Volume 4, Issue 11, November 2014 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

An Analysis on Cloud Security Mechanism

[1]Priyanka Ora*, [2]P. R. Pal
[1]PAHER University, Udaipur, Rajasthan, India
[2]Lakshmi Naryan College of Technology, MCA Department & University, Madhya Pradesh, India

Abstract*: *In this paper we give a short description on cloud computing ,its architecture which contains IaaS, PaaS and SaaS its deployment model Public,Private,Hybrid and Community cloud is described. Cloud computing has some severe issues(data availability,security,network) which affects its adaptation .Many security models are available among which we analyze the working and architecture of IDS. we describe IDS types, its methods and its specially designed cloud architecture(CIDSS).

Keywords: Cloud computing, IaaS, PaaS, SaaS, IDS, CIDSS.

I. INTRODUCTION

Cloud computing is a well known term in the field of software industry .It can be a type of utility based system in which virtual shared server provides resources to its customer as a pay on you go model .Although there is no proper definition of cloud but some of the researchers defined in their term as NIST defined cloud as "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"[1].

Cloud computing is a technology that uses the internet and central remote servers to maintain data and applications[2] . The National Institute of Standards and Technology (NIST) defined five essential characteristics of cloud computing ,namely: on-demand self-service, broad network access, resource pooling ,rapid elasticity or expansion and measured service[1].

If we define architectural design of cloud computing which contains three layers and on the basis of which it provides its services.

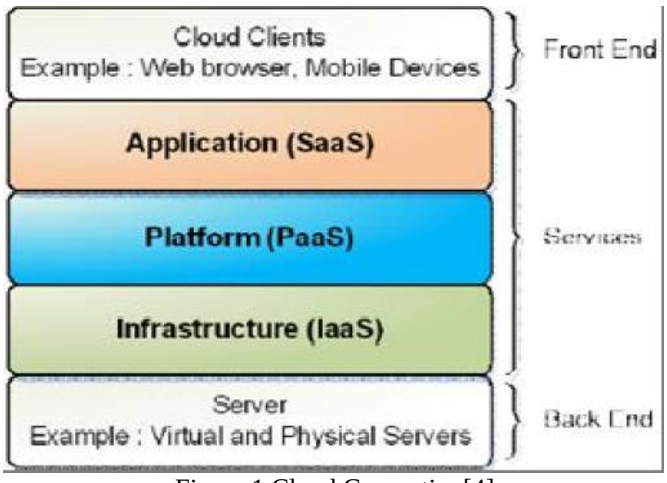

Figure 1 Cloud Computing[4]

The lowest layer Infrastructure as a service(IaaS) provides resources as (processor, memory storage). IaaS is able to provide from single server up to entire data center[5]. This layer is able to provide storage, processing and other computational resources so that consumer can utilize and able to deploy software and run their applications. Consumer has control over operating system but it cannot manage cloud infrastructure. Moving on above layer where PaaS is present, it provide platform to customers and the last most important SaaS which provides software to customers. This architecture follows bottom up approach where in at infrastructure level infrastructure is provided**.**

Cloud computing can be deployed on the basis of below model, these deployment model based on how resources are organized and make available to users.

a) Public Cloud : This cloud is used when access is available to all .Any user can access and utilize the service of cloud.

b) Private Cloud : This cloud only provides its services to authorized users. It is used by single organization and the customers who are having authority can log in and utilize private cloud services.

c) **Hybrid Cloud:** Using Private and Public cloud both in any environment comes under hybrid cloud. This cloud is combination of both public and private. It is related with cloud bursting . In Cloud bursting organization use their own computing infrastructure for normal usage, but access the cloud for high/peak load requirements[7].

d) **Community Cloud:** infrastructure is provisioned for exclusive use of a specific user community (organizations with common interest)[4].

Although cloud computing provides many facilities to its consumer but it also comes with some demerits like Data Integrity, availability, Security etc.

II. CLOUD ISSUES

Many customers faces the problem while using cloud computing .After studying all these issues we summarize these problem and make five categories of it. The categories are as follows:

a) **Security**
b) **Network**
c) **Data Access Control**
d) **Cloud Infrastructure**

The description of all these are as follows:

a) **Security:** This section covers all the issues related to cloud security which is faced by consumers. After analysis some major security issues are identified which are Lack of security standards, Compliance Risk, Lack of auditing, Lack of legal aspects ,Trust.

b) **Network:** The most important area of cloud computing is networking ,all the issues related with network connectivity , internet protocol are comes under this categories. Important issues related with network are: Internet Dependence (in which If customer migrate from one cloud to another then customer dependency on internet would increased ,in this case if due to some attack internet connection get damaged and cloud service become unavailable.) Internet protocol vulnerabilities, (Proper installation of network firewalls in which Lack of proper installation of firewall within cloud network make a gateway for hackers to access cloud environment easily.) all these issues comes under network category.

c) **Data Access Control:** The problem related with data loss ,data recovery, data availability comes under in this category.

d) **Cloud infrastructure:** It covers all problems related with cloud infrastructure like privileged insiders and tempered binaries.

III. ANALYSIS ON CLOUD SECURITY MECHANISM

The European Union Agency for network and information Security(ENISA) has done significant work in addressing many security issues related to the cloud [3].It provide information to consumer and helps them to understand and manage the risk while using cloud. Many Security methods has been evolved among which IDS is used at major level. The description of IDS and its security mechanism is as follows:

IV. INTRUSION DETECTION SYSTEM (IDS)

While using IaaS user information may be lost or attacked by massive users. It has been shown that attackers can easily get information regarding victim machines in the IaaS component of the cloud[8]. The attack is mainly targeted on data i.e. Data availability ,confidentiality ,integrity etc. Data are in trouble by sharing infrastructure. To overcome from this attack there is a solution implemented IDS (intruder detection system) .This IDS is used to detect many kinds of attack like warm, viruses, unauthorized login etc .It's functionality is defined as a network system which collect information on a number of key points and then observe this information to check whether there is violation of network security behavior .Basically this IDS was aimed to design a system which detect information attacks and provide specified response .It contain the following component:

a. Sensor**:** It is used to generate security attack.
b. Console to monitor events and inform the sensor.
c. Central Engine that records events logged by the sensors in a database and uses a system of rules to generate alerts from security events received[6].

On the basis of sources of information IDS is divided into two parts which are Network based Intrusion detection system and Host based intrusion detection system.

a. **Host Based Intrusion Detection System:**
It is the first type of IDS . Host-based IDSs operate on information collected from within an individual computer system[6].In this system monitors are arranged as inbound and outbound packets and alert the administrator to if any threat is detected.

b. **Network Based Intrusion Detection System**
This system mainly focuses on network connection of computers rather than individual hosting. It analyze each and every packets . Listening on a network segment or switch, one network-based IDS can monitor the

network traffic affecting multiple hosts that are connected to the network segment, thereby protecting those hosts[6].

V. INTRUSION DETECTION METHODS

a. Misuse Detection Method:

In this detection approach predefined patterns are matched with a event or set of event. This predefined pattern can be a known attack [6].This detection method is very effective , as it use signature database for detection they are limited up to that database if a new attack get evolve that cannot be detected.

b. Anomaly Detection Method:

This detection method analyze the abnormal behavior of host or network or of the system .This method is used to detect known and unknown attack. They create a profile based on past behavior of host or network This detection method observe any change in behavior of host or network, if the result comes positive then it produce alarm. Disadvantage of this method is many times it produce false alarm because network normal behavior may vary and if this behavior is not present in the database then it produce false alarm.

VI. CLOUD INTRUSION DETECTION SYSTEM SERVICE (CIDSS)

IDS also developed a model for cloud computing known as cloud intrusion detection system . As security is most important aspect in cloud computing .It is beneficial for both cloud users and cloud providers because both are having security problem in their domains.

Using network based IDS in cloud for security purpose gives the explosion of different type IDS threat detection methods on a single domain. Cloud Intrusion Detection System Service(CIDSS) is mainly introduced to overcome from cyber attack problem. It's designing is totally based on SaaS model of any cloud user .The architecture of CIDSS is based on three components which are Intrusion Detection Service agent ,Cloud computer service component ,Intrusion detection service component.

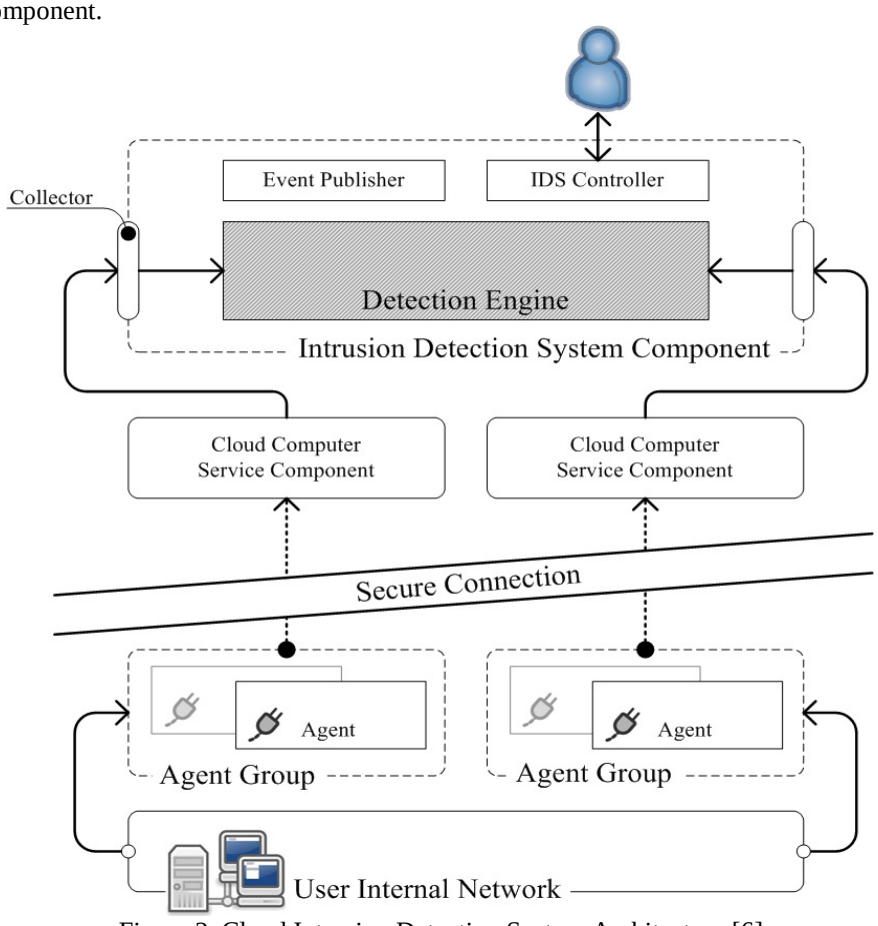

Figure 2 Cloud Intrusion Detection System Architecture [6]

working of each component are as follows:

Intrusion detection service agent: It is a light weight single purpose equipment. It is a dedicated hardware and software which is integrated inside the user for collection of information. According to the location of the agent, the CIDSS could protect a segment of the network or the whole network [6].

Cloud computer service component: It collect information from agent .Messages which are passed by agent come across with a secure connection path and then come to CCSC. This path is necessary because it absorbs information passed by agents to overcome from external intrusion . all the messages are formatted by CCSC and then send to service component.

Intrusion detection service component: It is the main domain of CIDSS because it detect abnormal behavior of information .It contains 4 domains

Collector: It is responsible for scanning the messages forwarded by CCSC .It select the item and then send to detection engine.

Engine: It receives the messages from collector and match it with signature database ,if it identifies abnormal behavior then it make alert through event publisher.

Event Publisher: It shows the output of the input. It generates report for all messages.

IDS Controller: It is the controller part for the whole CIDSS .It is having control over all agents. Its operation is based on user demand.

VII. CONCLUSION

Although cloud computing is the fastest growing technology in IT field. For improving its adaptation its defects must be resolved. There are many security architecture techniques are available which are trying to remove remedies from cloud. In this paper we through a light on Intrusion Detection System.IDS which has one domain for cloud computing known as cloud intrusion detection security service (CIDSS).although this concept is still evolving and many new methods are considered to be deploy in cloud so that up to some extent cloud issues can be solved.

REFERENCE

[1] Final Version of NIST Cloud Computing Definition Published. Available online: http://www.nist.gov/itl/csd/cloud-102511.cfm.

[2] http://www.wikinvest.com/concept/Cloud_Computing.

[3] Issa M.Khalil, Abdallah Khreishah, Muhammad Azeem "Cloud Computing Security : A Survey" *Computers* 2014, *3*, 1-35; doi:10.3390/computers3010001 (www.mdpi.com/journal/computers).

[4] Akash G Mohod, Satish J Alaspurkar ,"Analysis of IDS for cloud computing", *International Journal of Application or Innovation in Engineering & Management (IJAIEM) vol 2 Issue3 March 2013*.

[5] Axelsson, "Research in Intrusion-Detection Systems: A Survey", tech. report TR-98-17, Dept. Computer Eng. ,Chalmers Univ. of Technology, 1999.

[6] Amirreza Zarrabi, Alireza Zarrabi, "Internet Intrusion Detection System Service in a Cloud", International Journal of Computer Science Issues(IJCSI), Vol. 9, Issue 5, No 2, September 2012.

[7] Mohiuddin Ahmed, Abu Sina Md. Raju Chowdhury, Mustaq Ahmed, Md. Mahmudul Hasan Rafee, An Advanced Survey on Cloud Computing and State-of-the-art Research Issues, International Journal of Computer Science Issues(IJCSI), Vol. 9, Issue 1, No 1, January 2012.

[8] Tupakula, U.; Varadharajan, V.; Akku, N. Intrusion detection techniques for infrastructure as a service cloud. In Proceedings of the 2011 IEEE Ninth International Conference on Dependable, Autonomic and Secure Computing (DASC), Sydney, Australia, 12–14 Dec. 2011; pp. 744–751.

