International Journal of Emerging Trends & Technology in Computer Science (IJETTCS)
Web Site: www.ijettcs.org Email: editor@ijettcs.org
Volume 4, Issue 6, November - December 2015 ISSN 2278-6856

Cloud security through Intrusion Detection System (IDS): Review of Existing Solutions

Yakuta Tayyebi [1] and Dr D. S. Bhilare [2]

[1]ILVA Commerce & Science College Indore,

[2]Head IT Centre SCSIT DAVV Indore,

Abstract

Cloud computing is a new and emerging information technology that is changing the way IT services are providing solutions. Cloud security was revealed as the top most challenge of cloud computing [5]. Security risks associated with each cloud service model hinders its widespread adoption. This paper is a survey of different intrusions affecting availability, confidentiality and integrity of Cloud resources and services. It examines proposals incorporating Intrusion Detection Systems (IDS) in Cloud and discusses various types and techniques of IDS and Intrusion Prevention Systems (IPS), and recommends IDS/IPS positioning in Cloud architecture to achieve higher security.

Keywords: Cloud Computing, Cloud Security, IDS, IPS HIDS, NIDS.

1. INTRODUCTION

Cloud computing environment provide convenient, on-demand, network access to a shared pool of configurable computing resources such as networks, servers, storage, applications and services. Cloud computing is targeted to provide better utilization of resources using virtualization techniques and to take up much of the work load from the client. Gartner defined Cloud computing as "A style of computing where scalable and elastic IT capabilities are provided as a service to multiple external customers using Internet technologies." Cloud infrastructure makes use of virtualization techniques, integrated technologies and runs through standard Internet protocols. These vulnerabilities in cloud computing environment attract intruders and make security of Cloud services a key issue to be considered.

Firewall protects the front access points of system and is treated as the first line of defense. Firewalls are used to deny or allow protocols, ports or IP addresses. It diverts incoming traffic according to predefined policy. As firewalls sniff the network packets at the boundary of a network, insider attacks cannot be detected by traditional firewalls. Few DoS or DDoS attacks are also too complex to detect using traditional firewalls. Firewall can be a good option to prevent outside attacks but does not work for insider attacks.

Efficient intrusion detection systems (IDS) and intrusion prevention systems (IPS) should be incorporated in Cloud infrastructure to mitigate insider attacks. The efficiency of IDS/IPS depends on parameters like technique used in IDS, its positioning within network, its configuration etc.

Rest of the paper is organized as follows. Section II discusses basic components of IDPS and Intrusion detection techniques are covered in Section III. Section IV, presents various techniques for IDS/IPS. Section V concludes with references at the end.

2. BASIC COMPONENTS OF IDPS

Intrusion detection systems are a hardware or software system that continuously monitors the events occurring in a computer system or network, analyzing them for malicious activities or policy violations. IDPS typically consist of three subsystems or components:

- **Data Pre-processor**: It is responsible for collecting and providing the audit data in a specific format to the next component (analyzer) to make decision. This data is referred as audit log.
- **Analyzer (Intrusion Detector**): It is the core component which analyzes the audit log to detect attack. Various pattern matching, machine learning, data mining and statistical techniques can be used as intrusion detectors. The capability of the analyzer to detect attack often determines the strength of the overall system.
- **Response Engine:** The response engine is responsible for controlling the reaction mechanism and determine how to response when an attack is detected. The action depends upon the predefined security policies.

3 INTRUSION DETECTION TECHNIQUES

3.1 Signature Detection (SD)

Signature based intrusion detection works on defined set of rules or signatures or predefined knowledge base that can be used to decide that a given pattern is that of an intruder. As a result, signature based systems are capable of attaining high levels of accuracy and minimal number of false positives. It is an efficient solution for detecting known attacks but fails to detect unknown attacks or variation of known attacks. One of the motivating reasons to use signature based detection is its easy in maintaining and updating preconfigured rules. These signatures are composed by several elements that identify the traffic. In Cloud, signature based intrusion detection technique can be used to detect known attack. It can be used either at front end of Cloud to detect external intrusions or at back end of Cloud to detect external/internal intrusions. Like

traditional network, it cannot be used to detect unknown attacks in Cloud.

3.2 Anomaly Detection (AD)

Anomaly (or behavioural) detection technique is concerned with identifying events that appear to be anomalous with respect to normal system behaviour. It involves the collection of data relating to the behaviour of legitimate users over a period of time, and then applies statistical tests to the observed behaviour, which determines whether that behaviour is legitimate or not. It has the advantage of detecting attacks which have not been found previously. A wide variety of techniques including data mining and statistical modelling have been explored as different ways to approach the anomaly detection problem. The key element for using this approach efficiently is to generate rules in such a way that it can lower the false alarm rate for unknown as well as known attacks. In Cloud, large numbers of events (network level or system level) occur, which makes it difficult to monitor or control them using anomaly detection technique.

3.3.Soft Computing based detection

The ability of soft computing techniques to deal with uncertain and partially true data makes them attractive to be applied in intrusion detection. There are many soft computing techniques such as Artificial Neural Network (ANN), Fuzzy logic, Association rule mining etc used to improve detection accuracy and efficiency of signature or anomaly detection based IDS.

The goal of using ANNs for intrusion detection is to be able to generalize data from incomplete data and to be able to classify data as being normal or intrusive. The types of ANN used in IDS are as follows: Multi-Layer Feed- Forward (MLFF) neural nets, Multi-Layer Perceptron (MLP) and Back Propagation (BP). ANN based IDS is an efficient solution for unstructured network data. The intrusion detection accuracy of this approach is based on number of hidden layers and training phase of ANN. However, it requires more training samples and time for effective learning of ANN. Use of only ANN based IDS cannot be an efficient solution to detect intrusions for Cloud as it requires quick intrusion detection mechanism[2].

Fuzzy logic can be used to deal with inexact description of intrusions. It provides some flexibility to the uncertain problem of intrusion detection. To reduce training time of ANN, fuzzy logic with ANN can be used for fast detection of unknown attacks in Cloud. In Cloud, association rules can be used to generate new signatures. Using newly generated signatures, variations of known attacks can be detected in real time [2].

It is advantageous to use soft computing techniques on traditional IDS for Cloud environment. However, each technique has some advantages and limitations, which affect the performance of IDS. Hybrid techniques use the combination two or more of above techniques. It is advantageous since each technique has some advantages and drawbacks.

4 VARIOUS TYPES OF IDS USED IN CLOUD COMPUTING

There are mainly four types of IDS used in Cloud: Host based intrusion detection system (HIDS), Network based intrusion detection system (NIDS), Hypervisor based intrusion detection system and Distributed intrusion detection system (DIDS).

4.1 HIDS: A host-based intrusion detection system (HIDS) is an intrusion detection system that monitors and analyzes the information collected from a specific host machine. HIDS running on a host machine detects intrusion for the machine by collecting information such as file system used, network events, system calls etc. HIDS observes modification in host kernel, host file system and behaviour of the program. Upon detection of deviation from expected behaviour, it reports the existence of attack. The efficiency of HIDS depends on chosen system characteristics to monitor. Each HIDS detects intrusion for the machines in which it is placed. With respect to Cloud computing, HIDS can be placed on a host machine, VM or hypervisor to detect intrusive behavior through monitoring and analyzing log file, security access control policies, and user login information. If installed on VM, HIDS should be monitored by Cloud user whereas in case of installing it on Hypervisor, Cloud provider should monitor it.

4.2 NIDS: A Network based Intrusion Detection System (NIDS) is an intrusion detection system that tries to detect malicious activity such as DoS attacks, port scans or even attempts to crack into computers by monitoring network traffic. The information collected from network is compared with known attacks for intrusion detection. NIDS has stronger detection mechanism to detect network intruders by comparing current behaviour with already observed behaviour in real time. NIDS mostly monitors IP and transport layer headers of individual packet and detects intrusion activity. NIDS uses signature based and anomaly based intrusion detection techniques. NIDS has very limited visibility inside the host machines. If the network traffic is encrypted, there is really no effective way for the NIDS to decrypt the traffic for analysis. NIDS can be deployed on Cloud server interacting with external network, for detecting network attacks on the VMs and hypervisor. However, it has several limitations. It cannot help when it comes to attack within a virtual network that runs entirely inside the hypervisor. In Cloud environment, installing NIDS is the responsibility of Cloud provider.

4.3 DIDS: A Distributed IDS (DIDS) consists of several IDS (E.g. HIDS, NIDS etc.) over a large network, all of which communicate with each other, or with a central server that enables network monitoring. The intrusion detection components collect the system information and convert it into a standardized form to be passed to central analyzer. Central analyzer is machine that aggregates

information from multiple IDS and analyzes the same. Combination of anomaly and signature based detection approaches are used for the analysis purpose. DIDS can be used for detecting known and unknown attacks since it takes advantages of both the NIDS and HIDS, which are complement of each other. In Cloud environment, DIDS can be placed at host machine or at the processing server in backend [6].

4.4 Hypervisor-based IDS: A Hypervisor-based intrusion detection system is an intrusion detection system specifically designed for hypervisors. Hypervisor is a platform to run VMs. Running at hypervisor layer, this type of IDS allows user to monitor and analyze communications between VMs, between hypervisor and VM and within the hypervisor based virtual network. Availability of information is one of the benefits of hypervisor based IDS. Hypervisor based IDS is one of the important techniques, specifically in Cloud computing, to detect intrusion in virtual environment [8].

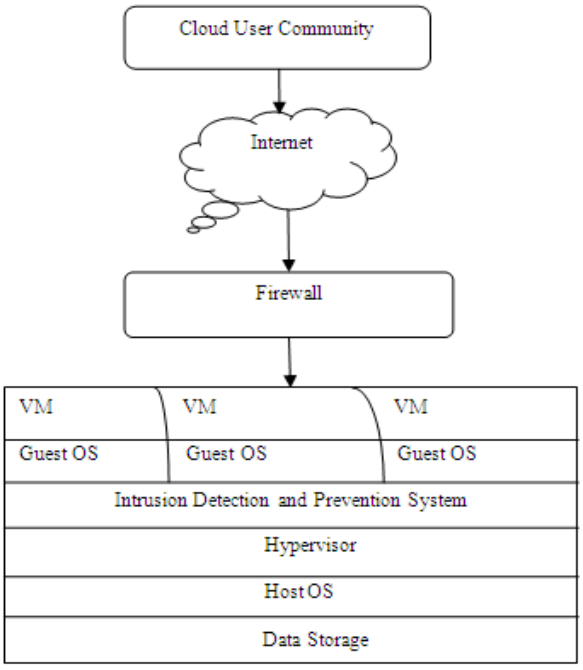

Figure 1 Architecture of Cloud Environment with IDPS

5 CONCLUSIONS

This paper, discussed several intrusions which can threat integrity, confidentiality and availability of Cloud services in the future. One of the existing solutions viz. firewall may not be sufficient to solve Cloud security issues. The paper emphasized the usage of alternative options to incorporate intrusion detection or intrusion prevention techniques into Cloud and explored locations in Cloud where IDS/IPS can be positioned for efficient detection and prevention of intrusion. Recent research findings incorporating IDS/IPS specifically in Cloud have been discussed and their advantages and disadvantages have been highlighted. The adaptation of soft computing techniques in IDS/IPS can optimistically improve the security.

References

[1] A. Bakshi and Y. Dujodwala, "Securing cloud from DDoS Attacks using Intrusion Detection System in Virtual Machine," Second International Conference on Communication Software and networks (ICCSN), IEEE Computer Society, USA, ISBN: 978-0-7695-3961-4, 2010, pp. 260-264.

[2] C. Modi, D. Patel, H. Patel, B. Borisaniya, A. Patel and M. Rajarajan, "A survey of intrusion detection techniques in Cloud," Journal of Network and Computer Applications, 2012, Available: http://dx.doi.org/10.1016/j.jnca.2012.05.003.

[3] Chi-Chun Lo, Chun-Chieh Huang and Joy Ku, "A Cooperative Intrusion Detection System Framework for Cloud Computing Networks," 39th International Conference on Parallel Processing Workshops (ICPPW), IEEE Computer Society, Washington DC, USA, ISBN: 978-0-7695-4157-0, 2010, pp. 280-284.

[4] Cloud Security Alliance (CSA, 2012), "SecaaS Implementation Guidance," Category 6: Intrusion Management.

[5] Cloud Security Alliance (CSA, 2013), "The Notorious Nine: Cloud Computing Threats," Available: http://www.cloudsecurityalliance.org/topthreats

[6] J D. Krishnan and M. Chatterjee , "An Adaptive Distributed Intrusion Detection System for Cloud Computing Framework," Recent Trends in Computer Networks and Distributed Systems Security Communications in Computer and Information Science, Springer-Verlag Berlin Heidelberg, Volume 335, ISBN:978-3-642-34134-2, 2012, pp. 466-473.

[7] S. Gupta, P. Kumar and A. Abraham, "A Profile Based Network Intrusion Detection and Prevention System for Securing Cloud Environment," International Journal of Distributed Sensor Networks, Research Article: Hindawi Publishing Corporation, 2013, Article ID 364575 (http://dx.doi.org/10.1155/2013/364575).

[8] S. Gupta, S. Horrow and A. Sardana, "A Hybrid Intrusion Detection Architecture for Defense against DDoS Attacks in Cloud Environment," Contemporary Computing Communications in Computer and Information Science, Vol. 306, ISBN: 978-3-642-32129-0, 2012, pp. 498-499.

[9] Jun-Ho Lee, Min-Woo Park, Jung-Ho Eom and Tai-Myoung Chung, "Multi-level Intrusion Detection System and log management in Cloud Computing," 13th International Conference on Advanced Communication Technology (ICACT), ISBN: 978-1-4244-8830-8, 2011, pp. 552-555.

[10] J. Hurwitz, R. Bloor, M. Kaufman and F. Halper, Cloud Computing for Dummies, Wiley Publishing, Inc, 2010.

[11] T. Mather, S. Kumaraswamy and S. Latif, Cloud Security and Privacy, O'Reilly Media, Inc, 2009.