International Journal of Computer and Communication Technology

Volume 6 | Issue 1 Article 3

January 2015

Enhanced Security In Cloud With Multi-Level Intrusion Detection System

M. KUZHALISAI
Computer Science And Engineering, Sri Sairam Engineering College, Chennai, India,
kuzhalisai6@gmail.com

G. GAYATHRI
Computer Science And Engineering, Sri Sairam Engineering College, Chennai, India,
gayu.govindaraj@gmail.com

Follow this and additional works at: https://www.interscience.in/ijcct

Recommended Citation
KUZHALISAI, M. and GAYATHRI, G. (2015) "Enhanced Security In Cloud With Multi-Level Intrusion Detection System," *International Journal of Computer and Communication Technology*: Vol. 6 : Iss. 1 , Article 3.
Available at: https://www.interscience.in/ijcct/vol6/iss1/3

This Article is brought to you for free and open access by Interscience Research Network. It has been accepted for inclusion in International Journal of Computer and Communication Technology by an authorized editor of Interscience Research Network. For more information, please contact sritampatnaik@gmail.com.

Enhanced Security In Cloud With Multi-Level Intrusion Detection System

[1]M.KUZHALISAI & [2]G.GAYATHRI

Computer Science And Engineering, Sri Sairam Engineering College, Chennai, India
E-mail : kuzhalisai6@gmail.com & gayu.govindaraj@gmail.com
Co-author : Mrs. MANIMALA G M.E

Abstract- Cloud computing is a new type of service which provides large scale computing resource to each customer. Cloud Computing Systems can be easily threatened by various cyber attacks, because most of Cloud computing system needs to contain some Intrusion Detection Systems (IDS) for protecting each Virtual Machine (VM) against threats. In this case, there exists a trade-off between the security level of the IDS and the system performance. If the IDS provide stronger security service using more rules or patterns, then it needs much more computing resources in proportion to the strength of security. So the amount of resources allocating for customers decreases. Another problem in Cloud Computing is that, huge amount of logs makes system administrators hard to analyse them. In this paper, we 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.

Keywords- *IDS, Cloud Computing, Intrusion Detection, Multi-level IDS, Cooperative IDS.*

I. INTRODUCTION

As Green IT has been issued, many companies have started to find ways to decrease IT cost and overcome economic recession. Cloud Computing Service is a new computing paradigm in which people only need to pay for use of services without cost of purchasing physical hardware. For this reason, Cloud Computing has been rapidly developed along with the trend of IT services. Cloud Computing can be defined as internet-based computing, whereby shared resources, software, and information are provided to companies and other devices on demand (1).

It is efficient and cost economical for consumers to use computing resources as much as they need or use services they want from Cloud Computing provider. Especially, Cloud Computing has been recentlymore spotlighted than other computing services because of its capacity of providing unlimited amount of resources. Moreover, consumers can use the services wherever Internet access is possible, so Cloud Computing is excellent in the aspect of accessibility. Cloud Computing systems have a lot of resources and private information, therefore they are easily threatened by attackers (2). Especially, System administrators potentially can become attackers. Therefore, Cloud Computing providers must protect the systems safely against both insiders and outsiders.

IDSs are one of the most popular devices for protecting Cloud Computing systems from various types of attack. Because an IDS observes the traffic from each VM and generates alert logs, it can manage Cloud Computing globally (3).

In this paper, we propose Multi-level IDS and log management method based on consumer behavior for applying IDS effectively to Cloud Computing system. The rest of the paper is organized as follows. In Chapter II we describe related works which are Cloud Computing and IDS. After that, we describe our proposal method in Chapter III. In Chapter IV, we evaluate our method. Finally, we conclude the paper in chapter in Chapter V.

II. RELATED WORK

A. Cloud Computing

Cloud Computing is a service that assigns virtualized resources picked from a large-scale resource pool, which consists of distributed computing resources in a Cloud Computing infra, to each consumer, Cloud Computing is a fused-type computing paradigm which includes Virtualization, Grid Computing , Utility Computing ,Server Based Computing (SBC) , and Network Computing , rather

than a entirely new type of computing technique (3)(4).

Table 1 shows the description of each computing technique. Cloud Computing provider can assign large-scale resources to each consumer using these techniques. Cloud Computing uses hypervisor in order to provide virtual OS for users by using unified resource. Hypervisor is software which enables several OSs to be executed in a host computer at the same time. Hypervisor also can map the virtualized, logical resources onto physical resource. Hypervisor is sometimes called Virtual Machine Monitor (VMM), and several OSs which are operated in a host computer are called the guest Oss. A Hypervisor provides isolated Virtual hardware platform for operating guest Oss. Therefore, guest Oss are operated in each VM environment instead of real hardware. A host OS which provides the image of original OS to guest OS, can assign various type of OS other than the type OS of host itself. Figure I conceptually describes the organization of hypervisor, host OS, and guest OS.

TABLE I. USER RISK LEVEL

Technology	Definition
Virtualization	The creation of a virtual version of something, such as an operating system, a server, a storage device or network resources
Grid Computing	The virtualized combinationof computing power from multiple domain getting high capacity of computing resource(distributed computing architecture)
Utility Computing	Consumers pay for computing resources as much as they use without buying them.
Server Based Computing (SBC)	Any applications and data exist in server. Clients access the server and utilize them using Servers' computing power.
Network Computing	It is similar to SBC, but client loads applications and data from Server and utilizes them using local computing power.

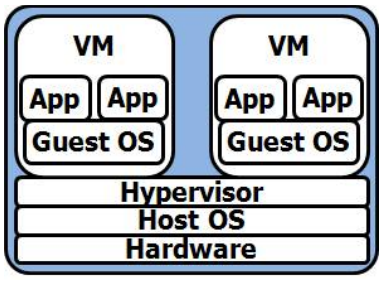

Figure2Proposal Multi-Level IDS Architecture

As figure 1, resource, instruction, and traffic of guest Oss in a hypervisor are mapped to a physical hardware through host OS.

Cloud Computing is a set which consists large amount and various types of computing resource, hypervisor, and data. Therefore Cloud Computing providers should own database centers to maintain their resources and data. Cloud Computing service is very attractive to consumers in the aspects of infinite scalability and payment cost in accordance with the amount of computing resource they used, however there also exists the risk that personal and private data are stored in uncontrolled place themselves (5). So Cloud Computing providers must protect their Cloud Computing system against all users include administrators and intruders (6).

B. IDS

IDS are software or hardware systems that automate the process of monitoring the events occurring in a computer system or network, analyzing them for signs of security problems (7). IDSs are one of widely used security technologies. An IDS alerts to system administrators, generate log about attack when it detects signature of accident according to host or network security policy. An IDS can be installedin a host or a network according to purpose.

An IDS detects attacks based on lots of rules each of which have unique signatures that describes attack patterns. So, the detection power of IDS increases when the number of rule grows. However the existence of more rules means that each incoming packet needs to be compared with more patterns. Thus large scale of rule causes system to become overloaded. In the Cloud Computing service, it isnecessary to allocate resources to users as much as possible. So it is important issue ot manage resources for reducing consumption of resources caused by implementing IDS.

In this paper, we propose the method for maintaining strength of security while minimizing waste of resources

III. MULTI-LEVEL IDS AND LO MANAGEMENT METHOD

We propose the Multi –level IDS method for implementing effective IDS in Cloud Computing system. Multi-level IDS method leads to effective resource usage by applying differentiated level of security strength to users based on the degree of anomaly. It is true that Cloud Computing is easy to be target of attach (9). For this reason, it is possible to judge all users and administrators as potential attacker and apply strong security policy to all traffic, but it is not efficient at all. So we propose the method that binds users to different security group in accordance with degree of anomaly, called anomaly level in this paper. Our proposal architecture is as shown in figure 2.

AAA is a management module for authentication, authorization, and accounting. When a user tries to access Cloud Computing system, then AAA checks the user's authentication information. If the user is authenticated, then AAA gets the user's anomaly level, which has been most recently generated, by inspecting the user's information in the database. After that, AAA chooses suitable IDS which have the security level correspondent to the user's anomaly level. Then AAA requests the host OS, in which the chosen IDS is installed, to assign guest OS image for the user.

Storage center stores private data of users. All users ' data is logically isolated. So nobody can access the data except owners of the data and users who have been given access right by owner. After a user is assigned a guest OS, the connection between the guest OS and data owned by the user in storage center is then established. Figure 3 shows this relationship.

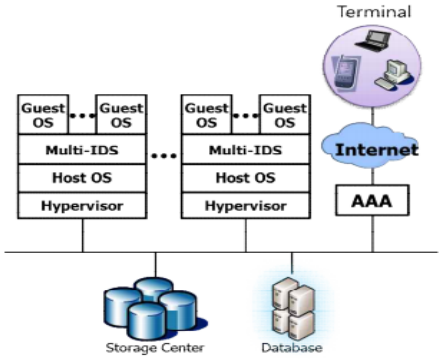

Figure 2. Proposal Multi-level IDS Architecture

In our paper, we divide security level in to three, such as High, Medium, and Low for effective IDS construction. High-level is a group which applies patterns of all known attacks and a portion of anomaly detection method when it needs, for providing strong security services. Medium-level is a group of middle grade which apply patterns of all known attacks to rules for providing comparatively strong security service. Finally, Low-level is a group for flexible resource management which apply patterns of chosen malicious attacks that occur with high frequency and that affect fatally to the system.

In Multi-level IDS scheme, an IDS consumes more resource when providing higher level security, because higher level security apply more rules than lower level. On the other hand, if an IDS provides lower level security policy, then the amount of resource usage is decreased although the detecting power of attacks also drops. The assignment of VM to a user is determined in accordance with security level. The grade of VM is proportional to user criteria of anomaly level. Anomaly levels of users are estimated by their behaviors during the usage of service based on saved user anomalylevel in system. For instance, when a user access Cloud Computing system first time, Multi-level IDS judges anomaly level of user using following matters: the user's IP coverage, vulnerable ports to attack, the number of ID/PW failure, and so on. The most important element for estimating anomaly level is how fatal it is. The rest of judgment criteria are possibility to attack success, possibility to attack occurrence, and OS on (1). Possibility to attack success is an experimental value which indicates the probability of success for an attack. Possibility to attack occurrence is a value based on the frequency of specific attack.

TABLE 2. USER RISK LEVEL

	Likelihood of incident scenario	Very Low	Low	Medium	High	Very High
Business Impact	Very Low	0	1	2	3	4
	Low	1	2	3	4	5
	Medium	2	3	4	5	6
	High	3	4	5	6	7
	Very High	4	5	6	7	8

Multi-level IDS defines the anomaly behaviors by risk level policy such as table-1. The risk levels assign risk points in proportion to risk of anomaly behavior. The criteria of behaviors for judging that some traffic is anomalous are described in table 3(2).

Cloud Computing security system evaluates user anomaly level according to assessment criteria in table 3. Multi-level IDS accumulates risk point to each user when they are against more than one rule in assessment rules. When a user is assigned a VM by the system first time, there is no data for determining which security level of IDS is suitable for the user, so a high-level IDS should be assigned to the user.

Since, first provisioning, the decision of which VM is to be assigned to the user may change according to anomaly level of the user, and a migration may occur. Migratio is a technique to move VM to other VM space (8). Cloud Computing system checks users' behaviors everyday and decreases 1 risk point if a user uses Cloud Computing service more than one hour and increases less than 3 risk points a day .

Anomalous activity traffic	Risk point
Attempt to administrator account without working time	8
Guest OS attempt to unauthorized memory space	7
The user set Network Interface Card to promiscuous mode	6
Traffic of a guest OS increases up to 500% than usual traffic	6
IP address of user terminal is changed during the usage Cloud service	6
Host OS manager attempts to access some guest OSs	5
An guest OS attempts to other guest OSs	5
Traffic of a guest OS increases up to 300% than usual traffic	4
Administrator access some host OSs without notice	4
Login failure for 5 times	3
Unlicensed IP coverage	3
Known-vulnerable port number	3
Undertaking malicious probes or scans	3
Non-updated Guest OS	3
Between guest OS connect session in the same host OS	2
Abnormal guest OS power-off	2
Traffic of a guest OS increases up to 150% than usual traffic	1

IV. ESTIMATION

In this paper, our method increases resource availability of Cloud Computing system and handle the potential threats by deploying Multi-level IDS and managing user logs per group according to anomaly level. We can suppose that VMs have equal quantity of resource, then host OS can assign less guest OS with IDS, because IDS use much resource.

The criteria of anomaly level for deciding security group with risk point is shown in table 4.

Table 4.CRITERIA FOR ANAMALY LEVEL

IDS group	Standard
High-Level IDS	More then 6
Medium-Level IDS	3-5
Low-Level IDS	0-2

On the other hands, we can assign more guest OS with Multi-level IDS, because the user classified as low-level group are judged that they are normal user. As a result low-level IDSs maintain little rules for managing effective resource, so it can assign more guest OS than high and medium-level. Our method also supports classifying the logs by anomaly level, so it makes the system administrator to analyze logs of the most suspected users first. Therefore our method provides high speed of detecting attacks.

V. CONCLUSION

Cloud Computing technology provides human to the advantages such as economical cost reduction and effective resource management, However, if security accidents occurs, ruinous economic damages are inevitable. The system is very effective for the varied applications. The type of IDS that is needed for the specified purpose can be adapted as per the needs . Also the data traffic in the cloud is minimized and security is enhanced .

ACKNOWLEDGMENT

It is a pleasure to express our heartfelt thanks to Prof. N. NITYANANDAM, Head of the Department, Computer Science and Engineering for his encouragement and valuable guidance. We express our heartfelt gratitude to our project coordinator Mrs.V.HEMA, Senior Lecturer, Computer Science and Engineering, for his guidance to our project .We express our gratitude and sincere thanks to our guide Mrs. MANIMALA G, Senior Lecturer, Computer Science and Engineering, for her invaluable suggestions and constant encouragement for successful completion of this project. Finally we wish to thank all the members of our college, staff, lab coordinators and technicians without whom, this project would not have been successful.

REFERENCES

[1] Wikipedia, http:// en.wikipedia.org/ wiki/ Cloud_computing

[2] Ensia, Cloud Computing Risk Assessment, Nov. 2009

[3] Roberto Di Pietro and Luigi V .Mancini, Intrusion Detection Systems,Springer, Jan 2008.

[4] JaeHyuk Jang, Cisco, Cloud Computing: Drive Business Paradigm Shift, 2010.

[5] Cloud Security Alliance, Security Guidance for Critical Areas Of Focus in Cloud Computing, Dec.2009.

[6] N. Gruschka and M.Jensen, "Attack Surface: A Taxonomy for Attacks on Cloud Services", IEEE 3rd International Conference on Cloud Computing, pp 276-279, 2010.

[7] Rebecca Nace and Peter Mell, NIST Special Publication on Intrusion Detection Systems, 16 Aug.2001

[8] Kento S, Hitoshi. S Satoshi. M, "A Model-based Algorithm for Optimizing I/O Intensive Applications in Cloud using VM-Based Migration", 9th IEEE? ACM International Symposium, Cluster Computing and Grid, 2009.

◈◈◈