Volume 7, Issue 3, March 2017 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

A Brief Survey of Intrusion Detection and Prevention Systems in Cloud Computing Environment

D. Ragupathi
Ph.D., Scholar, Department of Computer Science,
A.V.V.M Sri Pushpam College, Poondi,
Thanjavur, Tamilnadu, India

Dr. N. Jayaveeran
Associate Professor, PG & Research Department of
Computer Science, Khadir Mohideen College,
Adirampattinam, Tamilnadu, India

Abstract— The traditional intrusion detection system is not flexible in giving security in cloud computing since of the distributed structure of cloud computing. This paper studies the intrusion detection and prevention strategies and possible solutions in Host Based and system Based Intrusion Detection system. It discusses DDoS attacks in Cloud environment. Distinctive Intrusion Detection strategies are also examined namely anomaly based strategies and signature based techniques. It also studies distinctive approaches of Intrusion Prevention system. Intrusion Detection Systems (IDS) have been used broadly to detect pernicious practices in system communication and hosts. It is defined as a PC system system to gather information on a number of key points, and dissect this information to see whether there are infringement of system security arrangement conduct and signs of attack.

Keywords— Intrusion Detection System, Cloud Computing, Intrusion Prevention, DDoS Attacks.

I. INTRODUCTION

Cloud computing is a large-scale distributed computing paradigm. It is a collection of sources in request to enable resource sharing in terms of scalability, overseen computing administrations that are conveyed on request over the network. Its clients need not to buy infrastructure, software, resources, as a result saving a substantial sum of expenditure. Cloud basically gives administrations through a third party. The third party gives administrations and assets on rent and clients pay per use. This will save a lot of money and gives a greater flexibility to move from one administration to another service.

Fig: 1. Cloud Computing Architecture

In the past three decades, the world of computation has changed from centralized (client-server not web based) to distributed systems and now we are getting back to the virtual centralization (Cloud Computing). Cloud computing is emerging day by day. People are using its administrations exceptionally frequently and they don't have any other alternative for its services. But clients are unaware about the security and security concerns in a cloud environment. Since cloud computing is distributed in nature, supports multi-client and multi-domain platform, it is more prone to security threats. Security dangers can be in terms of intrusion prospects and DDoS attacks. Associations need to give firewalls, intrusion detection and prevention techniques, authentication, encryption and other powerful equipment and programming security to secure the stored data. Aggressors attempt to find loopholes for breaking security. Associations are using IDPS for giving security and security in the cloud environment. Attacks that have originated from interior sources are called interior attacks. It incorporates unauthorized access of interior user. Attacks that originate from outside sources are called outside attacks.

At present the safety of commonly used advancements such as message encryption, firewalls secure the system and can be used as a first line of defence, but only these advancements is not enough. Intrusion Detection systems (IDS) has been proposed for years as an efficient security measure and is nowadays broadly sent for securing critical IT-

Infrastructures. Numerous business and open source implementations have emerged and been broadly used in practice for identifying pernicious practices against ensured hosts or system environments. They can offer security measures by investigating configurations, logs, system traffic, and client activities to perceive typical attack behaviour.

In classical endeavour settings, an IDS is normally sent on committed equipment at the edge of the defended organizing foundation or run on person hosts on the network, in request to secure respective system or host from outside attacks. Today small and medium organizations are increasingly realizing that simply by tapping into the Cloud they can gain fast access to best business applications, without preparing new personnel, or licensing new software. IDS is not an exception to this tread and the interests for embedding IDS to a Cloud environment is undeniable.

The remainder of this paper is organized as follow: In portion II, basic concepts of IDS are discussed. The intrusion detection strategies are detailed in portion III. In portion IV, an overview of Cloud Computing model is presented. In the last section, future work and conclusion are presented.

II. INTRUSION DETECTION SYSTEM

Intrusion detection systems are programming or equipment systems that automate the process of observing the occasions occurring in a PC system or network, dissecting them for pernicious activities or arrangement infringement and produces reports to a administration station.

An IDS is made of several components:

→ Sensors which produce security events.
→ Console to screen occasions and alarms and control the sensors.
→ Central Engine that records occasions logged by the sensors in a database and uses a system of rules to produce alarms from security occasions received.

Based on the ensured objective or the information source, IDS can be classified into Host-based Intrusion Detection system and Network-based Intrusion Detection system.

A. Host-Based Intrusion Detection system

Host-based Intrusion Detection system was the first type of intrusion detection programming to be designed, with the original target system being the mainframe PC where outside cooperation was infrequent.

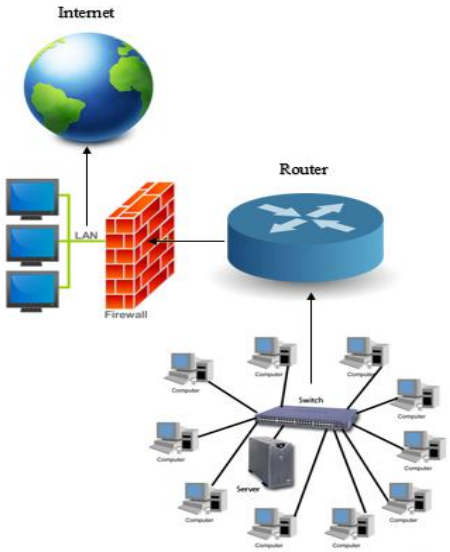

Fig: 2.Process of HIDS

Host-based IDSs operate on information gathered from within an person PC system. A Host-based IDS screens the inbound and outbound bundles from the PC system only and would alert the client or administrator if suspicious action is detected. Besides the benefits acquired when utilizing this model of IDS, there are some disadvantages, which discourage deploying Host-based IDS:

- Host-based IDSs are harder to manage, as information must be configured and overseen for eexceptionally host monitored.
- Since the information sources and the examination engines for Host-based IDSs reside on the host targeted by attacks, the IDS may be attacked and disabled as part of the attack.
- Host-based IDSs use the computing assets of the hosts they are monitoring, subsequently inflicting a execution cost on the checked systems.

B. Network-Based Intrusion Detection system

Network-based Intrusion Detection systems focus more greatly on the system than a particular host. Network-based IDS detects attacks by capturing and dissecting system packets. Listening on a system portion or switch, one network-based IDS can screen the system action affecting multiple hosts that are connected to the system segment, thereby protecting those hosts.

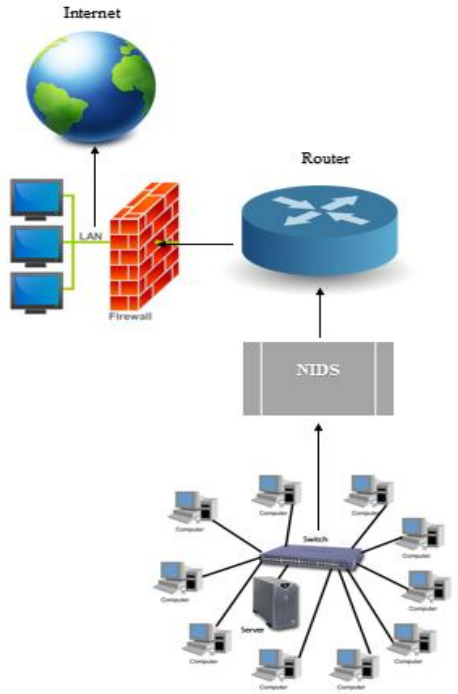

Fig: 3.Process of NIDS

Network-based IDSs frequently consist of a set of single purpose sensors placed at distinctive focuses in a network. These units screen system traffic, performing local examination of that action and reporting attacks to a central administration console. As the sensors are restricted to running the IDS, they can be more easily secured against attacks, e.g. run the IDS sensors in stealth mode.

The design of the Network-based IDS would eliminate the impediments which are mentioned for Host based IDS. There is no need to arrange and oversee every host as one IDS sensor in a system portion could take the responsibility of all analysis. Attacks to a particular host in a system would not affect IDS and securing the IDS sensor is simpler. Network-based IDS would utilize committed assets for its functionalities which is isolated from any host in the network. Therefore, it does not inflict a execution cost on the checked systems.

Table: 1 Difference between HIDS & NIDS

HIDS	**NIDS**
Insider detection is solid while outsider detection is weak.	Outsider detection is solid while insider detection is frail
Frail genuine time reaction but awesome for long term attacks.	Solid reaction against outside attacks.
Harm appraisal capable is excellent.	Harm appraisal capable is exceptionally weak.
It dissects logs and consists of information related to the status of the system.	It dissects system action directly and checks exceptionally system event.
It offers security even if the LAN is off.	It offers security only on LAN.
It is more versatile.	It is less versatile.
It can detect suspicious conduct designs properly.	It can’t detect suspicious patterns.
These systems are more costly to implement.	These systems are less costly to implement.
Its scope is narrow	Its scope is broad.
It is complex to setup and configure.	Is easier to setup and configure.
In these systems, detection is based on records in any single machine.	In these systems, detection is based on records in entire network.
It is working system specific.	It is working system independent.

III. INTRUSION DETECTION METHODS

There are two essential approaches for dissecting occasions to detect attacks: Misuse Detection Approach and Anomaly Detection Approach. Misuse detection, in which the examination targets something known to be attack pattern, is the strategy used by most business systems.

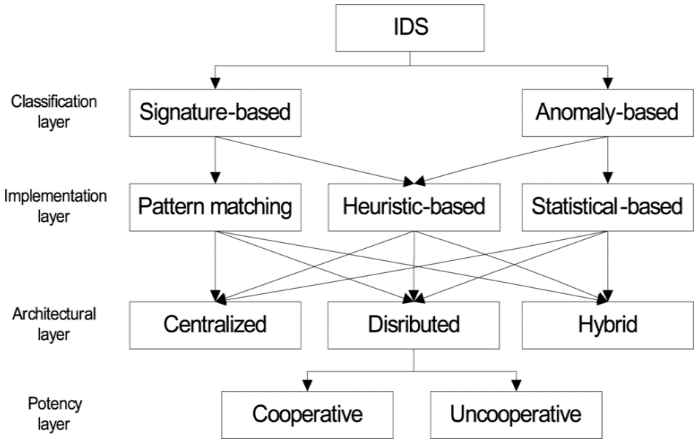

Fig: 4. IDS Methods

Anomaly detection, in which the examination looks for abtypical designs of activity, has been the subject of a awesome deal of research. Anomaly detection is used in restricted structure by a number of IDSs. The most powerful IDSs use mostly misuse detection approaches.

A. Anomaly Detection Approach

Anomaly detectors perceive typical unusual conduct on a host or network. They function on the assumption that attacks are distinctive from legitimate action and can subsequently be detected by systems that perceive these differences. Anomaly detectors construct profiles representing typical conduct of users, hosts, or system connections. These profiles are constructed from historical information gathered over a period of typical operation. The detectors then gather occasion information and use a variety of measures to decide when checked action deviates from the typical routine.

Anomaly detection approaches frequently require broad preparing in request to characterize typical conduct patterns. Unfortunately, the IDSs based on anomaly detection frequently produce a substantial number of false alarms, as typical designs of client and system conduct can vary wildly. Modern day endeavor system situations amplify this disadvantage due to the massive amounts of dynamic and diverse information that needs to be analyzed. Despite this shortcoming, specialists assert that IDSs based on anomaly detection are able to detect new attack forms.

B. Misuse Detection Approach

Misuse detectors dissect system activity, looking for occasions or sets of occasions that match a predefined design of occasions that describe a known attack. As the designs comparing to known attacks are called signatures, misuse detection is sometimes called signature-based detection. The most common structure of misuse detection used in business products specifies each design of occasions comparing to an attack as a separate signature. However, there are more sophisticated approaches to doing misuse detection that can leverage a single signature to detect groups of attacks.

There are some advantages which rouse utilizing misuse detection approach:

- Misuse detectors are exceptionally powerful at detecting attacks without generating an overwhelming number of false alarms.
- Misuse detector approach does not require broad preparing in request to detect attacks.

As misuse detectors use the signature databases for attack detection, they can only detect those attacks they know about and their signature are present in the database. Therefore, they must be constantly updated with marks of new attacks.

C. Distributed Dissent of Administration (DDoS) Attacks

Security concerns in the cloud environment are the main obstacles in cloud adoption. To deny use of administrations facilitated by a cloud administration provider, dissent of administration (DoS) or distributed dissent of administration (DDoS) attacks is used by the offender. These attacks frequently disrupt the cloud services. Aggressors attempt to alter their tools to avoid bypass these security systems and specialists attempt to find new ways to handle the new attacks. There are four elements of DDoS attacks namely; attacker machine, the handlers, specialists or zombie hosts, target machine. The handlers run some malware and act as an intermediate interface to control the specialists and route to them the attacker commands. They are controlled by the attacker. The specialists or zombie hosts also run some malware programming and generates a stream of bundles towards the target system.

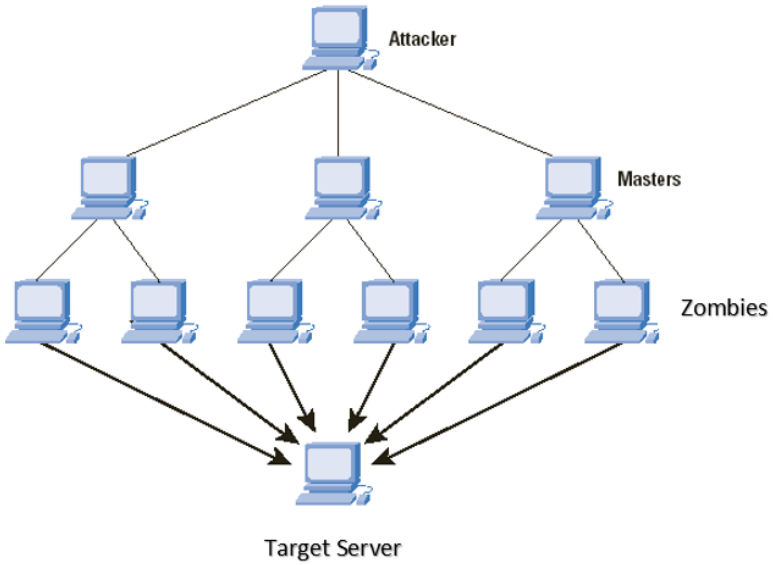

Fig: 5. Design of DDoS Attack

DDoS Aggressors capture optional casualty systems using them to wage a comparing substantial scale attack against essential casualty systems. By using optional casualty systems in a DDoS attack, the attacker can make a much larger and more disruptive attack. It is exceptionally troublesome for system forensics to track the genuine attacker since the optional casualty itself performs the attack. One of the best strategies to proccasion DDoS attack is that the optional casualty systems must attempt to proccasion themselves from participating in the attack. This requires a awesome sum of awareness about security issues and prevention techniques. In request to proccasion optional victims from becoming contaminated with the DDoS, these systems must frequently screen their own security. They must ensure that no specialist programs have been introduced on their systems and also make sure that they are not indirectly sending specialist action into the network. As the internet is distributed, with so Numerous distinctive equipment and programming platforms, it becomes quite troublesome for clients to actualize the right defensive measures such as an anti-Trojan software.

DDoS attacks can be prevented by detecting and neutralizing handlers. It incorporates a strategy to study the communication convention and action designs between client and handlers or specialist and handlers. It helps to find out the system nodes that might be contaminated with handler code. A DDoS attack can be neutralized by shutting down a few numbers of handlers.

IV. CLOUD COMPUTING

Numerous practitioners in the business and academic spheres have attempted to define exactly what "Cloud Computing" is and what unique characteristics it presents. The National Institute of Standards and Technology (NIST) defines Cloud Computing as a pay-per-use model for enabling available, convenient, on-request system access to a shared pool of configurable computing assets that can be quickly provisioned and discharged with minimal administration effort or administration supplier interaction.

The Cloud design can be divided in three layers: The system Layer, the Stage Layer, and the Application Layer. The hidden equipment is not considered as a part of the Cloud, but as the fundamental basis and is operated by the Cloud providers.

- *The system Layer:* The system layer is the lowest layer in the Cloud design and incorporates virtualized hosts and networks. Administration model conveyed at this layer is alluded to as Infrastructure-as-a-Administration (IaaS). IaaS completely changes the way developers convey their applications. Instead of spending big with their own information centers or overseen hosting organizations or administrations and then hiring operations staff to get it going, they can just get a virtual server running in minutes and pay only for the assets they use.
- *The Stage Layer:* The Stage layer is the second layer in the design and incorporates virtualized working systems as well as runtimes and APIs. Administration model conveyed at this layer is alluded to as Stage as a Administration (PaaS). This offers an integrated set of developer environment that a developer can tap to build their applications without having any clue about what is going on underneath the service.
- *The Application Layer:* The application layer is the top level of the design and gives virtual applications. Administration model conveyed at this layer is alluded to as Programming as a Administration (SaaS). Applications are remotely facilitated by the application or administration supplier and made accessible to clients on demand, over the Internet.

The Cloud suppliers need a certain kind of administration on each layer to simplify the configuration of the Cloud infrastructure. The administration parts make the related virtual parts on their particular layer. Figure 1 depicts the layered structure of Cloud Computing architecture.

In the layered design administrations of a higher layer can be made from administrations of the hidden layer. A core middleware manages physical assets and the virtual machines (VMs) sent on top of them. Cloud improvement situations are built on top of foundation administrations to offer application improvement and deployment capabilities. Once sent in the Cloud, these applications can be consumed by end users.

There are some highlights applied to a Cloud Computing which rouse clients to migrate to Mists and convey its services, among those are:

- *Self-Service:* Consumers of Cloud Computing administrations anticipate on-demand, nearly instant access to resources. To support this expectation, mists must allow self-administration access so that clients can request, customize, pay, and use administrations without intervention of human operators.
- *Elasticity:* Cloud Computing gives the illusion of infinite computing assets accessible on demand. Subsequently clients anticipate mists to quickly give assets in any quantity at any time. In particular, it is expected that the additional assets can be (a) provisioned, possibly automatically, when an application load increases and (b) discharged when load decreases.
- *Massive scalability:* Although organizations might have hundreds or thousands of systems, Cloud Computing gives the capacity to scale to tens of thousands of systems, as well as the capacity to massively scale bandwidth and storage space.

A. Intrusion Prevention In Cloud Computing

Intrusion Prevention system (IPS) is a new approach to barrier organizing systems, which combine the strategy firewall with that of intrusion detection properly, which is a proactive technique, proccasion the attacks from entering the system by examining distinctive information record and detection demeanor of design recognition sensor, when an attack is identified, intrusion prevention piece and log the offending data. IPS screens system and take activities based on recommended rules when an occasion occurs. It sits inline on the system and passive in nature. IPSs take detection a step further, some see them as next generation IDS systems. Intrusion prevention is an extension of intrusion detection. An organization can't secure its system with only firewall, an additional layer of security must be provided. An intrusion prevention system gives an additional layer of security by scanning all the system action and particular browser protection.

B. Approaches of IPS

One problem faced by all detection in IPS is troublesome to perceive and perceive examination of bundles in real-time traffic. Two approaches to detect dangers are;

(i) Host based approach

It is a popular approach, it checks for suspicious action from the host or working system level. It gives intrusion prevention by triggering an alarm.

(ii) System based approach

It perceive packet all inbound-outbound in the network. In this approach, a system is introduced in the system and used to make physical security zones, the system becomes intelligent and is able to quickly and precisely perceive awesome action from bad traffic.

Some of the other approaches used in Intrusion prevention system are;

→ Sandbox Approach

Java applets and distinctive scripting languages are quarantined in a sandbox - an zone with restricted access to the system resources. The system runs the code in the sandbox and screens its behavior. If the code deviates from the predefined behavior, it stops the execution of code.

→ Programming based heuristic approach

This approach is similar to IDS anomaly detection using neural networks. But it has capacity to act against intrusions and piece them.

→ Hybrid Approach

On network-based IPS, distinctive detection methods, convention anomaly, action anomaly, and signature detection work together to decide a forthcoming attack and piece action coming from comparing router.

V. CONCLUSION

Cloud Computing has given rise to a new administrations worldview to the information technology. Cloud computing is distributed in nature, hence chances of intrusion is more. Dissecting distinctive strategies of intrusion detection and prevention systems has revealed that either using anomaly or signature based strategies stand alone will not give desired security features. Hence, a hybrid mechanism can be implemented to enhance the detection rate. It also motivates us to explore this zone further and to work on cloud IDS approach administered by a third party IDS provider.

REFERENCES

[1] Mohammed A. Ambusaidi, Xiangjian He, Priyadarsi Nanda & Zhiyuan Tan, "*Building an Intrusion Detection System Using a Filter-Based Feature Selection Algorithm*", in IEEE transactions on Computers, Vol: 65, Issue: 10, PP: 2986 – 2998, 2016.

[2] Xiujuan Wang, Chenxi Zhang & Kangfeng Zheng, "*Intrusion detection algorithm based on density, cluster centers, and nearest neighbors*", in China Communications, Vol: 13, Issue: 7, PP: 24 – 31, 2016.

[3] Zhiyuan Tan, Aruna Jamdagni, Xiangjian He, Priyadarsi Nanda & Ren Ping Liu, "*A System for Denial-of-Service Attack Detection Based on Multivariate Correlation Analysis*", in IEEE transactions on Parallel and Distributed Systems, Vol: 25, Issue: 2, PP: 447 – 456, 2014.

[4] Daniel Sun, Min Fu, Liming Zhu, Guoqiang Li & Qinghua Lu, "*Non-Intrusive Anomaly Detection With Streaming Performance Metrics and Logs for DevOps in Public Clouds: A Case Study in AWS*", in IEEE transactions on Emerging Topics in Computing, Vol: 4, Issue: 2, PP: 278 – 289, 2016.

[5] Ajay Kumara M. A & Jaidhar C. D, "*Hypervisor and virtual machine dependent Intrusion Detection and Prevention System for virtualized cloud environment*", in 1st International Conference on Telematics and Future Generation Networks (TAFGEN), PP: 28 – 33, 2014.

[6] Zhiyuan Tan, Upasana T. Nagar, Xiangjian He, Priyadarsi Nanda, Ren Ping Liu, Song Wang & Jiankun Hu, "*Enhancing Big Data Security with Collaborative Intrusion Detection*", in IEEE transaction on Cloud Computing, Vol: 1, Issue: 3, PP: 27 – 33, 2014.

[7] Shui Yu, Yonghong Tian, Song Guo & Dapeng Oliver Wu, "*Can We Beat DDoS Attacks in Clouds?*", in IEEE Transactions on Parallel and Distributed Systems, Vol: 25, Issue: 9, PP: 2245 – 2254, 2014.

[8] Pasquale Donadio, "*Virtual intrusion detection systems in the cloud*", in Bell Labs Technical Journal, Vol: 17, Issue: 3, PP: 113 – 128, 2012.

