Volume 8, No. 2, March 2017 (Special Issue)
ISSN No. 0976-5697
International Journal of Advanced Research in Computer Science
REVIEW ARTICLE
Available Online at www.ijarcs.info

Cloud Security Enhancement Through Intrusion Detection System

Haiqa Fayaz
Department of CSE, SEST
JamiaHamdard, New Delhi, India
haiqafayaz.92@gmail.com

Abstract: Cloud Computing is a flexible, cost-effective, and an efficient delivery platform for providing consumer IT services and business services over the Internet.However, Cloud Computing presents a great level of risk because essential services are often outsourced to a third party, which brings in risk to data security and privacy. In this paper, we explore the different concepts involved in cloud computing, vulnerabilities in this kind of systems and various ways to handle these security concerns. Advanced technologies such as intrusion detection and prevention system (IDPS) and analysis tools have become prominent in the network environment. They involve with organizations to enhance the security of their information assets and make the systems and networks more secure.

Keywords:Cloud Computing; Cloud Security; Vulnerabilities; Intrusion Detection System; Intrusion Prevention System.

INTRODUCTION

The realization of benefits by maximizing the overall efficiency of the present computing era has become the focus of present scientists and researchers. Internet is bringing in a variety of novel applications that promise to improve the quality of our lives in many ways [1]. The utilization of technological resources has led to a new area of concern which includes concept of efficient cloud computing. There is enormous potential in the said field to make services available at a much faster, secure and cost effective way. The use of cloud computing is increasing and it is receiving a growing attention in the scientific and industrial communities. Cloud computing ensures ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., servers, storage, applications, and services) [2]. Cloud Computing appears as a computational paradigm as well as a distribution architecture and its main objective is to provide secure, quick, convenient data storage and internet computing service, with all computing resources visualized as services and delivered over the Internet [3].

Cloud services are divided into three service models such as Infrastructure-as-a-service (IaaS), Platform-as-a-service (PaaS), and Software-as-a-service (SaaS). Each service has various implementations [4].

Figure 1 gives the basic cloud service model including its implementations. Although there are many benefits of cloud computing, there are also some significant barriers to its adoption. One of the most significant barriers is security, followed by issues regarding compliance, privacy and legal matters [5].

The remainder of the paper is organized as Section II, which presents the literature review related to the undertaken topic. Next, the Section III presents the security considerations in cloud computing. Next, in Section IV, Intrusion Detection System is explained followed by different Intrusion Detection tools in section V. Finally, in Section VI, there are some conclusions that are derived at the end of the study.

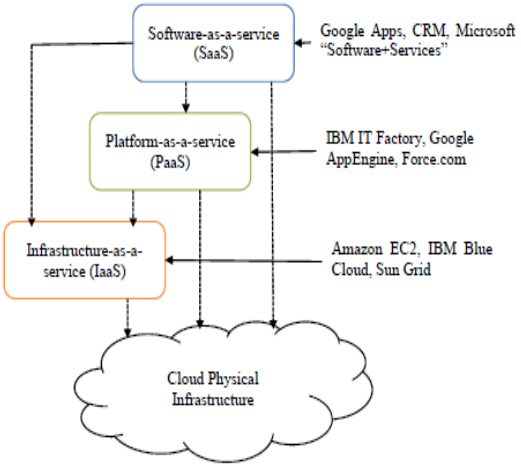

Figure. 1. Cloud Service Model

II. LITERATURE REVIEW

The most comprehensive survey about currently existing literature addressing cloud security issues is given by **Vaquero et al.** in [8]. It distributes the cloud security issues into three different domains of the Infrastructure as a Service (IaaS) model: machine virtualization, network virtualization and physical domain.

HIDS based architecture for Cloud environment was proposed in 2010 by **Vieira et al.** In this architecture, each node of Cloud contains IDS which provides interaction among service offered (e.g. IaaS), IDS service and storage service [11].

Arshad et al. proposed a model for intrusion detection and severity analysis to provide the overall security of the Cloud. It consists of six components; system call handler, detection module, security analysis module, profile engine, global components and intrusion response system [13].

For effective usage of Cloud resources, **Lee et al.** suggested multilevel IDS and log management should be applied at different level of security strength. Databases are used to store user information, system

log, transaction of user and system, whereas storage center stores user's private data which are isolated from one user to another. This approach provides fast detection mechanism in case of any intrusions [12].

SECURITY CONSIDERATION IN CLOUD COMPUTING

With the use of virtualization technologies, Cloud computing virtually and dynamically distributes the computing and data resources to a variety of users, based on their needs. As Cloud computing is a shared utility and is accessed remotely, it is vulnerable to many attacks including host and network based attacks and hence requires immediate attention. Cloud environment is vulnerable to a large number of attacks because of its distributed nature. To ensure security, there has to be a secure cloud architecture which enhances its security. Figure 2 gives the details of a secure cloud architecture. Intrusion prevention and detection components are implemented with virtual firewall and IPS should be installed to protect the cloud network. Also, for protecting the cloud network, the single management console is used [5].

Cloud computing architecture is separated into two different sections such as Front end and Back end. The Front end side is the client or user and the cloud provider is on the back end. The cloud developers are required to take care of cloud attacks when the implementation is done. This can be achieved by utilizing Intrusion Prevention System (IPS) and Intrusion Detection Systems (IDS).

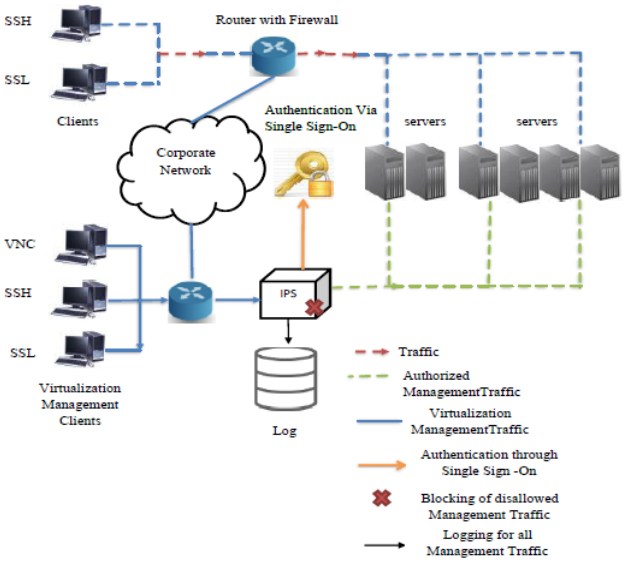

Figure 2. Secure Cloud Architecture

INTRUSION DETECTION SYSTEMS

An Intrusion Detection System is an application which ensures monitoring the network and protecting it from the intruder. Malicious users or hackers use the organization's internal systems to collect information and cause vulnerabilities, leaving systems to default configurations. The malicious users use different techniques like cracking of passwords, detecting unencrypted text to cause vulnerabilities to the system. Hence, security is needed for the users to secure their system from the intruders [7].

The basic types of intrusion detection systems are:

1. Host Based IDS
2. Network Based IDS
3. Application Based IDS

Host based IDS views any sign of intrusion in the local system. They use host system's logging and other information for the required analysis. Host based handler is referred to as a sensor. HIDS are used efficiently for analyzing the network attacks, for example, it can often tell exactly what the attacker did, which commands were used, which files he opened, rather than just a vague accusation.

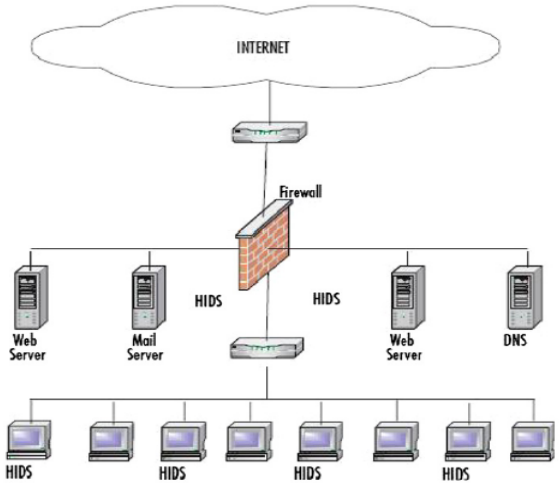

Figure 3. Host Based Intrusion Detection System (HIDS).

The efficiency of HIDS depends on the characteristics of the system to be monitored. Each HIDS detects intrusions for the machines in which it is placed as shown in Figure 3.

Network Intrusion Detection System (NIDS) monitors for cyber threats at the network layer by evaluating network traffic. The implementation of NIDS is shown in Figure 4.

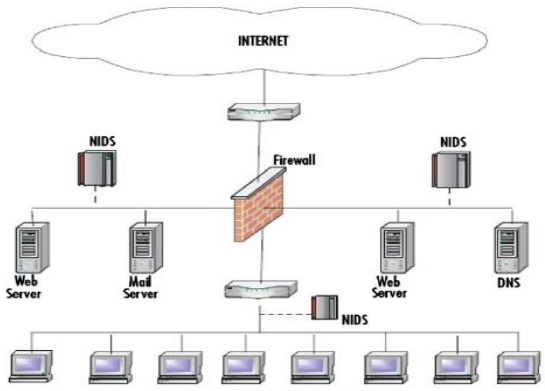

Figure 4. Network Based Intrusion Detection System (NIDS)

Application based IDS (APIDS) will check the effective behavior and event of the protocol. The system or agent is placed between a process and group

of servers. It monitors and analyzes the application protocol between devices [9].

TOOLS IN INTRUSION DETECTION

An intrusion detection product addresses a range of organizational security goals. This section discusses about few security tools.

i. *Snort:* Snort is a lightweight and open source software. It uses a flexible rule-based language to describe the traffic. It records the packets in human readable form. Through protocol analysis, content searching and various pre-processors, Snort detects thousands of worms, vulnerability exploit attempts, port scans, and other suspicious behavior [10].

ii. *Ossec-HIDS:* OSSEC (open source security) is an open source software. It will run on major operating systems and uses a Client/Server based architecture. OSSEC sends the OS logs to the server for analysis and storage. Authentication logs and firewalls are monitored and analyzed by HIDS.

iii. *Fragroute:* It is termed as fragmenting router. Here, from the attacker to the fragrouter the IP packet is sent and then fragmented and lastly transferred to the party.

iv. *Honeyd:* Honeyd is a tool that creates virtual hosts on the network. The services are used by the host. Honeyd allows a single host to request multiple addresses on a LAN for networks simulation. Any type of service on the virtual machine can be simulated according to a simple configuration file [10].

v. *Kismet:* It is termed as fragmenting router. Here, from the attacker to the fragrouter the IP packet is sent and then fragmented and lastly transferred to the party.

vi. *Wireshark:* Wireshark is used in [16] for investigating DHCP and DNS protocols.

CONCLUSION

Cloud Computing is nowadays changing the horizon of information technology. It ultimately has turned the utility computing into a big reality. However, the security risks are also enormous, since Cloud Computing is a combination of many technologies and that inherits their security issues too. This paper presented the usage of intrusion detection and intrusion prevention techniques into Cloud. It also specifies the locations in Cloud where IDS/IPS can be positioned for efficient detection and prevention of attacks. Also, we listed some current solutions in order to mitigate the risks. However, new security techniques are needed as well as integrating traditional solutions with new ones is being done that can work with cloud architectures much efficiently. The same becomes the future work of this paper.

REFERENCES

[1] H. Fayaz, A. Khalique, "A Review on Sociological Impacts of Social Networking". *International Journal of Engineering Applied Sciences and Technology*, Vol. 1, pp. 6-12, 2016.

[2] K. Hashizume, D. G. Rosado, E. F. Medina and E. B. Fernandez, "An Analysis of Security Issues for Cloud Computing". *Journal of Internet Services and Applications*, 2013.

[3] Zhao G, Liu J, Tang Y, Sun W, Zhang F, Ye X, Tang N (2009) Cloud Computing: A Statistics Aspect of Users. In: *First International Conference on Cloud Computing, Beijing, China. Springer Berlin, Heidelberg*, pp. 347–358

[4] B. R Cyril, S. B. R Kumar, "Cloud Computing Data Security Issues, Challenges, Architecture and Methods- A Survey", *International Research Journal of Engineering and Technology*, vol. 2-No. 4, 2015.

[5] KPMG (2010) From hype to future: KPMG's 2010 Cloud Computing survey.

[6] A. A. Thu, "Integrated Intrusion Detection and Prevention System with Honeypot on Cloud Computing Environment", *International Journal of Computer Applications*, Vol. 67, No.4, 2013.

[7] V. S and M. S, "Intrusion Detection System – A Study", International Journal of Security, *Privacy and Trust Management*, Vol. 4, No. 1, pp. 31-44, 2015.

[8] Vaquero L, Rodero-Merino L, Moran D (2011) Locking the sky: a survey on IaaS cloud security. *Computing* 91: 93–118

[9] Karthikeyan .K.R and A. Indra- "Intrusion Detection Tools and Techniques a Survey".

[10] "Top 125 Network Security Tools"- SecTools.Org- http://sectools.org/tag/ids/sec

[11] Vieira K, Schulter A, Westphall C, Westphall C. "Intrusion detection techniques in grid and cloud computing environment". *IEEE IT Professional Magazine* 2010.

[12] Lee, J-H, Park M-W, Eorn J-H, Chung T-M. Multi-level Intrusion detection system and log management in cloud computing. In: *13th International conference on advanced communication technology (ICACT)*; 2011, pp. 552–5.

[13] Arshad J, Townend P, Xu J. "An abstract model for integrated intrusion detection and severity analysis for clouds". *International Journal of Cloud Applications and Computing* 2011; 1(1):1–17.

[14] T. Bazaz, A. Khalique, "A Review On Single Sign On Enabling Technologies And Protocols". *International Journal Of Computer Applications*; Vol. 151, No. 11, 2016.

[15] B. Bashir, A. Khalique, "A Review On Security Versus Ethics", *International Journal OfComputer Applications*; Vol. 151, No. 11, 2016.

[16] Sameena Naaz, Firdoos Ahmad Badroo, "Investigating DHCP and DNS Protocols using Wireshark", IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 18, Issue 3, Ver. II (May-Jun. 2016), PP 01-08