Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 48 (2015) 325 – 329

Procedia Computer Science

International Conference on Intelligent Computing, Communication & Convergence

(ICCC-2015)

Conference Organized by Interscience Institute of Management and Technology,

Bhubaneswar, Odisha, India

Hybrid Intrusion Detection System for Private Cloud: A Systematic Approach

Praveen Kumar Rajendran[a*], B.Muthukumar[b], G.Nagarajan[c]

[a]*Department of Computer Science and Engineering, Sathyabama University, Chennai, India.*

[b]*Professor, Faculty of Computing, Sathyabama University, Chennai, India.*

[c]*Assistant Professor, Faculty of Electrical and Electronic Engineering, Sathyabama University, India.*

Abstract

Cloud computing is one of the latest and an emerging area in the Information and Technology (IT) sector, which has given a different dimension to the organizations. Performance and security aspects of private cloud and widely used public cloud are the major issues which have to be addressed in Cloud Computing. Intrusion is one such critical and important security problem for Cloud Computing. This paper will attempt to 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.

Keywords: Cloud computing, Types of cloud, Services of Cloud, Issues in Cloud, Intrusion, Hybrid Intrusion Detection System.

1. Cloud computing

The term Cloud computing is neither a new concept nor a new technology yet it is considered to be the new paradigm for hosting of service and delivery of service over Internet. Hacking, Intrusion, Data loss, Data theft, Data destruction is the major security issues of Internet [1]. The term Cloud computing came into picture, when Internet has got evolved. Cloud computing can also be termed as Internet Computing. In simple words the term Cloud computing can be defined as the practise of using the Internet for computing purpose. In Cloud computing applications, hardware, system software are delivered as service over the Internet [1].Internet is represented using cloud symbol in the network diagram, hence this type of computing has got cloud has its metaphor. The major advantage of the Cloud computing is, the resources can be utilized anywhere, anytime and also anything can be stored in the resource provided. The person who provides all these service are said to be Cloud Service Provider (CSP). All the computational resource may not be provided by a single Service Provider. The end user has to be depending upon on several service providers for complete computational requirement. Another major advantage for the organization is, the capital expenditure spent on building the organizational resource can be reduced dramatically, thus giving a path for the young entrepreneurs. In other point of view Cloud computing can be defined as general utilities that can be rented and released via Internet on

Peer-review under responsibility of scientific committee of International Conference on Computer, Communication and Convergence (ICCC 2015)
doi:10.1016/j.procs.2015.04.189

demand [2]. To add further about this point, all the resources that are required for computing purpose are given on demand, either as free service or paid service. Paid service of Cloud computing is often called as "Pay as you go manner". Since it works in an on demand fashion, the requirements of the user are delivered in a fast manner. In other words it can also be said as, service of readily available resources [3]. Cloud Computing can also be called as On Demand Computing. Another interesting fact about Cloud computing is that, Cloud computing is like an elephant, for those who see this elephant in front will say it as snake, for those whose see in the side will say it as wall etc, yet few are able to say it is an elephant. There is no proper definition or none has defined Cloud computing in a standardized manner. Everyone defines Cloud computing in their own perspective. And it was Google's CEO Eric Schmidt used the word cloud in the year 2006 to describe the business model of providing the computing resources across the Internet [2].

* Corresponding author. Tel.: +91-9597941892
E-mail address: praveenkumar558@gmail.com

2. Issues in Cloud computing

Even though Cloud computing has got many advantages, certain limitations makes the end user or the customer to think before implementing the cloud environment in their organization. Security is one of the important problems in all type of network, especially in Internet the security issues are more in number [8]. The data that is being stored in the cloud has to be highly secured; the data has to be secured from various vulnerabilities such as Hacking, Intrusions etc. The later part of the paper discusses about the Intrusion issues of cloud and a hybrid security model has been proposed to detect and prevent the intrusions. All the issues of Cloud computing is tabulated in the Table I. The level of issue in the below column denotes which issue has to be addressed very seriously with the priority number and solution as follows. Least Number indicates the highest priority

TABLE 1
Issues of Cloud Computing & Priority

Issue	Level of Issue	Priority	Solution
Network Connectivity	Medium	3	Reduction in the load of cloud
Data Loss	High	2	Distribution of Data to multiple location
Performance	Medium	4	Constant Internet Connection
Security	Very High	1	Establishing Security applications

3. Hybrid Intrusion Detection System

As discussed in the section 2 of this paper, intrusion is one of the important issues in all the networks, especially in Cloud computing where all the service are served via Internet. The term intrusion can be defined as the process of entering into a network without proper authentication. The two major type of Intrusion Detection technique are Anomaly based Intrusion Detection and Misuse base Intrusion Detection. The major drawback with anomaly based detection method is that, it cannot detect any new kind of attacks. It also cannot detect anything other than the predefined profile by the network administrator. Although these drawbacks are overcome in misuse detection method, misuse detection method cannot detect anything other than the predefined rules and also the system rules have to be updated constantly. Hence it is necessary to build an Intrusion Detection System that overcomes the drawbacks of both the intrusion detection system and also much more efficient than the existing system. Hybrid Intrusion Detection would be the solution for the above problem statement. Hybrid Intrusion Detection System can be defined as a system that has the combination of both anomaly detection method and misuse detection method. This Hybrid Intrusion Detection System can be implemented in the cloud based environment. The following section of the paper, the related works on the problem statement and the proposal of Hybrid Intrusion Detection System design have been discussed.

3.1 Related Works