DOI: http://dx.doi.org/10.26483/ijarcs.v8i7.4505

ISSN No. 0976-5697

Volume 8, No. 7, July – August 2017

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

IDS CRITERIA FOR ENHANCED SECURITY OVER CLOUD

Vimmi Pandey
Rani Durgavati Vishwavidyalaya,
Jabalpur,India

Dr. Mridula Dubey
Rani Durgavati Vishwavidyalaya,
Jabalpur,India

Abstract: Intrusion Detection Systems are being used in every software whether it is web based or not. But application of IDS in public networks such as cloud, grid computing has many applications and has been proven to be boon. The application of IDS is used in creating an alarming system for the networks so that security measures can be applied to prevent the possible loss of data and avoiding non functioning systems. Because of the enhanced technology there are many ways of the hacking and compromising any networked system has been evolved and causing huge loses. Since direct application of security methods affects the performance of the system heavily, therefore application of IDS is increasing widely. Since IDS can be applied on gateways therefore a quick and better alarming system can be created which will prompt the administrators to apply security techniques to avoid the problems. In this work, different IDS mechanisms have been studied and list of possible criteria has been enlisted to provide IDS over the cloud. This work also proposes to take one of the IDS mechanisms to study the criteria of IDS, their behaviours, advantages and possible alarming for Cloud.

Keywords: Cloud Computing, Security, Intrusion Detection System, Alarming criteria, abnormal behaviours, Encryption, Decryption, Authentication, Authorization, non-repudiation.

1. INTRODUCTION

Intrusion Detection can be defined as "...the act of detecting actions that attempt to compromise the confidentiality, integrity or availability of a resource."1 More specifically, the goal of intrusion detection is to identify entities attempting to subvert in-place security controls. [1, 2]
Common types of Intrusion Detection:
A) Network Based (Network IDS)
Network based intrusion detection attempts to identify unauthorized, illicit, and anomalous behaviour based solely on network traffic. A network IDS, using either a network tap, span port, or hub collects packets that traverse a given network. Using the captured data, the IDS system processes and flags any suspicious traffic. Unlike an intrusion prevention system, an intrusion detection system does not actively block network traffic. The role of a network IDS is passive, only gathering, identifying, logging and alerting. Examples of Network IDS: [1, 2]

- SNORT

B) Host Based (HIDS)
Often referred to as HIDS, host based intrusion detection attempts to identify unauthorized, illicit, and anomalous behavior on a specific device. HIDS generally involves an agent installed on each system, monitoring and alerting on local OS and application activity. The installed agent uses a combination of signatures, rules, and heuristics to identify unauthorized activity. The role of a host IDS is passive, only gathering, identifying, logging, and alerting. Examples of HIDS: [2]

- OSSEC - Open Source Host-based Intrusion Detection System
- Tripwire
- AIDE - Advanced Intrusion Detection Environment
- Prelude Hybrid IDS

C) Physical (Physical IDS)
Physical intrusion detection is the act of identifying threats to physical systems. Physical intrusion detection is most often seen as physical controls put in place to ensure CIA. In many cases physical intrusion detection systems act as prevention systems as well. Examples of Physical intrusion detections are: [2]

- Security Guards
- Security Cameras
- Access Control Systems (Card, Biometric)
- Firewalls
- Man Traps
- Motion Sensors

Intrusion Prevention
Intrusion prevention follows the same process of gathering and identifying data and behaviour, with the added ability to block (prevent) the activity. This can be done with Network, Host, and Physical intrusion detection systems.
As the amount of data being generated and transmitted over to the cloud increases, so too do research proposals to combat security issues with advanced cryptography. Often these proposals involve complex policy algorithms and new infrastructures, which work in theory, but would require high overhead in reality. [2, 3]

2. ISSUES IN CLOUD DATA STORAGE

Cloud Computing moves the applying software system and information bases to the big data centres, wherever the management of the information and services might not be totally trustworthy. This distinctive attribute, however, poses several new security challenges that haven't been well understood. In this, we tend to target cloud information storage security, which has invariably been a very important side of quality of service to make sure the correctness of user's information within the cloud. [3, 4, 5, 6, 8, 9, 11, 13, 15]
A. Trust:

B. Privacy
C. Security
D. Ownership
E. Performance and Availability

A. REVIEW OF THE SECURITY ISSUES IN CLOUD ENVIRONMENT

One of the strength of the cloud environment is its distributed nature of the renounces. For huge and rapid processing of the data, a CSP may use resources which are available at that time of operation. This feature exposes the user data over entire network which may cause serious security threat. To overcome this issue, an intrusion detection system (IDS) mechanism is generally preferred in the cloud paradigm. [4, 6, 8, 15]

From its first report in 1987, IDS has got prime importance as a tool to prevent and mitigate the unauthorized access to the user data over the network.

I. Taxonomy of the security threats and attacks

The security of the data has got a prime importance in the present era cloud computing owing to its distributed nature. In fact, it is a major bottleneck in the deployment and acceptance of the cloud services over the globe.

SECURITY THREATS IN CLOUD SENARIO

Nature of the threat				
	Security Threats			
	Nomenclature	**Description**	**Vulnerability**	**Prevention**
Basic Security	SQL injection attack	A malicious code is placed in standard SQL code.	Unauthorized access to a database by the hackers.	May be avoided by the use of dynamically generated SQL in the code and filtering of user input.
	Cross site scripting (XSS) attack	A malicious script is injected into Web content.	Website content may be modified by the hackers.	Active content filtering, Content based data leakage prevention technique, Web application vulnerability detection technique.
	Man in middle attack (MIM)	Intruder tries to tap the conversion between sender and receiver.	Important data/ information may be available to the intruder.	Robust encryption tools like Dsniff, Cain, Ettercap, Wsniff and Airjack may be used for prevention.
Network Layer Security	DNS attack	Intruder may change the domain name request by changing the internal mapping of the users.	Users may be diverted to some other evil cloud location other than the intended one.	Domain name system security extensions (DNSSEC) may reduce the effect of DNS attack.
	Sniffer attack	Intruder may capture the data packet flow in a network.	Intruder may record, read and trace the user's vital information.	ARP based sniffing detection platform and round trip time (RTT) can be used to detect and prevent the sniffing attack.
	IP address reuse attack	Intruder may take advantage of switchover time/cache clearing time of an IP address in DNS.	Intruder may access the data of a user as the IP address is still exists in DNS cache.	A fixed time lag definition of ideal time of an IP may prevent this vulnerability.
	Prefix Hijacking	Wrong announcement of an IP address related with a system is made.	Data leakage is possible due to wrong routing of the information.	Border gateway protocol with autonomous IDS may prevent it.
	Fragmentation attack	Malicious insider(user) or an outsider may generate this attack	This attack use different IP datagram fragments to mask their TCP packets from targets IP filtering mechanism.	A multilevel IDS and log management in the cloud may prevent these attacks
	Deep packet inspection	Malicious insider (user)	Malicious user may analyse the internal or external network and acquire the network information	
	Active and passive eavesdropping	Malicious insiders and network users	Intruder may get network information and prevent the authentic packets to reach its destination.	
	Port Scan	Malicious user may attempt to access the network	Malicious user may get the complete activity status of the network	Continuous observation of port scan logs by IDS may prevent this attack.
Application Layer Attacks	Denial of service attack	The usage of cloud network may get unusable due to redundant and continuous packet flooding.	Downgraded network services to the authorized user, Increases the bandwidth usage.	Separate IDS for each cloud may prevent this attack.
	Cookie Poisoning	Changing or modifying the contents of cookies to impersonate an authorized user	Intruder may get unauthorized access to a web page or an application of the authorized user.	A regular cookie cleanup and encryption of cookie data may prevent this vulnerability
	Captcha Breaking	Spammers may break the Captcha	Intruder may spam and over exhaust the network resources	A secure speech and text encryption mechanism may prevent this attack by bots

The top nine notorious attacks on the cloud may be categorized as: data infringe loss of the important data, account or service traffic capturing, insecure interfaces and APIs, service denial, malicious insiders, abuse of cloud services, lack of due diligence and shared technology vulnerabilities. The cloud security threats may be classified and categorized based on the nature and vulnerability of attacks. Table II provides the categorization of different security threats in the cloud computing scenario. [5, 8, 13, 14]

B. IDS Taxonomy

IDS may be defined as a "software entity that runs on a host, which monitors the activities of users and programs on the same host and/or the traffic on networks to which that host is connected". IDS are employed to aware the system administrator against any suspicious and possibly disturbing incident taking place in the system that is being analysed. Out of many available features of internal working, IDS may be classified on the basis of detection method, monitoring scope, and behaviour on detection [5, 2, 3, and 8]. Depending on the need of the application a specific model may be chosen for the deployment in the cloud. Table III briefly characterize the IDS used in the cloud scenario.

CHARACTERIZATION OF IDS

IDS Characterization	
Parameter	**Classification**
Detection Method	Anomaly based, Specification based
Monitoring Method	Network based, Host based
Behavior Pattern	Passive and active IDS
Usage Frequency	Online and offline analysis

Initially, signature analysis was used as the fundamental criteria in most widely deployed and commercially available IDS. SNORT [3] is a signature-based open source network-based IDS used to execute real-time traffic categorization and analysis over IP networks. Machine learning approach is used for misuse detection. This approach is based on automatic discovery of patterns and classes of attacks. Data-mining-based IDS depends on nontrivial guess regarding the availability and the quality of training data. However, this approach fails if the training dataset contains some intrusions, the IDS may assume that they are normal traffic and may fail to detect future instances of these attacks. [5, 3, 8]

The statistical methods of IDS is based on the building the user activity profile as 'Normal' or else. Based on the profile information, the IDS may classify the events as normal or an intrusive one. An ID based on immune system concept is one of the latest approaches. Besides its appealing and interesting aspect of intrusion detection, this method is difficult to build practically.

3. EXISTING SYSTEM

Cloud computing promises to increase innovation and the velocity with which applications are deployed all while helping any enterprise meet most IT service needs at a lower total cost of ownership and higher return investment. As the march of cloud continues, it brings both new opportunities and new security challenges. To take advantage of those opportunities while minimizing risks, we argue that Intrusion Detection Systems (IDS) integrated in the cloud is one of the best existing solutions nowadays in the field. The concept of intrusion detection was known since past and was first proposed in 1980s. Since that time IDSs are evolving. However, even several efforts have been made in the area of Intrusion Detection Systems for cloud computing environment, many attacks still prevail. Therefore, the work presented in this paper proposes a multi-criteria analysis and a comparative study between several IDS architectures designed to work in cloud computing environments. Cloud computing is emerging as a promising IT paradigm. Many challenges are still hanging ahead for the Cloud to jump into the maturity stage. Thus, security is deemed as a main challenge. In this paper, we develop the performance of intrusion detection solutions (IDS) by analyzing their performance in terms of recognition, security and capacity. The main aim of our work is to help engineers to implement adequate solution (IDS) depending on the security levels of cloud computing. Our proposed method is based on two-stage. The first stage consists on studying the needed requirements of IDS solution in cloud computing. The second stage classifies security attacks based on four levels. The classification identifies attacks that we should treat with the fitting solution. [6]

With the growing trends of cloud computing, the security issues in this area are growing at the same speed as its development. Some malicious intruders and other malware activities tend to find the inner vulnerabilities and spare no effort to control the administration or conduct the pure break-down service with curiosity or on purpose. Traditional defence systems such as firewall, intrusion detection and malware code system are still utilized in nowadays network scenes, but they may not support enough in cloud computing environment with old-fashioned architectures. Here we focus on intrusion detection system (IDS) to defend against intruders and other attacks. In this paper, we proposed a collaborative intrusion detection service and our goal is to make use of the state-of-the-art computing framework in cloud environment and to provide a rounded IDS service for both cloud providers and cloud tenants, while the collaborative architecture will help to respond to the attacks promptly. We set up our system prototype and discuss the empirical results on the preference. The experimental results demonstrate that our system does enhance the security when some network-based attacks happen and ensure that both cloud service providers and tenants are protected with satisfaction. [7]

This paper reports a detailed analysis and categorization of various security threats in a cloud computing environment along with a brief taxonomy of intrusion detection system. The security attacks are launched on a private cloud and the detection and prevention are carried out by using SNORT IDS. A port scan and TCP Flood attack are used for the analysis purpose. [8]

4. PROPOSED SCHEME

An integrated solution of the security threats in cloud is a possible scheme which is going to be helpful for all the different types of users of the cloud. It will be a combination of the IDS, encryption, authentication and authorization. In the first phase it is being proposed to implement IDS for achieving the alarming mechanism, which shall be working on the cloud boundary to send alarm to the internal system for prevention of attacks before they can harm the system. For implementation of IDS following steps shall be used:

Phase I

Log collection module: The network packets are collected from network, Includes: network source port, destination port, the length of the connection over time, the use of network bandwidth. Collect log data from Super Manager hypervisor. Collected logs shall be added in repository. Repository shall have various log data for providing the comparison and forming rule set to detect the intrusions.

The rule set shall be updated dynamically for evaluating the system with latest mechanism of the intrusions.

Phase II

Log data Evaluation module: The collected log data are matched with the rule base. If the behaviour is abnormal, alarms are generated and transmitted to security management centre for response.

Phase III

Analysis module: The logs are collected and saved into the log table, then passed to analysis module based on rough set to process, new decision-making rules are generated.

Phase IV

Alarming module: The collected logs are matched with the decision-making rules in the rule database. If it is abnormal behaviour then system will generate alarms.

5. CONCLUSIONS

Cloud is an open platform which allows using its services on the basis of Service Level Agreement between the users and the cloud service provider. Security of the data of the users of the Cloud is a mandatory requirement and the factors involved in security threats are too many. For security over the cloud various techniques are used such as intrusion Detection System, Firewall, Anti Virus software etc. For achieving security compromise is done in the performance of the cloud services because each packet requires going through a security mechanism involved. This opens the various research gates for achieving high security and performance both. Intrusion detection system is one of the most promising techniques applied for security. This work provides a survey of the various IDS criteria applied to avail high security.

This work shall further be providing a proposition of a novel & efficient approach over the cloud environment that will eliminate all potential threats related to cloud security.

REFERENCES

[1] Maqsood, R.; Shahabuddin, N.; Upadhyay, D., "A Scheme for Detecting Intrusions and Minimising Data Loss in Virtual Networks," in Computational Intelligence and Communication Networks (CICN), 2014 International Conference on , vol., no., pp.738-743, 14-16 Nov. 2014 doi: 10.1109/CICN.2014.160

[2] A. J. Duncan, S. Creese, and M. Goldsmith, “Insider Attacks in Cloud Computing,” Proc. IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications, Liverpool, 2012, pp. 857–862.

[3] Kene, S.G.; Theng, D.P., "A review on intrusion detection techniques for cloud computing and security challenges," in Electronics and Communication Systems (ICECS), 2015 2nd International Conference on , vol., no., pp.227-232, 26-27 Feb. 2015 doi: 10.1109/ECS.2015.7124898

[4] C. Modi, D. Patel, B. Borisaniya, H. Patel, A. Patel, and M. Rajarajan, “A survey of intrusion detection techniques in Cloud,” Journal of Network and Computer Applications, vol. 36, no. 1, pp. 42–57, January 2013.

[5] Anup ghosh, Chrish greamo, page 79-82, 2011, “Sandboxing and Virtualization”, Security and privacy,IEEE.

[6] M. Ezzarii, H. El Ghazi, H. Elghazi and T. Sadiki, "Performance analysis of a two stage security approach in cloud computing," Cloud Technologies and Applications (CloudTech), 2015 International Conference on, Marrakech, 2015, pp. 1-7. doi: 10.1109/CloudTech.2015.7336990

[7] Hong Liang, Yufei Ge, Wenjiao Wang and Lin Chen, "Collaborative intrusion detection as a service in cloud computing environment," 2015 IEEE International Conference on Progress in Informatics and Computing (PIC), Nanjing, 2015, pp. 476-480. doi: 10.1109/PIC.2015.7489893

[8] P. Deshpande, S. C. Sharma and P. S. Kumar, "Security threats in cloud computing," Computing, Communication & Automation (ICCCA), 2015 International Conference on, Noida, 2015, pp. 632-636. doi: 10.1109/CCAA.2015.7148450

[9] M. Zbakh, K. Elmahdi, R. Cherkaoui and S. Enniari, "A multi-criteria analysis of intrusion detection architectures in cloud environments," Cloud Technologies and Applications (CloudTech), 2015 International Conference on, Marrakech, 2015, pp. 1-9. doi: 10.1109/CloudTech.2015.7336967

[10] Riquet, D.; Grimaud, G.; Hauspie, M., "Discus: A massively distributed IDS architecture using a DSL-based configuration," in Information Science, Electronics and Electrical Engineering (ISEEE), 2014 International Conference on , vol.2, no., pp.1193-1197, 26-28 April 2014 doi: 10.1109/InfoSEEE.2014.6947859

[11] Donadio, P.; Fioccola, G.B.; Canonico, R.; Ventre, G., "Network security for Hybrid Cloud," in Euro Med Telco Conference (EMTC), 2014 , vol., no., pp.1-6, 12-15 Nov. 2014 doi: 10.1109/EMTC.2014.6996640

[12] Bousselham, A.; Sadiki, T., "Security of virtual networks in cloud computing for education," in Web and Open Access to Learning (ICWOAL), 2014 International Conference on , vol., no., pp.1-5, 25-27 Nov. 2014 doi: 10.1109/ICWOAL.2014.7009218

[13] Kajal, N.; Ikram, N.; Prachi, "Security threats in cloud computing," in Computing, Communication & Automation (ICCCA), 2015 International Conference on , vol., no., pp.691-694, 15-16 May 2015 doi: 10.1109/CCAA.2015.7148463

[14] Goel, R.; Garuba, M.; Grima, A., "Cloud Computing Vulnerability: DDoS as Its Main Security Threat, and Analysis of IDS as a Solution Model," in Information Technology: New Generations (ITNG), 2014 11th International Conference on , vol., no., pp.307-312, 7-9 April 2014 doi: 10.1109/ITNG.2014.77

[15] C. B. Westphall and F. R. Lamin. SLA Perspective in Security Management for Cloud Computing. In Proc. of the Int. Conf. on Networking and Services (ICNS), 2010. Pp. 212-217.