International Journal of Research in Advent Technology, Vol.2, No.2, February 2014

E-ISSN: 2321-9637

Intrusion Detection System for Cloud Computing

Yogita A. More[1], Nitin Y. Suryawanshi[2]
Computer Science & Engineering Department
S.S.B.T.College of Engineering & Technology, Bambhori, Jalgaon
Email:-yogita.more298@gmail.com[1]

Abstract - Cloud computing is services which provides computing resources to each customer. There are various issues that need to be dealt with respect to security and privacy in a cloud computing scenario. One of the security issues is how to reduce the impact of denial of- service (DoS) attack or distributed denial-of-service (DDoS) or many other different attacks in this environment. To counter these kinds of attacks a intrusion detection system is highly needed for protecting each virtual machine against threats. An Intrusion detection System (IDS) constantly monitors actions in a certain environment and decides whether they are part of a possible hostile attack or a legitimate use of the environment. 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. In this paper, we propose a method that enables cloud computing system to achieve both electiveness of using the system resource and strength of the security service without trade-off between them.

Keywords: IaaS**;** PaaS**;** NaaS**;** SaaS; IDS; HIDS; NIDS,DIDS;CIDS.

1. INTRODUCTION

The Cloud Computing is one of the emerging technologies in the world. It is an Internet-based computing technology, where shared resources such as software, platform, storage and information are provided to customers on demand. Cloud computing is a model of information processing, storage, and delivery in which physical resources are provided to customer on demand. Instead of purchasing actual physical de-vices servers, storage, or any networking equipment, clients lease these resources from a cloud provider as an outsourced service. It can also be called as "management of resources, applications and information as services over the cloud (internet) on demand". Cloud computing is a model for enabling convenient and on demand network access to a shared group of computing resources that can be rapidly released with minimal management effort or service provider interaction. Cloud computing has different layers i.e. System layer(which is virtual machine abstraction of server, the platform layer (a ritualized operating system of server),application layer(that include a web application)[1].Cloud Computing has four service models namely Infrastructure as a service(IaaS),Platform as a service(PaaS),Software as a service(SaaS).Network as a service(NaaS) models. IaaS deliver services to users by maintaining large infrastructures like hosting servers, managing networks and other resources for clients. PaaS model facilitates users by providing platform on which applications can be developed and run. SaaS model makes user worry free of installing and running software services on its own machines. Naas involves the optimization of resource allocations by considering network and computing resources.

Figure 1 Architecture of Cloud Computing

Cloud computing has three deployment model namely public cloud, private cloud, hybrid cloud. In public cloud, customer can access web applications and services over the internet. Customer of public cloud services are considered to be untrusted. In private cloud customer has complete control over that how data is manage and what security measure are less while data processing in cloud. The customers of the service are considered trusted. Hybrid cloud are combination of public and private cloud within same network. Data, application and services non-availability can be imposed through Denial of Service (DOS) or Distributed Denial of Service (DDOS) attacks and both cloud service provider and users become handicap to provide or receive cloud services [2]. For such type of attacks Intrusion Detection System (IDS) can be emplaced as a strong defensive mechanism. IDSs are host-based, network-based and distributed IDSs. Host based IDS (HIDS) monitors specific host machines, network-based IDS (NIDS) identifies intrusions on key network points and distributed IDS (DIDS) operates both on host as well as network. Intrusion detection systems are main

tools for providing security in networks, cloud and grid. Intrusion detection system provides stronger security services using more rules and patterns. Intrusion Detection System (IDS) constantly monitors actions in a certain environment and decides whether they are part of a possible hostile attack or a legitimate use of the environment. The environment may be a computer, several computers connected in a network or the network itself. The IDS analyzes various kinds of information about actions emanating from the environment and evaluates the probability that they are symptoms of intrusions. Such information includes, for example, configuration information about the current state of the system, audit information describing the events that occur in the system or network traffic. In Intrusion detection system different measures are used. These measures Include accuracy, completeness, performance, efficiency, fault tolerance, timeliness, and adaptively. The more widely used measures are the True Positive (TP) rate, that is, the percentage of intrusive actions (e.g., error related pages) detected by the system, False Positive (FP) rate which is the percentage of normal actions (e.g., pages viewed by normal users) the system incorrectly identifies as intrusive, and Accuracy which is the percentage of alarms found to represent abnormal behavior out of the total number of alarms.

2. SECURITY ISSUE IN CLOUD COMPUTING

Cloud computing provide different facilities to customer but its security issues are impeding it's a widespread adoption. Security threats can be categorized as follow

2.1 Network and host based attacks on remote Server

Host and network intrusion attacks on remote servers are a major security concern, as cloud vendors use virtual machine technology. DOS and DDOS attacks are launched to deny service availability to end users.

2.2 Sub-contracting cloud services

Cloud user makes a contract or agreement for service provisioning with the cloud service provider. Subcontracting of cloud services by cloud service provider to another service provider poses security issues like non-repudiation or not owing the responsibility, if some-thing goes wrong with precious data and application of cloud users.

2.3 Lack of data interoperability standards

It results into cloud user data lock-in state. If a cloud user wants to shift to other service provider due to certain reasons it would not be able to do so, as cloud users data and application may not be compatible with other vendors data storage format or platform. Security and confidentiality of data would be in the hands of cloud service provider and cloud user would be dependent on a single service provider.

2.4 Non-availability of cloud services

Non-availability of services due to Cloud outages can cause monetary loss to cloud user organization. A deliberate and comprehensive Service Level Agreement (SLA) must be written among user and provider covering all the relevant legal and service provisioning issues and details

2.5 Cloud security auditing

Cloud auditing is a difficult task to check compliance of all the security policies by the vendor. Cloud service provider has the control of sensitive user data and processes, so an automated or third party auditing mechanism for data integrity check and forensic analysis is needed. Privacy of data from third party auditor is another concern of cloud security.

2.6 Cloud data confidentiality issue

Confidentiality of data over cloud is one of the glaring security concerns. Encryption of data can be done with the traditional techniques. However, encrypted data can be secured from a malicious user but the privacy of data even from the administrator of data at service providers end could not be hidden. Searching and indexing on encrypted data remains a point of concern in that case.

3. LITERATURE SURVEY

3.1 Intrusion detection for grid and cloud computing

Intrusion Detection System (IDS) system is used for security purpose. In cloud and grid computing the most vulnerable targets for intruders attacks due to their distributed environment. For such environments, Intrusion Detection System (IDS) can be used to enhance the security measures by a systematic examination of logs, configurations and network traffic. Traditional IDSs are not suitable for cloud environment as network based IDSs (NIDS) cannot detect encrypted node communication, also host based IDSs (HIDS) are not able to find the hidden attack trail. In the paper [5] Kleber, schulter et al. have proposed the IDS service at cloud middleware layer, which has an audit system designed to cover attacks that NIDS and HIDS cannot detect. The architecture of IDS service includes the node, service, event auditor and storage. The node contains resources that are accessed through middleware which defines access-control policies. The service facilitates communication through middleware. The event auditor monitors and captures the network data, also analyzes which rule / policy is broken. The storage holds behavior-based (comparison of recent customer actions to usual behavior) and knowledge-based (known trails of previous attacks) databases. The audited data is sent to IDS service core, which analyzes the data and alarm to be an intrusion. The

authors have tested their IDS prototype with the help of simulation and found its performance satisfactory for real-time implementation in a cloud environment. Although they have not discussed the security policies compliance check for cloud service provider and their reporting procedures to cloud customer.

3.2 Intrusion detection in the cloud

It use Integration solution for central IDS management for Security in cloud computing. In cloud computing, user data and application is hosted on cloud service providers remote servers and cloud user has a limited control over its data and resources. In such case, the administration of IDS in cloud becomes the responsibility of cloud provider. Although the administrator of cloud IDS should be the user and not the provider of cloud services. Intrusion detection system plays an important role in the security and perseverance of active defense system against intruder hostile attacks for any business and IT organization. IDS implementation in cloud computing requires an efficient, scalable and visualization-based approach. Integration solution for central IDS management is used. In the paper [3], Roschke and Cheng et al. have proposed integration solution for central IDS management that can combine and integrate various renowned IDS sensors output reports on a single interface. The intrusion detection message exchange format (IDMEF) standard has been used for communication between different IDS sensors. The authors have suggested the deployment of IDS sensors on separate cloud layers like application layer, system layer and platform layer. Alerts generated are sent to Event Gatherer program. Event gatherer receives and convert alert messages in IDMEF standard and stores in event data base repository with the help of Sender, Receiver and Handler plug-ins. The analysis component analyzes complex attacks and presents it to user through IDS management system. The authors have proposed an effective cloud IDS management architecture, which could be monitored and administered by the cloud user. They have provided a central IDS management system based on different sensors using IDMEF standard for communication and monitored by cloud user.

3.3 Integrating a network IDS into an open source cloud computing environment

Security concerns in cloud computing are the main hurdles in cloud adoption. To deny use of services hosted by a cloud service provider, denial of service (DOS) or distributed denial of service (DDOS) attacks are used by the offender. Traditional IDSs need a special consideration for a dynamic and complex cloud environment. Network based IDSs are more appropriate for cloud infrastructure due to the advantage of monitoring the host virtual machine infrastructure without being compromised. Whereas in HIDS, if host is compromised the intrusion detection system monitoring would be neutralized and could jeopardize the security of whole system. In the paper [6], Claudio et al. have proposed to emplace a NIDS on virtual switch of the physical machine hosting virtual machines of clients using open source Eucalyptus cloud computing framework. The Eucalyptus based cloud IDS would be able to observe all in-bound and out-bound traffic from the entry point of traffic. The proposed idea is based on installation of IDS on each physical machine hosting other client virtual machines rather to deploy IDS on a single point. The suggested solution could proved to be effective and efficient in terms of load sharing of large volume of data, no packet loss and low computational consumption. The authors have validated their idea through experiment and found that IDS hosted at a single point consumes more CPU load than IDS placed at various physical machines and consuming local resources. Also in case if single IDS is compromised by the offender, it would not affect the working of other IDSs and they still be operating properly.

3.4 (CIDS): A frame work for Intrusion Detection System

Traditional NIDS and HIDS cannot identify suspicious activities in a cloud environment. As an example, a NIDS cannot detect an attack anytime node communication is encrypted. Attacks can also be invisible to HIDS, because they may not leave traces in the node operating system where the IDS reside. Some of these IDSs are scalable but they have the problem of single point of failure as most distributed hierarchical IDS. In the paper [7] ,author proposed architecture, each node has two IDSs detectors, CIDS and HIDS. In this way, the node can cooperatively participate in intrusion detection by identifying the local events that could represent security violations and by exchanging its audit data with other nodes. CIDS has a scalable and elastic architecture with a P2P solution and no central coordinator. Hence, there is no single point of failure. CIDS architecture distributes the processing load at several cloud locations and isolates the user tasks from the cloud by executing them in a monitored virtual machine. This helps in protecting CIDS components from threats that can control a task in the VM . Each node also includes an audit system that monitors messages among nodes and the middleware logging system, and collects events and logs from the VMs. By sharing both the knowledge and behavior databases in each node among the audit components, CIDS can detect the masqueraders that access from several nodes and both host-based and network-based attacks. Furthermore, to take into account the large volume of data in a cloud that prevents administrators from observing any action, a further CIDS component parses and summarizes a highly intensive number of alerts from a NIDS component in a physical or virtual

switch inside the cloud virtual network. A report for the administrators collects alert messages from all IDS detectors installed in the cloud system. CIDS resides inside the cloud middleware which provides a homogeneous environment for accessing all nodes. The middleware sets the access control policies and supports a service-oriented environment. Since the middleware can be install inside different grid and cloud systems, CIDS can be applied to several Grid and cloud systems.

4. CLOUD IDS MODEL

This model is an efficient and effective distributed Cloud IDS. This model uses multi-threading technique to improve IDS Performance over cloud infrastructure. The Multi-threading IDS would be able to process large amount of data and cloud reduce the packet loss. Multi-threading technique is uses sensor to monitors and sensitizes the network traffic. Multi-threading technique also check the malicious packets and after processing the system send or pass the monitor alerts to third party monitoring service. Then third party directly informs to cloud customers about their system attacks. Third party also provides expert advice to cloud service provider for mis-configurations and intrusion loop holes in the system. Figure 2 shows the cloud IDS model. Cloud computing provides application and storage services on remote servers. The clients do not have to worry about its maintenance and software or hardware up gradations. 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.

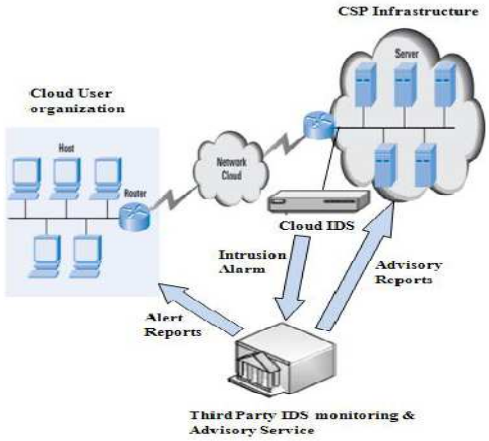

Figure 2 Cloud IDS Model

Deploying HIDS in hypervisor or host machine would allow the administrator to monitor the hypervisor and virtual machines on that hypervisor. But with the rapid flow of high volume of data as in cloud model, there would be issues of performance like overloading of VM hosting IDS and dropping of data packets. Also if host is compromised by an offending attack the HIDS employed on that host would be neutralized. In such a scenario, a network based IDS would be more suitable for deployment in cloud like infrastructure. NIDS would be placed outside the VM servers on bottle neck of network points such as switch, router or gateway for network traffic monitoring to have a global view of the system. Such NIDS would still be facing the issue of large amount of data through network access rate in cloud environment. The customer actions and request are monitored and logged through a multi-threaded NIDS. The alert logs are readily communicated to cloud user with an expert advice for cloud service provider. In multi-threaded NIDS model for distributed cloud environment is based on three modules: capture and queuing module, analysis/ processing module and reporting module. The capture module, receives the in-bound and out-bound (ICMP, TCP, IP, UDP) data packets. The captured data packets are sent to the shared queue for analysis. The analysis and process module receives data packets from the shared queue and analyze it against signature base and a pre-defined rule set. Each process in a shared queue can have multiple threads which work in a collaborative fashion to improve the system performance. The main process will receive TCP, IP, UDP and ICMP packets and multiple threads would concurrently process and match those packets against pre-defined set of rules. Through an efficient matching and analysis the bad packets would be identified and alerts generated. Reporting module could read the alerts from shared queue and prepares alert reports. The third party monitoring and advisory service having experience and resources would immediately generate a report for cloud user's information and sends a comprehensive expert advisory report for cloud service provider. Figure 3 depicts the flow chart of proposed multithreaded Cloud IDS.

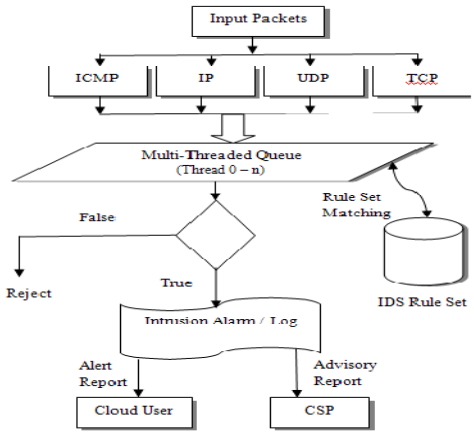

Figure 3 Flow Chart of Multithreaded IDS Model

5. ADVANTAGES

1. High volume of data in cloud environment cloud be handled by a single node IDS through a multi-threaded approach.

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 case the attacker would not allow be HIDS to send alerts to administrator and cloud play havoc with data and application. 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 report 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.

CONCLUSION

Cloud computing is a network of networks over the internet, therefore chances of intrusion is more with the erudition of intruders attacks. Cloud computing has revolutionized the IT world with its services provisioning infrastructure, less maintenance cost, data and services availability assurance, rapid accessibility and scalability. Different IDS techniques are used to counter malicious attacks in traditional networks. For Cloud computing, enormous network access rate, relinquishing the control of data and applications to service provider and distributed attacks vulnerability, an efficient, reliable and information transparent IDS is required. Multi-threaded cloud IDS which can be administered by a third party monitoring service for a better optimized efficiency and transparency for the cloud user.

REFERENCES

[1] Sebastian Roschke, Feng Cheng, Christoph Meinel,“ Intrusion Detection in the Cloud", Eighth IEEE International Conference on Dependable, Autonomic and Secure Computing, 2009.
[2] Chi-Chun Lo, Chun-Chieh Huang, Joy Ku, “A Cooperative Intrusion Detection System Framework forCloud Computing Networks", 39th International Conference on Parallel Processing Workshops, 2010.
[3]Sebastian Roschke, Feng Cheng, Christoph Meinel, “Intrusion Detection in the Cloud", Eighth IEEE International Conference on Dependable, Autonomic and Secure Computing, 2009.
[4]Irfan Gul, M. Hussain, “Distributed cloud intrusion detection model”, International Journal of Advanced Science and Technology Vol. 34, September, 2011.
[5]Kleber, schulter, “Intrusion Detection for Grid and Cloud computing”, IEEE Journal: IT Professional, 19 July 2010.
[6] Claudio Mazzariello,Roberto Bifulco and Roberto Canonico, “Integrating a Network IDS into an Open Source Cloud Computing Environment “, IEEE sixth international conference on Information Assurance and Security,2010.
[7]Hisham A. Kholidy, Fabrizio Baiardi,”CIDS: A framework for Intrusion Detection in Cloud System”,IEEE ninth International conference on Information Techonology,2012