IJDCST @October Issue- V-1, I-6, SW-90
ISSN-2320-7884 (Online)
ISSN-2321-0257 (Print)

Securing Cloud using Third Party Threaded IDS

Madagani Rajeswari, Madhu babu Janjanam

[1]**Student, Dept. of CSE, Vasireddy Venkatadri Institute of Technology, Guntur, AP**

[2]**Assistant Professor, Dept. of CSE, Vasireddy Venkatadri Institute of Technology, Guntur, AP**

Abstract: Cloud computing is universal, staying anywhere in the world user can access the Cloud Applications. Mainly Cloud computing will provide services to the users using Internet. Cloud storage services offer user-friendly, easily accessible and money-saving ways of storing and automatically backing up arbitrary data. These services are available on-demand on the Internet. A customer simply accesses the website of a cloud storage provider and rents storage space as necessary by selecting one of the provider's Packages. In this processing different types of attacks can be done in taking of resource from cloud computing. In recent years, this requires secure methods of preserving important data in order to prevent unrecoverable data loss, whilst constantly keeping up with increasing demands for storage space. In cloud network, attacks will be more when compare with other networks. This paper proposes a new multithreaded Network Intrusion Detection system that guards the virtual machines at the key network points. A new service multithreaded intrusion detection is added for the users of cloud infrastructure. The experimental results show the efficiency of multithreaded IDS over single threaded IDS.

Keywords—Cloudcomputing, Multithreaded Intrusion Detection System, Virtual machine, SaaS

I. INTRODUCTION

Cloud Computing is an expression used to describe the variety of computing concepts that involve a large number of computers. It is the synonym to distributed computing over network model. Cloud computing provides application and storage services to the users without any software and hardware requirement. Users can use any services that provided by the Cloud Admins. This distributed computing model offers lots of features like scalability, cloud storage, infrastructure and portability to the users irrespective of device and location they are accessing from.

Cloud computing supports many service models, in it Platform As A service (PaaS), Infrastructure as a Service (IaaS), and Software As A Service (SaaS) are widely used. PaaS model provides platform to users on which applications can be developed and run. IaaS model delivers infrastructure to the clients like hosting servers, managing network etc. This paper's main cloud computing model is SaaS. Software as a service (SaaS) is one of the important models for the cloud users which will offer the service on demand via Internet. When the software is hosted in cloud, the customer doesn't have to maintain it or support it.SaaS model is platform independent and software independent.

SaaS removes the burden of installing, running and maintaining the application on the user's local computer.

Software as a service (SaaS) is also called higher level layer. Multi Tenant is suitable name for Software-as-a-Service model. Tenant means organizations on common platform with compartmentalization (separation) of each tenant's data and configuration. It refers to the capability of an application, generally consisting of a software and database combination. SaaS will provide application as a service on demand. SaaS

is responsible for hosting of applications on the Internet for the users will follow the model called pay-per-use.

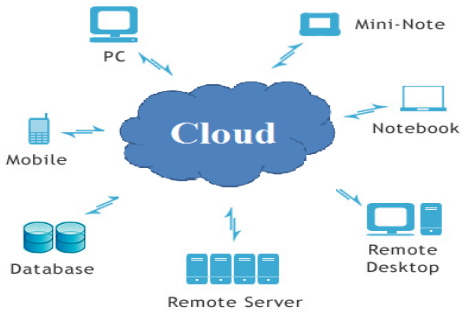

Figure 1: Cloud computing with different resource services.

Advantages of SaaS:

- Cost of the SaaS is less than buying the application.
- As the service provider is economical, more no of applications can be developed and implemented in different Companies.
- SaaS will provide easy customization to the applications.

SaaS will provide wide range of security SSL (Secure Sockets Layer). SSL allows all the users to access their applications easily without accessing the complex back-end configurations by an employee.

Cloud computing technology has different types of deployment models. Few of the deployment models are Private cloud and Public cloud. Private cloud is entirely owned by a single organization and quality of service provided by the private cloud can be controlled. This paper's main deployment model is Public cloud .Public cloud is a multi tenant cloud owned by a company. Typically sells the services it provides to the general public. Public cloud services are readily available to the users without delay.

For every fast growing applications there will be a lots of security issues. Cloud computing also faces major security threats such as Denial of Service (DoS) and Distributed Denial of service (DDOS). These attacks will affect both the users as well as service providers. To stop such attacks in the cloud network, the new Intrusion Detection System (IDS) can be a very effective and efficient mechanism. There are two types of IDS available 1.) Host based IDS (HIDS) 2.) Network based (NIDS). A Host based IDS looks after specific set of host machines. Network based Intrusion detection is deployed for real –time monitoring probes at vital locations in the network infrastructure.

For the administrator the IDS can generate two types of alerts

1.) True Alarms 2.) False Alarms.

- True alarm raises when there is an actual intrusion.
- False Alarm raised on the wrong detection of the intrusion.

A pre-defined rule called signatures is introduced in IDSs to detect intrusion by inspecting the network traffic. An observation will be made carefully for any deviations from the expected behavior of the network user.

In this paper, mainly focuses on the proposed system of the Intrusion detection System on SaaS based Public cloud environment. This paper proposes cloud Multithreaded Intrusion Detection System (CMIDS). The service providers have to subscribe for CMIDS, So that they can use this as a service based intrusion detection system. Cloud infrastructure has very huge network traffic; the traditional IDS approach is not an efficient idea.

The IDSs that are provided are single threaded and due to huge traffic in cloud, multithreaded IDSs are essential. In the traditional IDSs, attacker may create the overhead on the server by using the service continuously without giving any option to the user. This will affect the service provider for its poor performance .The service is under attack is not known to the service provider. To overcome the problem for the service provider, a neutral third party (NTP), type of service is required for monitoring and alerting to the service provider

. Sometimes cloud provider may not inform to the service provider for the sake of reputation about the attacks. Then this NTP will provide alerts about the attacks to cloud user and service provider through Email.

In the remaining sections of this paper we describe some of the currently published papers that are specific to cloud intrusion detection solutions.

II. Related Work

Several research activities were proposed to introduce IDS in cloud computing environment. One such work by Dastjerdi et. al. [1] proposed an agent based IDS for cloud networks, which is an improvement of the DIDMA [2]. This system mainly concentrates on safeguarding the networks' resources and cannot be used as a service. Bakshi et. al. [3] introduced a new intrusion detection system for the cloud computing. They focus on protecting the cloud from DDoS attacks. To detect the DDoS attacks a virtual switch containing an intrusion detection system is introduced.

Mazzariello et. al. [4] proposed a model for detecting DoS attacks against Session Initiation Protocol (SIP). This model only concentrates on SIP flooding attacks.

Hatem Hamad et. al. [5] showed their work on proposing an intrusion detection system as a service in cloud computing environment. Their results show the effective utilization of IDS in cloud.

III. BACKGROUND WORK

In this section the existing techniques for providing more security considerations for accessing services from cloud computing are described.

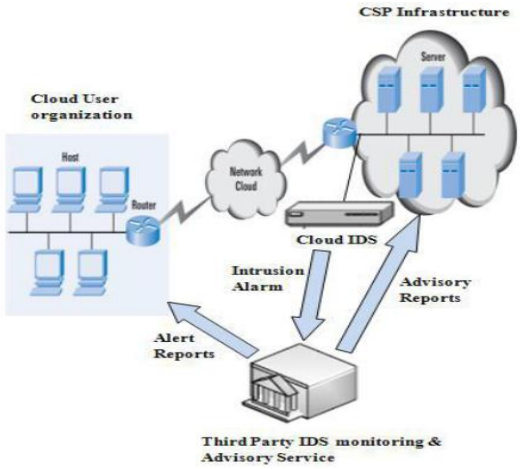

Figure 2: IDS Cloud Infrastructure with service accessing.

As shown in the above figure, security in distributed cloud computing environment is provided by using Neutral Third Party regarding attacks. The neutral third party provides alerts to both cloud users as well as service providers.

IV. Multithreaded Cloud Intrusion Detection System

Cloud computing infrastructure offers different types of services like SaaS, PaaS, IaaS and DaaS. Different types of services provided for different types of users. Cloud computing users need not to worry about the maintenance of the software and hardware up-gradations. Cloud computing users need not to worry about the maintenance of the software and hardware up-gradations. Cloud computing model hosts a more number of virtual machines (VM) on one physical machine. It is called as high-level server

in the cloud data center. Cloud model works on the „concept of virtualization" of resources, where a hypervisor server in cloud data center hosts a number of clients on one physical machine.

Administrator will monitor the network very easily, when the host based IDS is deployed in the high-level server. As the cloud computing model consists flooding flow of huge number of data, a problems like poor performance and overloading is occur. One of the important notes is that only a single system (High-level server) will monitor all the intrusions occur in the cloud and if the attacker got success in compromising the system, the network will be in the hands of the attacker.

To overcome all these attacks, a Network based IDS (NIDS) will be more preferable for the cloud environment. Note that the usage of NIDS. Placing the NIDS outside the VM servers and on key network points like switches, routers and gateways for network traffic monitoring would get the whole view of the system. a simply maintaining a multithreaded IDS approach is used to process huge amount of data, which could in turn to reduce the packet loss.

After the process is completed the proposed IDS will transfer the logged alerts to a third party monitoring service, who will directly communicate the service provider about their service under attack. Proposed system shows some of the different configuration failure and intrusion loop holes to the service provider.Figure-3, shows the data flow diagram of the proposed IDS model. Mainly Multi-threaded NIDS monitors the requests and actions of the cloud users. With an expert advice from the service these alerts are readily communicates the cloud provider.

In this way security considerations are provided to the network presented in cloud computing.

This presentation can decreases the workload of the every data aspect present in the cloud computing.

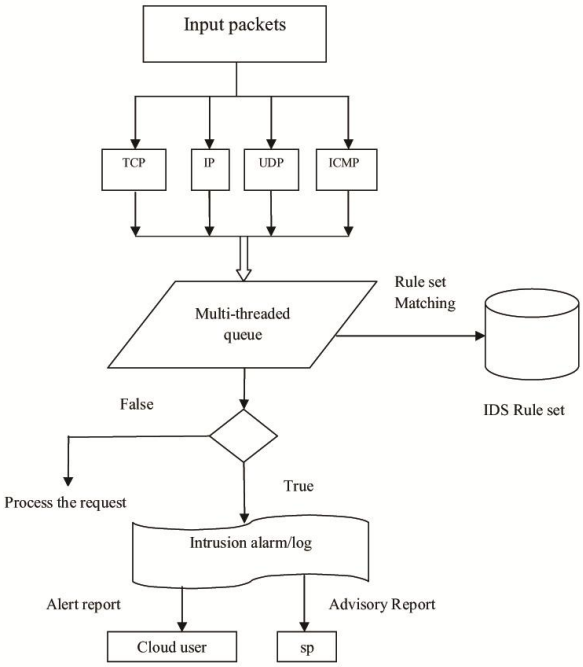

Figure 3: Data flow diagram of proposed multi threaded intrusion detection model

Proposed model in the public cloud environment is based on four phases: Lock, Queue, Analyze phase and reporting phase.

In the Lock phase, two bounds will be received the data that are the in-bound and out-bound. The locked data packets are sent to the Queue phase,

In queue phase these packets are arranged in a queue.

Predefined set of rules are used for analysis phases, checks whether the packets matches or not with those predefined rules. Every process in the Queue can have multiple threads which work in a collaborative fashion to improve system performance. The main process will receive all the protocols like TCP, IP, UDP and ICMP packets and multiple threads would concurrently process the match those packets against pre-defined set of signatures.

Reporting phase would check the alerts from the shared queue and prepares reports for alerts. The third party monitoring service generates a report for service provider, cloud provider immediately.

The proposed system can be used as a service by different service providers in the cloud. For this the service providers first has to send the registration requests to the cloud provider. Whenever the registration of a user is completed, a new standardized signature will be updated in the signature database of the IDS. Now the fully intrusion detection capable cloud service provider is provided for the normal service provider. .

Benefits of Proposed Cloud Service:

1. Multithreaded approach can handle large amount of data.

2. CPU, memory consumption as well as packet loss would be reduced to improve the overall efficiency of cloud IDS.

3. In a host based IDS (HIDS) scenario, if host becomes the victim of offending attacker and controlled by the intruder, HIDS on that host would be compromised. In such a case the attacker would not allow HIDS to send alerts to administrator and could play havoc with the data and applications. For better visibility and resistance, network IDS (NIDS) has been proposed for cloud infrastructure.

4. A third party monitoring and advisory service has been proposed, who has both experience and resources to observe/ handle intrusion data and generate reports for cloud user as well as advisory reports for cloud service provider.

5. Being at a central point, proposed Cloud IDS would be capable to carry out concurrent processing of data analysis, which is an efficient approach.

V. CONCLUSION

For cloud computing, enormous network access rate, relinquishing the control of data & applications to service providers and distributed attacks vulnerability, an efficient, reliable and information transparent IDS is required. In this paper, proposed a Multi-threaded Intrusion detection model for the cloud computing infrastructure. This model is best suitable for the cloud computing where different users request large amounts of data, which increases the network traffic. In this paper we propose to extend our multi thread concepts using different IDS rules using Encryption and decryption process of third party auditor presented in our cloud computing.

VI. REFERENCES

[1] A. V. Dastjerdi, K. Abu Bakar, and S. Tabatabaei, "Distributed Intrusion Detection in Clouds Using Mobile Agents," in Third International Conference on Advanced Engineering Computing and Applications in Sciences, 2009, pp. 175-180.

[2] P.Kannadiga and M.Zulkernine, "Distributed Intrusion Detection System Using Mobile Agents," in Software Engineering, Artificial Intelligence, Networking and Parallel/ Distributed Computing, 2005.

[3] A. Bakshi and Yogesh B, "Securing cloud from DDOS Attacks using Intrusion Detection System in Virtual Machine," in Second International Conference on Communication Software and Networks, Singapore, 2010, pp. 260-264.

[4] C. Mazzariello, R. Bifulco, and R. Canonico, "Integrating a Network IDS into an Open Source Cloud Computing Environment," in Sixth International Conference on Information Assurance and Security, Atlanta, 2010, pp. 265-270.

[5] Hatem Hamad, Mahmoud Al-Hoby, “Managing Intrusion Detection as a service in cloud

Networks", in International Journal of Computer Applications, 2012, volume 41-No.1.

[6] Madhu Babu Janjanam, "Managing Multithreaded IDS as a Service in. Cloud Computing", in IJACEEE. http://bhavanaresearch.org/doc/IJACEEE/Special/24.pdf.