloud Computing provides different types of services such as SaaS, PaaS, IaaS. Each of them have their own security challenges, but IaaS undertakes all types of challenges viz., network attack ,behaviour based attack, request based attacks i.e handling the requests from untrusted users, XSS (cross site scripting attack), DDOS and many more. These attacks are independent of each other and consequently the QoS provided by cloud is compromised. This paper proposes a History aware Behaviour based IDS (Intrusion Detection System) BIDS. BIDS provides detection of untrusted users, false requests that may lead to spoofing, XSS or DOS attack and many more such attacks. In addition, certain cases where user login or password is compromised. History aware BIDs can be helpful in detecting such attacks and maintaining the QoS provided to the user in cloud IaaS (Infrastructure as a service).

Keywords: Cloud, QoS, Cloud IaaS, IDS, XSS, DDOS attack, Behavior based IDS.

Council for Innovative Research
Peer Review Research Publishing System
Journal: INTERNATIONAL JOURNAL OF COMPUTERS & TECHNOLOGY

Vol 10, No 6.
editor@cirworld.com
www.cirworld.com, member.cirworld.com

ISSN 22773061

I. INTRODUCTION

Cloud environment is best example of Distributed computing, where all types of services are provided to user that may be software or platform based or simply hosting services. With the evolvement of Cloud IaaS, it has also provided the resources in the form of complete platform i.e the resources required by the Operating systems. Cloud IaaS provides the resources to the users as per their demands based on the feasible system configurations. This has significantly improved the resource utilization of servers. With the evolvement of these services, there are threats of new types of attacks, which pose various types of challenges for these varied services .Cloud IaaS service providers inculcate basic security measures at infrastructure level like firewalls, protection from different types of viruses by developing and updating the antivirus software on regular basis as deemed necessary. Virtual Machines installed on top of the Operating Systems also provide security in different ways[2]. However, network attacks, faced by virtual machines at network level, cannot be solved using firewalls or antiviruses. So a check is required at network level using some techniques at globalised network security system at the datacenter level.There are many cloud IaaS frameworks that provide cloud computing services and virtualization services to the user like OpenNode [17], CloudStack [18], CloudSigma [19], Eucalyptus [20], EMOTIVE(Elastic Management of Tasks in Virtualized Environments) and Archive. These take into consideration only network based attacks for cloud infrastructure services.

Many proposals have been made for network security models and systems but they only take into consideration network attacks for example signatures based, packet behavior based and anomaly based. The traditional security systems can be classified into two types IDS (Intrusion detection system) and IPS (Intrusion prevention system). Intrusion detection system (IDS) is a proactive monitoring technology and defensive mechanism in protecting critical IT infrastructures from malicious behaviors [3], which may compromise sensitive data and critical applications through cyber attacks. Intrusion prevention system (IPS) is similar to IDS but IDS is more like an alert system, whereas IPS not only alerts, but also takes the required action by blocking a particular service. These security techniques are no more secure for detection of new type of attacks, such as XSS(cross site scripting attack), DOS, DDoS (Distributed Denial of Service)[1][6] as the security systems mentioned above take into account attacks at network level i.e. at network packet level rather than at request level. This paper deals with: 1) Masquerade attacks: where the threats impersonate the legitimate users, 2) Host-based attacks: these are the consequence of masquerade attacks and generally result in an observable user behavior anomaly [9].

Cloud IaaS provide services in form of virtual machines (VM), which are operating systems or machine independent of each other and can be controlled from remote sites. So there exists a threat of request type i.e. when a user tries to request beyond its limits like a VM with higher configuration or the attacks can be in form of scripting attacks. These problems have been addressed by using different techniques independently which take into consideration only single parameter like tracking the log file [5], tracking the IP of user etc.

A Behavior based IDS is proposed to overcome these problems. BIDS takes into consideration the behavior of user requests and the user activities over the cloud, to track its behavior.

II. RELATED WORK

A. Intrusion Detection System (IDS)

Intrusion detection is the process of monitoring the events occurring in a computer system or network and analyzing them for signs of possible incidents, which are violations or imminent threats of violation of computer security policies, acceptable use policies, or standard security practices [7].

IDS analyze the activity in the system and determine the malicious behavior in the system that may be when there is change in behavior. IDS are generally referred to as network based analyzer which is used to seek the behavior of network packet over network in the system.

IDS can be categorized in following types of technologies [8]:

- Network-Based (NIDS), which monitors network traffic for particular network segments or devices and analyzes the network and application protocol activity to identify suspicious activity.
- Host-Based (HIDS), which monitors the characteristics of a single host and the events occurring within that host for suspicious activity.

In Both type of IDS explained above, the issue that is taken into consideration is the activeness of network packet whether it is used to find anomaly at network using signature or the pattern of network packet but they only take into consideration the behavior of the packet. Such behavior can only detect the network attacks.

Traditional NIDS and HIDS cannot identify suspicious activities in a cloud environment. As an example, a NIDS may not detect an attack sometime when node communication is encrypted. Attacks can also be invisible to HIDS, because they may not leave traces in the node operating system where the IDS resides [9].

Many IDS Models have been proposed for cloud SaaS (Software as a service) and IaaS (Infrastructure as a Service). Shun-fa Yang [9] used Hadoop cloud SaaS platform MapReduction algorithm log file and analyzed it for intrusion detection. Nascimento et al. [10] presented a study of the use of anomaly-based IDS with data from a production environment in SaaS cloud infrastructure. Jun-Ho Lee et al. [11] proposed a method that enables cloud computing system to achieve both

effectiveness of using the system resource. Gustavo [12] has proposed an anomaly based IDS for SaaS. This paper discusses many anomaly based IDS approaches proposed in different domains like in network and grid computing.

Wang et al. [13], proposed a content anomaly detector based in n-gram analysis, which uses bloom filters and offers resistance to mimicry and polymorphic attacks. Robertson et al. [14] use heuristics to infer the class of web-based attacks. It attempts to address the limitations of anomaly-based intrusion detection systems by using both generalization and characterization techniques. By using generalization, a more abstract description of an anomaly can be created which enables one to group similar attacks.

Jun-ho Lee [15] proposed a Multilevel IDS based on log file analysis. This model proposes an authentication scheme for user .In this whenever a user requests for data, first the user is authenticated at datacenter /node level then only data is supplied. This proposal is given for cloud Infrastructure which talks about virtualization and virtual machines. Here the intrusion alerts are divided into low, medium and high

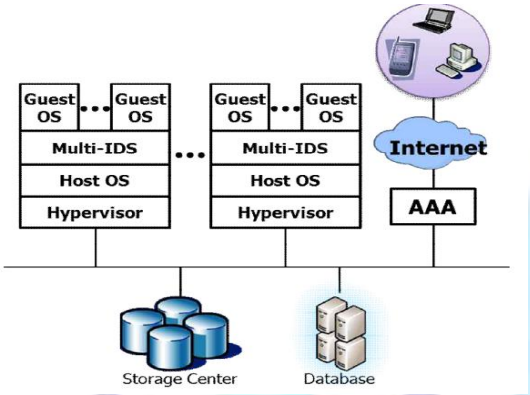

Fig 1: Proposed Multi-level IDS Architecture

Hisham A. Kholidy [16] discusses about various classifications of IDS from various domains that may be mobile computing, grid computing and basic computer network. [16] proposed a Cloud based Intrusion Detection System for cloud platform but the drawback is that it does not take into consideration the behavior based attack at infrastructure level, only taken into consideration network based attacks at infrastructure level have been considered.

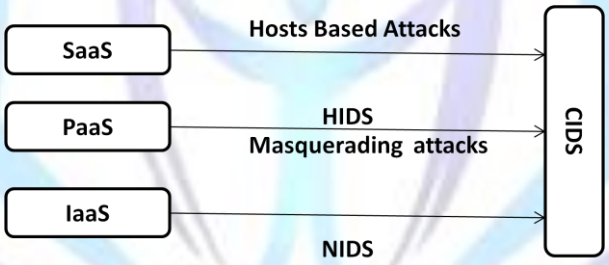

Fig 2: attacks covered by CIDS

III.PROPOSED WORK

A behavior based Intrusion detection system (BIDS) has been proposed, which takes into account multiple parameters to track the behavior and activities of user over the cloud. This proposed model is based on auditing the log files to decide the behavior of user based on the user activities in the past, but these systems are not real time. Whereas the network based intrusion detection system (NIDS) as discussed above are capable of stopping the network based attacks. Basically the network packet signature based attacks and network behavior based attacks are not sufficient to handle all types of attacks because there exist many other types of attacks like DOS attack, DDOS attack and scripting attacks[1][6] and many more. So a behavior based IDS (BIDS) which takes into account both network behavior based attack and anomaly based attacks such as DOS attack has been advanced.

Parameters which are taken into consideration for study of behavior of a user are:

a) IP of user system.
b) Mac address of user system.
c) Browser used by client.
d) Request rate.
e) Request type.
f) Operating system.
g) Network Traffic into the user virtual machine.
h) Network traffic coming out from user virtual machine.
i) Attempt to access unauthorized memory space.
j) Network spoofing using virtual machine.

For each parameter there exists a threshold which is considered to be a limiting factor beyond which the activity of user is considered to be as an intrusion. The above parameters are narrated individually.

a) IP (Internet protocol) of user system.

Taking into consideration the IP of the user from which the user generally accesses the cloud, if it is a registered IP i.e. the IP which the user has previously registered to the cloud controller. If the account is accessed from an IP which is not registered, then it is considered as an intrusion. And accordingly an alert is generated to both the user and the cloud administrator.

b) Mac address of user system.

Taking into consideration the Mac-Id of the user from which the user generally accesses the cloud, if it is a registered address i.e. the Id which the user has previously registered to the cloud controller. If the account is accessed from a Mac-Id which is not registered, then it is considered as an intrusion. And accordingly an alert is generated to both the user and the cloud administrator.

c) Browser used by client.

Taking into consideration the browser used by user to access cloud platform, a count is maintained to analyze and get the most frequent browsers used by the user. If a user account is accessed by a browser whose count is below the threshold value, then it is considered as an intrusion. In this way, when a new account is started all the browser counts are initialized with default value. So that alert is not generated in the first user account access.

d) Request rate.

The number of requests sent by user in a specified time is referred to as request rate .If the number of requests submitted by user is large, then that may lead to denial of service to other users. So request rate is very important parameter for cloud controller, so as to keep resources available to all the users. To manage the above situations, this count is maintained which restricts the user to a certain defined number of requests. If the number of requests submitted by the user exceeds the request rate threshold, then it is considered as intrusion. This helps to detect DOS attacks at request level.

e) Request type.

Here the track of user requests is taken into account. In cloud IaaS (Infrastructure as a Service), request is for allocation of a machine which has a user specific configuration. Requests are in the form of XML files. So there is a chance of cross site scripting attack by modifying the request attributes. These attacks modify the request configuration. So to overcome this, each user is allotted a threshold for request parameters. Users are divided into two categories free user and a premium user. Free user can only request for restricted VM (Virtual Machine) configuration of restricted RAM, Memory, CPU and MIPS. Whereas the premium user also do have restricted request parameters, but somewhat higher than a free users. Whenever a request is received from a free user with unwanted request parameter, it is considered as intrusion, similarly for premium user as well.

f) Operating system.

Here the operating system used by user to access the cloud system is tracked, as a user behavior. Here a count for each operating system type i.e. Windows, Macintosh and Linux. If the user uses a specific OS (operating system) then the count of that OS will be higher. If there is an access from different OS, it is considered as an intrusion if the value for that OS parameter is less than threshold.

g) Network Traffic into the user virtual machine.

This is most important parameter for detection of network based intrusion. In this, the traffic moving inside the VM is tracked, if it exceeds beyond a threshold value, then it is considered as intrusion.

h) Network traffic coming out from user virtual machine.

This is the most important parameter for detection of network based intrusion. In this, the traffic moving outside the VM is tracked, if it exceeds beyond a threshold value it is considered as intrusion. Since this can be the indication of intrusion in terms of overloading the network.

i) Attempt to access unauthorized memory space.

This is the case when a user tries to access the memory beyond the space allocated to a VM. This can be explained by an example that if a server has 200GB of memory and 100GB is allocated to VM. When the user tries to access the memory space beyond the allocated space i.e. 100GB, it is treated as intrusion.

j) Network spoofing using virtual machine.

The packets moving outside the user VM are tracked and if the user tries to ping or send packet to any other VM, IP or MAC addresses, it is considered as intrusion i.e., Network spoofing, unless there are permissions to send packets to specific destination .

In proposed system we also take into consideration the time of last intrusion, if the time for a specific intrusion type is beyond threshold of time. Then particular intrusion previous record is reset. On the other hand if the similar attack is done again and again frequently then user network connection and requests are suspended for a particular interval of time.

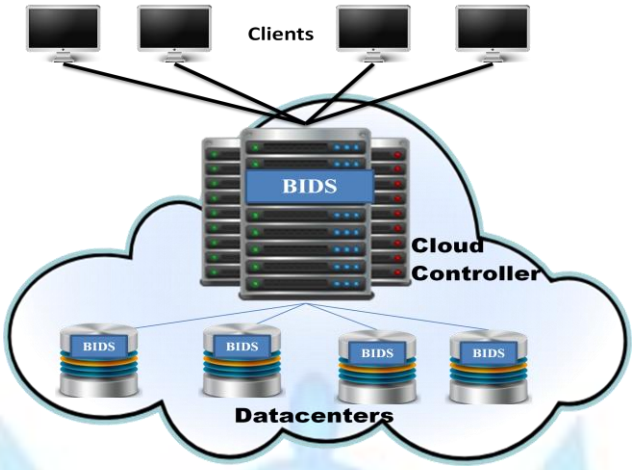

Fig 3: BIDS model

Fig. 3 shows the design and location of BIDS in cloud architecture. In above shown model, BIDS is located at two levels; one at cloud controller to detect behavior based attacks and the second at nodes or datacenter level are used for network level attacks

IV. EXPERIMENTAL RESULTS

For testing the performance of the proposed Behavior based IDS, the implementation is done on cloud IaaS environment using 'Qemu' [10] and 'Libvirt' [21][22][23] library as driver to control and interact with Qemu . This is tested with 6 datacenters, 200 and 300 user requests. For comparison, Network based IDS is used. This framework is tested first with NIDS and then with proposed behavior based IDS. Testing is done with both network based attacks like spoofing; increasing the traffic in both the direction. Behavior based attacks are tested with DOS, scripting attack and many more.

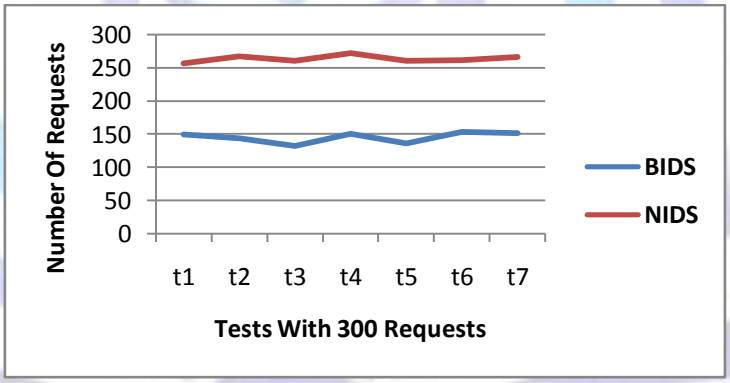

Fig 4 :Comparison of number of attacks captured

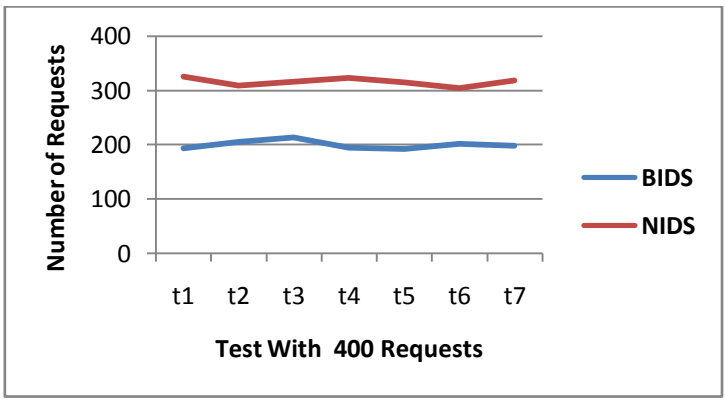

Fig 5 :Comparison of number of attacks captured for 400 requets

Since the above mentioned NIDS is not able to detect DOS, scripting attacks and other request attacks, but Behavior based IDS is capable of dealing with all such attacks. Comparing Intrusion detection systems using 300 and 200 requests on a network using 5 datacenters. For above given scenario many network based and behavior based attacks are generated randomly, and then BIDS is tested over this scenario. Fig 4 shows the tests t1-t7 over the same setup.

V. CONCLUSION

In this paper different type of attacks, IDS models have been discussed with their characteristics and drawbacks. To overcome the drawbacks, a Behavior based IDS is proposed which performs better than other previously proposed models in terms of security provided to the user from different attacks. For future work proposed IDS may be merged with other models and observations be made regarding further improvement in the security.

REFERENCES

[1] Roschke, S. ; Feng Cheng ; Meinel, C," Intrusion Detection in the Cloud", Autonomic and Secure Computing, 2009. DASC '09. E ,pp: 729-734.

[2] Amazon Web Services, "Risk and Compliance," 2012.

[3] M.N. Doan and H. Eui-Nam, "A Collaborative Intrusion Detection System Framework for Cloud Computing", Lecture Notes in Electrical Engineering, Vol. 120, Part 2, pp. 91-109,2012.

[4] Ashley Chonka , Yang Xiang, , Wanlei Zhou , Alessio Bonti,"Cloud security defence to protect cloud computing against HTTP-DoS and XML-DoS attacks

[5] Sathya, G. ; Vasanthraj., K "Network activity classification schema in IDS and log audit for cloud computing",Information Communication and Embedded Systems (ICICES), 2013,PP:502-506.

[6] Roberto Di Pietro and Luigi V. Mancini, Intrusion Detection Systems, Springer, Jan. 2008.

[7] Security Guidance for Critical Areas of Focus in Cloud Computing V2.1by Cloud Security Alliance 2009 https://cloudsecurityalliance.org.

[8] Saad, E.N. ; Mahdi, K.E. ; Zbakh, M."Cloud computing architectures based IDS",Complex Systems (ICCS), 2012,PP:1-6.

[9] Shun-Fa Yang, Wei-Yu Chen, and Yao-Tsung Wang, "ICAS: An inter-VM IDS Log Cloud Analysis System," Proc. Cloud Computing and Intelligence Systems (CCIS), IEEE Press, Sep. 2011, pp. 285-289,

[10] Jun-Ho Lee, Min-Woo Park, Jung-Ho Eom, and Tai-Myoung Chung,"Multi-level Intrusion Detection System and log management in Cloud Computing," Proc. Advanced Communication Technology (ICACT), IEEE Press, Feb. 2011, pp. 552-555.

[11] Nascimento, G., and Correia, M., "Anomaly-based intrusion detection in software as a service," Proc. Dependable Systems and Networks Workshops (DSN-W), IEEE Press, Jun. 2011, pp. 19-24.

[12] Nascimento, G. ; Correia, M,"Anomaly-based intrusion detection in software as a service",Dependable Systems and Networks Workshops (DSN-W), 2011,PP:19-24.

[13] K. Wang, J. Parekh, and S. Stolfo. Anagram: A content anomaly detector resistant to mimicry attack. In Proceedings of the 9th International Conference on Recent Advances in Intrusion Detection, pages 226–248. Springer, 2006.

[14] W. Robertson, G. Vigna, C. Kruegel, R.A. Kemmerer, et al.Using generalization and characterization techniques in the anomaly-based detection of web attacks. In Proceedings of the 13th Symposium on Network and Distributed System Security,February 2006.

[15] Jun-Ho Lee ; Min-Woo Park ; Jung-Ho Eom ; Tai-Myoung Chung,"Multi-level Intrusion Detection System and log management in Cloud Computing" Advanced Communication Technology (ICACT), 2011,PP:552-555.

[16] Kholidy, H.A. ; Baiardi, F."CIDS: A Framework for Intrusion Detection in Cloud Systems".Information Technology: New Generations (ITNG), 2012,PP:379-385.

[17] OpenNode .www.opennodecloud.com

[18] CloudStack. www.cloudstack.org

[19] CloudSigma. www.cloudsigma.com

[20] Eucalyptus Public Cloud. http://open.eucalyptus.com.

[21] Daniel Nurmi, Rich Wolski, ChrisGrzegorczyk, Graziano Obertelli,Sunil Soman, Lamia Youseff, Dmitrii Zagorodnov," The Eucalyptus Open-source Cloud-computing System",In Proceedings of Cloud Computing and Its Applications,chicago,Illinois.

[22] libvirt virtualization API. http://www.libvirt.org.

[23] OpenNebula Open Source Toolkit for Cloud Computing. http://opennebula.org.