International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169
Volume: 4 Issue: 1 164 - 167

Intrusion Detection System in Cloud Computing: An Overview

Mrs. Vaishali B. Kosamkar
Dept. of Information Technology
Shah & Anchor Kutchhi Polytechnic,
Mumbai, India.
hodif@sakp.ac.in

***Abstract*:-**Cloud Computing represents both a technology for using computing infrastructures in a more efficient way, and a business model for selling computing resources and services. On the other hand, such complex and distributed architectures becomes an attractive target for intruders.Cloud computing offers great potential to improve productivity and reduce costs, but at the same time it possesses many new security risks. Intrusion Detection Systems (IDS) have been used widely to detect malicious behaviors in network communication and hosts. It is defined as a computer network system to collect information on a number of key points, and analyze this information to see whether there are violations of network security policy behavior and signs of attack. The traditional intrusion detection system is not flexible in providing security in cloud computing because of the distributed structure of cloud computing. This paper presents the survey of intrusion detection systems in cloud computingfor the effective identification of both known and unknown patterns of attacks, thereby helping the users to develop secure information systems.

Keywords*:-Intrusion Detection, Intrusion Detection System, Cloud, Cloud Computing,Attacks.*

*****

I. INTRODUCTION

Today, many organizations are moving their computing services towards the Cloud. This makes their computer processing available much more conveniently to users. However, it also brings new security threats and challenges about safety and reliability.Cloud computing is a "network of networks" over the internet, therefore chances of intrusion is more with the erudition of intruder's attacks. Cloud computing is distributed in nature, hence chances of intrusion is more. Analyzing various techniques of intrusion detection and prevention is essential. Different IDS techniques are used to counter malicious attacks in traditional networks. For Cloud computing, enormous network access rate, relinquishing the control of data & applications to service provider and distributed attacks vulnerability, an efficient, reliable and information transparent IDS is required.

II. INTRUSION AND INTRUSION DETECTION SYSTEM

An intrusion detection system (IDS) is a device or software application that monitors network or system activities for malicious activities or policy violations and produces reports to a Management Station that is illustrated in Figure 1 [3].

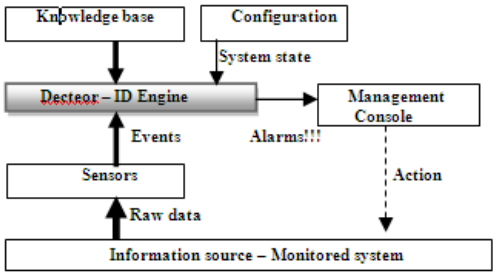

Figure 1.IDS Model [3]

There are several approaches on the implementation of an ID:

1.1 IDS based on Technique

Anomaly detection: This technique is based on the detection of traffic anomalies. The deviation of the monitored traffic from the normal profile is measured. Various different implementations of this technique have been proposed, based on the metrics used for measuring traffic profile deviation.
Misuse/Signature detection: This technique looks for patterns and signatures of already known attacks in the network traffic. A constantly updated database is usually used to store the signatures of known attacks. The way this technique deals with intrusion detection resembles the way that anti-virus software operates.

Hybrid detection: This technique uses combination of both Anomaly detection and Misuse detection.

1.2 IDS based on Data Target

Hosed based IDS (HBIDS): Its data come from the records of various host activities, including audit record of operation system, system logs, application programs information, and so on.

Network based IDS (NBIDS): Its data is mainly collected network generic stream going through network segments, such as: Internet packets.

Hybrid IDS (HIDS): It is combination of hosed based IDS and Network based IDS.

III. WORKING OF INTRUSION DETECTION SYSTEM

Denatious, and D.K John have presented a four step approach [14] for the generalized working of IDS

• Data collection: It involves collecting network traffic using particular software and thus helps to get the information about the traffic like types of packets, hosts and protocol details.

• Feature Selection: The collected data is substantially large because of the huge network traffic; we generate feature vectors that contain only necessary information. In network based intrusion detection, it can be IP header information, which consists of source and destination IP address, packet type, layer 4 protocol type and other flags.

• Analysis: The collected data is analyzed in this step to determine whether data is anomalous or not. Here we use various methods for detecting intrusions.

• Action: IDS alarm the system administrator that an attack has happened and it tells about the nature of the attack. IDS also participate in controlling the attacks by closing the network port or killing the processes.

IV. CLOUD COMPUTING

Cloud computing refers to the provision of computational resources on demand via a computer network (Figure 2). 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 the Internet.

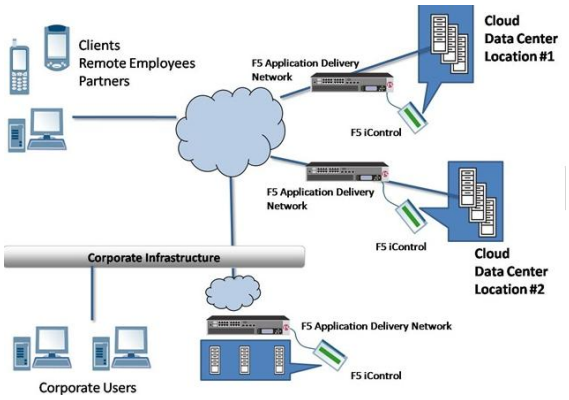

Figure 2.Cloud Computing[15]

4.1 Service models in cloud computing

There are various Cloud service delivery models that are developed, which can be divided into three layers [11] depending on the type of resources provided by the Cloud, distinct layers can be defined (see Figure 3).

1.2.1 Software as a Service (SaaS)

SaaS is a model for which the applications are hosted asservices to customers who access it via the Internet. When thesoftware is hosted off-site, the customer doesn't have tomaintain it or support it. On the other hand, it is out of thecustomer's hands when the hosting service decides to changeit.

1.2.2 Platform as a Service (PaaS)

PaaS on the other hand, delivers the cloud servicesdifferently. As the name suggests, PaaS supplies all theresources required to build applications and servicescompletely from the Internet, without having to download orinstall any kind of software.The services provided in PaaSmodel include application design, development, testing, deployment, hosting, team collaboration, web serviceintegration, database integration, and versioning.However, PaaS lacks the interoperability and portabilityamong different providers. In other words, if an application iscreated with one cloud provider and then the customerdecides to move to another provider, then she may not be ableto do so or it may require high prices for the application torun in the new provider's cloud. Google App Engine is anexample of PaaS clouds where users can create their ownapplications with either python or Java and deploy it onGoogle's cloud.

1.2.3 Infrastructure as a Service (IaaS)

Sometimes referred to as HaaS or Hardware as a Service , it isconsidered the next form of services available in cloudcomputing. Where SaaS and PaaS are providing applicationsto customers, IaaS doesn't. In the simplest form, IaaSprovides the organizations with hardware resources that canbe used for anything. The advantage is that instead of buyingservers, software, racks, and having to pay for the datacenterspace for them, the service provider rents those resources.And by renting resources we mean any resources than aperson can think of, including Server Space, Network Equipment, Memory, CPU Cycles, Storage Space, etc. Additionally, the infrastructure resources can be scaled up ordown based on the application resource needs.

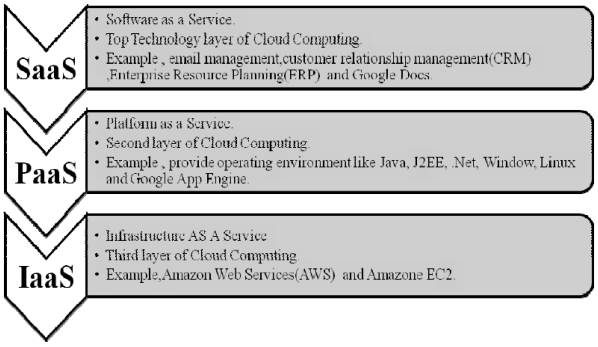

Figure 3.Layers in Cloud Computing [11]

4.2 Cloud attacks

We will focus on specific problems for various kinds of attacks in the cloud [10]:

4.2.1 Wrapping Attack

Whenever a user sends a request from virtual machine then this request received by a web server which generates a SOAP message which is exchanged between client and server and SOAP header contains the address of its destination. Wrapping attacks are performed during the translation of a soap message in the TLS (Transport Layer Service) and after that it can intrude in the cloud and can performs malicious attempts into the data.

4.2.2 Malware Injection Attack

In this the attacker can embeds the false commands, intrudes malicious code or can exchange the metadata into the

correctly running system and appears to be valid. Now he/she is able to modify the data, can change the functionality of the system and it force the legitimate user to wait for completion of the task which is not requested by the user.

4.2.3 Flooding Attack Problem

As in a cloud infrastructure, the servers are working in such a manner that they communicate with each other easily. So whenever the load of a single server comes at its extreme level then server can offload itself by transferring some of its work to the nearer servers. In flooding attack the attackers sends useless and not required requests to the server to make it busy and overloaded so that, the server forced to transfer its tasks to other servers.

4.2.4 Data Stealing Problem

Data stealing as the name implies to steal the data, user accounts encrypted keys, files and passwords by any ways.

4.2.5 Accounting Check Problem

Whenever a customer uses the cloud services then the duration in which he/she uses the service, and the amount of data he use or access, and number of CPU cycles per customer are all recorded. Therefore, based on these recorded information, the user has been charged and when an attacker sends the useless requests and data into the cloud to making the cloud engaged then it raise the consumption power of server, which charges the legitimate user who is unknown from the malicious services.

V. INTRUSION DETECTION SYSTEM IN CLOUD COMPUTING

As mentioned before, Intrusion detection is the process of monitoring the events occurring in a computer system or network and analyzing them for signs of intrusions, defined as attempts to compromise the confidentiality, integrity, availability, or to bypass the security mechanisms of a computer or network. Intrusions are caused by attackers accessing the systems from the Internet or by authorized users of the systems who attempt to gain additional privileges for which they are not authorized or by authorized users who misuse the privileges given to them. IDS are software or hardware products that automate this monitoring and analysis process. The Intrusion Detection Service (IDS) service increases a Cloud's security level by providing two methods of intrusion detection. First method is behavior-based method which dictates how to compare recent user actions to the usual behavior. The second approach is knowledge-based method that detects known trails left by attacks or certain sequences of actions from a user who might represent an attack. The audited data is sent to the IDS service core, which analyzes the behavior using artificial intelligence to detect deviations. This has two subsystems namely analyzer system and alert system.

VI. AN OVERVIEW OF INTRUSION DETECTION SYSTEM IN CLOUD COMPUTING

Reference [2] surveys the intrusion detection and prevention techniques and possible solutions in Host Based and Network Based Intrusion Detection System. It discusses DDoS attacks in Cloud environment. Different Intrusion Detection techniques are also discussed namely anomaly-based techniques and signature based techniques. It also surveys different approaches of Intrusion Prevention System.In Reference [4], a multi-threaded cloud IDS model is proposed which can be administered by a third party monitoring service for better optimized efficiency and transparency for the cloud user. RichaSondhiya et al., [5] propose a method that enables cloud computing system to achieve both effectiveness of using the system resource and strength of the security service without trade-off between them. In this paper, we propose a soft Computing technique such as MLP Algorithm for detecting the unknown intrusion in network intrusion detection in cloud computing environment.It also study the possible use of the neural networks learning capabilities to classify the intrusion data set. the proposed approach is to identify the unseen or unknown attach using neural network technique.PiyushYadav et al., [6] proposes the various security, privacy and trust issues and what the legal methodologies. The various issues are discussed that tells that cloud in spite of being very productive services has various security loopholes and vulnerabilities. Therefore, it is necessary for the users to know about all the terms and services and the legal aspects before going to cloud. It is necessary for the user as well as provider to be alert as attacker can do any innovative malicious activity at any time. So clouds cannot deplete if you are vigil.Should be drafted and adopted so that the problems can be overcome. Reference [7] proposed a system is to detect intrusions in the cloud computing using Behavior-based approach and knowledge-based approach. If first approach unable to detect the data, second approach again verifies the data and compare it with the signatures within the database. The proposed system will have very low false positive alarm. Aye Aye Thu [8] propose system plan to deploy a Honeypot in the IDPS architecture to ensure improve performance, it is desire to increase the level of security in the Cloud computing environment and decrease the threats to Cloud environments through concentrating on the problem of how data are stored in the Cloud. The propose system is effective and efficient model term as the integrated Intrusion Detection and Prevention System (IDPS) and Honeypot that can be used to guard an organization. This system also integrates two methods namely, Anomaly Detection (AD) and Signature Detection (SD) that can do in cooperation to detect various attacks and deny them through the ability of IPS. The goal of the paper is to detect internal attackers by Honeypot. Reference [9] introduces 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.

Hassen Mohammed Alsafi et al., [11] propose 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. The proposed 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.This paper also discussed different techniques of an intrusion detection system that has been used to counter malicious attacks in Cloud computing environment.Soumya Mathew et al., [12] focus on proposing deployment architecture of Intrusion Detection Systems in the Cloud. It discuss and list several existing threats for a Cloud infrastructure and are motivated to use Intrusion Detection Systems (IDS) and its management in the Cloud. We propose the deployment of integrated and layered IDS on cloud that designed to cover various attacks. This IDS integrates knowledge and behavior analysis to increases a cloud's security. The two intrusion detection techniques are distinct. But the deficiency of one technique will be complimented byother one. Layered IDS offers effective resource and log management.

VII. CONCLUSION

After studying the number of journals, white papers, cloud computing articles, I come to know that cloud computing is the largest buzz in the world of computer now a days. It gains popularity in almost every field like in industry and in educational systems. This paper gives the knowledge of cloud computing introduction, its concepts, models and services. It also gives knowledge of IDS and how IDS can be used for protecting cloud.The paper also discussed the comparison of different IDS proposed for protecting cloud.

The next step is to propose IDS model or a architecture which can detect and prevent the various threats, attacks and other security related issues which continuously depletes the efficiency and the productivity of the cloud.

REFERENCES

[1] Gudadhe, M.,Prasad,P., Wankhade,K. "A New Data Mining Based Network Intrusion Detection Model" Computer and Communication Technology (ICCCT), 2010 International Conference on Digital Object Identifier: 10.1109/ICCCT.2010.5640375 Publication Year: 2010, Page(s): 731 – 735.

[2] ItiRaghav,ShashiChhikara,NitashaHasteer "Intrusion Detection and Prevention in Cloud Environment: A Systematic Review" International Journal of Computer Applications (0975 – 8887) Volume 68– No.24, April 2013.

[3] MrsVaishali B Kosamkar, MrsSangita S Chaudhari "Data Mining Algorithms for Intrusion Detection System: An Overview". Proceedings published in International Journal of Computer Applications (IJCA) (0975 – 8887) 17-18 December 2012, ICRTITCS – 2012, TCSC, Mumbai, India.

[4] M.Madhavi "An Approach For Intrusion Detection System In Cloud Computing" International Journal of Computer Science and Information Technologies (IJCSIT), Vol. 3 (5) , 2012,5219 – 5222.

[5] RichaSondhiya, ManeeshShreevastav, Mahendra Mishra "To Improve Security in Cloud Computing with Intrusion detection system using Neural Network" International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-3, Issue-2, May 2013.

[6] PiyushYadav, Gaurav Gupta **"**Depleting Clouds.ASurvey on Security, Privacy, Accountability and Trust Issues in Cloud Computing" International Journal of Engineering Research & Technology (IJERT) Vol. 2 Issue 4, April - 2013 ISSN: 2278-0181.

[7] S.V. Narwane, S. L. Vaikol "Intrusion Detection System in Cloud Computing Environment" International Conference on Advances in Communication and Computing Technologies (ICACACT) 2012 Proceedings published by International Journal of Computer Applications (IJCA).

[8] Aye Aye Thu "Integrated Intrusion Detection and Prevention System with Honeypot on Cloud Computing Environment"International Journal of Computer Applications (0975 – 8887) Volume 67– No.4, April 2013.

[9] AmirrezaZarrabi, AlirezaZarrabi, "Internet Intrusion Detection System Service in a Cloud"IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 5, No 2, September 2012.ISSN (Online): 1694-0814.

[10] Kimmy," A Comparative Study Of Clouds In Cloud Computing" International Journal of Computer Science & Engineering Technology (IJCSET) ISSN: Vol. 4 No. 06Jun2013.

[11] Hassen Mohammed Alsafi ,Wafaa Mustafa Abduallah and Al-Sakib Khan Pathan "IDPS: An Integrated Intrusion Handling Model for Cloud Computing Environment".

[12] Soumya Mathew, Ann Preetha Jose , "Securing Cloud from Attacks based on Intrusion Detection System" International Journal of Advanced Research in Computer and Communication Engineering Vol. 1, Issue 10, December 2012.

[13] VaishaliKosamkar, Sangita S Chaudhari "Improved Intrusion Detection System using C4.5 Decision Tree and Support Vector Machine" International Journal of Computer Science and Information Technologies (IJCSIT) , Vol. 5 (2) , 2014, 1463-1467.

[14] Deepthy K Denatious and Anita John. "Survey on data mining techniques to enhance intrusion detection". In Computer Communication and Informatics (ICCCI), 2012 International Conference on Digital Object Identifier, p. 1–5. IEEE, 2012.

[15] https://en.wikipedia.org/wiki/Cloud_computing