International Journal of Scientific Research in Computer Science and Engineering
Vol.6, Issue.3, pp.13-17 , June (2018)

Research Paper

E-ISSN: 2320-7639

An Integrated approach for effective Intrusion Detection with Elasticsearch

Piyush Pareta [1*], Manish Rai[2], Mohit Gangwar[3]

Department of Computer Science and Engineering. RKDF College of Engineering, Bhopal, India
Department of Computer Science and Engineering. RKDF College of Engineering, Bhopal, India
Department of Computer Science and Engineering. RKDF College of Engineering, Bhopal, India

Available online at: www.isroset.org

Received: 03/Jun/2018, Revised: 11/Jun/2018, Accepted: 21/Jun/2018, Online: 30/Jun/ 2018

***Abstract*—** Cloud computing environments are easy targets for intruders and pose new risks and threats to an organization because of their service and operational models, the underlying technologies, and their distributed nature that relies on the network for its working. However, IDSs are among the efficient security mechanisms that can handle most of the threats of cloud computing. In spite this, several deficiencies of current IDSs technologies and solutions hinder their adoption in a cloud. The proposed work focuses on developing improved IDS that provides an integrated approach of both techniques i.e. anomaly based as well as knowledge based whether implement on network or host based IDS for cloud computing to detect masquerade, host, and network attacks and provides efficient deployments to detect DDoS attacks. The work comprises of integration of two powerful open source tool Suricata and Snort together with the proposed DDoS detection rule make the working of IDS more effective and high alarm rate generating Hybrid IDS.

Keywords— Cloud Security, Distributed Denial of Service Attack (DDoS), Intrusion Detection System (IDS), Suricata, Snort, Hybrid IDS.

I. INTRODUCTION

In September 2011, the definition and specifications of cloud computing were standardized by the U.S. National Institute of Standards and Technology (NIST). The definition[1] of Cloud Computing introduced by the NIST is Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

Cloud computing has number of advantages like cost reduction of computation, resource sharing that may be software or hardware, time saving, etc. But still this type of computing mainly rely on network for its working and it is well known that there are number of vulnerabilities like hardware, software or protocol vulnerability in the network. This results in many security and privacy problem as the cloud data are present and accessed using various intermediate servers working in distributive environment. Security issues such as Confidentiality, Integrity, Authentication, Availability and Trust [6][8] are the major concern in this type of computing.

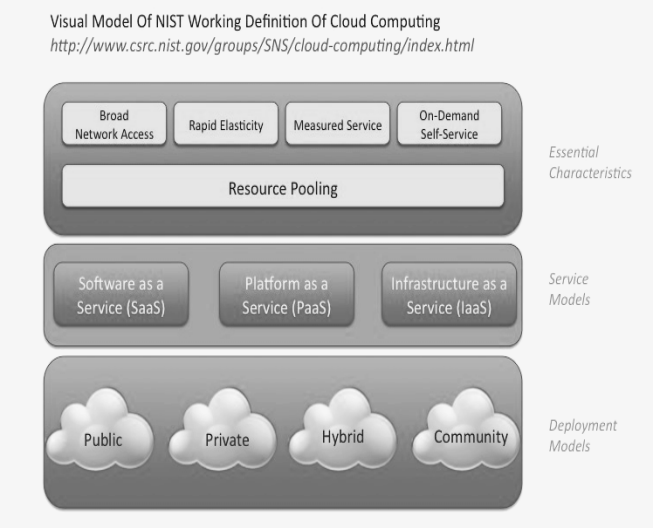


Fig.1 NIST visual model of cloud

1.1 DEPLOYMENT MODEL

Four basic deployment models have been identified for cloud architecture solutions are described below:

A Private cloud is owned or rented by an organization. The whole cloud resource is dedicated to that organization for its private use.

A Public cloud is owned by a service provider and its resources are sold to the public. End users can rent parts of the resources and can typically scale their resource consumption up (or down) to their requirements.

A Community cloud is similar to a private cloud, but where the cloud resource is shared among members of a closed community with similar interests. An example of a community cloud is the Media Cloud set up by Siemens IT Solutions and Services for the media industry and many others.

II. INTRUSION DETECTION SYSTEM

An intrusion detection system (IDS) is defined as the system that consists of any hardware or software application that is used for detecting unwanted behaviour that may occur in any network or any computer [2]. It monitors network as well as any system activities that may arise from any malicious activities or policy violations. Besides this intrusion detection system also generates various alarm in order to generated reports to a management station. It is mainly meant for detecting various Passive Attacks in any network. Intrusion detection system are implemented in variety of ways such as Host-Based IDS, Network based IDS, Hybrid IDS, etc.

2.1 Intrusion Detection Techniques

IDS are classified into three broad categories. These classifications are according to various approaches that are used to detect the abnormal behaviour. The detailed explanation of these is techniques are illustrated below:

Anomaly-based intrusion detection (ABID) systems flag as anomalous observed activities that that behave differently than the defined normal behaviour of the system. This system basically works by detecting the processes deviating from the expected behaviour or the nodes behaving abnormally. The other name used for ABID systems is behaviour-based intrusion detection. The process of modelling the normal behaviour of network nodes is known as training. The model additionally goes about as a profile of client or system conduct. A profile comprises of data about the arrangement of parameters which are particularly equipped to the target being checked. Testing for interruption includes analysis of the typical conduct model inferred throughout the preparation stage with the current model of the system or clients.

Knowledge based intrusion detection systems keep up an information base that holds marks or examples of well-known attacks and searches for these examples trying to discover them. KBID relies on knowledge about attacks so anything not explicitly recognized as an attack based on existing knowledge is declared as nonintrusive or acceptable. However, the case of an event or a series of events that has degraded the network performance can be identified as an unknown attack because it does not match the existing rules of attacks, and the system can update the knowledge base by adding a certain new rules or policies. Some KBID systems use expert systems for intrusion detection. An expert system maintains the knowledge of known attacks in a knowledge base in the form of a set of rules. Captured audit data from a monitoring network are translated into facts and then an inference engine uses these facts and rules present in the knowledge base to detect a malicious activity in the network.

III. RELATED WORK

In the paper [1] author proposed a multi-threaded cloud to IDS to handle intrusion and attacks in cloud computing. It focuses on various security threats and challenges about safety and reliability of cloud. In fact, 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. The proposed model uses integrated scheme of host based as well as network based IDS to create a scenario of multi-threaded cloud. But still it uses on signature based approach for detection of intruders.

The paper [2] defines various different attack types, which affect the availability, confidentiality and integrity of resources and services in cloud computing environment. Additionally, the paper also introduces related intrusion detection models to identify and prevent these types of attacks. It mainly gives the survey of various IDS model used together with different attacks they focus on for its working.

The paper [3] gives about an intrusion detection system that is used to detect the attacks efficiently by using anomaly based approach in IDS. It explain about importance to detect attacks at a beginning stage in order to reduce their impacts. This research work proposed a new approach called outlier detection where, the anomaly dataset is measured by the Neighbourhood Outlier Factor (NOF). Here, trained model consists of big datasets with distributed storage environment for improving the performance of Intrusion Detection system.

The paper[4], proposed encryption algorithm Hybrid DESCAST has been designed to provide the security of huge, volume of data sent through the media and the same will remain encrypted in the cloud sever. This cipher text will

be decrypted only when the same is required to be used by the authenticated user. Problems of individual DES and CAST Block Cipher Algorithm have been tackled by our proposed encryption algorithm. Complexity and Computation time for encryption and decryption for our proposed algorithm is higher than the individual DES and CAST algorithm. This paper is focused to provide security of data in cloud server, as well as for the data while transferring from client to cloud server and vice versa.

In paper [5], author proposed distributed IDS that handle large flow of data packets, analyze them and generate reports efficiently. Transparent reports are instantly send for information of cloud user and expert advice for cloud service provider's network mis-configurations through a third party IDS monitoring and advisory service.

The paper [6] explains about give an overall idea about Cloud computing, Intrusion, types of Intrusion Detection Systems and earlier works done on Intrusion Detection System. The key proposal of this paper is to give an overall idea for building a Hybrid Intrusion Detection System that would detect any type of intrusion into the cloud. This paper is the source of inspiration of my research work. It explains about hybrid concept and implemented using.Net framework as front end and SQL Server as back end to store the information. The Hybrid Intrusion Detection system has been deployed in Microsoft Azure Cloud environment. The Dynamic characteristic of Hybrid Intrusion Detection System is achieved by building a simple and informative User Interface.

The paper [7] proposed an effective and efficient model termed as the Integrated Intrusion Detection and Prevention System (IDPS) which combines both IDS and IPS in a single mechanism. Our mechanism also integrates two techniques namely, Anomaly Detection (AD) and Signature Detection (SD) that can work in cooperation to detect various numbers of attacks and stop them through the capability of IPS.

IV. PROBLEM DESCRIPTION

Cloud computing is the innovative technology that is making computation easy and user friendly with the use of Internet dramatically. Instead such advance innovation their exits certain problems that are present in such computing. The problem statement comprises of the securities issues in cloud computing. An existing typical method for detecting passive attacks in cloud computing is Intrusion Detection System. These intrusion detection systems are totally based on the schemes of anomaly based detection or knowledge based detection which are not very effective for intrusion detection. The problem that is found in cloud computing IDS are Lack of auditing and monitoring mechanism in anomaly based detection; In existing system there exist either independent anomaly based ids or independent knowledge based ids that are not much efficient model; Lack of prevention schemes as compared to detection schemes.

V. PROPOSED SCHEME

Proposed system contains a framework that has been structured to provide effective security to cloud by integrating and enhancing the current working schemes of Intrusion Detection System. The work consists of approaches that will deal with attacks like masquerade, DDoS attack in cloud. In the proposed model the three important functionality has been integrated in a single dedicated system that will we responsible for detection and identification of various Intruder present inside of the cloud computing. These three important functionalities are firstly, the Cloud Intrusion Dataset. Secondly, the signature based or knowledge based detection using digital signature and lastly, the anomaly based detection also known as Behaviour based approaches. The strategy improves the overall detection by integrating the last two strategies through a neural network. The first contribution is CDS i.e. Cloud intrusion data set that will be used to train and test any cloud IDS. It consists of both knowledge and behaviour based audit data and has real instances of host and network based attacks and masquerades. It will provide complete diverse audit parameters from several environments to evaluate the effectiveness of detection techniques. The second contribution is related to behaviour based detection. The third contribution is the signature based analysis techniques for treating the problem due to DDoS. In this thesis, my work is based on proposing a framework for IDS that must work efficiently and effectively in order to detect the intruders and their attacks. The main focus of the work was based on availability problem which is one of the security concern in cloud computing and is occurring due to Distributed Denial-of-Service (DDoS) attack. The key challenge, which we address, is to build a traffic information platform to collect, organize traffic information. In order to solve this problem Suricata tool were used. In order to make Intrusion Detection System more effective an open source IDS Snort is also enabled in the system. The rules were proposed and written in Linux scripting for detecting DDoS Attack more efficiently. Furthermore, the proposed work also helped in defensive scenario as it collect the details in its log file which can be further used for working of IDS.

VI. EXPERIMENT & RESULTS

The experiments were performed with number of scenarios. Firstly by simply using Ossec Tool, then Suricata followed with Snort and lastly with proposed mechanism will defining rule set in combination of Snort and Suricata. The cloud computing infrastructure is made by using Open Nebula cloud environment. In order to implement IDS with proposed rules for detecting DDoS Attack, Suricata and Snort is used. The cloud environment of Open Nebula is

created using Linux operating system where we installed KVM hypervisor above which Open Nebula is installed and nodes were created. The proposed model is implemented and test upon creating private cloud using Hadoop by creating only one cluster, one name node and only one data node. In order to provide Hadoop Environment for cloud a system with Ubuntu is used. Ubuntu can also be used on top of the Virtual Box if one does not want to configure in full real mode. After creating this setup a Kali or Ubuntu Linux is used for configuring Suricata and NMAP. Kali Linux is the Linux distribution for security research. Instead of them any other Linux Distribution can also be used. The tests were formed using Linux machine as a centralised dedicated workstation for intrusion detection. The network traffic was monitored using this system by running the proposed rule script in Suricata. In the same system the Snort open source tool is also configured and run in order for packet capturing and policy implementation of default white and black list file present in Snort. The system is connected in between the cloud service provider and the open outside network i.e. Internet. As soon this IDS start working it collects and show output of the data using Suricata, Snort and NMAP. Data collected for evaluation included network sniffing data from both inside and outside sniffers and audit event logs for security. This data was collected over the course of time. It collects data for several million connections for TCP services. It monitors all web traffic and other mailing services, various port services, etc.

The proposed system is mainly focused on one of the security issue that hinders Availability using Denial of Service Attacks. In this attack, the attacker makes the computing resources too busy that it denies the legitimate user to avail the desired services on time. In order for creation of such attack the TCP packets were send to the system again and again using ping command. The traffic was collected for about 2-3 days for evaluation purpose. The system is being tested for different entries in the log files. For getting the important information about the DDoS attack the proposed script is used and is further utilized for analysing of DDoS attack. The main information that was utilized for comparing and extracting were Source IP address, Destination IP address, Port Addresses for both source and destination and lastly the attack descripting comparing it with Snort and Suricata. The result that has been found out is that the proposed Hybrid approach score high well compared with either Anomaly or Behaviour based approaches of Intrusion Detection System. It is found out that the percentage of attack identification is high in our proposed work for DDoS attacks as compared with the existing solution. The graph showing the results is provided in next section Fig.2

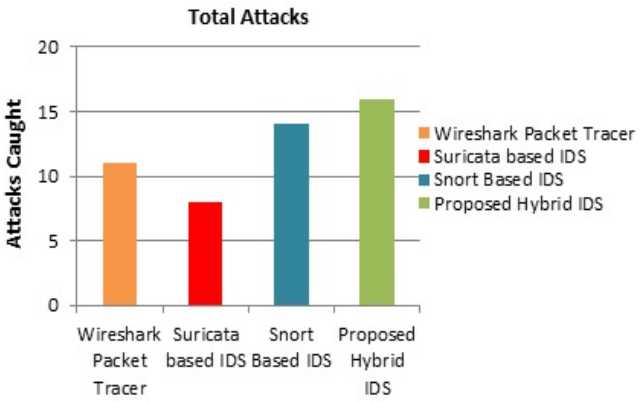
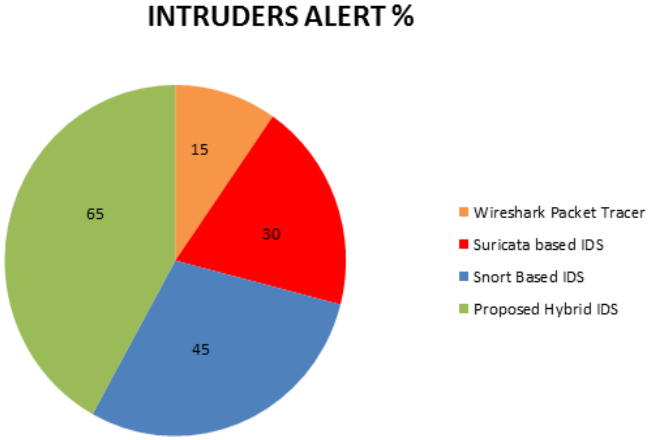


Fig.2 Comparison of various IDS



VII. CONCLUSION & WORK

Experiments were conducted for multiple scenarios and it is found that the proposed hybrid scheme is better as compared with only one kind of IDS deployment technique. The detail description of the tool Suricata and result are explained in the next section of the thesis. In this thesis, my work is based on proposing a framework for IDS that must work efficiently and effectively in order to detect the intruders and their attacks. The main focus of the work was based on availability problem which is one of the security concern in cloud computing and is occurring due to Distributed Denial-of-Service (DDoS) attack. The key challenge, which we address, is to build a traffic information platform to collect, organize traffic information. In order to solve this problem Suricata tool were used. In order to make Intrusion Detection System more effective an open source IDS Snort is also enabled in the system. The rules were proposed and written in Linux scripting for detecting DDoS Attack more efficiently. Furthermore, the proposed work also helped in defensive scenario as it collect the details in its log file which can be further used for working of IDS as knowledge based system. Some other security application like Topology

Manager, Network Reconfiguration Pool is also being used for during the system configuration. The conclusion that is found out is that it would be better and effective using both type of IDS configuration of Signature based and Knowledge based together instead using any single type of configuration. In order for implementing security in Cloud Computing, the Intrusion Detection System plays a vital role. Since cloud computing is network centric and hence more prone to cyber-attacks, it is very challenging to develop an effective Intrusion Detection System. The work shown in my work is effectively identifying the attackers and mainly for DDoS attacks. In future this work of creating and deploying Hybrid Approach of Intrusion Detection System can be implemented for other popular attacks related with Storage-as-a-Service of cloud such as SQL Injection, Buffer Overflow, etc. Even though the positive alert percentage is better as compared with existing system, the high false alarm rates continue be an another challenging problem with IDS.

REFERENCES

[1]. http://www.nist.gov/itl/cloud/upload/cloud-defv15.pdf
[2]. M. Madhavi, "*An Approach for Intrusion Detection System in Cloud Computing*", Elsevier, (2012).
[3]. U. Oktay, O.K. Sahingoz et al, "*Attack Types and Intrusion Detection System in Cloud Computing*", Elsevier, (2013)
[4]. Jabej J, Dr.B. Muthu Kumar, "*Intrusion Detection System (IDS): Anomaly Detection using Outlier Detection Approach*", Science Direct, 2015.
[5]. Nandita Sengupta, Ramya Chinnasamy "*Contriving Hybrid DESCAST Algorithm for Cloud Security*", Elsevier, 2015.
[6]. Anitha H M, P.Jayarekha "Security Challenges of Virtualization in Cloud Environment", IJCSE, 2018.
[7]. Praveen Kumar Rajendran, B. Muthukumar, G.Nagarajan, "*Hybrid Intrusion Detection System for Private Cloud: A Systematic Approach*", Elsevier, 2015
[8]. Hassen Mohammed Alsafi , Wafaa Mustafa Abduallah, "*IDPS: An Integrated Intrusion Handling Model for Cloud Computing Environment*", Elsevier, 2014
[9]. Amirreza Zarrabi, Alireza, "*Internet Intrusion Detection System Service in a Cloud*", 2012
[10]. Ahmed Patel, Mona Taghavi, et al, "*An intrusion detection and prevention system in cloud computing: A systematic review*", Elsevier , 2012
[11]. Seyed Mojtaba Hosseini Bamakan, et al., "*New Intrusion Detection Approach using PSO based Multiple Criteria Linear Programming*", Elsevier, 2015
[12]. Cong Wang, Qian Wang, and Kui Ren, "*Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing*", IEEE INFOCOM 2010.
[13]. Dimitrios Zissis, Dimitrios Lekkas "Addressing cloud computing security issues" Future Generation Computer Systems, Elsevier, (2012).
[14]. Kshetri,N. Privacy and security issues in cloud computing: The role of institutions and institutional evolution. Telecommunications Policy (2012)
[15]. http://www.nist.gov/itl/cloud/upload/cloud-defv15.pdf
[16]. K. Salah, J. M. Alcaraz-Calero,S. Zeadally, S. Almulla and M. Alzaabi "*Using Cloud Computing to Implement a Security Overlay Network*", IEEE, Security and Privacy, (2011).
[17]. N. Cao, Z. Yang, C. Wang, K. Ren, W. Lou, "*Privacy-preserving query over encrypted graph-structured data in cloud computing"*, in: IEEE International Conference on Distributed ComputingSystems, ICDCS'11, (2011), pp. 393–402
[18]. S. Marston et al. / *Decision Support Systems* 51 (2011) 176–189
[19]. Cong Wang, Qian Wang, and Kui Ren, "*Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing"*, IEEE INFOCOM (2010).
[20]. Shuai Zhang and Shufen Zhang "*Cloud Computing Research and Development Trend*", IEEE, Second International Conference on Future Networks, (2010)
[21]. J. Yao, S. Chen, S. Nepal, D. Levy, J. Zic, "*Truststore: making Amazon S3 trustworthy with services composition"*, in: Proceedings of the " 10th IEEE/ACM International Conference on Cluster, Cloud and Grid Computing, CCGRID'08, Melbourne, Australia, (2010), pp. 600–605
[22]. Goscinski, M. Brock / *Future Generation Computer Systems* 26 (2010) 947_970\
[23]. Groce, J. Katz, *"A new framework for efficient password-based authenticated key exchange"*, in: Proceedings of the 17th ACM Conference on Computer and Communications Security, CCS'10, Chicago, USA, (2010), pp. 516–525
[24]. R. Buyya, C.S. Yeo, S. Venugopal, J. Broberg, I. Brandic, "*Cloud computing and emerging it platforms: vision, hype, and reality for delivering computing as the 5th utility, Future Generation Computer Systems*" 25 (2009) 599–616.

Authors Profile

Mr. Piyush Pareta pursed Bachelor of Engineering from Rajiv Gandhi Proudyogiki Vishwavidyalaya bhopal in 2014. He is currently pursuing Master of Technology from Rajiv Gandhi Proudyogiki Vishwavidyalaya Bhopal. and currently working as Software Developer in Department of Information Technology.

