Attack Monitoring and Protection in Cloud Computing Environment through IDS

Dhara Shah
School of Information Technology,
Artificial Intelligence and Cyber Security
Rashtriya Raksha University, Gandhinagar,
Gujarat, India.
dharaa.shah9@gmail.com

Dharati Dholariya
School of Information Technology,
Artificial Intelligence and Cyber Security
Rashtriya Raksha University, Gandhinagar,
Gujarat, India.
dharati.dholariya@rru.ac.in

Chandresh Parekh
School of Information Technology,
Artificial Intelligence and Cyber Security
Rashtriya Raksha University, Gandhinagar,
Gujarat, India.
Chandresh.parekh@rru.ac.in

Cloud computing has now established itself as a significant computing model and processing method in almost all industries. The use of cloud computing is widespread in today's world. Cloud computing is becoming a part of every IT company due to its more versatile, secure, and PAYG (Pay-as-you-go) services, and the privacy and protection of the cloud is a major concern. In addition, the cloud is open and available. The next move is to enforce the snort intrusion detection system in the cloud environment, as well as new policies within snort, in order to improve the level of protection within the cloud environment, and to examine the snort log report to ensure that the message in the log record is properly alerted. As a result, the administrator may make similar security choices in the event of an attack. Next step is enforcing snort intrusion detection system in cloud environment and new policies within the snort to improving the extent of security within the cloud environment and studying the snort log report, to see that it nicely alert the message in log record. So that administrator can take similarly protection selections associated with attacks.

Keywords: Cloud security, Intrusion detection system, Snort, Cloud attacks, Intrusion.

I. INTRODUCTION

Cloud computing gives you full access to a shared team of powerful, convenient, on-demand adaptable computer resources (storage, network, offer packages, as well as servers, among other things) that can be swiftly established and started with little effort or service provider contact. Infrastructure as a service (IaaS), in which the host administers the entire digital machine, as well as Eucalyptus and Open Nebula, are among the services it provides to its customers. Platform as a Service (PaaS), which enables customers to set up consumer-created packages in the cloud if the provider assists with languages, APIs, and other technical aspects. Google App Engine and Microsoft Azure are examples of platforms and devices that can be utilised to develop apps. Customers can also use the software to operate provider packages with Google apps as a service (SASS). These services are available via the internet. The cloud can be sorted in four different ways: The infrastructure of a public cloud is designed to be accessible to the general public via an internet connection and controlled by a third party or cloud service provider. Private cloud that's been set up for a single company with two users. It is the employer's responsibility to use own offerings or those of a third party.

Because the cloud's design is totally dispersed and open, there are greater opportunities for intrusion attacks in the cloud computing environment. As a result, the cloud environment's security is jeopardised. These cloud intrusion attacks also pose a threat to cloud users, which might include individuals like us as well as small and large businesses. According to IDG Enterprise's 2013 Cloud Computing survey, the risk in a cloud environment is higher, and cloud security is a big concern, making it harder for businesses and organisations to adopt the cloud computing paradigm. Furthermore, there is no on-premise solution that can protect a business from all forms of network-based threats. The most common network-based attacks that affect cloud security at the network layer include Address Resolution Protocol (ARP) spoofing, IP spoofing, DNS poisoning, port scanning, man-in-the-middle attacks, Routing Information Protocol (RIP) attacks, Denial of Service (DoS), and Distributed Denial of Service (DDoS) attacks. Organizations have tried standard network security measures in the past, such as firewalls and network security technologies, but these only help to stop outsider attacks. These tools are not intended for attacks that occur within the network, such as DoS and DDoS. As a result, the Intrusion Detection System is utilised. It is crucial in preventing intrusion attacks. The intrusion detection system (IDS) is used to detect both known and new attacks on systems, as well as to provide an additional security layer to prevent intrusion attempts.

The term "intrusion" in the Intrusion Detection System refers to a breach of the "CIA Triad," which stands for Confidentiality, Integrity, and Availability. When attackers strive to gain unofficial access to cloud sources, and legitimate users do not use or misuse their permissions effectively, the system is vulnerable to incursions. Intrusion Detection Systems are used to keep track of what's going on in a network or system, analyse what's going on, and alert the user through alarm if an intrusion attack occurs. The Intrusion Detection System (IDS) can be software, hardware, or a mixture of both, but the basic function of the IDS stays the same regardless of whether it is software or hardware. It detects malicious behaviours in the network or system and sends

notifications to the system manager or authorised person if any malicious behaviour is discovered in the network or system.

II HOW INTRUSION DETECTION SYSTEM WORKS

Intrusion Detection Systems can identify suspected intrusions using a variety of approaches. Pattern matching and statistical anomaly detection are the two most popular broad categories used for detecting suspected intrusions in Intrusion Detection Systems.

Pattern matching

Pattern matching can be used to detect known attacks based on their signatures. Signature-based Intrusion Detection Technique is another name for it. This Intrusion Detection Technique searches for traffic and behaviour that resembles known attack patterns. This method's effectiveness is determined by the signature database, which must be kept up to date.

The most serious flaw in this method is that it fails to detect new assaults for which the programme lacks a defined signature in its database.

Statistical anomaly

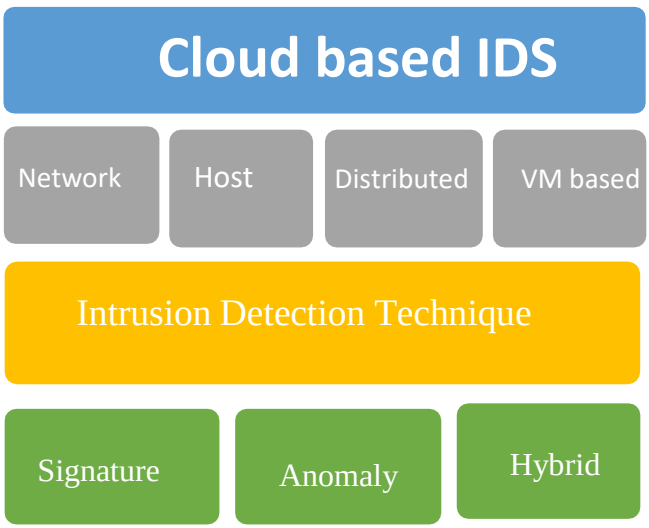
Anomaly-based detection looks for departures from standard usage patterns. This method necessitates first establishing a baseline profile to define the norm, and then monitoring for behaviours that deviate from those parameters. This strategy enables you to detect fresh incursions or attacks that have yet to be identified in a signature database.

Limitations of existing IDS

Traditional IDS has the drawback of not being able to prevent attacks; instead, it is only effective for uncovering or adding another layer of security. Traditional IDSs are quite useful for network monitoring, but how beneficial they are largely on what you do with the information they provide. A network intrusion detection system (NIDS) analyses protocols as they are collected, which implies they are vulnerable to the same protocol-based assaults as network hosts.

III LITERATURE RIVEW

ANALYSIS OF EXISTING CLOUD BASED INTRUSION DETECTION SYSTEMS (CIDS)



Depending on where the IDS sensors are situated (on a host/endpoint or on a network), intrusion detection software systems are categorised as either host-based or network-based. The four primary types of cloud-based IDS are host-based, network-based, VM or Hypervisor-based, and Distributed IDS. The most prominent IDS techniques include signature-based techniques, anomaly-based techniques, and hybrid techniques (which integrate both signature and anomaly-based techniques). Regardless of the type, the technologies are all meant to detect intrusions on sensors and inform security investigators.

Signature Based IDS

Signature-based detection works by comparing the facts gathered from a network or system to a signature database. A signature is a set of rules or patterns that are associated with a certain assault. This method is also known as abuse detection. It is capable of detecting known assaults with few false alarms. The signature-based methodology aids network managers with basic security understanding in effectively identifying intrusions. It's a flexible solution since new signatures can be added to the database without affecting existing ones. It is, however, incapable of detecting unknown attacks. A signature-based fully intrusion detection methodology can be used on the cloud's front-end (that is, the host) to identify known attacks from the outside network in a cloud context. If implemented on the cloud's back end (processing servers), it can detect both internal and external intrusions.

To counter DoS and DDoS attacks, C. C. Lo et al. suggested and simulated an IDS that functions in a cooperative manner. It is made up of four parts, each of which serves a specific purpose. 1st By capturing and analysing network packets, the primary one detects intrusions.[1It immediately eliminates packets that match the block table criteria; on the other hand, aberrant packets that don't match the rules are transmitted to the alert clustering component, which determines the alert level of the received suspicious packet. The third component will block intrusion packets before notifying other IDSs. The fourth component will collect alerts from other IDSs and make a decision regarding the packet based on which IDS received the most votes. Because it uses a signature-based intrusion detection methodology, this IDS is good for known attacks but not for unknown ones.

J.K. Khatri and G. Clary have proposed a design for implementing the Sericata IDS Network IDS backend in the cloud. [6] The Sericotta IDS is designed to protect virtualized servers running on hypervisors within the cloud operating system from various attacks. The majority of Ceriyatim IDS's network capability is to capture all packets coming from the external or outside network and allocate them to virtualized servers, which will analyse and process them and It will deliver alerts if any of the rules stored in the Siriatim configuration file apply.

T. Alhargan and colleagues Martin developed an IDS that acts as an intrusion detection service (IDSAS) to assist users in protecting their virtual computers from both internal and external threats. [5] IDSaaS is a network and signature-based intrusion detection solution that targets the cloud environment's infrastructure.

Anomaly Based IDS

When comparing current user roles to preloaded profiles of users or networks, anomaly based detection can detect disruptive abnormal behaviour. Profiles can be dynamic or static, and they can correlate to intended or harmless actions by users. The everyday activities of users, network links, and hosts are tracked for a specified period of time, referred to as the training period or monitoring period, in order to build a profile. Multiple files and various capabilities, such as failed login attempts, a given time span by a specific user, and CPU use, are used to build profiles. In the face of unknown attacks, anomaly based detection is more useful.

Lee, J. H., and others it proposes a fully novel approach to detecting intrusions, allowing users to reduce their clutter and make better use of resources. [2] The authentication, authorization, and accounting (AAA) module is the most critical part of the proposed framework. A user is allowed to use the AAA module when attempting to use cloud services. The user's disorder status is restored after effective authentication, as expected by the most recent information about the user in the database. As a result, the AAA chooses an appropriate IDS with a protection level that corresponds to the user's level of disorder. The AAA asks the user to delegate the guest OS after the selected IDS is used on the host OS (OS). There is a connection between the guest OS and the user data in the storage centre when you allocate a guest OS to the user. Levels of IDS Security: Includes all highly known attack modes and parts of the disorder system that need the most security, using medium and low selective attack modes that provide somewhat robust protection using all known attack modes that can cause malicious and serious damage to the system, This method provides high speed for detecting attacks and the medium and low-level IDS often allocate more guest OS as it uses less resources. The proposed system helps them by auditing system administrators logs supported the random amount of users.

Al-Shadaifat et al. proposed an anomaly intrusion detection model to combat attacks and security breaches in the cloud. [7] Dataset Grouping, Hopfield Artificial Neural Network (HANN), and Simulating Annealing Aggregator are the three stages of this anomaly-based IDS system.

Hybrid IDS

The hybrid detection technique, which combines signature-based and anomaly-based techniques, will enhance the IDS's output in detail. The aim of combining these technologies is to be able to detect any known and unknown attack using signature-based and anomaly-based detection techniques.

Ms. Parag K. Shelke et al proposed a wide NIDS Unpack on the topic of cross-site scripting (XXS) and DDoS attacks. [3] The proposed NIDS is made up of three modules, each of which serves a specific purpose: the capture module gathers incoming and outgoing packets (UTP, TCP, ICMB, IP) and sends them in a predetermined order for analysis. Data packets collected by the processing module are analysed and evaluated. It compares them to an information domain and a collection of pre-defined rules. This will aid in the detection of malicious packets and the generation of alerts. The reporting module extracts data from the partition queue to help warning reports. The third-party service, which is monitoring the entire scene, notifies the customer of the attack information right away and sends the service provider a consultation report. Despite the fact that this is a completely new method, no implementation specifics are given to back up the claim.

C. N. Modi et al. proposed and introduced a network-based intrusion detection system. To detect both known and unknown attacks, this IDS employs Snort and a Bayesian classifier. [4] The following are the main components of the proposed system: Packet Proposing is a technique for picking up network packets and removing information that isn't relevant to detection. An analyzer classifies the packet as natural or invasive, including snort and warning log, and if it is an intruder, records the intrusion and saves it to NIDS on other servers, according to the signature-based or anomaly detection process. When network packets are detected, they are first used for snort detection, and infiltration events are then saved in the warning log. The anomaly is then discovered by pre-processing non infiltration packets and then documenting the final measured infiltrations into the alert database, taking into account the actions based on calculating their class mark (infiltration or default) using the Bayesian classifier. Overall, servers collaborated by adding alerts to their information domain, making it easier to detect unknown attacks, according to NIDS. Following signature-based detection and anomaly-based detection, the unusual detection technique in this technology leads to a faster detection time by detecting unknown attacks. Furthermore, sending warnings to other NIDSs in the cloud setting improves the detection rate.

To secure the Cloud environment from intrusions, P. Ghosh et al. suggested an Intrusion Detection System. [8] The system is built on a multithreaded Network Intrusion Detection System (NIDS) and a Host Intrusion Detection System (HIDS) combination (HIDS). Hostbased IDS is used to monitor traffic to the selected host.

To detect all forms of attacks, Y.Guan et al. suggested using principles focused on alternative factors. This method is largely focused on the records and opportunity theory. All attacks are treated as a pattern region in this technique. The collection has then been decomposed using records centred entirely on jointly distinct sets. The infiltration detection algorithm is collected using established subgroups from the sample region.

However, there have been no reports of test results or implementation problems so far. Distributed IDS (DIDS) consists of numerous IDSs spread around a wide network that communicate with one another or with a central server that allows community monitoring.

Hisham A. Kholidy et al. proposed a cloud IDS architecture. A dispensed structure without critical detail is suggested, balancing workload across cloud nodes and, as a result, preventing a single point of failure because critical detail is no longer needed. [10] The constant exchange of information among nodes to maintain database consistency, on the other hand, can degrade system performance.

The network-based IDS detects malicious behaviour by monitoring network traffic. A framework for detecting DDoS attacks in VM was proposed by A.Bakshi et al.as. In the virtual switch, IDS systems are installed to record incoming and outgoing traffic into a database. The logged packets are analysed and compared in real time with known signatures via the IDS to detect unknown attacks. This technique will guard against DDoS attacks in virtualized environments and protect virtual machine

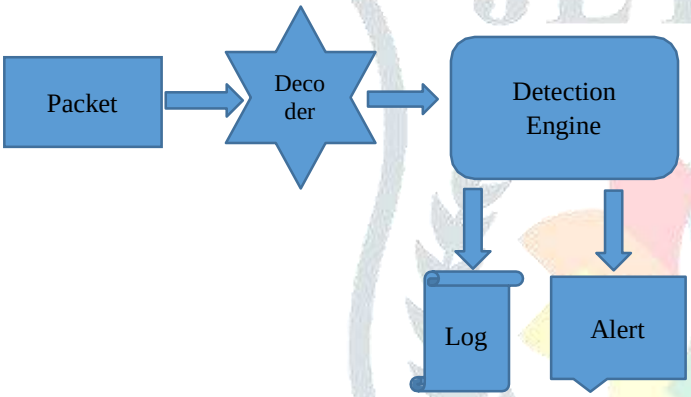
services. However, since the method used here is a snort, it won't be able to detect all types of attacks. It recognises the most well-liked assaults.

Snoring Based Misuse Detection Proposed in Open Source Eucalyptus Cloud,C.Mazzariello et al. [10] Snort is installed on physical machines or virtual machines in this form. It's also installed on the cloud controller to detect intrusions from the outside or outside the network. Since it is a quick and efficient solution, this approach solves the issue of multiple IDS deployments. Of all the current IDS, Snort is the most useful. Best-known attacks, on the other hand, are detected when snort is used.

IV. SNORT AS INTRUSION DETECION SYSTEM

Snort is one of the most well-known and widely used network intrusion detection and prevention systems. Snort Intrusion Detection System works in three various modes, as sniffer, as packet logger and network intrusion detection system. It can analyze real-time traffic in network. It checks packet against rule written by user. The rules are easy for the user to read and modify. The attack can be easily detected if the method complies with the rules, but the system will fail when a new attack arrives. Snort is therefore only used to analyze real-time traffic.

Architecture of Snort



Installing Snort

apt-get install libpcap-dev bison flex

Then we run: apt-get install
snort

In order to save Snort's reports we need to specify to Snort a log directory, if we want Snort to show only headers and log the traffic on the disk type:

```
# mkdir snortlogs
# snort -d -l snortlogs
```

V. FUTURE WORK AND CONCLUSION

To secure the cloud network, we proposed a Network Intrusion Detection System (NIDS). The characteristics of network traffic that make exploiting the attack and gathering information from the user network possible. The system architecture proposed in this paper ensures Confidentiality, Integrity, and Availability. Snort is a tool for improving intrusion detection efficiency. In this paper, the snort IDS approach is used to detect intrusions in a cloud environment. The next move is to enforce the snort intrusion detection system in the cloud environment, as well as new policies within snort, in order to improve the level of protection within the cloud environment, and to examine the snort log report to ensure that the message in the log record is properly alerted. As a result, the administrator may make similar security choices in the event of an attack. IDS in cloud environment can become more secure, effective and reliable to detect the intrusion. Future work will include introducing IDS such as snort in the cloud environment and adding new rules to existing IDS to improve protection in the cloud environment, as well as analysing the existing IDS log file to ensure that it correctly alerts the message in the log file.

VI. REFERENCES

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

2. "Multilevel Intrusion Detection System and Log Management in Cloud Computing," ICACT, 2011, pp. 552-555. J. H. Lee, M. W. Park, J. H. Eom, and T. M. Chung, "Multilevel Intrusion Detection System and Log Management in Cloud Computing," ICACT, 2011, pp. 552-555.

3. "Intrusion Detection System for Cloud Computing," International Journal of Scientific & Technology Research Volume 1, Issue 4, May 2012, pp. 67-71, by Ms. P. K. Shelke, Ms. S. Sontakke, and Dr. A. D. Gawande.

4. C.N. Modi and D. Patel, "A new Hybrid-Network Intrusion Detection System (H-NIDS) in Cloud Computing," IEEE Symposium on Computational Intelligence in Cyber Security (CICS), 2013, pp. 23- 30.

5. T. Alharkan and P. Martin, "IDSaaS: Intrusion Detection System as a Service in Public Clouds," Proceedings of the 12th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing (CCGrid), 2012

6. J.K. Khatri and G. Khilari, "Advancement of a Virtualization-Based Intrusion Detection System in a Cloud Environment, International Journal of Science, Engineering, and Technology Research (IJSETR), vol. 4, 2015, pp.1510-1514.

7. B. Al-Shdaifat, W.S. Alsharafat and M. El-bashir, "Using Hopfield Artificial Networks and Simulating Annealing for Cloud Intrusion Detection," Journal of Information Security Research, vol. 6, no. 6, 2015, pp.49-53.

8. P. Ghosh, A.K. Mandal and R. Kumar, "An Efficient Network Intrusion Detection System, Chapter Information Systems Design and Intelligent Applications, Advances in Intelligent Systems and Computing, vol. 339, pp. 91-99, 2015.

9. A.bakshi, and B. Yogesh. Securing the Cloud from DDOS Attacks Using an Intrusion Detection System in

a Virtual Machine, in Proceedings of the Second International Conference on Communication Software and Networks, pp. 260-264, 2010.

10. C. Mazzariello, R. Bifulco, and R. Canonoco. Integrating a network intrusion detection system into an open source cloud computing environment, in Proceedings of the Sixth International Conference on Information Assurance and Security (IAS), 2010, pp. 265-270.

11. M. Rajeswari, M.S. Moorthy Manthira. " "Cloud-based Intrusion Detection System Based on Virtual Hosts." International Journal of Engineering and Technology 5(6):5023-5029, January 2013.

12. Rabeb ZARAI." Based on an Intrusion Detection System, Recurrent Neural Networks and Deep Neural Networks". Open Access Library Journal 07(03):1-11, January 2020

13. Putra Wanda and Huang Jin Jie are the names of two people. November 2018: "A Survey of Intrusion Detection Systems.

14. Muna Al-Hawawreh, Mouhammd Al-kasassbeh, An anomaly-based approach for detecting DDoS attacks in the cloud January 2018International Journal of Computer Applications in Technology 57(4):312-324

15. "Cloud Based IDS and IPS Solutions [Updated 2019]," Frank Siemons, August 23, 2019.

16. Yasir Mehmood, Awais Shibli, Umme Habiba, Rahat Masood"Cloud Computing Intrusion Detection System: Challenges and Opportunities" In December 2013

17. Teri Radichel. "IDS and IPS in the Cloud". 2nd Sight Lab 2020

18. Vaikunth Pai T, P. S. Aithal. " Security Concerns in Cloud Computing - Challenges and Opportunities DOI/10.5281/zenodo.569920.2 May 2017 International Journal of Management, Technology, and Social Sciences (IJMTS), Vol. 1(1), p. 33-42, 2017.

19. Lei Chen; Ming Xian; Jian Liu; Huimei Wang. In the Cloud Computing Environment, an Intrusion Detection System 2020 International Conference on Computer Communication and Network Security (CCNS), November 2nd, 2020

20. Manas Kumar Nanda; Manas Ranjan Patra. Detection and monitoring of network intrusions in cloud-based systems. 10 February 2020: 2019 International Conference on Applied Machine Learning (ICAML).