Academic Guru Publication House

Advances in Cloud Computing Security
Techniques and Applications
Volume 1
Year: 2021

AG PH Books

A Survey of Intrusion Detection Systems for Cloud Computing

Ms. Savita Singh[1*]

[1]*Assistant Professor, IT Department, Institute of Management Studies, Noida*

Abstract

End customers benefit from scalable, virtualized, on-demand services delivered through the cloud, all while spending less money on infrastructure. Internet-based delivery of such services is made possible by the use of well-established networking protocols as well as formats, which are overseen by a variety of organisations. Deficiencies and flaws in the underlying technology and old protocols may lead to intrusions. Cloud resources as well as services are protected from a variety of threats and assaults by (IDS) that is Intrusion Detection System, which is the most often utilised component of the computer security as well as compliance. Cloud incursions, IDS detection methods, including IDS based over the Cloud Computing are all discussed in this study.

Keywords: Cloud computing, Firewalls, Intrusion detection system, Intrusion prevention system.

1. INTRODUCTION

In today's IT environment, (CC) that is the cloud computingis a rapidly expanding computational paradigm. Internet-based computer resources (example- network, server, storage, apps, and etc.) are made available as the "service" via internet again for benefit of consumers [1]. Platform (the virtualized operating system for the server) as well as application (including web applications) layers are the three primary abstraction levels of this system [2]. CC has a number of distinct features:

- **Virtual**: It's easy for users to know where they are and what's going on below.

* ISBN No. 978-81-955340-6-7

- **Scalable**: Having the ability to decompose large and difficult jobs into smaller, more manageable chunks.
- **Efficient**: Dynamic provisioning of the shared computing resources using the Services Oriented Architectures.
- **Flexible**: It can handle a wide range of workloads, from consumer to business. Platform as a Service also represented as (PaaS), Infrastructure as a Service also represented as (IaaS), and SaaS models are all examples of cloud computing's 3-service models. Using infrastructure as a service approach, consumers may have access to a variety of resources, including hosting servers as well as networks. In tools, PaaS, languages, including APIs are provided for the creation, deployment, including operation of cloud-based applications, whereas in SaaS, even systems provide fully-functional online applications which customers may operate without the need for additional hardware or software installation.

There are two types of NICs in network intrusion detection system also represented as (NIDS) : one for licentious mode and one for management mode. When IDS is installed in network or even at the network's edge, it keeps tabs on all of the traffic that flows through it. (HIDS) that is Intrusion detection systems and software-based programmes are installed on the host to be watched by shareholders. Whenever an assault is detected, the agents would monitor an operating system as well as write data into the log Rles. The Host Intrusion Detection Systems also represented as (HIDS) are able to monitor installed agents on every unique host. It is possible to keep track of any attempted intrusions on crucial servers using Host-based IDS systems.

1.1. INTRUSIONS TO CLOUD SYSTEMS

This section demonstrates a number of common intrusions, that can cause Cloud resources as well as services to be unavailable, compromised, or otherwise compromised.

A. **Insider attack:**Unauthorized rights may be gained by authorised Cloud users. There is a risk that insiders may perpetrate frauds and leak confidential information (or even destroy information with an intent). This raises severe concerns about a person's ability to put their faith in the organisation. As an illustration, an internal denial-of-service attack against an Amazon Elastic Compute Cloud that is represented as (EC2) was presented [4].

B. **User to Root attacks:**their account. In order to get root-level access to the system, someone may take advantage of these vulnerabilities. This may be accomplished by exploiting buffer overflows in a process that is already executing as root. When the application programme code exceeds the static buffer, it results in an error. Weak password recovery procedures, phishing assaults, keyloggers, as well as other forms of security risk can't be prevented by using security methods that are universally accepted as standard practise. In the Cloud, even an attacker may get root access to the VMs or hosts by acquiring access to a legitimate user's instances.

C. **Flooding attack:**In this scenario, the attacker aims to overwhelm the victim through the sending a large number of packets from innocent host (zombies) in network. Packets can be of type TCP, UDP, ICMP or a mix of them. This kind of attack may be possible due to illegitimate network connections. In case of Cloud, the requests for VMs are accessible by anyone through Internet, which may cause DoS (or DDoS) attack via zombies. Flooding attack affects the service's availability to authorized user. By attacking a single server providing a certain service, attacker can cause a loss of availability on the intended service. Such an attack is called direct DoS attack. If the server's hardware resources are completely exhausted by processing the flood requests, the other service instances on the same hardware machine are no longer able to perform their intended tasks. Such type of distributed attack is called indirect attack. Flooding attack may raise the usage bills drastically as the Cloud would not be able to distinguish between the normal usage and fake usage.

D. **Attacks on Virtual Machine (VM) or hypervisor:** On compromise the lower layer hypervisor, attacker can gain control over installed VMs. E.g. BLUEPILL [5], SubVir [6] and DKSM [7] are some well-known attacks on virtual layer. Through these attacks, hackers can be able to compromise installed-hypervisor to gain control over the host. New vulnerabilities, such as zero-day vulnerability, are found in Virtual Machines (VMs) [8] that attract an attacker to gain access to hypervisor or other installed VMs. A zero-day vulnerability is a threat that tries to exploit application vulnerabilities that are unknown to others or the software developer. Zero-day exploits are used by attackers before the developer of the target software knows about the vulnerability. A zero-day vulnerability was exploited in the HyperVM virtualization application which resulted in destruction of many virtual server based websites [9]

E. **User to Root attacks :** Here, a criminal gains access to the user's account via posing as the user. sniffing password. This makes him able to exploit vulnerabilities for gaining root level access to system. For example, Buffer overflows are used to generate root shells from a process running as root. It occurs when application program code overfills static buffer. The mechanisms used to secure the authentication process are a frequent target since there are no universal standard security mechanisms that can be used to prevent security risks like weak password recovery workflows, phishing attacks, keyloggers etc. In the Cloud, an attacker may get root access to the VMs or hosts by acquiring access to the legitimate user's account.

F. **Port Scanning:** It gives a list of the ports that are open, closed, or even filtered. Attackers may locate open ports by scanning for them, and then launch attacks against the services that use those ports. This attack may provide information about the network's IP address, router, MAC address gateway filtering, the firewall rules, and more. TCP scanning,, the SYN scanning, the UDP scanning, even the FIN scanning, the Window scanning, the ACK scanning, (similar as ACK scanning but it examines any alterations in window field of packets) and so on. Are some of several port scanning methods available. Via port scanning, the attacker inside a Cloud environment may find open ports on that these services are offered and exploit them.

2. IDS ARCHITECTURES IN CLOUD

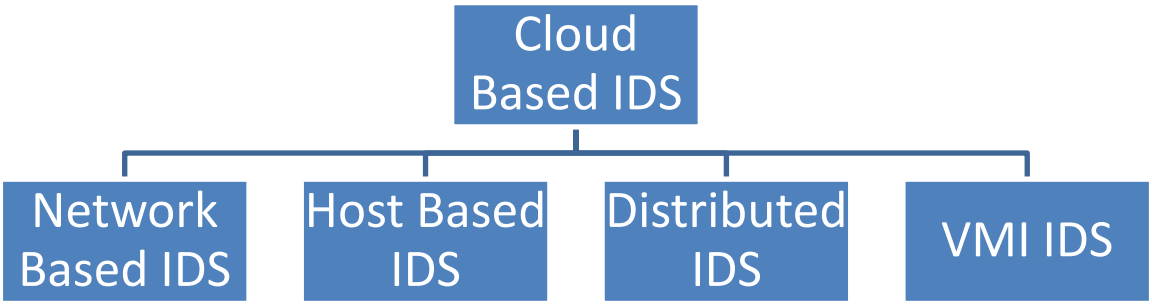

Figure: 1 Types of Cloud-Based IDS

2.1. Network intrusion detection systems

An example of a common network intrusion detection system (NIDS) for virtualized settings is presented by [10]. A virtual switch has an NIDS placed on it (through that the traffic of all the VMs together passes). In a typical computer context, an NIDS would be installed on the border server. There is a strong resemblance between this method and the standard NIDS. A virtualized environment has been designed to fit its needs and tested as a result of the work done by authors All the VM traffic is collected and logged by NIDS just on vSwitch. To detect DoS or even DDoS attacks, it employs SNORT [11] tools. The starting IP address is being used to analyse traffic. Unusual traffic coming from an IP address is immediately stopped, and the affected application is relocated to the different data centre. DDoS assaults and the botnets may be detected and blocked using this method. Only the known attacks may be detected by using SNORT, and also no performance data are provided in the publication [12]. This research does not address the issue of supporting large virtual networks with high traffic volumes [13]. Large virtual networks might provide problems for the detection of attacks by NIDS, since it may not be able to analyse all of the packets in the network at the same time. To recognize DoS attacks on the virtual SIP-based hosts, [14] having simulated IDS at several cloud locations. Detection is done using a signature-based approach. SNORT has indeed been chosen as that of network IDS for testing in Eucalyptus cloud computing environment. [15] Point out the major drawbacks of past strategies and provide a solution to remedy them. The added complexity that comes with checking all virtual machines for possible threats. In their study, they argue that the introduction of profile-based IDS may alleviate this issue. For the cloud, they propose an NIDS-based VMI that creates an individual profile for every virtual machine by comparing known attacks signatures as well as divergence from typical threshold values.

2.2. Host intrusion detection systems

There are three basic deployment-based categories for HIDS approaches with regard to the cloud in general. HIDS may be installed inside the host OS (in which it could monitor either host OS or even guest OS by communication by the VMM [16]) or even in the separate guest OS for the monitoring purposes. The poor attack resilience of an IDS that is totally controlled by the client is a downside of such first scenario. Because it's been widely panned in the literature, it's been ruled out for use in the cloud [17]. They [16] refer to this as a type I or type II situation where VMM seems to be the sole host process running as well as many VMs are operating over it. An alternative type II scenario assumes the virtual machine manager operates as software over host computer. In addition to host's normal processes, VM runs on host's virtual machine manager (VMM). [18] By using concepts of automated computing, we present an intrusion prevention system based on autonomous agents. The employment of the autonomous sensors to keep tabs on system activity including network traffic is indeed an anomaly-based detection strategy for spotting hostile activity. Detection of intrusions is based on abnormal levels of resource use by a user, according to [19]. (AAA) which is Authentication, Authorization, and Accounting is indeed the primary component of approach. The user's current use history is used to calculate the anomalous level. More guest OS may be introduced with no worry about the detection speed thanks to IDS of the medium as well as low-level security using less resources. The administrator has access to log files and may do audits on them.

2.3. Distributed intrusion detection systems

[20] has developed as well as simulated the intrusion detection system to fight DoS as well as DDoS assaults in the cloud. The IDS consists of four parts, each of which serves a distinct purpose. This prevents the single point of the failure inside the system. As a result, it does not identify unknown assaults since it relies on signature-based detections. The authors [21] propose a three-dimensional IDS. It is a cloud-based IDS for the IaaS users. A server as well as several agents make up 3-D IDS. The architecture is offered as a theoretical concept with no accompanying experimental proof. It also needs that the server be installed at the user end that is not always the case for all users. The Multithreaded network intrusion detection systems (MITIDS) are being proposed by [22] to combat Cross Site Scripting (XXS) as well as DDoS assaults. A capture module, an analysis as well as processing module, and just a report generation module make up the approach. In theory, it's a new technique, but no proof has been presented by the researcher. Another intrusion detection system relying on VMs is Siren [23]. Sniffer detects malicious software operating in the VM that tries to communicate with the network it is connected to. Virtual machines (VMs) should not produce traffic on network in absence of the human intervention, according to Siren's design. Siren labels traffic as dangerous if it detects such a situation. Siren's capability to insert designed human input to explore for ad-on malware is among the strongest capabilities. But producing traffic which closely mimics human input is the main issue with this method.

2.4. Virtual Machine Introspection (VMI) based techniques

Out-of-the-box intrusion detection is based on the virtual machine introspection also represented as (VMI). In VMI, inspection module is moved outside of virtual machine. Detection of any intrusions in guest system's software is carried out outside. One benefit of this method would be such malware detection is undisturbed even if an incursion occurs. HIDS as well as NIDS do not have this feature. Confidence is lost when HIDS reports inaccurately when NIDS has restricted sight. VMI-based intrusion detection systems have recently been proven in works by [24], [25], [26], as well as [27]. We'll go into these strategies in a minute. [28] Livewire, an intrusion detection prototype relying on VMI, is proposed. The VMM must be basic and well implemented for this method to work. VMM is protected by such a feature, making it harder for an attacker to get access. VMM's isolating, inspections, as well as interposition features are key to the technique's success. Livewire's OS library interface must be written in the safe programming language for multiple operating systems in order to avoid an attack upon itself. Revolutionary accomplishment in field of the virtual machine IDS, Livewire is regarded to be.

[28] Propose VMwatcher, that is a pre-configured intrusion detection system that is more accurate and resistant to tampering. The underlying VMM is assumed to be safe by VMwatcher. Type -II VMs may make use of this strategy. VMwatcher's best-known feature is its capability to close a semantic gap2 which is always present when obtaining an external perspective of guest OS. VMwatcher employs two distinct strategies: VM introspection that isn't obtrusive, as well as guest viewpoint casting. VMI is a kind of non-intrusive introspection. View casting is a technique used to create VM’s semantics view (— for example, file systems, processes, as well as directories). Memory states are captured in VM raw picture as well as a semantic representation is reconstructed. For both Windows as well as Linux, the prototype has been thoroughly tested. The semantic view is carefully crafted by VMwatcher to retain VM view. Furthermore, authors claim their VMwatcher has indeed the capacity to identify stealthy malware through comparing the internal and exterior views.

CONCLUSION

Intrusion detection would play an increasingly significant role in research landscape now that most of our current computer infrastructure migrates to cloud. Spending large sums of money on information security as well as privacy is a must to secure infrastructures throughout the globe. With the help of an IDS, a computer system may be kept safe and secure. IDSs for the cloud computing are in high demand since the number of people using the cloud increases at such a rapid rate. There are a number of cloud-based intrusion detection technologies now in use. In the cloud-based IDS world, there are four main subtypes to choose from: networks, hosts, distributions, and also introspection-based virtual machines (VMs). According to this poll, a number of potential threats to the security of Cloud services have been identified in future. Cloud security might not have been adequately addressed by one of the conventional options, such as a firewall.

REFERENCES

1. B. Zarpelao, "A survey of intrusion detection in internet of things;' Journal of Network and Computer Applications, 2017.
2. S. Raza, Wallgren , "Svelte: Real-time intrusion detection in the internet of things," Adhocnetworks, vol. 11, no. 8, 2013.
3. M. Nobakht, "A host-based intrusion detection and mitigation framework for smart home IoT using open flow," in Availability, Reliability and Security, 2016 11thInternational Conference on IEEE, 2016.
4. M. Slaviero, "BlackHat presentation demo vids: Amazon." [Online]. Available: http://www.sensepost.com/blog/3797.html
5. J. Rutkowska, "Subverting VistaTM Kernel for Fun and Profit," Black Hat Conference, 2006.
6. S. King, P. Chen, and Y-M. Wang, "SubVirt: Implementing malware with virtual machines," 2006 IEEE Symposium on Security and Privacy, 2006, pp.314-327.
7. S. Bahram, X. Jiang, Z. Wang, and M. Grace, "DKSM: Subverting Virtual Machine Introspection for Fun and Profit," Proceedings of the 29th IEEE International Symposium on Reliable Distributed Systems, 2010.
8. NIST: National vulnerability database. [Online]. Available: http://web.nvd.nist.gov/view/ vuln/detail?vulnId=CVE-2009-3733
9. D. Goodin, "Webhost Hack Wipes Out Data for 100,000 Sites." [Online]. Available: http://www.theregister.co.uk/2009/06/08/webhost_attack/.
10. A. Bakshi, and Y. B. Dujodwala, "Securing Cloud from DDOS Attacks Using Intrusion Detection System in Virtual Machine," Communication Software and Networks, 2010. ICCSN'10. Second International Conference on, pp. 260-264, 2010.
11. "Home - Snort.Org," https://www.snort.org/.
12. C. Modi, D. Patel, B. Borisaniya, H. Patel, A. Patel, and M. Rajarajan, "A survey of intrusion detection techniques in Cloud," Journal of Network and Computer Applications, vol. 36, no. 1, pp. 42-57, 2013.
13. N. A. Premathilaka, A. C. Aponso, and N. Krishnarajah, "Review on state of art intrusion detection systems designed for the cloud computing paradigm," 2013 47th International Carnahan Conference on Security Technology (ICCST), pp. 1 - 6, 2013.
14. C. Mazzariello, R. Bifulco, and R. Canonico, "Integrating a network IDS into an open source Cloud Computing environment," 2010 Sixth International Conference on Information Assurance and Security, pp. 265 - 270, 2010.

15. S. Gupta, P. Kumar, and A. Abraham, "A Profile Based Network Intrusion Detection and Prevention System for Securing Cloud Environment," International Journal of Distributed Sensor Networks, vol. 2013, pp. 1-12, 2013.

16. M. Laureano, C. Maziero, and E. Jamhour, "Intrusion Detection in Virtual Machine Environments," Proceedings. 30th Euromicro Conference, 2004., pp. 520 - 525, 2004.

17. S. Alarifi, and S. Wolthusen, "Anomaly detection for ephemeral cloud IaaS virtual machines," Network and System Security, pp. 321-335, 2013.

18. A. Patel, Q. Qassim, Z. Shukor, J. Nogueira, J. Júnior, C. Wills, and P. Federal, "Autonomic agent-based self-managed intrusion detection and prevention system," In Proceedings of the South African Information Security Multi-Conference pp. 223-234, 2011.

19. J.-H. Lee, M.-W. Park, J.-H. Eom, and T.-M. Chung, "Multi-level intrusion detection system and log management in cloud computing," Advanced Communication Technology (ICACT), 2011 13th International Conference pp. 552-555, 2011.

20. C.-C. Lo, C.-C. Huang, and J. Ku, "A Cooperative Intrusion Detection System Framework for Cloud Computing Networks," 2010 39th International Conference on Parallel Processing Workshops, pp. 280-284, 2010.

21. J. He, C. Tang, Y. Yang, Y. Qiao, and C. Liu, "3D-IDS: IaaS User-oriented Intrusion Detection System," Information Science and Engineering (ISISE), 2012 International Symposium on, pp. 12-15, 2012.

22. M. P. K. Shelke, M. S. Sontakke, and A. D. Gawande., "Intrusion detection system for cloud computing," International Journal of Scientific & Technology Research, pp. 67-71, 2012.

23. X. Zhao, B. Kevin, and P. Atul, "Virtual Machine Security Systems," Advances in Computer Science and Engineering, pp. 339-365, 2009.

24. T. Garfinkel, and M. Rosenblum, "A Virtual Machine Introspection Based Architecture for Intrusion Detection," In NDSS vol. 3, pp. 191-206, 2003. 35] X. Jiang, X. Wang, and D. Xu, "Stealthy malware detection through vmm-based out-of-the-box semantic view reconstruction," Proceedings of the 14th ACM conference on Computer and communications security - CCS '07, pp. 128-138 2007.

25. M. Laureano, C. Maziero, and E. Jamhour, "Intrusion Detection in Virtual Machine Environments," Proceedings. 30th Euromicro Conference, 2004., pp. 520 - 525, 2004.

26. B. D. Payne, M. Carbone, M. Sharif, and W. Lee, "Lares: An Architecture for Secure Active Monitoring Using Virtualization," 2008 IEEE Symposium on Security and Privacy (sp 2008), pp. 233-247, 2008.

27. T. Garfinkel, and M. Rosenblum, “A Virtual Machine Introspection Based Architecture for Intrusion Detection,” In NDSS vol. 3, pp. 191-206, 2003.

28. X. Jiang, X. Wang, and D. Xu, “Stealthy malware detection through vmm-based out-of-the-box semantic view reconstruction,” Proceedings of the 14th ACM conference on Computer and communications security - CCS '07, pp. 128-138 2007.