Volume 3, Issue 11, November 2013 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Implementation of Intrusion Detection System for Cloud Computing

Ms Deepavali p Patil, Prof.Archana C.Lomte

Department of Computer Science and Engineering

Bhivarabai Sawant Institute of Technology & Research (BSIOTR), India

Abstract:- ***Nowadays all are working with cloud i.e. distributed network over an internet, it is very important to maintain a high level security to ensure safe and trusted communication of information in a distributed network. But secured data communication over internet and distributed network is always under threat of intrusions and misuses. So Intrusion Detection Systems have become a needful component in terms of network security. For providing security in a distributed system requires more than user authentication with passwords or digital certificates and confidentiality in data transmission. Distributed model of cloud makes it vulnerable and prone to sophisticated distributed intrusion attacks like Distributed Denial of Service (DDOS) and Cross Site Scripting (XSS). To handle large scale network access traffic and administrative control of data and application in cloud, a new multi-threaded distributed cloud IDS model has been proposed. Our proposed cloud IDS handles large flow of data packets, analyze them by using FC-ANN, based on ANN and fuzzy clustering, to solve the problem and help IDS to achieve higher detection rate, less false positive rate and stronger stability and generate reports efficiently by integrating knowledge and behavior analysis to detect intrusions. To implement and measure the performance of our system we used the KDD99 benchmark dataset and obtained reasonable detection rate.***

Keyword:-ANN DDOS KDD .

I. Introduction:-

In recent years, Intrusion Detection System (IDS) has become one of the hottest research areas in Computer Security. It is an important detection technology and is used as a countermeasure to preserve data integrity and system availability during an intrusion. When an intruder attempts to break into an information system or performs an action not legally allowed, we refer to this activity as an intrusion. This type of intrusion is always on distributed network like cloud computing. It is a recent an innovative technology that we all prefer this technology promises reliable services delivered through next-generation data centers that are built on virtualized compute and storage technologies. The term cloud is analogical to "Internet". The term cloud computing is based on cloud drawings used in the past to represent telephone networks later to depict internet in.

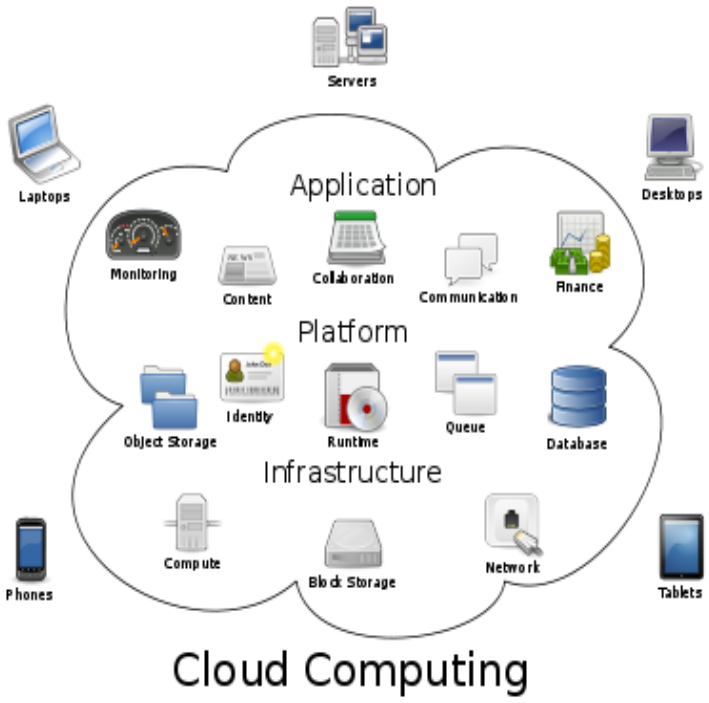

Fig. 1 Cloud Computing Infrastructure

© 2013, IJARCSSE All Rights Reserved

Cloud computing is an internet based computing where virtual shared servers provide software, infrastructure, platform, devices and other resources and hosting to customer as a service on pay-as you-use basis. Fig1. shows the concept. All the information that a digitized system has to offer is provided as a service in the cloud computing model. Users can access these services available on the "internet cloud" without having any previous know-how on managing the resources involved. Cloud users do not own the physical infrastructure; rather they rent the usage from a third- party provider. They consume resources as a service and pay only for resources that they use. What they only need is a personal computer and internet connection. Cloud computing has revolutionized the IT world with its service provisioning infrastructure, less maintenance cost, data & services availability assurance, rapid accessibility and scalability. Cloud computing has three basic abstraction layers i.e. system layer (which is a virtual machine abstraction of a server), the platform layer (a virtualized operating system of a server) and application layer (that includes web applications). Hardware layer is not included as it does not directly offer to users. Cloud computing also has three service models namely Platform as a Service (PaaS), Infrastructure as a Service (IaaS) and Software as a Service (SaaS) models. PaaS model facilitates users by providing platform on which applications can be developed and run. IaaS deliver services to users by maintaining large infrastructures like hosting servers, managing networks and other resources for clients. SaaS model makes user worry free of installing and running software services on its own machines. Presently, Salesforce.com, Google and Amazon are the leading cloud service providers who extend their services for storage, application and computation on pay as peruse basis. 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. For such type of attacks Intrusion Detection System (IDS) can be emplaced as a strong defensive mechanism .

II. Intrusion Detection System

Intrusion detection systems (IDS) are an essential component of defensive measures protecting computer systems and network against harm abuse . It becomes crucial part in the Cloud computing environment. The main aim of IDS is to detect computer attacks and provide the proper response. An IDS is defined as the technique that is used to detect and respond to intrusion activities from malicious host or network. There are mainly two categories of IDSs, network based and host based. In addition, the IDS can be defined as a defense system, which detects hostile activities in a network. The key is to detect and possibly prevent activities that may compromise system security, or some hacking attempt in progress including reconnaissance/data collection phases that involve for example, port scans. One key feature of intrusion detection systems is their ability to provide a view of unusual activity and to issue alerts notifying administrators and/or blocking a suspected connection.

Intrusion detection is defined as the process of identifying and responding to malicious activity targeted at computing and networking resources. In addition, IDS tools are capable of distinguishing between insider attacks. originating from inside the organization (coming from own employees or customers) and external ones (attacks and the threat posed by hackers). Once an intrusion has been detected.IDS issues alerts notifying administrators of this fact. The next step is undertaken either by the administrators or the IDS itself, by taking advantage of additional countermeasures (specific block functions to terminate sessions, backup systems, routing connections to a system trap, legal infrastructure etc.) – following the organization's security policy (Figure 2). An IDS is an element of the security policy. Among various IDS tasks, intruder identification is one of the fundamental ones. It can be useful in the forensic research of incidents and installing appropriate patches to enable the detection of future attack attempts targeted on specific persons or resources.

Fig 2.Intrusion Detection System Infrastructure

III. Intrusion Detection Overview

The below sections give a short overview of networking attacks, classifications and various components of Intrusion Detection System

.

Networking Attacks

This section is an overview of the four major categories of networking attacks. Every attack on a network can comfortably be placed into one of these groupings.

1. **Denial of Service (DoS/ DDoS):** A Denial of service or distributed denial of service is an attack is an attempt to make a machine or network resource unavailable to its intended users. Although the means to carry out, motives for, and targets of a DoS attack may vary, it generally consists of efforts to temporarily or indefinitely interrupt or suspend services of a host connected to the Internet. Example of Dos attacks are: apache, smurf, Neptune, ping of death, back, mail bomb, UDP storm etc.

© 2013, IJARCSSE All Rights Reserved

2. **Remote to User Attacks (R2L):** A remote to user attack is an attack in which a user sends packets to a machine over the internet, which s/he does not have access to in order to expose the machines vulnerabilities and exploit privileges which a local user would have on the computer e.g. xlock, guest, xnsnoop, phf, sendmail dictionary etc.

3. **User to Root Attacks (U2R):** These attacks are exploitations in which the hacker start off on the system with a normal user account and attempts to abuse vulnerabilities in the system in order to gain super user privileges e.g. perl, xterm.

4. **Probing:** Probing is an attack in which the hacker scans a machine or a networking device in order to determine weaknesses or vulnerabilities that may later be exploited so as to compromise the system. This technique is commonly used in data mining e.g.saint, portsweep, mscan, nmap etc.

A. Host Based Intrusion Detection System (HIDS)

This type of IDS involves software or agent components, which is run on the server, router, switch or network appliance. However, the agent versions must report to a console or can be run together on the same host as depicted in Fig 3. Basically, HIDS provides poor real-time response and cannot effectively defend against one-time catastrophic events. In fact, HIDSs are much better in detecting and responding to long term attacks such as data thieving .

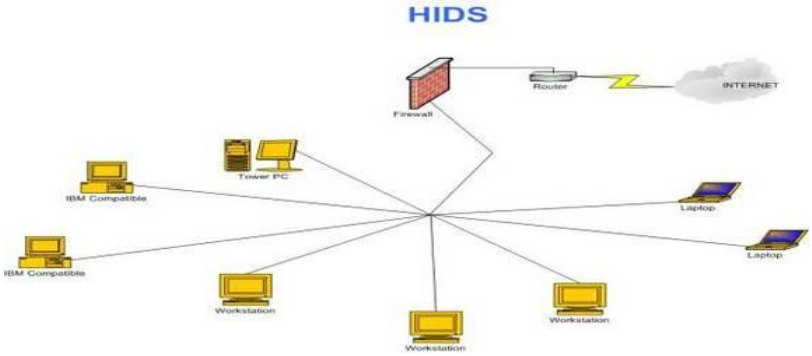

Fig 3 Host Based Intrusion Detection System

B. Network Based Intrusion Detection system(NIDS)

This type of IDS captures network traffic packets such as TCP, UDP and IPX/SPX) and analyzes the content against a set of RULES or SIGNATURES to determine if a POSSIBLE event took place. False positives are common when an IDS system is not configured or "tuned" to the environment traffic it is trying to analyze . Fig 4 shows the network based Intrusion Detection System .

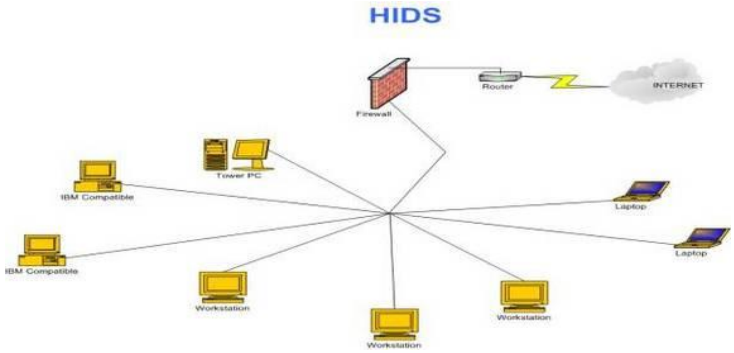

Fig 4 Network Based Intrusion Detection System

The host-based and network-based systems are both required in the Cloud computing environment because they offer significantly different benefits

IV. Related existing techniques

1. Intrusion detection for grid and cloud computing

Cloud and Grid computing are the most vulnerable targets for intruder's 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. have proposed an 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 throurgh middleware. The event auditor monitors and captures the

© 2013, IJARCSSE All Rights Reserved

network data, also analyzes which rule / policy is broken. The storage holds behavior based (comparison of recent user 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.

2. Intrusion detection in the cloud

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 virtualization-based approach. In cloud computing, user data and application is hosted on cloud service provider's 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. In the paper. have proposed an 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 Security Issues in Cloud Computing:

1. 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 provider ‟s end could not be hidden.

2. Network and host based attacks on remote Server Host and network intrusion attacks on remote hypervisors 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.

3. 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

4. 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 user's data and application may not be compatible with other vendor's 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.

V. Conclusion:-

Cloud computing is a "network of networks" over the internet, therefore chances of intrusion is more with the erudition of intruder's attacks. Different IDS techniques are used to counter malicious attacks in traditional networks. For Cloud computing, enormous network access rate, relinquishing the control of data & applications to service provider and distributed attacks vulnerability, an efficient, reliable and information transparent IDS is required. In this report, a multi-threaded cloud IDS model is proposed which can be administered by a third party monitoring service for a better optimized efficiency and transparency for the cloud user.

References

[1] Vincent Shi-Ming Huang, Robert Huang, Ming Chiang, "A DDoS Mitigation System with Multi-Stage Detection and Text-Based Turing Testing in Cloud Computing," 2013 27th International Conference on Advanced Information Networking and Applications Workshops.

[2] Gang Wang, Jinxing Hao, Jian Ma, Lihua Huang "A new approach to intrusion detection using Artificial Neural Networks and fuzzy clustering," IEEE Internet Computing.

[3] G. Goth, "Fast-moving zombies: Botnets stay a step ahead of the fixes," IEEE Internet Computing, vol. 11, pp. 7–9, 2007.

[4] P. Salvador, A. Nogueira, U. Franca, and R. Valadas, "Framework for zombie detection using neural networks," in Internet Monitoring and Protection, 2009. ICIMP '09. Fourth International Conference on, may 2009, pp. 14 –20.

[5] F. Giroire, J. Chandrashekar, N. Taft, E. Schooler, and D. Papagiannaki, "Exploiting temporal persistence to detect covert botnet channels," in Recent Advances in Intrusion Detection, ser. Lecture Notes in Computer Science. Springer Berlin / Heidelberg, 2009, vol. 5758, pp. 326–345.

© 2013, IJARCSSE All Rights Reserved