ACTA SCIENTIFIC COMPUTER SCIENCES

Volume 2 Issue 2 February 2020

Research Article

A Survey Paper on Hypervisor-Based Cloud Intrusion Detection System (IDS)

Imran Mahmood*

IQRA University, Pakistan

***Corresponding Author:** Imran Mahmood, IQRA University, Pakistan.

Received: January 04, 2020

Published: January 31, 2020

Abstract

Cloud computing is a type of computing that relies on sharing computing resources rather than having local servers or personal devices to handle applications. In cloud computing, the word cloud (also phrased as "the cloud") is used as a metaphor for "the Internet," so the phrase cloud computing means "a type of Internet-based computing," where different services such as servers, storage and applications, are delivered to an organization's computers and devices through the Internet.

Cloud computing has many common characteristics with distributed systems like use of networking and sharing. Thus security is the biggest issue. Cloud computing intrusion detection is an active research area. A cloud computing environment requires some intrusion detection systems (IDSs) for protecting each machine against attacks. An IDS is a system that will analyze all the traffic on the network. They will compare them against their database, and decide whether or not it's an attack, in order to alert an administrator, or an IPS, to stop the intrusion.

In the cloud environment Hypervisor and Virtual Machine are more significant for protecting valuable data from attackers. A hypervisor or virtual machine monitor (VMM) is computer software, firmware or hardware that creates and runs virtual machines. A computer on which a hypervisor runs one or more virtual machines is called a host machine, and each virtual machine is called a guest machine. Cloud providers use the virtualization technology to share the sources, which is available in two levels including virtual machine and hypervisor. In the infrastructure, the cloud virtual machines are shared with other organizations virtual machines as the service. It is tried to use the virtualization properties in the hypervisor level and improve the IDS in the infrastructure layer of cloud computing.

Keywords: Hypervisor; Intrusion Detection System

Introduction

Cloud computing is an emerging technology adopted by organizations of all scale due to its low-cost and pay-as-you-go structure. It has revolutionized the IT world with its unique and ubiquitous capabilities. Organization prefers cloud as it replaces the high price infrastructure and need of maintenance. It offers three service models of software as a service (e.g. Google Apps [1]), platform as a service (e.g. Google App Engine [2], Microsoft's Azure [3]) and infrastructure as a service (e.g. Amazon Web Service [4], Eucalyptus [5], Open Nebula [6]). Virtualization enables cloud to provide elasticity, ease of use, scalability and on-demand network access to a shared pool of configurable computing resources [7]. Cloud computing paradigm has a service-oriented architecture which has led to a drastic alteration on how services are provided and managed. Intrusion detection techniques are used in any computing environment as a layer of defense. The basic aim is to detect any malicious activity well before any significant harm is possible. The general idea is to detect and identify attacks by either analyzing system artifacts (such as log files, process lists, etc.), or by keeping track of network traffic. Two main approaches used are signature based detection and anomaly-based detection. Signature based detection works by defining patterns of known attack signatures. If the system is found to be processing any code similar to those signatures, it is detected suspicious and marked as an intrusion. On the other hand, anomaly based detection works by analyzing activities performed on the system. Initially, a profile for a particular system is created by recording normal activities (e.g., by setting thresholds for normal bandwidth usage). If later on, the system's behavior is analyzed as anomalous to the profile defined, it is marked as an intrusion. Whereas signature-based detection techniques (also called misuse pattern matching) cannot detect unknown attacks, anomaly based techniques usually result in huge false positives or negatives.

The distributed nature of cloud environment makes it most vulnerable and attractive environment for the intruders to perform attacks. Intrusion detection systems can be used to enhance the security of such systems by systematically examining the logs, network traffic as well as configurations. However conventional intrusion detection systems (IDSs)—which can be classified into host-based intrusion detection systems (HIDS) and network-based intrusion detection systems (NIDS)—are not appropriate for cloud environment as these are unable to locate the hidden attack trail, e.g., the network-based IDS is unable to detect any event in case of

encrypted node communication and it is possible for the attacker to gain control over the installed virtual machines if the hypervisor is compromised. Some of the popular attacks on virtual machine include DKSM [8], SubVirt [9], and Bluepill [10]. Attackers can use the compromised hypervisor to gain control over the host. Owing to the fact that the IDS techniques were not designed with the specific context of virtualization under consideration, they do not offer the same protection in such environments. There are certain trade-offs that need to be faced when deploying IDS in the virtual environment, mostly because of their inability to inspect the internal working of the operating systems. Despite the huge benefits that are offered by virtualization, there are a number of security risks that are associated with it. It introduces a number of new problems that did not exist in a traditional computing environment. Cloud computing providers are adopting software-defined networking (SDN) to achieve on-demand provisioning of network services, since SDN can provide a centralized system to manage the network. The network administrator is empowered by SDN to easily access and manage individual flows by facilitating them to implement monitoring applications, i.e., firewall and IDS. Furthermore, scalable monitoring and dynamic reconfiguration requirements of the network in cloud makes SDN a perfect choice.

Intrusions in Cloud

An attempt to compromise the confidentiality, integrity, or availability of a system or network is known as an intrusion. In this section important classes of intrusion that commonly affect the cloud are described. This is followed by a presentation of various attacks in the cloud, classified with respect to cloud's deployment model.

Denial of service (DoS) attack

The hacker uses bots (zombies) for flooding a system with a large number of packets to render the available resources unreachable. Subsequently, the services for the time being are not available on the Internet. According to some vulnerability experts, an attacker can affect more users by launching a DoS attack on cloud [17].

Insider attack

Insider is defined as a former or current employee/associate of the cloud service provider which has privileged access and authority to perform modifications in the cloud environment [17]. Insider attacks are organized as they have information about the user and provider. This is fatal as many attacks can be executed from inside and an intruder can easily evade detection in the absence of proper controllers [17]. A DoS attack by an insider was launched on Amazon Elastic Compute Cloud (EC2) [17], cloud consumers' confidentiality was breached in this attack.

User to Root (U2R) attack

In this attack, the intruder accesses the credentials of an authentic user and then exploit the system vulnerabilities (buffer overflow) to access root privileges. In the cloud, the attacker first accesses an instance and exploits its vulnerabilities to achieve root privileges of a virtual machine or host. By this attack, integrity of the cloud is being violated [13].

Port scanning

Port scanning is used by the attacker to obtain information about open, closed, filtered, and unfiltered ports [13]. The attacker then uses this information to launch attacks on open ports. Different techniques are used in order to perform port scanning. This attack targets the confidentiality and integrity of the cloud.

Attacks on virtualization

If an attacker compromises the hypervisor, the virtual machines can be easily infiltrated [13]. The best option to capture virtual machines via hypervisor is to exploit a zero-day vulnerability. Zero-day attacks are exploitation of vulnerabilities for which system administrator or developer has not applied the patch. Since many virtual machines use the same resources, i.e. hardware, side channel data is vulnerable due to this type of access among virtual machines [17].

Backdoor channel attack

This is a passive attack in which a node in cloud is compromised and in future the node is used as a bot to carry out attacks like DDoS attack. The system is compromised by shellcode, Trojan, and other similar exploitations. After the node is compromised the intruder has full access to the system and data available [13].

An alternative model of virtualization based intrusion detection system in cloud computing

Partha Ghosh, Ria Ghosh, Ruma Dutta This proposed model is based on the concept of Virtualization of IDS 'in cloud environment. Whenever a user starts a session an instance of IDS i.e. Mini IDS is created and works on the specific user. It monitors, supervises and achieves protection. Mini IDS contains a term called Agent. Each instance supervises on each user activities and sends a report of all the activities to the IDS Controller via cloud NIDS after the end of each session. IDS Controller manages all the instances. IDS Controller works through three steps named as Agents, Directors and Notifiers. Information from the data sources of log files, processes and network are captured by agents and are sent them to director. Agents lie in IDS instances and Directors are located in the IDS Controller. Directors make the analysis of information, which determines whether an attack is happening. Notifier takes the necessary action. To handle the heavy flow of network traffic a multithreaded cloud IDS is placed on the bottleneck of network points such as router, gateway outside the virtual machine and monitor the network traffic.

Virtualization is prone to attacker for its distributed environment. So to protect the cloud efficiently the best solution is that incorporate both NIDS and HIDS. An efficient, reliable and scalable Intrusion Detection System is needed for Cloud environment. Virtualization provides the best solution for the IDS/IPS systems and provides security against attacks (Figure 2).

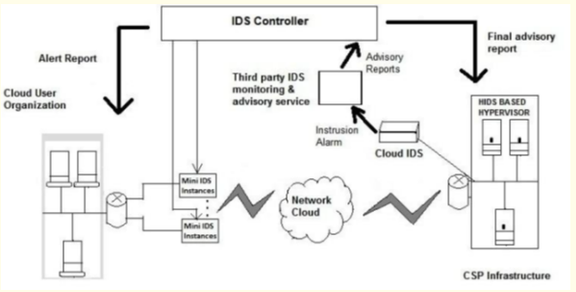

Figure 1: Proposed Cloud IDS Model.

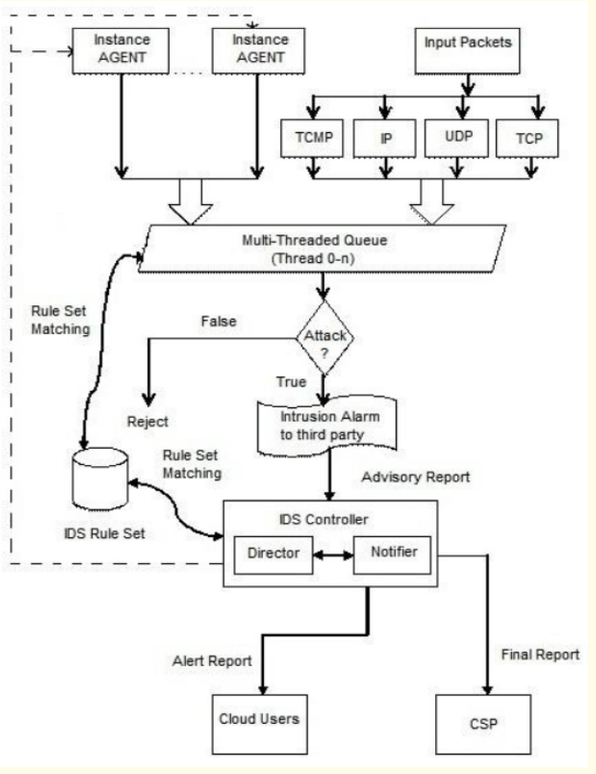

Figure 2: Flowchart of proposed model.

Automated approach to intrusion detection in vm-based dynamic execution environment

Feng Zhao, Hai Jin The technique of virtual memory introspection was introduced by Bryan D. Payne., *et al.* They design the Xen Access architecture and present the Xen Access monitoring library to provide virtual memory inspection and virtual disk monitoring Automated Intrusion Detection in VM-based Environment capabilities based on six high-level requirements [14]. Monitoring virtual memory with Xen Access requires no changes to the VMM, VM and OS. Using introspection, Xen Access can view the memory of another VM access with the target to infer OS data at an abstract level. Attacks, especially those that attempt to compromise a computer system using the system call interface, are an increasingly important threat to virtual computing environment. Using virtual memory introspection provided by Xen Access, monitoring system call at the abstract level becomes feasible and more convenient, which can detect and control guest applications by checking them at runtime. Monitoring system calls of guest VM and specifying the program's normal behavior is an effective approach for stopping a large class of malicious attacks [15]. Essentially, it is helpful to convert a potentially successful attack into a fail-stop failure of the compromised process The Hidden Markov Model (HMM) is a powerful statistical tool for modeling generative sequences that can be characterized by an underlying process generating an observable sequence [16].

HMM is a special type of Bayesian Network. The formal definition of a HMM is as follows:

$\lambda = (S, V, A, B, \pi).$, (1)

where S is the state set, and V is the observation set. Suppose n is the total number of states, and m is the maximum number of observed sequence:

$S = (s1, s2..., sn).$, (2)

$V = (v1, v2..., vm).$ (3)

A is the state transition probability matrix, storing the probability of state j following state i.

$A = [aij]n \times n$, $aij = p$ (step t at sj|step (t − 1) at si). (4)

B is the observation probability array, storing the probability of observation k from state i. $B = \{bi(k)\}$, $bi(k) = p(vk|si)$. (5)

π is the initial probability array, storing the probability of state i at first step.

$\pi = \{\pi i\}$, $\pi i = p$ (si at initial step).

For HMM model $\lambda = (S,V,A,B,\pi)$, the system call sequences are compared to the observation V, the observed sequences will be either normal or attack Paulo Ver´ıssimo., *et al.* represent a well-defined relationship between attack, vulnerability, and intrusion which is called AVI composite fault model [17].

The scheme given by Feng Zhao, Hai Jin uses dynamic graph structure to monitor the dynamic changing of computing environment. And hidden Markov model strategy for abnormality detection using frequent system call sequences to identify and detect attacks. the automated mining algorithm, named AGAS, to generate frequent system call sequences. Rather than setting a user-defined threshold on mining frequent sequences, AGAS algorithm utilizes related probabilities to identify frequent sequences.

A study of intrusion detection system for cloud network using FC-ANN algorithm

Gayatri K. Chaturvedi, Arjun K. Chaturvedi, Varsha R. The intrusions may bring all kinds of misuses. Intrusion Detection Systems (IDS) play a very important role in the security of today's networks by detecting when an attack is happening. Due to increasing incidents of cyber-attacks, building effective intrusion detection systems are essential for protecting information systems security. Intrusion detection attempts to detect computer attacks by exam-

ining various data records observed in processes on the network. Detection precision and detection stability are two key indicators to evaluate intrusion detection systems (IDS). In early stage in order to enhance the detection precision and detection stability, the research focuses lies in using rule-based expert systems and statistical approaches. But when encountering larger datasets, the results of rule-based expert systems and statistical approaches become worse. Thus a lot of data mining techniques have been introduced to solve the problem. Among these techniques Artificial Neural Network (ANN) is one of the widely used techniques and has been successful in solving many complex practical problems and ANN has been successfully applied into IDS. However, the main drawbacks of ANN-based IDS exist in two aspects: (1) lower detection precision and (2) weaker detection stability. The main reason of above problem is that distribution of different types of attack is imbalanced. To solve the above two problems, we propose FC-ANN (Fuzzy-Clustering Artificial Neural Network) to enhance the detection precision for low frequent attacks and detection stability.

Evaluation of Intrusion detection system has two key indicators: detection precision and detection stability. In order to enhance the detection precision and detection stability, in the early stage the research focus lies in using rule based expert systems and statistical approaches. But for larger datasets rule based expert systems and statistical approaches becomes worse. To solve this problem lots of data-mining techniques have been introduced. Among these Artificial Neural Network (ANN) is one of the widely used techniques. The main drawbacks of ANN-based IDS exist in two aspects: lower detection precision for low-frequent attacks and weaker detection stability. The main reason of these problems is the distribution of different types of attack is imbalanced. For low-frequent attacks, the leaning sample size is too small compared to high-frequent attacks. It makes ANN not easy to learn the characters of these attacks and therefore detection precision is much lower. To solve the above two problems, a novel approach is introduced for ANN-based IDS, FC-ANN to enhance the detection precision for low-frequent attacks and detection stability.

Benefits of FC-ANN based IDS.

The general procedure of FC-ANN approach is divided into three stages. In the first stage, a fuzzy clustering technique is used to generate different training subsets. Based on different training sets, different ANNs are trained in the second stage. In the third stage, in order to eliminate the errors of different ANNs, a meta-learner with fuzzy aggregation module, is introduced to learn again and combine the different ANNs results. By fuzzy clustering, the whole training set is divided into subsets which have less number and lower complexity. Thus the ANN can learn each subset more quickly, robustly and precisely, especially for low-frequent attacks, such as U2R and R2L attacks.

Multi-threaded NIDS model for distributed cloud environment is based on three modules: capture and queuing module, analysis/processing module and reporting module.

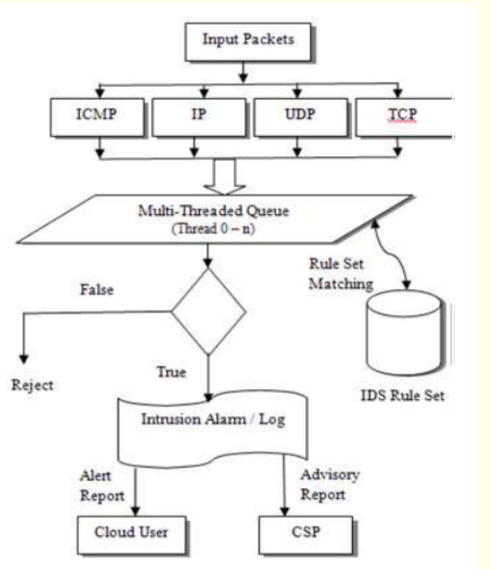

Figure 3: Flowchart of cloud IDS.

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 As ANN is new in field of networking specially cloud I needs to get trained well to detect intrusions. The more trained the FC-ANN is more it will be able to detect intrusions. the proposed techniques also provide many different subsets which can be applied during detection which makes the process less complex and efficient.

Impact of DOS attacks

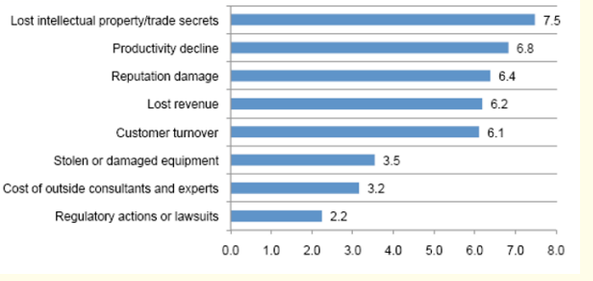

Figure 4

Showing different types of attacks on cloud

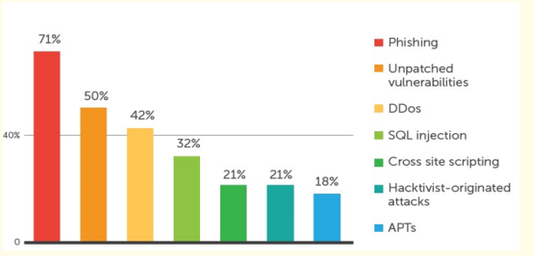

Figure 5

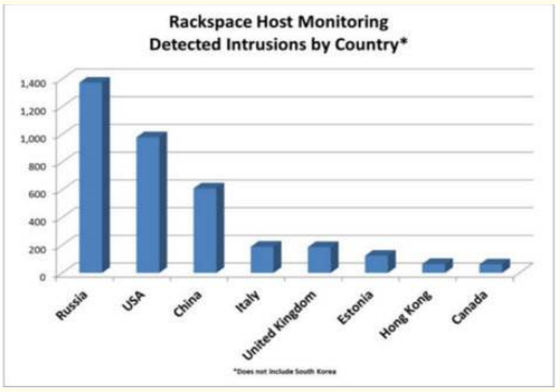

Figure 6

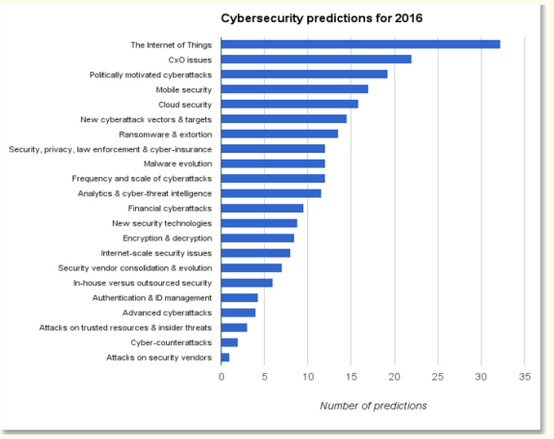

Figure 7

An Alternative Model of Virtualization Based Intrusion Detection System In Cloud Computing	Automatic but manual help available	Real time cloud base specific less complex	Good performance	Flexibility for 3rd party IDS/ IPS
Automated approach to intrusion detection in vm-based dynamic execution environment	Automatic	Real time complex	High performance	Rigid not flexible
A study of Intrusion Detection System for Cloud Network Using FC-ANN Algorithm	Automatic Training possible	Real time training and also protection simple	Good performance	Flexible

Table 1

Discussion and Conclusion

Security is not a standstill activity its always evolving with the passage of time and experience. There are many techniques are applied in the field of IDS/IPS systems. All have success in almost in the start but with the passage of time if IDS systems are not updated and changes according to situation. The success rate decreases with the evolution of cloud technology there are many solutions present. the solutions are enormous.

We should not reinvent the wheel its invented long ago. meaning there are many solutions present in the market we can use them for our convenience. cloud computing also provides us with customize services. There are 3rd party softwares present which can provide us with the level of security required by us. Examples can be snort cisco IDS/IPS. they are able to give the better service and software for the IDS.

Bibliography

1. "Google Apps for Work – Gmail, Drive, Docs and More,"
2. "Google apps engine,"
3. "Azure services platform,"
4. "Amazon web services,"
5. "Eucalyptus,"
6. Opennebula.
7. P Mell and T Grance. "The NIST Definition of Cloud Computing (Draft),".
8. S Bahram., *et al.* "DKSM: Subverting Virtual Machine Introspection for Fun and Profit". In Reliable Distributed Systems, 2010 29th IEEE Symposium on (2010): 82-91.
9. ST King., *et al.* "SubVirt- Implementing malware with virtual machines". IEEE Symposium on Security and Privacy (2006): 314-327.
10. J Rutkowska. "Subverting Vista TM kernel for fun and profit". In Black Hat Conference (2006).
11. A Patel., *et al.* "An intrusion detection and prevention system in cloud computing: A systematic review". *Journal of Network and Computer Applications* 36.1 (2013): 25-41.
12. M Zbakh., *et al.* "A multi-criteria analysis of intrusion detection architectures in cloud environments". Cloud Technologies and Applications (Cloud Tech) International Conference on (2015): 1-9.
13. C Modi., *et al.* "A survey of intrusion detection techniques in Cloud". *Journal of Network and Computer Applications* 36.1 (2013): 42-57.

14. Payne BD., *et al.* "Secure and Flexible Monitoring of Virtual Machines". In: Proceedings of 23rd Annual Computer Security Applications Conference, ACSAC, Miami Beach (Florida), USA (2007): 385-397.

15. Rajagopalan M., *et al.* "System Call Monitoring Using Authenticated System Calls". IEEE Transactions on Dependable and Secure Computing 3.3 (2006): 216-229.

16. Khanna R and Liu H. "Control Theoretic Approach to Intrusion Detection Using a Distributed Hidden Markov Model". *IEEE Wireless Communications* 15.8 (2008): 24-33.

17. Bessani A., *et al.* "Cheap Intrusion-Tolerant Protection for Crutial Things". *Technical Report* (2009).