ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 6, June 2015

An Innovative Intrusion Detection System using SNORT for Cloud Environment

Sumalatha Potteti, Namita Parati

Assistant Professor, Department of CSE, BRECW, Hyderabad, India

Assistant Professor, Department of CSE, BRECW, Hyderabad, India

ABSTRACT: Cloud Computing is an attractive and cost-saving service for buyers as it provides accessibility and reliability options for users and scalable sales for providers. In spite of being attractive, Cloud feature poses various new security threats and challenges when it comes to deploying Intrusion Detection System (IDS) in Cloud environments. Cloud Computing is a method to increase the capacity or add capabilities dynamically without investing in new infrastructure, training new personnel or licensing new software. We introduce a Cloud Intrusion Detection System Services (CIDSS) which is developed based on Cloud Computing and can make up for the deficiency of traditional intrusion detection, and proved to be great scalable. CIDSS can be utilized to overcome the critical challenge of keeping the client secure from cyber attacks while benefit the features which are presented by Cloud Computing technology. To handle large scale network access traffic and administrative control of data and application in cloud, we have to develop a new cloud IDS model that can assure maximum security in cloud. In this paper we will talk about the snort IDS on Linux which ensure enough security, efficient management into virtualization based system.

KEY WORDS: Cloud Computing, Cloud Intrusion Detection System Service, Snort as IDS.

I. INTRODUCTION

The last century, computer turned out to be an inseparable part of daily human life. For recent years and with the invent of the Internet, it has been deployed for communication and accessing data. However, currently people rely on the Internet to satisfy their demands utilizing its services, which can be defined as some computing function, rather than accessing the mass data from the Internet. Along with the proposal of the Cloud Computing concepts, a new paradigm of software development and deployment of resources has emerged. It is possible to get rid of the great amount of the spending for fixed assets, such as expensive network servers and software. At present the safety of commonly used technologies such as message encryption, firewalls protect the network and can be used as a first line of defense, but only these technologies is not enough. Virtual Private Network (VPN) is utilized as a means of grouping and information exchange facility. A standardized interface is designed to provide a view of result reports for users. A single server handles multiple requests from a user. It may leads to loss of data and n/w traffic. To overcome this problem we use the concept of cloud environment. It provides an application that is to be accessible through the internet. It is a way to use the internet from a single machine where all the tools installed on the computer. Using a cloud computing we do not take a pain about the location and storage of own data. The main tool of this technology is virtualization. For the virtualization, we use hypervisor software inside the computer. Each virtual machine provides a complete environment having its own operating system, application and network services. Virtualization provides a set of resources as a service to a user. A user needs only a browser and internet connection to consume these resources [1]. In this paper we discuss a new cloud IDS Model and snort IDS on Linux which gives the security in the virtualization environment.

II. CLOUD COMPUTING

Cloud computing refers to the provision of computational resources on demand via a computer network (Figure 1). Users or clients can submit a task, such as word processing, to the service provider, such as Google, without actually possessing the required software or hardware. The consumer's computer may contain very little software or data (perhaps a minimal operating system and web browser only), serving as little more than a display terminal connected to

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 6, June 2015

the Internet. Since the Cloud is the underlying delivery mechanism, Cloud based applications and services may support any type of software application or service in use today [6]. The essential characteristics of Cloud Computing include [7]:

1. On-demand self-service that enables users to consume computing capabilities (e.g., applications, server time, network storage) as and when required.

2. Resource pooling that allows combining computing resources (e.g., hardware, software, processing, network bandwidth) to serve multiple consumers - such resources being dynamically assigned.

3. Rapid elasticity and scalability that allow functionalities and resources to be rapidly and automatically provisioned and scaled.

4. Measured provision to optimize resource allocation and to provide a metering capability to determine usage for billing purposes Extension to existing hardware and application resources, thus, reducing the cost of additional resource provisioning.

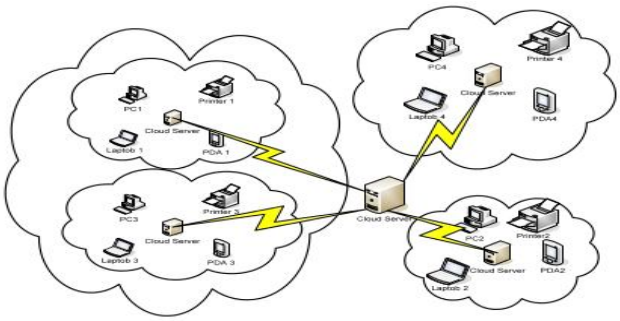

Fig 1: Cloud Computer Architecture

Cloud computing comprises of two different services components for the users namely as software and hardware over the Internet .However , there are various Cloud service delivery models that are developed, which can be divided into three layers [8] depending on the type of resources provided by the Cloud, distinct layers can be defined (see Figure 2). The bottom-most layer provides basic infrastructure components such as CPUs, memory, and storage, and is henceforth often denoted as Infrastructure as a Service (**IaaS)**. Amazon's Elastic Compute Cloud (EC2) is a prominent example for an IaaS offer. On top of IaaS, more platform-oriented services allow the usage of hosting environments tailored to a specific need. Google App Engine is an example for a Web platform as a service (**PaaS**) which enables to deploy and dynamically scale Python and Java based Web applications. Finally, the top-most layer provides the users with ready to use applications also known as Software as a Service (**SaaS**) [8] [9].

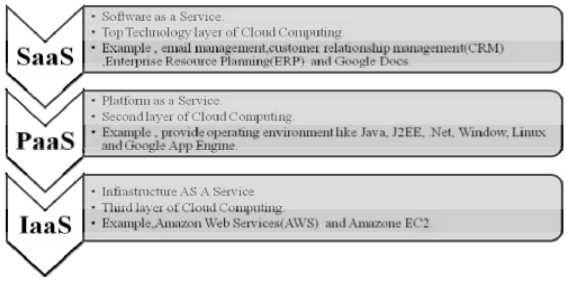

Fig 2: Layers in Cloud Computing

In addition, it is possible to observe the significant interaction between the services model in the Cloud computing which are Software as a service (SaaS), Platform as a service (PaaS) and Infrastructure as a Service (IaaS) as shown in Figure 3. Each one of these models provides unique service to the users in the Cloud computing environment.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 6, June 2015

Fig 3: Conceptual View of Services Model in the Cloud Computing

III.INTRUSION DETECTION IN THE CLOUD

Intrusion detection system plays an important role in the security and perseverance of active defense system against intruder hostile attacks for any business and IT organization. IDS implementation in cloud computing requires an efficient, scalable and virtualization based approach. In cloud computing, user data and application is hosted on cloud service providers remote servers and cloud user has a limited control over its data and resources. In such case, the administration of IDS in cloud becomes the responsibility of cloud provider. Although the administrator of cloud IDS should be the user and not the provider of cloud services. In the paper [1], Roschke and Cheng et al. have proposed an integration solution for central IDS management that can combine and integrate various renowned IDS sensors output reports on a single interface. The intrusion detection message exchange format (IDMEF) standard has been used for communication between different IDS sensors. The authors have suggested the deployment of IDS sensors on separate cloud layers like application layer, system layer and platform layer. Alerts generated are sent to "Event Gatherer" program. Event gatherer receives and convert alert messages in IDMEF standard and stores in event data base repository with the help of Sender, Receiver and Handler plug-ins. The analysis component analyzes complex attacks and presents it to user through IDS management system. The authors have proposed an effective cloud IDS management architecture, which could be monitored and administered by the cloud user. They have provided a central IDS management system based on different sensors using IDMEF standard for communication and monitored by cloud user.

IV. SECURITY ISSUES IN CLOUD COMPUTING

Security threats can be categorized as follow [4];

A. Cloud data confidentiality issue:

Confidentiality of data over cloud is one of the glaring security concerns. Encryption of data can be done with the traditional techniques. However, encrypted data can be secured from a malicious user but the privacy of data even from the administrator of data at service providers end could not be hidden. Searching and indexing on encrypted data remains a point of concern in that case. Above mentioned cloud security issues are a few and dynamicity of cloud architecture are facing new challenges with rapid implementation of new service paradigm.

B. Network and host based attacks on remote Server:

Host and network intrusion attacks on remote hypervisors are a major security concern, as cloud vendors use virtual machine technology. DOS and DDOS attacks are launched to deny service availability to end users.

C. Cloud security auditing:

Cloud auditing is a difficult task to check compliance of all the security policies by the vendor. Cloud service provider has the control of sensitive user data and processes, so an automated or third party auditing mechanism for data integrity check and forensic analysis is needed. Privacy of data from third party auditor is another concern of cloud security.

D. Lack of data interoperability standards:

It results into cloud user data lock-in state. If a cloud user wants to shift to other service provider due to certain reasons it would not be able to do so, as cloud user's data and application may not be compatible with other vendor's data storage format or platform. Security and confidentiality of data would be in the hands of cloud service provider and cloud user would be dependent on a single service provider.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 6, June 2015

V.CLOUD INTRUSION DETECTION SYSTEM SERVICE(CIDSS)

Developing IDS mechanism in the Cloud environment is highly motivated for both Cloud users and Cloud providers. There are some factors which instruct user for this tendency. Apart from the normal features which are obtained when using a service provided by a Cloud such as fast access to best business applications, eliminating the rule of trained new personnel, or licensing new software, some aspect of IDS in Cloud would be tempting for this migration.
Accessing to Network-based IDS on the Cloud to protect a network gives the possibility of exploiting different type of IDS detection methods on a single segment based on user demands almost instantly. It gives the illusion of a Network-based IDS which try to protect all segments of a network which are communicating over the internet with each other. It uses dedicated resources on the cloud for IDS functionalities which are isolated from any host on user network.

A. Cloud Intrusion Detection Service Architecture:

We introduce a Cloud Intrusion Detection System Service (CIDSS) to overcome the critical challenge of keeping the client secure from cyber attacks. It is designed based on software as a service model for security of any Cloud based user. The CIDSS is composed of three components:

1) Intrusion Detection Service Agent
2) Cloud Computer Service Component (CCSC)
3) Intrusion Detection Service Component (IDSC).

1) Intrusion Detection Service Agent: The agent is a light weight, single purpose equipment – dedicated hardware or software - integrated inside the user network to collect necessary information. According to the location of the agent, the CIDSS could protect a segment of the network or the whole network. Agents are grouped based on rule-sets and thresholds or network traffic to improve the service efficiency and protection flexibility.

2) Cloud Computer Service Component: The CCSC collects messages from agents. It formats all messages and send them to the IDSC according to grouping constrains defined for messages. A secure connection path should be established by CCSC to absorb information gathered by agents otherwise the system behavior could be tainted by external intrusion.

3) Intrusion Detection Service Component: The IDSC is responsible for intrusion detection. There are four sub components playing major rule in IDSC.

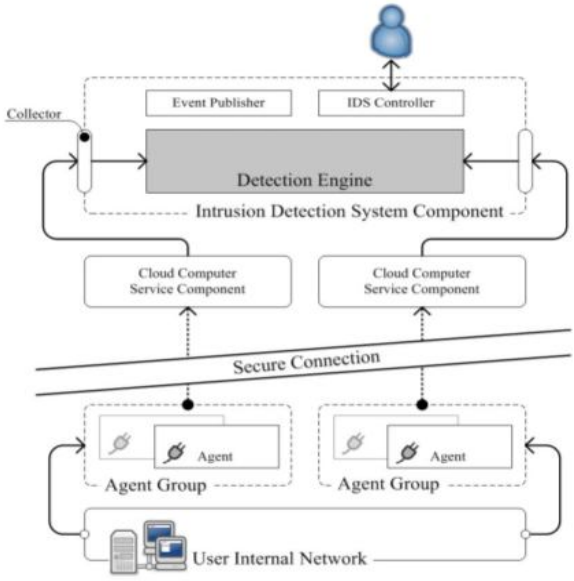

Fig 4: Cloud Intrusion Detection System Architecture

. Collector: Collector is responsible for reading all information received by CCSC, selecting items of interest, and forwarding them to the appropriate analysis engine.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 6, June 2015

• **Analysis Engine/Detection Engine:** Analysis engine is a sophisticated decision and pattern matching mechanism. It analysis data came from the collector and matches it to known patterns of activity stored in the signature database. It identifies malicious behavior and generates alerts through the event publisher.
• **Event Publisher:** It is a standardized interface to provide a unified view of result report for users as the analysis engine could be an independent process which can be implemented using any IDS, e.g. Snort. Intrusion Detection Message Exchange Format (IDMEF) [14] would be used as standard representation of IDS alerts.
• **IDS Controller:** It is responsible for remote configuration and control of all agent groups. It has access to IDSC configuration for fine tuning its operation based on user demands.

B. Cloud Intrusion Detection Service Requirements:
There are a number of challenges that must be considered when implementing CIDSS. Some of these challenges are inherent in what an IDS does and others are simply part of the way that a network is configured. Normally, the construction of a network would include switches and routers. The collision domains which is defined as the extend to which a signal can be propagated inside a network would be separated by these devices [15]. An agent needs to be able to look at all of the traffic on a protected network segment even on different collision domains. There are a number of ways to achieve this goal including: adding a hub inline at a choke point, connecting a network Test Access Port (TAP) to allow passive access to all the traffics, using Switched Port Analyzer (SPAN) port on the switch being monitored.
High-speed networks are a problem for any IDS solutions. A normal IDS would do the processing of every packets on the network. The speed of the network could increase ahead of the processing power available to pull every packet off the wire and process it [16].CIDSS mostly targets the Small and Medium Businesses (SMB) as users and they do not typically have very high networking bandwidth as soon as they become available. Anyhow, agent grouping would provide the flexibility to cope with this issue. Three basic rules are applied when grouping the agents, listed in Table 1.According to the rules, the agent utilized to protect whole user network from internet attacked should be in a separate group while the agents deployed to protect two small segments of user network with similar rule-sets could be in one group if their traffics are negligible.

Table 1: Agent Grouping Basic Rules

Network Segment Configuration	*Group*
Segments with different rule-set	Separate Group
Segments with similar rule-set	Similar Group
Segments with high traffics	Separate Group

The security of agents is a preliminary factor while implementing and embedding one inside the user network. They are operating in stealth mode and a distinct connection form user network internet connection would be employed for communication with the cloud. Even though it is not considered as a requirement for agents operation but single purpose internet connection could enforce more security as the respective firewall could be configure more strictly for a single service.

C. Capturing Interested Packets:
Agent should do the early filtering to reduce the load on the Analysis engine and on the overall system, as the process of sending packets from the agent to the CCSC can often be avoided. Considering an internet connection with n Mbps bandwidth, at most a channel with 2n Mbps (upstream plus downstream) bandwidth should be sniffed by an agent. For almost real time IDS, the captured packets should be discarded to 50% of total packets in the worst case. Otherwise, detection delay should be introduced. Some unique feature of network traffics can be exploited to this end. Refer to Figure 5 for internal structure of agent. Since a fraction of packets is only subject to header analysis, this could be performed by agent and only packets prone to intrusion effects would be transferred [17]. Packets with no payload which do not show any indication of intrusion are simply discarded.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 6, June 2015

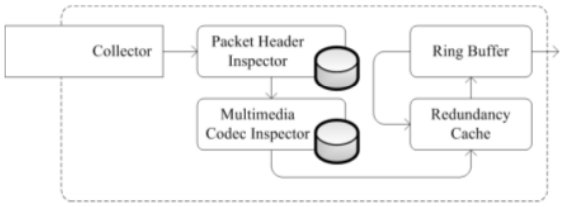

Fig 5: Agent Internal Structure

According to the researches 30% of all incoming traffic and 60% of all outgoing traffic is redundant by measures[18]. Therefore, agent and the respective CCSC should cooperate to eliminate the redundant data in packets. Caches are place at both agent and CCSC, which are used to hold the most recent packets. The cache at agent end would replace the redundant data inside the packet into light weight tokens and passes the encoded, smaller packet to CCSC, where the original packet would be reconstructed. The technique developed by Manber for finding similar files in a huge file system utilizing Robin fingerprint would be adopted to implement a network traffic tunable duplication detection strategy [19]. Packet losses should be prevented in order to preserve the required consistency between caches.

• Multimedia data which constitutes most of the traffic in the internet communications could be inspected by agent. Multimedia traffic can be uniquely identified by certain characteristics, e.g. the header in an AVI file, and once the traffic has been recognized the remaining packets for the stream containing the multimedia content can bypass the analysis engine [20].

• Ring buffer is a method for adapting the packet stream speed in a way that prevent packet loss [21]. The latency introduced by ring buffers is not particularly important for a CIDSS operation where the latency does only affect detection delay and no packet forwarding happens as no prevention is intended by CIDSS. The ring buffer should tune the performance of redundancy cache. In the best case it would be disabled if the detection latency is negligible.

D. Secure Connection and Group Management:

As the CIDSS intends to protect the user network from the cyber attacks, the agent should sniff all internet inbound and outbound traffics. A whole user network can be protected by assigning an agent group. Similarly, different network segments of a user network which are connected to each other using a VPN over the internet can be protected by assigning a single agent group for all segments. Therefore, independent to the network structure, the user network can be protected against cyber attacks using a central IDS in a cloud.All of the agents in a single agent group would communicate with a single instance of CCSC. Therefore, similar analysis engine an ultimately same rule-sets would be applied for all agents in an agent group.

VI. SNORT AS IDS

Snort is an open source network intrusion detection and prevention system (www.snort.org). It can analyze real-time traffic analysis and data flow in network. It is able to detect different type of attack. It checks packet against rule written by user. Rules in Snort can be written in any language. Rules can be easily read and modify. If pattern matches then attack can be easily found but when a new attack comes then system fails. To overcome this limitation we use snort to analyzing the real-time traffic. Whenever any packet comes into network then snort checks the behavior of network [4]. Snort has some common aspects

• **A packet sniffer:** A program will capture and display packets from the network on the console.
• **Packet logger:** Log data in text file and log packets to the disk.
• **NIDS:** Network intrusion detection system (NIDS) is an intrusion detection system which tries to detect malicious into computers by monitoring network traffic [4].

A. Components of SNORT:

• **Packet decoder:** It collects packet from network interfaces and then send to be preprocessor or sent to the detection engine.
• **Preprocessors:** It works with snort to modify or arrange the packet before detection engine to apply some operation on packet if packet is corrupted. It matches the whole string, and re- arranges the string and IDS can detect the string.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 6, June 2015

Preprocessor perform a task i.e. defragmentation. Because sometimes intruder break the signature into two parts and send them in two packets.

• **The Detection Engine:** The main task of the detection engine is to find out intrusion activity presents in packet with the help of snort rules and if we found the intrusion then apply rule on it otherwise it drops the packet. To detect the packet, it takes different time.

• **Logging and Alerting System:** Whenever detection engine finds in the packet then it might generate an alert or used to log file.

• **Output Modules:** Whenever logging and alerting system of Snort generates alert and log file then Output modules save that output and it also control the different output due to logging and alerting system.

The Architecture of Snort can be seen in figure-7 below where we defined how snort works.

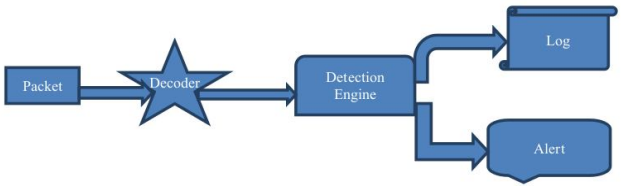

Fig 7: Snort Architecture

B. SNORT IDS in Cloud Environment:

Implementation of Snort IDS in cloud environment can be seen in Fig.8 below. The goal is deal with attacks like pretense attacks (where threats pose as legitimate users) and Network based attacks. Snort IDS also summarizes the intensive network IDS alerts by sending summary reports to the administrator of the cloud. In which we will use the virtualization environment (such as VM 1, VM 2, and VM 3) and snort IDS which is connected to each virtual network.

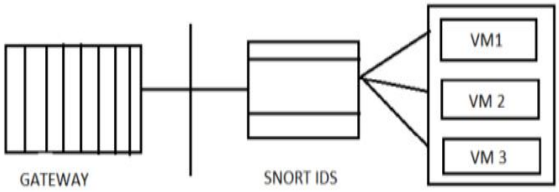

Fig 8: Snort IDS in cloud environment

VII. PROPOSED WORK

There are several ways for the attackers to attack the target system and then taking advantage of the known vulnerabilities of computer systems. In fact, such attack leads to loss and disclosure of sensitive information and data stored in the computer. However, the IDS usually is placed in the layer which is after the firewall, what has been termed as defense in-depth strategy. In this paper, we propose a new way of protecting data and resources in the Cloud computing environment. It is based on the rational implementation of intrusion detection system (IDS) over the Cloud computing infrastructure. We focused on one layer of the Cloud computing which is known as Infrastructure as a service (Iaas).

- Terminate the user session that is being used for the attack
- Block access to the target (or possibly other likely targets) from the offending user account, IP address, or other attacker attribute
- Block all access to the targeted host, service, application, or other resource.

The integrated model uses signature matching with normal traffic profiling to enhance attack detection. Furthermore, we propose to deploy our IDS in the virtual machine itself as well as the virtual network in order to monitor the activities of the system in addition of monitoring the packet traffic in the network to filter

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 6, June 2015

the malicious packets coming from untrusted sources (see Figure 9). The fact is that in the Cloud computing most of the resources will be stored and accessed on the remote servers. However, the consumers do not have to worry about the maintenance and the upgrading of the software and hardware. But, the issue is when there is a flow of the packets from one source to destination; the security in terms of data integrity will not be accurate as we have the SNORT IDS placed in specific location in the NIDS. Figure 10 demonstrates the close view of our proposed method to protect the data and resources in the Cloud.

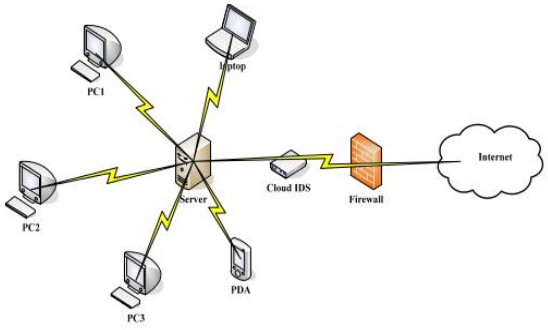

Fig 9: Proposed Snort IDS

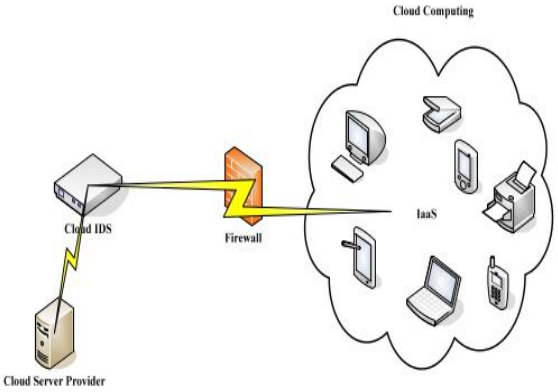

Fig 10: Conceptual view of the Snort IDS location

VIII. CONCLUSION & FUTURE WORK

In this paper we introduce IDS as a Service in a cloud to protect user network. It exploits some characteristics in network traffics that make it possible to extract the required data from the user network for evaluation. This architecture is intended to be scalable by allowing users to tab into different type of IDSCs simultaneously to combine the features of different product for more reliable IDS solution. Different segments of the user network on remote settings could be monitored by same infrastructure which results in ease of deployment of IDS solutions in dynamic environments. The concept is proved to be practical in local network by implementing a simplified version of the proposed architecture. An interesting future topic is the implementation of the fully functional agent on the real internet testbed and cloud infrastructure. In this paper we have work for cloud computing environment on intrusion detection using Snort. Next step will be implementing Snort IDS in cloud environment and new rules in the snort to enhancing the level of security in the cloud environment and analyzing the snort log file, to see that it properly alert the message in log file. So that administrator can take further security decisions related to attacks.

REFERENCES

[1] S. Roschke, F. Cheng, and C. Meinel, "Intrusion detection in the cloud," in 2009 Eighth IEEE International Conference on Dependable, Autonomic and Secure Computing. IEEE,2009, pp. 729–734.
[2] R. Buyya, J. Broberg, and A. Goscinski, Cloud Computing Principles and Paradigms. Wiley, 2011, vol. 81.
[3] P. Mell and T. Grance, "The nist definition of cloud computing," National Institute of Standards and Technology,vol. 53, no. 6, 2009.
[4] S. Subashini and V. Kavitha, "A survey on security issues in service delivery models of cloud computing," Journal of Network and Computer Applications, vol. 34, no. 1, pp. 1–11, 2011.
[5] Sebastian Roschke, Feng Cheng, Christoph Meinel," Intrusion Detection in the Cloud", Eighth IEEE International Conference on Dependable, Autonomic and Secure Computing, 2009.
[6] H. Debar, D. Curry, and B. Feinstein, "The intrusion detection message exchange format (idmef)," 2007.
[7] G. Tomsho, Guide to Networking Essentials. Course Technology Ptr, 2011.
[8] Network-Based Intrusion Detection Systems in the Small/Midsize Business. [Online]. Available: http://danielowen.com/NIDS.
[9] I Charitakis, K. Anagnostakis, and E. Markatos, "An active traffic splitter architecture for intrusion detection," in Modeling, Analysis and Simulation of Computer Telecommunications Systems, 2003. MASCOTS 2003. 11th IEEE/ACM International Symposium on. IEEE, 2003, pp. 238–241.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 6, June 2015

[10] N. Spring and D. Wetherall, "A protocol-independent technique for eliminating redundant network traffic," ACM SIGCOMM Computer Communication Review, vol. 30, no.4, pp. 87–95, 2000.
[11] U. Manber et al., "Finding similar files in a large file system," in Proceedings of the USENIX winter 1994 technical conference. San Fransisco, CA, USA, 1994, pp. 1–10.
[12] O. Marques and P. Baillargeon, "A multimedia traffic classification scheme for intrusion detection systems," in Information Technology and Applications, 2005. ICITA 2005. Third International Conference on, vol. 2. IEEE, 2005,pp. 496–501.
[13] Lossless Gigabit Remote Packet Capture With Linux[Online].Available:http://staff.washington.edu/corey/gulp/315
[14] Sousa, F. R. C.; Moreira, L. O.; Machado, J. C. ComputaçãoemNuvem:Conceitos, Tecnologias, Aplicações e Desafios. Ercemapi 2009: Edufpi, pp 1-26, 2009.
[15] NIST(NationalInstituteofStandardsandTechnology)http://csrc.nist.gov/publications/nistpubs800145/SP800- 145.pdf
[16] Sebastian Roschke, Feng Cheng, ChristophMeinel (2009), Intrusion Detection in the Cloud", Eighth IEEE International Conference on Dependable, Autonomic and Secure Computing.
[17] S N Dhage, B BMeshram, R Rawat (2011), Intrusion Detection System in Cloud Computing Environment", "International Conference and Workshop on Emerging Trends in Technology TCET, Mumbai, India.
[18] P. Jain, D. Rane, and S. Patidar, "A Survey and Analysis of Cloud Model-Based Security for Computing Secure Cloud Bursting and Aggregation in Renal Environment", IEEE 2011 World Congress on Information and Communication Technologies, pp. 456-461, 2011.
[19] Z. Mahmood, "Cloud Computing: Characteristics and Deployment Approaches", 11th IEEE International Conference on Computer and Information Technology, pp. 121-126, 2011.
[20] M. Jensen, N. Gruschka, L. L. Iacono, and G. Horst, "On Technical Security Issues in Cloud Computing", 2009 IEEE International Conference on Cloud Computing, pp. 109-116, 2009.
[21] R. Wu, G.-joon Ahnl, and H. Hul, "Information Flow Control in Cloud Computing", IEEE Collaborative Computing: Networking, Applications and Worksharing (CollaborateCom) , pp. 1-7,2010.

BIOGRAPHY

Namita Parati is working as Assistant Professor at Bhoj Reddy Engineering College for Women, Hyderabad, INDIA. She has received B.E, M.Tech Degree in Computer Science and Engineering. Her main research interest includes intrusion detection using hybrid network.

Sumaltha Potteti is working as Assistant Professor at Bhoj Reddy Engineering College for Women, Hyderabad, INDIA. She has received B.Tech, M.Tech Degree in Computer Science and Engineering. Her main research interest includes Cloud computing and intrusion detection.