ADV MATH SCI JOURNAL

Advances in Mathematics: Scientific Journal **9** (2020), no.6, 3537–3548
ISSN: 1857-8365 (printed); 1857-8438 (electronic)
https://doi.org/10.37418/amsj.9.6.33 Spec. Issue on RDESTM-2020

A COMPREHENSIVE OUTLINE OF DIVERSE IDS/IPS WITH RESPECT TO HYPERVISORS

A. N. SESHU KUMAR[1], R. KUMAR YADAV, AND N. S. RAGHAVA

ABSTRACT. The wide exponential growth of cloud computing has opened its applications doors in almost all the areas ranging from business, communication, education, medical, scientific technologies and many more. This widespread on the other hand has given enough space for the intruders to carry out their tasks. Virtualization is the backbone of cloud computing concepts. With the help of virtualization , virtual machines are created in cloud. Virtualization cannot be carried out successfully without proper usage of hypervisors. Depending on the kind of application to be carried out on cloud a hypervisor can be either hardware, software or a firmware. Many instances can be carried out on a virtual machine with the help of these hypervisors which are helpful to run either on guest or host operating system. Intruders in order to gain control on cloud, they first try to achieve control over hypervisors. In this paper we discuss in detail about the various attacks which are being carried out on hypervisors and how to defend and offend them.

[1]*corresponding author*

2010 *Mathematics Subject Classification.* 68T99.

Key words and phrases. Anomaly based IDS (A-IDS), Artificial Intelligence (AI), Genetic Algorithms (GA), Hypervisor, Hybrid based IDS (H-IDS), Hypervisor-based Cloud Intrusion Detection System (HCIDS), Intrusion Detection System (IDS), Side-channel attack (SCA), and Signature based IDS (S-IDS), Virtual Machine (VM) and Virtual Machine Introspection (VMI), Visualization.

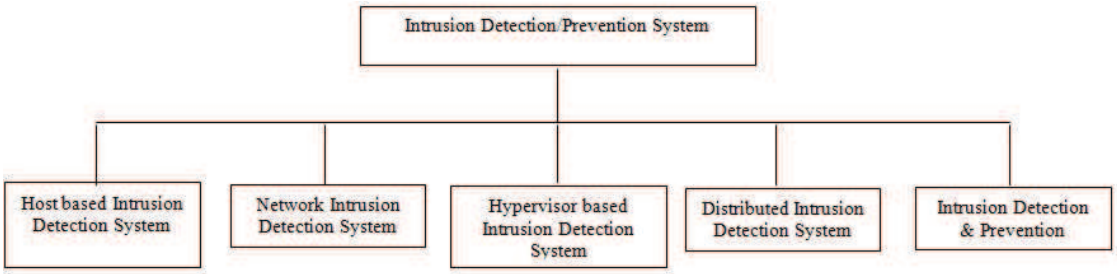

FIGURE 1. Classification of IDS/IPS

1. INTRODUCTION

Information services are deliberately delivered in an exponential order with the help of cloud computing where reliable platforms offer a variety of scalable dynamically provisioning resources for different users who are located at different geographical location. Besides providing computing at low cost and on demand infrastructures, the deliberate extensions of cloud in various fields varying from single user to multiuser, from small and medium business industries to multinational companies. Also, there are various additional features of cloud as irrespective device access, irrespective location access, availability of services throughout the clock, variation of services from public, private, community and hybrid clouds. Due to these numbers of free dimensions cloud has been considered as an opportunity by the intruders to carry out their task. One of the advanced technologies in towards techno world is cloud computing which is helpful for resource sharing through network at various geographically location irrespective of devices these things are performed at low cost. Cloud concepts support various models which are ranging as PaaS, SaaS, IaaS. Virtualization is considered as the backbone of cloud computing. With the help of which resource can be shared among many users at the same time. Entire paper is divided into six main sections where section I deals with the introduction of hypervisors along with certain basic background of cloud concepts, section II ,III and IV mainly deals with a detailed classification of IDS/IPS, Capabilities of IDS/IPS their responses during the attack scenario. Section V deals with an analysis of attacks which are being carried out on hypervisors how they were overcome by using methods along with their limitations. Section V deals with the conclusion

and contribution of future work with two proposals on overcoming the attacks associated with Type II hypervisors.

2. Classification Of IDS/IPS

In a general scenario we can classify various IDS/IPS in the following different categories which are discussed below depending on the position where they are installed.

A. Host Based Intrusion Detection Systems (HIDS)

Here the presence of an agent on the host carries out the required application logs, analyzing system calls, modified file systems; here software agents are present who carry out the task of IDS.

B. Network Based Intrusion Detection System (NIDS)

Unauthorized access of computers, port scans, DoS attacks are detected during monitoring of network by NIDS i.e. any kind of network-based threats can be detected. Intrusions can be detected with a comparison which is carried out with respect to existing attack database to the obtained report by monitoring the network. With the help of Xarp 2 tool using an ARP scanning method [1] attacks with respect to network traffic are traced out. Event collector and sensor [2] gathers information about attack behavior by the data which is sensed while the attack is going.

C. Hypervisor-Based Intrusion Detection System

Hypervisor is a software which when installed at the hypervisor layer between software and hardware then with the help of which VM are created with the help of which intrusion detection is carried out. [3] Proposed a method with the help of HIDS for intrusion detection in virtual environment with the help of VM monitors it observes events, software states, hardware states with the help of UNIX socket commands.

D. Distributed Intrusion Detection Systems (DIDS)

On a large network several intrusions detection systems are combined together for DIDS it is related to a central server with the help of which a continuous monitoring is carried out when any kind of new attack is detected an alert message is generated. An architecture with DIDS is used with a prototype of security monitoring is discussed by [4]. Intrusion is defined as the act

TABLE 1. Showing Comparison Of Different Kinds Of Ids

IDS technique Parameter	Host Based	Distributed	Network
Detection with respect to encrypted data	Does not detect	Detection is not perfect	Moderately used
Cost effectiveness	Less	Less	Moderate
Any OWASP top 10 attack conducted	Limited to two attacks	Limited to three attacks	Limited to four attacks
Accuracy to get the results	Moderate not satisfactory results	Moderate but not accurate results	Reliable
Does it work during high traffic	Works well for light traffic	Works well for moderate traffic	Does not work well for high traffic
Can be used for data segregation and analysis	Data is not perfectly segregated	Moderately segregated	Reliable for segregation
Used for cloud forensics	Moderately used	Moderately used	Moderately used
Does any protection of data methods include	It does not include a full-fledged protection	Provides moderate protection to data	Provides moderate protection to data

carried out by an intruder either to break an information system or to access the data illegally. Internal and External intruders are the two groups which are the classification from intruders. Unauthorized access of systems with the help of assorted techniques of penetrations is referred as external intruders. Unauthorized access of information internally in systems is termed in the category of internal intruders. Exploitation of specific protocols, cracking of passwords, unsecured traffic sniffing, system misconfiguration and software bugs exploiting software. A system which reports and detects intrusions accurately is known as IDS. They are generally operating system specific and operate as an important tool for implementing security policy of an organization. Importance of IDS in tracing out various attacks is being describe clearly by [6].

E. Intrusion Detection and Prevention System (IDPS)

A combination of IDS with firewall is generally used for intrusion prevention here signature with precise traffic rules are used. Passage or blocking of network traffic is decided by IPS depending on the rules which are preconfigured. As soon as an attack is detected by IPS it blocks the attacks and presents further damage. IDPS is obtained when both IDS and IPS are brought together. [5] Describes a network which is efficient for both intrusion detection and protection

where there is no need to install IDS at each node, it automatically generates alerts.

3. Capabilities Of IDS/IPS

A network which generally functions in a usual way deviates from its normal functioning when it is being affected by unauthorized activities either indirect or directly. This also causes serious effects to the persons who are connected to the same network. An IDS plays a vital role in order to trace such kind of activities where not only passive and active activities of the intruder are traced but also one can get an initiation about any kind of mischief which is being carried out with respect to the victims systems or the network associated with him. Following are certain capabilities of IDS.

- Authorized user of a network gets an auto notification or alert during intrusion attacks.
- The friendly environment of IDS allows even a non-IT person also to carryout effective measures during attacks.
- New or existing attacks can be tracked easily which helps to take the counter measures.
- Soon sniffing of any attack, these IDS prevents further loss of data through the network where they are actively implemented. With the help of specific rules set incorporated in the IDS gives more effective results than in normal states. An excellent style manual for science writers is [7].

4. Analysis Of Cloud Based IDS

A flavour of services is enjoyed by the end users delivered by the cloud service providers with respect to the remote servers which are located at certain geographical location. IDS based on cloud are generally classified in the following categories as signature based, Anomaly based, hybrid based.

A. Signature based (S-IDS)

Certain rules (signatures) are developed and maintained in the database. Basing on previous network attacks when similar kind of attacks are being felt in future, these rules are being activated automatically and maximum damage from the network is prevented and when new a attack is encountered its relevant

rules are being framed. The same is updated every time in the database [7]. A cloud-based IDS [8] which is a form or S-IDS is kept at each cloud region which is helpful in detecting any anonymous activities in the network. Beside alarming the fact, it also reduces the loss of data carried out by the intruders. Out of various kind of attacks, DoS and DDoS are traced out easily. The only drawback of this IDS is that it fails to detect new kind of attacks and during overhead computational process it is difficult to trace the attacks. For a given VM maximum protection with respect to DDOS can be carried out with the help of these IDS [9]. Integrated NIDS in an open source cloud environment is also considered as S-IDS [10].

B. Anomaly based IDS in cloud

Here comparison is carried out between a system working under normal condition to a system working during malicious event carried out by intruder on the system. During a long period of time user's legitimate behaviour is compared with various tests in statistical way. Even under the situations where a system is not updated there also unknown attacks are also traced out [11][12]. Its drawback is that it uses a greater number of resources in order to detect unknown attacks with high accuracy [13]. In cloud VM's with respect to every guest OS it is assigned it is a kind of host-based IDS. By the effective usage of Anomaly IDS [14], hyper-call based attacks are traced out for VMM that are affected by hyper call.

C. Hybrid based IDS in cloud

It's the combination of both S-IDS and A-IDS with the help of which both unknown and known attacks are being traced out [15]. These kinds of IDS can be used both in host and network. This kind of IDS is carried out in real time cloud environment even unknown attacks can also be detected with high accuracy with effective usage of ANN applications. [16]. Its drawback is that it must be performed on more and more data for getting correct results of the analyzed data [17]. In cloud if all the required activities are carried out in proper way then it may lead to green computing [18].

5. Overview Of Hypervisor Attacks

Hypervisor attacks can be classified into the following types which are described as below.

A. Hypervisor-based Cloud Intrusion Detection System

System performance during an attack with respect to a cloud instance can be traced successfully using HCIDS [19] where additional installation of software can be overcome. It provides a kind of cloud-based IDS; its performance can be evaluated effectively in real time cloud environment. With this system one can easily detect DoS attacks with respect to cloud instances. The detection of the intrusion system is carried out even outside the virtual machine and independent of the operating systems which are being running on a VM. Drawback of this system is that malicious activities with exact accuracy are missed to be found.

B. Empirical Evaluation of the Hypervisor Scheduling on Side Channel Attacks

A SCA deals with the collection of information related to operations done using cryptography with respect to a computing device. It's a kind of security exploit. [20]. SCA are going to occur when various resources are being shared among multiple VM's. Due to these end users hidden information is being theft which may include as encryption keys it is more effectively carried out by monitoring victim's patterns which are being accessed by him including hardware, CPU cache etc. scheduling schemes of hypervisors can be expressed as an effective way to overcome these kinds of attacks. This information is helpful to design effective hypervisor sharing schemes. The only drawback is that new attacks may not be traced out effectively.

C. Analysis of Potential Hypervisor Attack Vectors

For a reliable software and hardware hypervisor provide a channel. As they share an important part of cloud so they are more prone to attacks. Besides giving host for virtual machine they also share and are helpful in granting access to various resources. With respect to ESXi 5.0 hypervisor platform various kinds of vulnerabilities are discussed [21]. The drawback here is that new attacks cannot be traced out properly with high accuracy.

D. Analysis of Various Virtual Machine Attacks In Cloud Computing

Multi-tenancy is referred as sharing database among many. One way to secure cloud infrastructure is to use the concept of virtualization based on hypervisors. [22] Describes various attacks relevant to security and analyses of the same

with respect to hypervisor security are carried out in an environment of virtualization. A kind of security zone is created by every hypervisor itself. For a virtual machine which is running on a host it is mostly effected by the hypervisor. Within the hypervisor itself there are multiple security zones where it is a bit difficult to trace the attacks at a particular security zone and to provide it relevant measures. With respect to each kind of security zone there are different attacks which are being carried out the intruders. The drawback is that it fails in many issues to deliberately detecting attacks on hypervisors at high level of multi-tenancy.

E. Insider Attacks in Cloud Computing

When attacks made on the cloud are being classified into various groups i.e. whether the attack is insider or outsider attack then it would be easier to take the relevant measures. With the rapid growth of cloud in almost every sector of industry it is prone to number of attacks some of them are carried out from outside the cloud and some of them are carried out from inside the cloud. As our assets relevant to computing may be either inside or outside the cloud when more number or assets are inside the cloud then the risk of the attack is also more. [23] describes the methods to know the nature of insider's attack that would be helpful to take proper measure with respect to the cloud environment. The only drawback of this approach is that for complex attack it is a bit difficulty to classify the attacks into the required subsection which if done properly then necessary measure can be taken to prevent the future kind of such attacks. A detailed study of emerging challenges in the field of cloud computing are discussed by [24] clearly shows that though it constituted a decade for the research which are being carried out in cloud area but still there emerges new threats and security measures which has to be answered.

The below fig. shows the extension of holistic insider's scenario presence in the cloud ecosystem. The detailed description of various threat actors and the location of the insider with in the eco system are explained below.

A. Advanced Persistent Threat

An attacker or intruder present within a network for a long duration to gain the control of all the activities within the system lead to APT.

B. Familial Insiders

A client feels relaxes to himself when he is working in an environment where he feels safe and more secure where he can decrease the security levels.

C. Benigin-insiders coercion

Outsiders who have good relations with insiders in cloud environment may sometime compromise them with their good relations.

D. Malicious Hypervisor:

Without proper knowledge of hypervisor or in genuine usage of hypervisor may also be a reason for data loss or an hotspot for various attacks in clouds.

E. Malicious Clients and CSP:

Sometimes both client and CSP show that they are having trust of each other but they come to know at certain point that they both are lying each other.

6. Conclusion

From this literature study on various attacks carried out on hypervisors in cloud. As hypervisors act as the basic backbone of cloud concepts. Due to various importance's of hypervisors as mentioned in paper so there is an extensive need to protect hypervisor to carry out the sustainable applications on cloud without any halt. We would like to suggest two unique methods which we are going to discuss in our coming research papers which are useful to trace out various attacks on hypervisors. One method is with respect to effective usage of GA in order to find malicious attacks which are being carried out on the hypervisors in the cloud. Second method is to create an effective immune system in order to overcome these attacks thereby enhancing the security levels in cloud concepts with effective usage of certain active artificial intelligence applications.

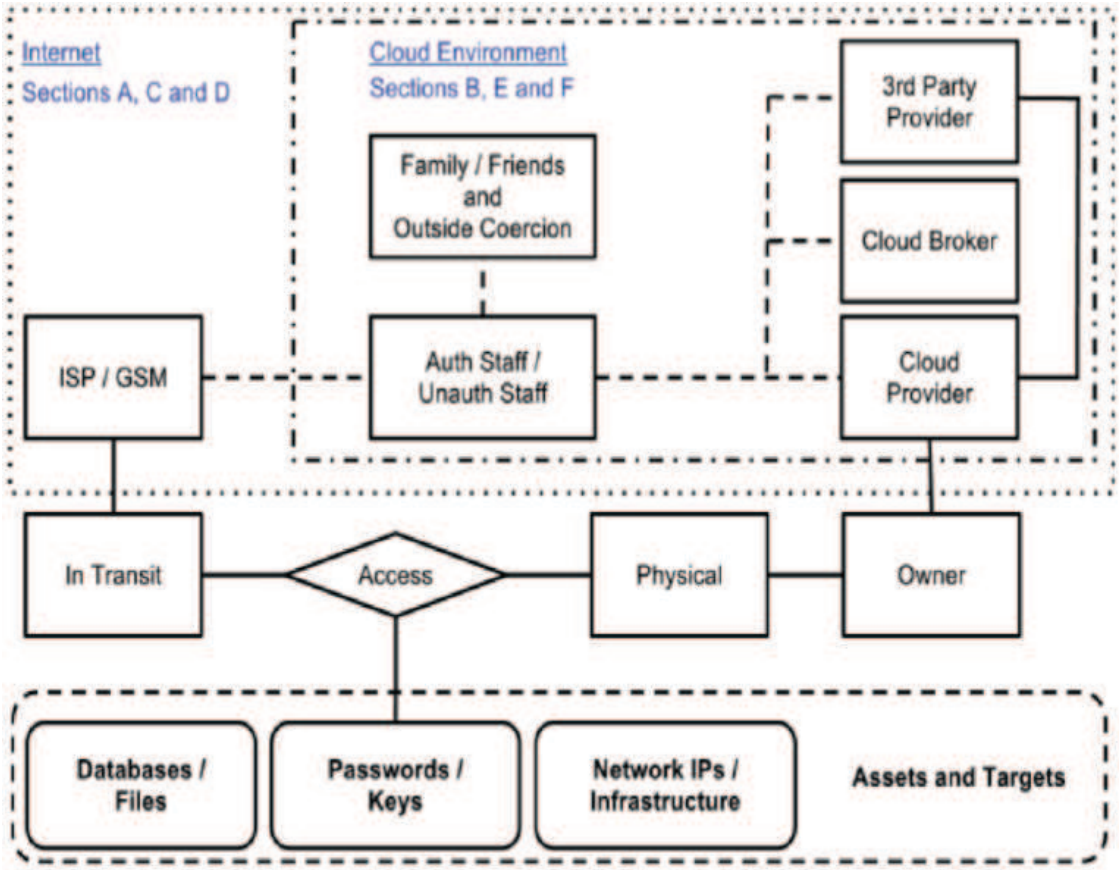

FIGURE 2. Mapping of insider contents to their sub section in cloud eco system

REFERENCES

[1] M.A. HEMAIRY, S. AMIN, Z. TRABELSI: *Towards more sophisticated ARP Spoofing detection/prevention systems in LAN networks*, International conference on the current trends in information technology (CTIT), 2009, 1–6.

[2] S. ROSCHKE, C. FENG, C. MEINEL: *An extensible and virtualization compatible IDS management architecture*, Fifth international conference on information assurance and security, **2** (2009), 130–134.

[3] S. LANIEPCE, M. LACOSTE, M. KASSI-LAHLOU, F. BIGNON: *Engineering Intrusion Prevention Services for IaaS Clouds: The Way of the Hypervisor*, Service Oriented System Engineering (SOSE), IEEE 7th International Symposium on March, 2013.

[4] S. R. SNAPP, J. BRENTANO, G. V. DIAS, T. L. GOAN, T. GRANCE, L. T. HEBERLEIN: *A system for distributed intrusion detection*, IEEE, Compcon, 1991, 170–176.

[5] M. AHMED, R. PAL, H. M. HOSSAIN, M. BIKAS, M. K. HASAN: *NIDS: A Network Based Approach to Intrusion Detection and Prevention*, Computer Science and Information Technology—Spring Conference, 2009, 141–148.

[6] S. K. MOHIDDIN, D. Y. S. BABU: *A Relevance Technical Approach for Screening the Significance of IDS in Cloud Forensics*, IJITEE, 2019, 2278–3075.

[7] J. C. FOSTER: *IDS: Signature versus anomaly detection*, http://search.security.techtarget.com/tip/IDS-Signature-versus-anomaly-detection, 2005.

[8] C. C. LO, C. C. HUANG, J. KU: *A Cooperative Intrusion Detection System Framework for Cloud Computing Networks*, 39th International Conference on Parallel Processing Workshops, 2010, 280–284.

[9] C. MAZZARIELLO, R. BIFULCO, R. CANONICO: *Integrating a Network IDS into an Open Source Cloud Computing Environment*, Sixth International Conference on Information Assurance and Security, 2010, 265–270.

[10] A. PATEL, Q. QASSIM, Z. SHUKOR, J. NOGUEIRA, J. JUNIOR, C. WILLS: *Autonomic Agent-Based Self-Managed Intrusion Detection and Prevention System*, Proceedings of the South African Information Security Multi-Conference (SAISMC), 2010, 223–234.

[11] D. COHEN: *What is a Zero-Day Exploit* http://what-is-what.com/ what is / zero_ day_exploit.html, 2007.

[12] D. MUDZINGWA, R. AGRAWAL: *A study of methodologies used in intrusion detection and prevention systems (IDPS)*, Proceedings of IEEE Southeastcon, 2012, 1–6.

[13] A. V. DASTJERDI, K. A. BAKAR, S. G. H. TABATABAEI: *Distributed Intrusion Detection in Clouds using Mobile Agents*, Third International Conference on Advanced Engineering Computing and Applications in Sciences, 2009, 175–180.

[14] S. BHARADWAJA, W. SUN, M. NIAMAT, F. SHEN: *Collabra: A Xen Hypervisor based Collaborative Intrusion Detection System*, Eighth International Conference on Information Technology: New Generations, 2011, 695–700.

[15] A. PATEL, M. TAGHAVI, K. BAKHTIYARI, J. C. JUNIOR: *An Intrusion Detection and Prevention System in Cloud Computing: A Systematic Overview*, Journal of Network and Computer Applications, **36** (2013), 25–42.

[16] K. VIEIRA, A. SCHULTER, C. B. WESTPHALL, C. M. WESTPHALL: *Intrusion Detection for Grid and Cloud Computing*, IEEE Computer Society, 2010, 38–43.

[17] S. N. DHAGE, B. B. MESHRAM, R. RAWAT, S. PADAWE, M. PAINGAOKAR: *Intrusion Detection System in Cloud Computing Environment*, International Conference and Workshop on Emerging Trends in Technology, 2011, 235–239.

[18] S. K. MOHIDDIN, Y.S. BABU: *Green computing an eco-friendly IT environment for upcoming technologies*, International Journal of Advanced Research in Computer Science, **6** (2015), 28–32.

[19] J. NIKOLAI, Y. WANG: *Hypervisor-based cloud intrusion detection system*, International Conference on Computing, Networking and Communications (ICNC), Honolulu, HI, 2014, 989–993.

[20] L. LIU, A. WANG, W. ZANG, M. YU, S. CHEN: *Empirical Evaluation of the Hypervisor Scheduling on Side Channel Attacks*, IEEE International Conference on Communications (ICC), Kansas City, MO, 2018, 1–6.

[21] L. TURNBULL, J. SHROPSHIRE: *Breakpoints: An analysis of potential hypervisor attack vectors*, Proceedings of IEEE Southeastcon, Jacksonville, FL, 2013, 1–6.

[22] S. ANNAPOORANI, B. SRINIVASAN, G. A. MYLAVATHI: *Analysis of various virtual machine attacks in cloud computing*, 2nd International Conference on Inventive Systems and Control (ICISC), Coimbatore, 2018, 1016–1019.

[23] A. J. DUNCAN, S. CREESE, M. GOLDSMITH: *Insider attacks in cloud computing*, IEEE 11th international conference on trust, security and privacy in computing and communications, 2012, 857–862.

[24] S. K. MOHIDDIN, S. B. YALAVARTHI: *Research Challenges in the Emerging trends of Cloud Computing*, International Journal of Advances in Computer Science and Technology (IJACST), **4**(1) (2015), 4–14.

DEPT. OF COMPUTER SCIENCE ENGG.
DELHI TECHNOLOGICAL UNIVERSITY
DELHI-110042. INDIA
Email address: seshu1203@gmail.com

DEPT. OF COMPUTER SCIENCE AND ENGINEERING
DELHI TECHNOLOGICAL UNIVERSITY
DELHI-110042. INDIA.
Email address: rkyadav6711@gmail.com

DEPT. OF ELECTRONICS AND COMMUNICATION ENGINEERING
DELHI TECHNOLOGICAL UNIVERSITY
DELHI-110042. INDIA
Email address: nsraghava@gmail.com