Indian Journal of Science and Technology, *Vol 9(22), DOI: 10.17485/ijst/2016/v9i22/95170, June 2016*
ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645

Integrated Intrusion Detection Approach for Cloud Computing

C. Ambikavathi[1]* and S. K. Srivatsa[2]

[1]Sathyabama University, Chennai, Tamil Nadu, India; ambikavathi@yahoo.co.in
[2]Prathyusha Institute of Technology and Management, Chennai, Tamil Nadu, India; profsks@rediffmail.com

Abstract

Objectives: Intrusion Detection System (IDS) models and methods are integrated for better detection of intruders and mitigation of false alarms. Integrated IDS is proposed to provide security in a cloud environment. **Methods:** The distributed and dynamic nature built-in of cloud environment leads to critical issues like huge log analysis, heterogeneous traffic aggregation and scalability, etc. Intrusion specific data classification and false alarms degrades performance. This integrated model integrates both IDS models and IDS methodologies. Host-based IDS (H-IDS) model integrates with network-based IDS (N-IDS) model, as well as signature and anomaly based IDS methods are integrated to get the best of each. **Findings:** Whenever a Virtual Machine (VM) is created, H-IDS is in-built into its operating system to monitor the activities within that VM. N-IDS is deployed at strategic locations within the cloud network to monitor the traffic between the virtual machines and from the outside environment. Any malicious activity initiated by a cloud user using their virtual machine is detected by H-IDS. The packets flowing through the cloud network are captured and analyzed by N-IDS to detect infected packets send by hackers. The weakness of one methodology is compromised by the other during integration, but if the methods are used separately they are ineffective. Known attacks can be detected by signature based IDS and the new/unknown attack patterns are identified by anomaly based IDS. The major drawback of anomaly based IDS is high false alarm rate. It can be overcome by signature based IDS. This proposed work is implemented using Opennebula, for constructing a cloud environment and tested with IDS tools. **Improvements:** This integration leads to improve cloud security and trust among consumers. IDS specific issues are also rectified such as false alarms, heterogeneity etc.

Keywords: Anomaly Based Detection, Cloud Computing, Intrusion Detection System, Signature Based Detection, Virtualization

1. Introduction

Cloud computing is defined by various standards. Amongst NIST[1] defines it, as a model for enabling convenient usage for consumers, provides access to a shared pool of configurable computing resources on demand through network which are rapidly provisioned and released with less management effort or service provider interaction. The cloud model is composed of three service models, four deployment models and five essential characteristics. The three service models are Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS). The four deployment models are private cloud, public cloud, hybrid cloud and community cloud. The five essential characteristics of cloud are on-demand self-service, broad network access, resource pooling, rapid elasticity and measured service. Cloud computing model is a Service Oriented Architecture (SOA). Cloud services are cheap and convenient as organizations need only to pay for the services they use. This convenient feature is rendered by means of virtualization. Demanded resources are virtually created from a physical infrastructure and rendered. However the widespread use of virtualization in implementing cloud infrastructure brings unique security concerns of customers or tenants of a public cloud service and for the service provider. The security concerns may be initiated from cloud users, insiders or hackers from the outside world. Unlike traditional attacks, a

*Author for correspondence

single attack can be penetrated as distributed attacks in the cloud network. False positives and false negatives are uncontrollable because of this unpredictable cloud environment. So suitable IDS models or methods should be selected for cloud computing.

2. IDS for Securing Cloud

Among various security tools, IDS can play a vital role in the security of cloud computing environment. Hifaa Bait Baraka and Huaglory Tianfield[2] have already validated intrusion detection system in detecting DDoS attack against the virtualized environment. A real world cloud IDS called Threat Manager, a product of Alert Logic[3] is used by Amazon Web Services. Cloud Security Report[4] 2014 of Alert Logic indicates that the threats in the cloud are growing in two dimensions: While the total number of attacks are increasing, historic attacks directed at on-premises environments are now targeting the cloud. So that the security measures taken in on-premises environments should be moved to the cloud. However the security measures taken must be adaptable to a cloud environment. As mentioned by Donadio[5] that any network security and reliability is a well defined process not a product, the process of securing the cloud environment has to be well defined by rectifying the issues of traditional IDS and cloud specific issues. Integrating both IDS models (H-IDS and N-IDS) and the IDS methods (SD and AD) can be a well defined process for cloud security. A better IDS must be capable of recognizing the origin of the anomalies before initiating detection process. To detect both known and unknown attacks, both supervised and unsupervised methods should be exploited at different layers of cloud computing. Also performance must be evaluated qualitatively and quantitatively. Cloud traffic aggregation and data classification are the key points of developing an IDS appropriate for the cloud computing model. Generally, data classification algorithms such as naive Bayes, k means, clustering are used to classify the intrusion specific data from the whole traffic and log information.

2.1 Problem Statement and Related Work

Integrated intrusion detection is a process of integrating both IDS models and methods to accurately identify intruders with less false alarms and make IDS as a valuable tool for cloud security. The dynamic and distributed nature of cloud leads to several problems for cloud IDS such as to analyze huge log files, to aggregate heterogeneous traffic and to correlate complex events. Defending intruders in a cloud environment differ in the aspects of virtualized resources and dynamic change from other networking models. Virtualization which is the base of cloud computing, leads to various loopholes. Large volume of VM logs has to be analyzed for detecting intrusions. Various applications and different types of Operating Systems (OS) are deployed which leads to heterogeneous traffic in the virtual network. Virtual machine security is essential in a cloud environment, and is obtained by H-IDS to detect the attacks initiated by cloud users. N-IDS contributes to detect outside hackers. This paper also addresses the two shortcomings of the traditional IDS: IDS cannot reason across multiple attacks; it does not consider the uncertainties in the parameter representation. By means of integrating IDS models and methods an adaptable cloud IDS is gained.

Integrated IDS models proposed by some authors have been discussed in the section. Virtual IDS (V-IDS)[5] presents a novel architecture for protecting cloud using IDS by combining the basic principles of cloud computing, virtualization, and the Generalized Multiprotocol Label Switching (GMPLS) control plane. The V-IDS architecture includes five modules which are monitoring, analysis, decisions, actions, and management. Monitoring and management modules are done by opennebula whereas other three modules are implemented by GMPLS. Grid and Cloud Computing Intrusion Detection System (GCCIDS)[6] integrates knowledge and behavior based analysis to detect specific intrusions. However, GCCIDS is not able to discover new types of attacks or create an attack database which must be considered for implementing IDS. Another integrated intrusion detection approach, called FCANN[7] is proposed based on Artificial Neural Networks (ANN) and Fuzzy Clustering (FC). Through fuzzy clustering technique, the heterogeneous training set is divided into several homogenous subsets and ANN learning algorithm is applied to each subset. Thus the complexity of each sub training set is reduced and consequently the detection performance is increased. Collaborative IDS[8] works as follows: H-IDSs and N-IDSs cooperately detects intrusion at the host and network levels. Both IDS types are equipped with signature and anomaly based detectors. This approach enhance the detection accuracy in both known and unknown attacks. The cooperative agent and central coordinator form a collaborative system in this approach. A framework for

integrating Network Intrusion Detection System (NIDS) in the Cloud[9] is proposed, in which the NIDS module consists of Snort and signature apriori algorithm. An Automatic intrusion diagnosis system[10] has proposed to combine supervised and unsupervised anomaly detection methods for intrusion diagnosis. However the dataset used do not contain virtual machine specific exploits. A hybrid intrusion detection system[11] combines decision table with naïve Bayes data mining techniques and proves with a detection rate of 97%.

As the lessons learnt from the above related works, here it is proposed to build an integrated IDS. However, our approach is also apprehensive by the efforts taken for data collection, classification and rules updating in the heterogeneous cloud environment.

3. Materials and Methods

An integrated intrusion detection approach is established by means of integrating H-IDS with N-IDS, each equipped with both SD and AD methods as shown in Figure 1. This integration is fruitful to cloud environment in the way that each VM is monitored by H-IDS for internal attacks and the cloud network is monitored by N-IDS for external attacks. Along with detection accuracy is improved by the combination of SD and AD methods.

The overview structure of the proposed architecture is shown in Figure 2. Each VM is built-in with OSSEC H-IDS to monitor user activities by analyzing shell commands and tracing system calls made by cloud user. OS auditing mechanisms of OSSEC audit the events generated by the virtual machine. It uses both anomaly based and signature based techniques. It also checks the execution of system programs, network usage, memory usage and processor usage by the VM to detect intrusion. N-IDS is located at the entry point of the cloud environment. It uses two N-IDS tools that are Bro-IDS for anomaly detection and Snort for signature-based detection. Using both detection methods (SD and AD) enhances intrusion detection accuracy and reduces response time. N-IDS can reduce false alarms in the cloud environment by using two detection techniques which complement each other. A central coordinator module is deployed in the hypervisor for effective solution. Central coordinator is needed in order to aggregate the results such as events, attacks and alerts from both H-IDS and N-IDS. This aggregated report is used for updating the rules set for signature based detection, as Carl Endorf [12] et.al. has signified that rule based IDS analyzes elements to identify attacks, derived from the observations such as signatures, irregularities in protocol behavior, unusual system events, changes in files or directories and so on. Also the aggregated report can be used for alert correlation. Event or attack correlation is a tedious task in a complex cloud environment. Attack graph is used for alert correlation[13]. A Security event correlation approach[14] is proposed where complex event processing is done by preprocessing, filtering and diagnosing. However event or alert correlation is out of scope of this research and may be considered as further updating.

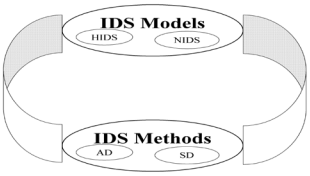

Figure 1. Integration of IDS models and methods.

3.1 Implementation and Tools Used

This proposed work is implemented using Opennebula, for constructing a cloud environment and tested with IDS tools such as SNORT and BRO-IDS for N-IDS and OSSEC for H-IDS.

3.1.1 OpenNebula

OpenNebula[15] is chosen for constructing a cloud computing platform because of it's simplicity, openness, reliability and flexibility. This platform manages a data center's virtual infrastructure to build private, public and hybrid clouds of IaaS.

3.1.2 Snort

Snort[16] is an open source signature based N-IDS. It does real-time traffic analysis and packet logging on the installed network. It performs protocol analysis, content

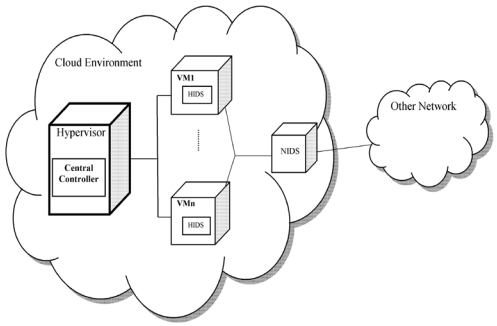

Figure 2. Overview structure of proposed architecture.

searching and matching process. It can also be used to detect probes or attacks and stealthy port scans. It can be configured to work in three modes: sniffer mode, packet logger mode, and network intrusion detection mode. Sniffer mode is used to capture network packets and display them on the console. Packet logger mode is to record packets to the disk. In intrusion detection mode, it will monitor and analyze the network traffic and analyze it against a rule set defined by the user. Action will be taken based on what has been identified. Here Snort is installed in an intrusion detection mode. New rules are updated in the snort knowledge base while new attacks detected.

3.1.3 BRO-IDS

Bro-IDS[17] is an open source anomaly based N-IDS. Its technology is especially effective at traffic analysis, and is often used in forensics and related usecases. Here it is employed in conjunction with snort, as they two complement each other quite nicely.

3.1.4 OSSEC

OSSEC[18] is an Open Source H-IDS that functions using both SD and AD. It performs log analysis, file integrity checking, policy monitoring, rootkit detection, real-time alerting and active response. Here it is deployed in each VM during creation of VM.

4. Results and Discussion

A cloud environment is established by creating ten VMs(2 redhat, 3 Ubuntu, 3 ttylinux, 2 windows machines) using Opennebula as shown in Figure 3. OSSEC is attached as a disk block to each VM which acts as H-IDS. A VM is instantiated with Ubuntu OS to act as N-IDS, with a snort and Bro-IDS installed, used for signature based and anomaly based detection respectively. This VM monitors the flow of packets within the cloud network. The alarms and reports generated by N-IDS (Snort and Bro-IDS) and H-IDS (OSSEC) are collected by the central coordinator located in hypervisor. This combined report is used for further updation of rules for signature based detection. An architecture proposed by S.N Dhage[19] uses a separate instance of IDS for each VM and uses a separate controller to manage all the IDS instances. Signature and learning based method are combined for detection, which takes care only VMs. Here N-IDS is added for detecting external attacks.

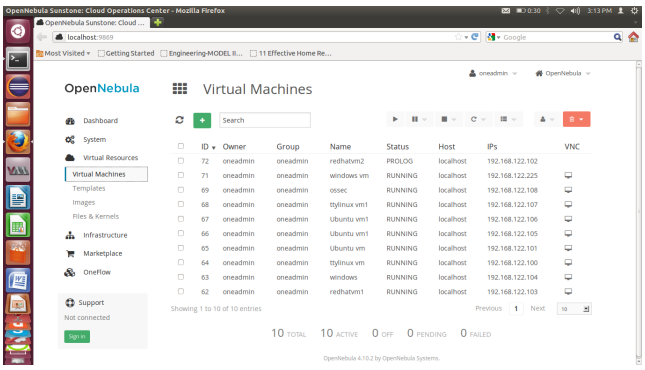

Figure 3. Cloud environment setup.

5. Conclusion and Future work

IDS can play a vital role in cloud security. A secured cloud environment can be gained by this integrated IDS approach. Integration leads to attaining the best of each model and method that is appropriate for cloud environment. The IDS models H-IDS and N-IDS are integrated to monitor the attacks initiated internally and externally with both SD and AD detection methods. As well as in signature based detection method, the rules/signatures are automatically updated using aggregated report generated by central coordinator. Thus the security of complex cloud environment has been gained by integrating both IDS models (H-IDS and N-IDS) and IDS methods (SD and AD). In future this integrated IDS can be enhanced by improving the ruleset appropriate for cloud computing.

6. References

1. The NIST definition of cloud computing. http://dx.doi.org/10.6028/NIST.SP.800–145.
2. Hifaa BB, Huaglory T. Intrusion detection system for cloud environment. 7th International Conference on Security of Information and Networks (SIN'14). Sep 2014. 9–11.
3. Alert Logic Threat Manager with Activewatch. https://www.alertlogic.com/.
4. Rahul B, Maureen R, Sheridan S. Alert logic cloud security report - research on the evolving state of cloud security. Spring 2014.
5. Pasquale D. Virtual intrusion detection systems in the cloud. Bell Labs Technical Journal 17(3), Alcatel-Lucent. DOI: 10.1002/bltj.21562. 2012. p. 113–128.
6. Vieira K, Schulter A, Westphall CB, Westphall CM. Intrusion detection for grid and cloud computing. IT Professional. 2010; 12(4):38–43.

7. Swati R, Rajesh D, Komal R. Intrusion detection system for cloud network using FC-ANN algorithm. Int. Journal of Advanced Research in Computer and Communication Engineering. Apr 2013; 2(4):1818–22.
8. Zhiyuan T, Upasana TN, Xiangjian He, Priyadarsi N, Ren PL, Song W et al. Enhancing big data security with collaborative intrusion detection. IEEE Cloud Computing. Sep 2014; 1(3):27–33.
9. Chirag N. Modia, Dhiren RP, Avi P, Muttukrishnan R. Integrating signature apriori based Network Intrusion Detection System (NIDS) in cloud computing. 2nd International Conference on Communication, Computing and Security (ICCCS-2012); 905–12.
10. Junaid A, Paul T. Jie X. An automatic intrusion diagnosis approach for clouds. International Journal of Automation and Computing. Aug 2011. p. 286–96.
11. Chandrashekar A, Vijay KJ. Data mining based hybrid intrusion detection system. Indian Journal of Science and Technology. Jan 2014; 7(6). Doi no: 10.17485/ijst/2014/v7i6/37551.
12. Carl E, Eugene S, Jim M. The book intrusion detection and prevention. The future of intrusion detection and prevention.
13. Chun-Jen C, Pankaj K, Tianyi XJL, Dijiang H. NICE: Network intrusion detection and countermeasure selection in virtual network systems. IEEE Transactions On Dependable And Secure Computing. July/August 2013; 10(4):198–211.
14. Massimo F. Security event correlation approach for cloud computing. Int. Journal of High Performance Computing and Networking. Jan 2013; 7(3):173–85.
15. OpenNebula. http://www.opennebula.org.
16. Snort. Available from: https://www.snort.org
17. Bro-IDS. Available from: https://www.bro.org
18. OSSEC. Available from: www.ossec.net/.
19. Sudhir ND, Meshram BB. Intrusion detection system in cloud computing environment. International Journal of Cloud Computing 2012; 1(2/3):261–82.