Rules based Enhancement in Cloud Intrusion Detection System Service

Shalini Garg
Lovely Professional University, Phagwara (Punjab)

Karanvir Kaur
Lovely Professional University, Phagwara (Punjab)

ABSTRACT
In cloud environment, chances of intrusion are more with cultivation of intruder's attacks because cloud computing is internet based computing where virtual servers provide software, Platform, Infrastructure or other computing resources to customer on pay-as-you-basis. With increment in need of computing services of cloud computing, demand of security as a service is also increasing with risks of vulnerabilities in cloud computing environment. Every cloud user wants to secure his/her resources which are shared by all users in cloud computing. In this paper cloud intrusion detection system service model is introduced which is based upon rules of CRG. The main purpose of this proposed model is to eliminate single point of failure vulnerability of IDS system in cloud computing by introducing concept of multiple IDSs so that if one IDS is compromised then other IDSs can be available for cloud users.

General Terms
Intrusion Detection Systems, Intrusion Detection Approaches.

Keywords
Cloud Rule Generator (CRG), Host Based IDS (HIDS), Network Based IDS (NIDS).

1. INTRODUCTION
Cloud user' trust is developed on basis of some parameters like hiding of data location by users, availability of data every time, regulatory compliance and privileged user access [5]. Cloud users want to secure their shared data on cloud. So there is need of intrusion detection system in cloud to monitor activities of users. An intruder is recognized as a system, program or any person who tries to perform illegal operations or actions which are not allowed, to break into information system successfully and intrusions is a set of actions which are attempt to compromise the confidentiality, integrity of any computer resource. Intrusion detection is process of detecting these kind of actions performed to compromise confidentiality, integrity and availability of computer resources. An intrusion detection system is a device or software application which is used to monitor network and/or system activities for malicious activities or policy violations by collecting information on the basis of some parameters and after analyzing this information, it produces alert reports [1].Based on the protected objective or the information source, IDS can be classified into Host-based Intrusion Detection System and Network-based Intrusion Detection System [3].Host-Based Intrusion Detection System operates on information collected from within an individual computer system. It monitors those packets which are inbounded and out bounded from computer system only; it does not capture and analyze the network packets but Network-Based Intrusion Detection System detects attacks by capturing and analyzing the network packets.

Network-based IDSs often consist of a set of single purpose sensors which are placed at various points in a network. These sensor units monitor network traffic, performing local analysis of that traffic and reporting attacks to a central management console. Using network-based IDS, there is no need to configure and manage every host because of IDS sensor which is responsible for all analysis. Network-based IDS can monitor the network traffic affecting multiple hosts that are connected to the network segment, thereby protecting those hosts. Attacks to a specific host in a network would not affect IDS and securing the IDS sensor is simpler. Network-based IDS would utilize dedicated resources for its functionalities which is isolated from any host in the network. Therefore, it does not inflict a performance cost on the monitored systems. For analyzing events to detect attacks, there are two primary approaches [2], [3]: Misuse Detection Approach and Anomaly Detection Approach. By using Misuse Detection Approach system activity or sets of events are analyzed that match a predefined pattern of events or attacks. This approach is sometimes called Signature -based detection. One of the biggest advantages of this approach is that we can add new rules without any modifications in previous or existing ones. Anomaly Detection Approach is used widely to identify abnormal behavior on host or network. Functionality of this approach is based on the assumption that attacks are different from legitimate activity and can therefore be detected by systems that identify these differences. Anomaly detection approach focuses on identifying user behavioral patterns and deviations from such patterns. With the help of this strategy, a wider range of unknown attacks can be covered.

2. RELATED WORK
There are various characteristics of cloud computing like service oriented concept abstracts the details of cloud computing implementation, loose coupling makes cloud computing system run well when part of it is destroyed and ease use user experience characteristic of cloud computing is widely accepted by non computer experts [4]. Some security issues related to cloud computing are XML signature element wrapping, Browser security, cloud malware injection, flooding attacks, Data protection, incomplete data deletion, Locks in [6]. Rashidi Ahmad et al. presented a model for trust in cloud computing, accounting for important elements which shape the users trust. In this paper, first the main cloud risks are recognized and then on the basis of eight parameters like Data location, Investigation, Data segregation Availability,

Long-term viability, Regulatory compliance, Backup and recovery, privileged user access, perspectives of user's trust have been synthesized in cloud computing environment. By analyzing the proposed model, the effect of each of these eight elements trust is investigated and described. Results of proposed model helps in recognizing the main parameters affecting users trust and characterizing importance of each parameter [5].Zarrabi Amirreza et al. proposed architecture of intrusion detection system in cloud to overcome the critical challenge of keeping the client secure from cyber attacks. This architecture is made of three components: Intrusion Detection Service Agent, Cloud Computer Service Component (CCSC), and Intrusion Detection Service Component (IDSC) [2]. Ms. Shelke Parag K et al. proposed Multithreaded Cloud IDS model which is beneficial for handling high volume of data in cloud environment by single node IDS. This model will help to prevent some attacks like trying for decryption of cloud data which is in encrypted form for confidentiality, Network and host based attacks on server and lack of data interoperability standards [8]. Raj Gaurav et al. proposed security system architecture with PCRE based rules approach on cloud network using SNORT as IDS and also described configuration details of SNORT for intrusion detection on cloud network. Author implemented both approaches of intrusion detection on cloud network by creating virtual environment. Snort can be configured in sniffer, packet logger and network intrusion detection modes [7].Grobauer Bernd et al. described cloud computing characteristics vulnerabilities like unauthorized access to management interface, metering and billing vision and vulnerabilities of Internet protocol and data recovery [9]. SAIKIRAN B defined that important task of each intrusion detection system is to aggregate the alerts generated by it. Author proposed a novel technique which is based upon dynamic and probabilistic model of current attack situation [10]. There is need of integrated scheme which can provide protection against whole spectrum of threats or attacks. It is noticed that IaaS (Infrastructure as a Service) service models have limited to support to offer intrusion detection as a service means cloud subscribers want to deploy IDS device on cloud network segment [11].

3. CLOUD INTRUSION DETECTION SYSTEM SERVICE

Proposed framework is based upon a concept that is if complexity of intrusion detection system is increased then it can be customized by us. Therefore proposed system is nicknamed as Cloud Rule Generator.CRG works upon three layers: User layer, Machine layer and Database layer.

1. At user layer, users can subscribe or unsubscribe for IDS service.

2. Machine layer is responsible for providing intrusion detection service to the users.

3. Database layer which trace the subscribers settings and store alerts generated by IDSs.

Firstly users subscribe for IDS service using CIDS web interface.IDS manager or administrator will provide IDS service to users and will balance load between multiple IDSs. Intrusion detection system will detect malicious activities from network and alerts will be generated which will be stored in Signature database. This signature database can be examined by administrator.

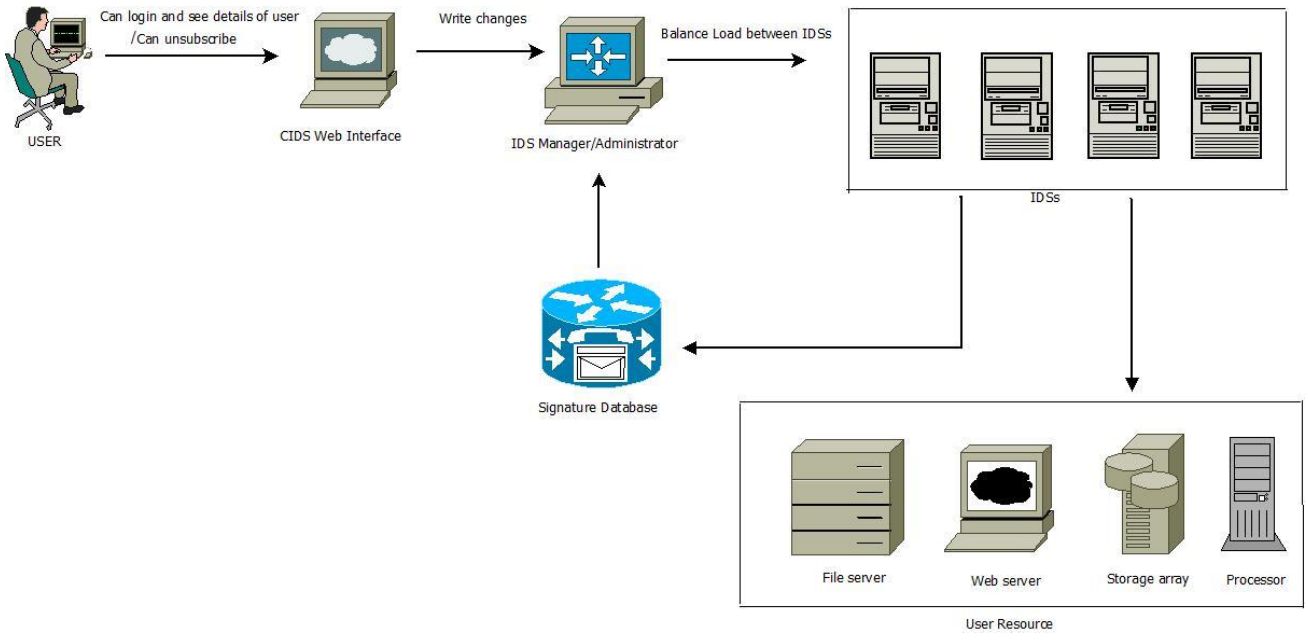

Figure 1: Proposed Cloud Intrusion Detection System Service (CIDSS) Architecture

3.1 Advantages of Proposed Model:

1) Proposed model provide security as a service to cloud users in terms of by detecting intrusions over resources of users on cloud.
2) This model helps in eliminating single point of failure by introducing concept of multiple intrusion detection systems in cloud environment.
3) Increase availability of IDS service for cloud users by balancing load between IDSs.

4. IMPLEMENTATION AND RESULTS

As a proof of concept implementation CIDSS was implemented using VMware workstation in which virtual machines are created to establish cloud network. Web Interface is developed using C# .Snort tool is used for intrusion detection and AAVAL tool is configured with Snort tool for displaying alerts. After analyzing results it is found that proposed CIDSS model is effiecient in increasing availability of IDS in cloud environment by using concept of multiple IDS. If first IDS is compromised then second IDS will be available to users. Figure 2 shows performance analysis of CIDSS model on the basis of availability of IDS to users.

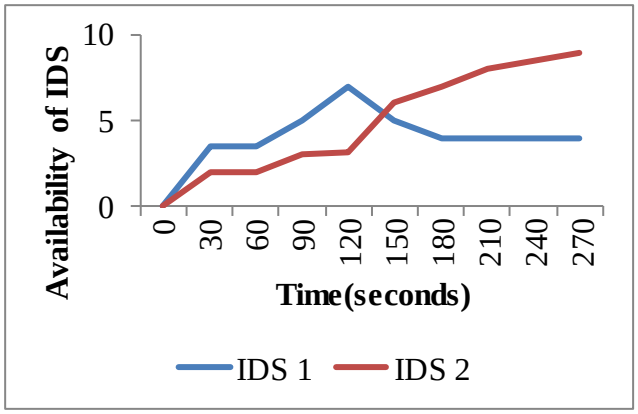

Figure 2: Performance Analysis of CIDSS

Proposed CIDSS model have advantages over another existing IDS models in cloud computing environment. The main goal of CIDSS model is to provide security as a service to cloud users in efficient manner. Table 1 represents the comparison of proposed CIDSS model with 2 existing models: Multithreaded Cloud IDS model and Cloud Intrusion Detection system (CIDS) model.

Table 1: Comparison of Cloud IDS

System/Characteristic	Proposed CIDSS	Multithread Cloud IDS	CIDS
Service-Based	yes	No	Yes
Customized Subscription	Yes	No	No
Client- Oriented	Yes	Yes	No
General Protection	Yes	Yes	No

5. CONCLUSION

It is concluded that in cloud environment, chances of intrusion are more with cultivation of intruder's attacks because cloud computing is internet based computing where virtual servers provide software, Platform, Infrastructure or other computing resources to customer on pay-as-you-basis. With increment in need of computing services of cloud computing, demand of security as a service is also increasing with risks of vulnerabilities in cloud computing environment. Every cloud user wants to secure his/her resources which are shared by all users in cloud computing. Intrusion detection systems (IDS) generate alerts for administrators if actually intrusions take place by critically scanning the network packets through applying signatures (pre-defined rules). In this paper cloud intrusion detection system service model is introduced which is based upon rules of CRG. The main purpose of this proposed model is to eliminate single point of failure vulnerability of IDS system in cloud computing by introducing concept of using multiple IDSs so that if one IDS is compromised then other IDSs can be available for cloud users. Communication and cooperation between multiple intrusion detection systems can be done in future so that amount of alerts can be reduced in database.

6. ACKNOWLEDGMENTS

Our special thanks to Prabhdeep Singh who supported us in developing proposed model.

7. REFERENCES

[1] Hoque Mohammad Sazzadul, Mukit Md. Abdul and Bikas Md. Abu Naser (2012) "An Implementation of Intrusion Detection System Using Genetic Algorithm" International Journal of Network Security & Its Applications (IJNSA), Vol. 4, No 2, March 2012

[2] Zarrabi Amirreza, Zarrabi Alireza (2012) "Internet Intrusion Detection System Service in a Cloud" InternationalJournal of Computer Science Issues Vol. 9, No 2, September, 2012.

[3] Wang Shenghui, Shenzhen (2011) "Research of Intrusion Detection Based on an Improved K-means Algorithm "Second International Conference on Innovations in Bio-inspired Computing and Applications, 2011.

[4] Ram M Sanjay, Vijayaraj A (2011) "Analysis of the characteristics and trusted security of cloud computing" International Journal on Cloud Computing Services and Architecture (IJCCSA) Vol. 1, No 3 November, 2011.

[5] Rashidi Ahmad and Movahhedinia Naser (2012) "A Model for User Trust in Cloud Computing" International Journal on Cloud Computing: Services and Architecture (IJCCSA), Vol. 2, No.2, April 2012.

[6] Sara Qaisar, Khawaja Kausar Fiaz (2012) "Cloud Computing: Network/Security Threats and Countermeasures" Interdisciplinary Journal of Contemporary Research in Business. Vol. 3, No 9, January, 2012.

[7] Raj Gaurav, Katoch Munish (2012) "Security Implementation through PCRE Signature over Cloud Network" Advanced Computing: An International Journal (ACIJ), Vol.3, No.3, May 2012.

[8] Ms. Shelke Parag K., Ms. Sontakke Sneha, Dr. Gawande A. D. (2012) "Intrusion Detection System for Cloud Computing" International Journal of Scientific & Technology Research Vol. 1, May, 2012.

[9] Grobauer Bernd, Walloschek Tobias, Stöcker Elmar (2011) "Understanding Cloud Computing Vulnerabilities" Security & Privacy, IEEE Vol. 9, 2011.

[10] SAIKIRAN B (2012) "Advance Techniques for the Detection of Interruption Alerts" International Journal of Advanced Computer and Mathematical Sciences ISSN 2230-9624.Vol 3, Issue 4, 2012, pp 424-429

[11] M.Madhavi (2012) "An Approach For Intrusion Detection System In Cloud Computing" International Journal

[12] Reddy V.Krishna (2011) "Security Architecture of Cloud Computing" International Journal of Engineering Science and Technology (IJEST), ISSN: 0975-5462 Vol. 3, 2011.

[13] Peter Mell, Timothy Grance (2011). National Institute of Standards and Technology Retrieved from http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf

[14] Phil Cox (2012). Intrusion Detection in a cloud computing.Retrievedfromhttp://searchcloudcomputing.techtarget.com/tip/Intrusion-detection-in-a-cloud-computing-environment.