Volume: 12 Issue: 06 Pages: 4770-4775(2021) ISSN: 0975-0290

A Perspective for Intrusion Detection & Prevention in Cloud Environment

Vaneeta
Research Scholar, Department of Computer Science, Punjabi University, Patiala.
Email id: vaneeta.dhawan@gmail.com
Sangeeta Rani
Assistant Professor, Department of Computer Science, Mata Gujri College, Fatehgarh Sahib
Email id: sangeeta@matagujricollege.org

ABSTRACT

The cloud environment is used in all sectors that provide different services to the users. The assistance provided by the cloud environment in different sectors such as business, entertainment, government, education, IT industry, etc. The services rendered by both the public and private organizations considering scalable, on a pay-as-you-go basis, on-demand services, etc. Due to its dispersed nature and viability in all the sectors, makes the system inefficient which causes numerous attacks in the environment. These attacks affect the confidentiality, integrity, and availability of cloud resources. Some examples of attacks are Ransomware, man-in-the-middle attacks, Denial of service attacks, insider attacks, etc. Thus, Intrusion Detection System (IDS) and Intrusion Prevention System (IPS) play a crucial role in the cloud environment by detecting and preventing the system from suspicious attacks. The objective of this paper is to provide information about attacks that affect the cloud environment. This paper also covers the different techniques of intrusion detection, intrusion prevention, and its hybrid approach.

Keywords - **Cloud Computing, Intrusion Detection System (IDS), Intrusion Prevention System (IPS), Intrusion Detection and Prevention System (IDPS)**

Date of Submission: Apr 26, 2021 Date of Acceptance: May 17, 2021

1. INTRODUCTION

Cloud computing connotes as a branch of IT, that offers services like infrastructure, software, platform, etc. on a usage and demand basis [1]. This environment provides the following services to its users such as multitenancy, versatility, scalability, on-demand access to services and resources, broad network access, pay-as-you-go, resource pooling, efficiency, etc. These attractive features enable the cloud to be adopted by all sectors [2]. Along with these advanced features, sensitive data that needs to be stored in the cloud is a major security challenge. Due to the sensitivity of the data, the security of a system is the highest priority. Multiple sources of threats are natural disasters, power failure, and internal and external attacks that harm cloud resources [3]. Therefore, maintaining the security and privacy of the user's data is the responsibility of the service providers [4].

The cloud environment provides a three-layer architecture of infrastructure, platform, and applications as a service[5]. Along with these excellent services, the cloud resources and data are still unsafe from security jeopardies. Some of the attacks like ransomware, data loss, malicious insiders, account hijacking, constitute the cloud environment threatening. Consequently, security and privacy are the major concern in the cloud environment. Some security frameworks like Microsoft Azure, Amazon, etc. use firewalls [6]. The firewall alone is not sufficient, because it can protect the system only from the preeminent location, and detecting complex attacks like insider attacks, Denial of service are difficult by the firewall. Thus, other solutions of security to detect and prevent attacks include Intrusion Detection system, Prevention systems, and the hybrid approach.

According to the Checkpoint Software Security Report', 68% of security organizations highlight the misconfiguration of the cloud environment that leads to data theft incidents, unauthorized access of 58%, 52% less secure interfaces, and 50% account hijacking [7]. These challenges arise due to the unavailability of security tools for the dynamic and virtual environment. Therefore, it is incredibly challenging to protect the resources and sensitive information for designing a system. Thus, to protect the cloud environment from malicious attacks, the Intrusion Detection and Prevention system (IDPS) is one of the advanced solutions. It is the combination of two systems where Intrusion Detection helps in detecting malicious activity and Intrusion Prevention helps in taking any defensive or preventive action. Therefore, IDPS proposes the strength of IDS and IPS at the same place. An effective intrusion detection and prevention system should perform quickly, self-checked, accessed without any interference, and free from false alarm error [8]. The objective of this paper is to cover techniques used for Intrusion detection and prevention systems in the cloud environment. The subsequent sections are given in the paper. Section 2 encompasses attacks and solutions for implementing security in the cloud environment. Section 3 incorporates the comparison of traditional IDPS and cloud-based IDPS. Section 4 embraces the challenges and requirements of cloud IDPS. Section 5 represents the

Volume: 12 Issue: 06 Pages: 4770-4775(2021) ISSN: 0975-0290

prospective solutions for IDPS and finally, is followed by a conclusion.

2. LITERATURE REVIEW

2.1 Security concerns in cloud

Various attacks interrupt the normal services of the cloud environment. Thus, to overcome the traditional attacks, the cloud provides numerous features however still, some attacks affect the available cloud resources and data. The security threats that target the cloud resources are as follows:

1. **Insider attack:** The authorized users of a particular organization maliciously misuse the cloud resources or services. The user may provide sensitive information to others or outside the organization. This may cause a serious trust issue [9].
2. **Denial of Service (DoS) attack**: The available resources can be destroyed by an attacker that floods the network with a large number of packets. This attack may violate the availability feature of the cloud. Therefore, the authorized users may not get the available resources at the required time [10].
3. **Man-in-the-Middle attack:** Attacker locates the data of real-time transactions and may get the login credentials, credit card numbers, etc. In this attack, a man lying in the middle as an attacker listens to information and may harm the confidentiality feature of the cloud environment [10].
4. **Attacks on Hypervisor or virtual machines:** An intruder gets control over the virtual machines and steals the data from the cloud. A zero-day attack is an example of a hypervisor attack [9].
5. **SQL injection attack**: An attacker may execute the wicked SQL commands and obtains confidential information such as login credentials, credit card details, etc. [11].
6. **Phishing attack:** This attack causes the loss of money or other kinds by sending fraud links via emails and also violates the confidentiality feature in the cloud environment [12].
7. **Remote to local Attack:** This attack helps in accessing the local system and an attacker executes the commands that run silently.
8. **User to Root Attack:** By scanning the password of the root user, an attacker can access the user account and the virtual machines can be accessed by obtaining the legal user credentials in the cloud [13].

2.2. Security Solutions for Cloud

Nowadays, a firewall alone is not adequate to handle complex attacks. Because it cannot detect complex attacks and also the attacks that are caused by insiders [14]. To protect the system from malicious attacks, several security measures for the detection and prevention of intrusions based on architecture and techniques are given[15].

2.2.1. Intrusion Detection System: An intrusion Detection System (IDS) acts as a defensive system that detects malicious activities in the cloud environment and protects the network from several security challenges. It can be implemented on a host or system or network and generates an alert if any malicious activity is found. Different methods of IDS are given in Figure 1.

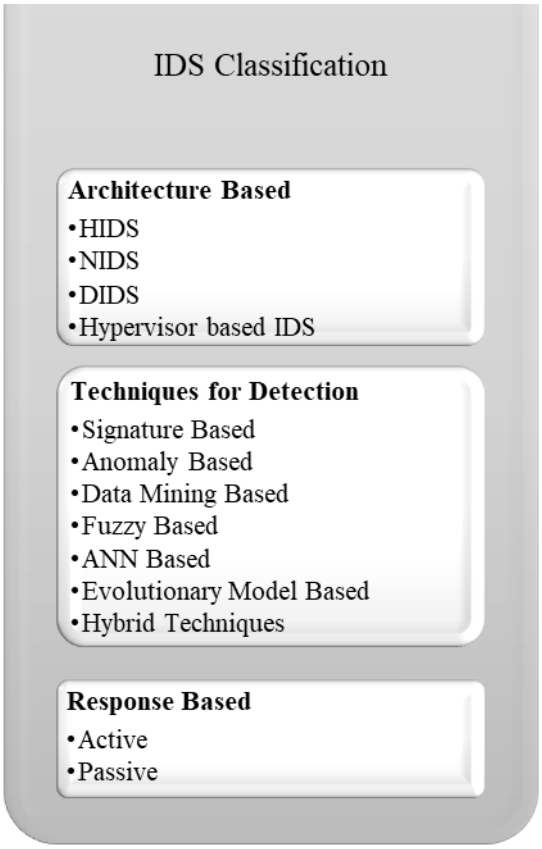

Figure:1 Classification of IDS

2.2.1.1. Detection based on Architecture: IDS can be placed at an individual host or network, based on the location IDS effectiveness can be determined[16]. It can be classified into four categories.

i) **Host-Based Intrusion Detection System**: Host-based IDS monitors the individual host on the network by checking the system log, detecting malicious behavior, incoming and outgoing packets of the host. It generates an alert if found any malicious activity [15]. HIDS relies heavily on system logs and audit trails to detect unusual activities [17].

ii) **Network-Based Intrusion Detection System**: Here, IDS monitors the incoming and outgoing packets of the entire network by analyzing various

Volume: 12 Issue: 06 Pages: 4770-4775(2021) ISSN: 0975-0290

hosts that are connected to the network. An alert is generated if any malicious activity is found in the network [15].

iii) Hypervisor Based Intrusion Detection system: It detects malicious activities during communication between virtual machines or between virtual machines and hypervisor etc. It provides a platform for running different virtual machines at the hypervisor layer of the cloud [15].

iv) Distributed Intrusion Detection System: DIDS is the combination of multiple IDS such as HIDS, NIDS, etc. It contains a central server that gathers information from multiple IDSs and then interprets it. Information is obtained from compound IDS and transcribed into a similar template and then stored on a central system for analysis [16].

2.2.2.2. Techniques for Detection: There exist numerous ways of intrusion detection in the cloud environment.:

i. **Signature Based IDS:** This technique compares the set of predefined patterns with the existing pattern to detect the intrusion for protecting the system from malicious activities. If the signature matches with the already existing pattern, then an alert is sent to the administrator. Otherwise, it will be added to the storage for later identification. It helps in recognizing only known attacks [15].

ii. **Anomaly Based IDS:** This technique can be used to diagnose anomalous behavior instead of identifying stored signatures[15]. Multidimensional approaches are used to detect attacks at different layers of the cloud that include different techniques such as data mining, statistical modeling, etc.[16]. This approach can be used to detect the performance of a user/system over a period and then compare it with normal behavior. if differs from normal behavior, it generates an alert and familiarized the admin about the attack.

iii. **Artificial Neural Network (ANN) Based IDS:** Artificial Neural network (ANN) based IDS filters the data and categorize the records according to complete or incomplete [16]. Thus, ANN filtering is similar to the biological neurons of the human brain that can classify the data as normal or intrusive. The different techniques used for ANN-based IDS are multilayer perceptron and backpropagation etc. [15].

iv. **Fuzzy logic IDS:** Fuzzy logic-based IDS works by forming fuzzy rules that provide a better way of identifying the intrusion. It generates a faster response as compared to other techniques [15].

v. **Evolutionary Model-Based IDS:** This approach uses a genetic algorithm, genetic Programming, etc. for efficient security handling in the cloud. This technique provides approximate solutions to problems that cannot be solved with the other methods. It can produce better results for dynamic and complex problems [15].

vi. **Data Mining Based IDS:** Data mining is a process concerning the extraction of significant hidden, implicit or useful information from data stored on the storage device [18]. Data mining-based IDS includes different techniques of extraction such as data clustering, data classification, etc. that are used to extract the data by acquiring valuable and hidden information [15].

vii. **Hybrid Technique for IDS:** Hybrid IDS is the unification of two or more distinct IDS techniques. It incorporates the hybrid approach such as ANN with GA or ANN with fuzzy-based methods that helps in improving the system performance [15]. Different approaches blended in IDS have some benefits and limitations. Consequently, merging different approaches overcome the limitations and additional benefits of others to get an improved IDS.

2.2.2.3. Response Based system: IDS can also be classified according to the responses it generates if any suspicious activity is noticed.

i. **Active IDS**: It is a combination of intrusion detection and prevention system in the cloud environment. This type of IDS can not only detect the attacks but also take preventive action against the detected attack [19].

ii. **Passive IDS**: Passive IDS works only for detecting the attack. It will not take any defensive action. Regular monitoring and identification of the network are to be performed on this IDS.

2.2.2. Intrusion Prevention System

Intrusion Prevention System (IPS) helps in detecting and preventing illicit entrance to the cloud environment. Instead of detecting the network packets, monitoring the files in the network is an efficient way to prevent sensitive data from modifying [20]. In this way, IPS is a combined approach to both IDS and IPS. IPS is a strict version than IDS. IPS removes the malicious part from an attack and makes it secure. It is also known as Active IDS [19].

2.2.3. Intrusion Detection and Prevention System (IDPS)

IDPS plays a significant role in protecting cloud resources from cybercrimes. Separately IDS and IPS have some strengths and shortcomings which restrict the overall security of the cloud environment [21]. Thus, combining IDS and IPS is recognized as IDPS. System activities can be monitored using IDPS as a hardware device or in the form of software. To secure the cloud environment, IDPS informs and blocks certain tasks if they found harmful activity in the cloud [19]. According to the position of IDPS, it helps in identifying internal and external attacks.

Volume: 12 Issue: 06 Pages: 4770-4775(2021) ISSN: 0975-0290

It can be categorized into three types as illustrated in Figure 2 [21].

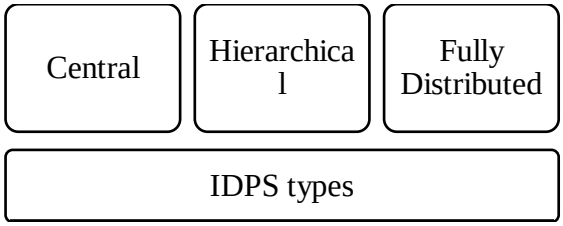

Figure 2: Types of IDPS

3. COMPARISON BETWEEN TRADITIONAL NETWORK IDPS AND CLOUD IDPS

The table comprises traditional network IDPS and cloud IDPS.

Parameters	Traditional IDPS	Cloud IDPS
Network Resources	It works for physical network resources.	It works for both physical and virtual network resources.
Nature of security	Security applied to this network is static.	According to the requirement of cloud users, Virtual machines are attached or detached dynamically. Due to its dynamic nature, IDPS needs updates periodically.
A large volume of traffic	It handles very limited network traffic.	Due to its dynamic nature, the cloud includes a huge collection of systems that handles a large volume of traffic generated by Virtual machines.
Scalability	It is difficult to restructure the layout. Thus, scalability is not applicable.	Scalability is applicable in the cloud by adding the number of virtual machines depends on hardware availability.

Table 1: Comparison between traditional and cloud IDPS

Various techniques of IDS and IPS have been considered that include the strengths and limitations of existing approaches. A comparison of traditional IDPS and cloud-based IDPS is given in table 1. The traditional IDPS is static that identifies the policies and their stable requirements gradually. Whereas, in the cloud environment virtual machines are added and removed dynamically. Thus, the security requirement of each virtual machine in the cloud environment varies [22]. Both the IDPS are compared based on different approaches.

4. CHALLENGES AND REQUIREMENTS OF CLOUD IDPS

Attacks of the traditional system also influence cloud resources. Thus, IDPS is one of the advanced solutions to protect the physical or virtual resources of the cloud. It helps in recording, informing the administrator about an attack, and then generates the reports. Following are the challenges and requirements of Cloud IDPS based upon existing IDS and IPS [16]. Cloud IDPS identify attacks for both physical and virtual environment. In that case, the cloud IDPS can also apply to the traditional network [15]. The challenges and requirements of the cloud IDPS are as follows:

i. **Controlling Extended system:** Traditionally, IDPS handles only the physical network. But in the cloud, depending on computing needs, virtual machines are added or removed. Cloud consists of a large network that manages the resources dynamically, though it is difficult to maintain the changes of resources without human intervention. Thus, IDPS handles the system in a real-time environment [15].

ii. **Identify known and unknown attacks**: A large number of vulnerabilities arise due to the virtual network. Thus, an IDPS is required for detecting and preventing both known and unknown attacks with an improved detection rate and less FAR. The system should be self-trained or learn by itself for identifying new attack patterns [15].

iii. **Issues Related to Security and Trust:** Security is the major concern in the distributed environment of the cloud that needs to be considered. Trust of the users can be achieved by applying proper security measures for user's sensitive information. Thus, IDPS is an effective mechanism for implementing security and protecting the system from attacks[22].

iv. **Advanced Detection and prevention approach:** The virtual machines in the cloud environment generate a huge number of packets. Thus, this approach resulted in preserving the network resources or information from intruders in the early phase of IDPS. In this way, this approach is effective in handling huge network traffic with endless services [15].

v. **Performance Parameters:** Following are the parameters that are considered in evaluating an efficient IDPS. These are detection rate, false-positive rate, true negative, true positive, false negative, computation cost, accuracy, etc. [15].

5. PROSPECTIVE SOLUTIONS FOR IDPS TO GOVERN SECURITY ISSUES

Security is the major concern in the cloud environment due to its distributed architecture. Thus,

Volume: 12 Issue: 06 Pages: 4770-4775(2021) ISSN: 0975-0290

various IDS and IPS techniques have been analyzed in this research work. IDS works as a detection and monitoring tool that does not take any action. It gets the notification about the occurrence of intrusion, then the other system or administrator takes necessary action. The IPS acts as a control system. It takes specific action according to the ruleset. The only condition with the IPS is that the database should be updated regularly. Thus, IDPS plays an efficient role that detects and prevents attacks on a single system. In the cloud environment, there are several techniques/ algorithms exist that achieve limited accuracy and low detection rate. Thus, the main focus of this research is to design an efficient hybrid approach of IDPS that resulted in improved performance parameters.

6. CONCLUSION AND FUTURE WORK

Intrusion Detection and Prevention System (IDPS) is an advanced solution for protection in the cloud environment that recognizes any abnormal behavior in the network. This paper analyzes the IDS, IPS and, hybrid approaches of IDPS, and a comparative analysis of traditional IDPS and cloud IDPS. The IDPS is designed in such a way to detect malicious attacks that cover both known as well as unknown attacks. Initially, the firewall was considered for maintaining security in the cloud. However, the firewalls lack in identifying recent unknown attacks. Thus, the hybrid approach of IDPS is an efficient method that detects and prevents recent attacks. Ultimately, the focus of this work includes the designing of an approach that detects and prevents intrusion in the cloud environment as well as also assists to overcome the problem of attacks to make the cloud environment secure.

REFERENCES

[1] J. K. Samriya and N. Kumar, “A novel intrusion detection system using hybrid clustering-optimization approach in cloud computing,” *Mater. Today Proc.*, no. xxxx, 2020, doi: 10.1016/j.matpr.2020.09.614.

[2] P. Singh and V. Ranga, “Attack and intrusion detection in cloud computing using an ensemble learning approach,” *Int. J. Inf. Technol.*, 2021, doi: 10.1007/s41870-020-00583-w.

[3] K. Pradeep Mohan Kumar, M. Saravanan, M. Thenmozhi, and K. Vijayakumar, “Intrusion detection system based on GA-fuzzy classifier for detecting malicious attacks,” *Concurr. Comput.* , vol. 33, no. 3, pp. 5–10, 2021, doi: 10.1002/cpe.5242.

[4] S. R. K. Tummalapalli and A. S. N. Chakravarthy, “Intrusion detection system for cloud forensics using bayesian fuzzy clustering and optimization based SVNN,” *Evol. Intell.*, no. 0123456789, 2020, doi: 10.1007/s12065-020-00410-y.

[5] G. Zhao, C. Rong, M. G. Jaatun, and F. E. Sandnes, “Reference deployment models for eliminating user concerns on cloud security,” *J. Supercomput.*, vol. 61, no. 2, pp. 337–352, 2012, doi: 10.1007/s11227-010-0460-9.

[6] C. N. Modi, D. R. Patel, A. Patel, and M. Rajarajan, “Integrating Signature Apriori based Network Intrusion Detection System (NIDS) in Cloud Computing,” *Procedia Technol.*, vol. 6, pp. 905–912, 2012, doi: 10.1016/j.protcy.2012.10.110.

[7] C. Point and S. Technologies, “SECURITY,” pp. 1–21, 2020.

[8] P. Sharma, J. Sengupta, and P. K. Suri, “WLI-FCM and Artificial Neural Network Based Cloud Intrusion Detection System,” *Int. J. Adv. Netw. Appl.*, vol. 10, no. 01, pp. 3698–3703, 2018, doi: 10.35444/ijana.2018.10014.

[9] S. M. Alturfi, D. K. Muhsen, M. A. Mohammed, I. T. Aziz, and M. Aljshamee, “A Combination Techniques of Intrusion Prevention and Detection for Cloud Computing,” *J. Phys. Conf. Ser.*, vol. 1804, no. 1, 2021, doi: 10.1088/1742-6596/1804/1/012121.

[10] C. Modi, D. Patel, B. Borisaniya, A. Patel, and M. Rajarajan, “A survey on security issues and solutions at different layers of Cloud computing,” *J. Supercomput.*, vol. 63, no. 2, pp. 561–592, 2013, doi: 10.1007/s11227-012-0831-5.

[11] A. Patil, A. Laturkar, S. V. Athawale, R. Takale, and P. Tathawade, “A multilevel system to mitigate DDOS, brute force and SQL injection attack for cloud security,” *IEEE Int. Conf. Information, Commun. Instrum. Control. ICICIC 2017*, vol. 2018-Janua, pp. 1–7, 2018, doi: 10.1109/ICOMICON.2017.8279028.

[12] A. Gursaran, “U Sing G Enetic a Lgorithm,” vol. 3, no. 3, pp. 447–450, 2010.

[13] C. Modi, D. Patel, B. Borisaniya, and H. Patel, “Journal of Network and Computer Applications A survey of intrusion detection techniques in Cloud,” *J. Netw. Comput. Appl.*, vol. 36, no. 1, pp. 42–57, 2013, doi: 10.1016/j.jnca.2012.05.003.

[14] K. W. I and V. Hou, “Detection Method of SQL injection Attack in Cloud,” pp. 487–493.

[15] C. N. Modi and K. Acha, “Virtualization layer security challenges and intrusion detection/prevention systems in cloud computing: a comprehensive review,” *J. Supercomput.*, vol. 73, no. 3, pp. 1192–1234, 2017, doi: 10.1007/s11227-016-1805-9.

Volume: 12 Issue: 06 Pages: 4770-4775(2021) ISSN: 0975-0290

[16] S. Alam, M. Shuaib, and A. Samad, *A Collaborative Study of Intrusion Detection and Prevention Techniques in Cloud Computing*. Springer Singapore.

[17] N. Das and T. Sarkar, "Survey on Host and Network Based Intrusion Detection System," *Int. J. Adv. Netw. Appl.*, vol. 6, no. 2, pp. 2266–2269, 2014.

[18] P. P. Chapke and R. R. Deshmukh, "Intrusion Detection System using fuzzy logic and data mining technique," *ACM Int. Conf. Proceeding Ser.*, vol. 06-07-Marc, 2015, doi: 10.1145/2743065.2743128.

[19] K. Bakour, G. S. Daş, and H. M. Ünver, "An intrusion detection system based on a hybrid tabu-genetic algorithm," *2nd Int. Conf. Comput. Sci. Eng. UBMK 2017*, pp. 215–220, 2017, doi: 10.1109/UBMK.2017.8093378.

[20] H. Jin *et al.*, "A VMM-based intrusion prevention system in cloud computing environment," *J. Supercomput.*, vol. 66, no. 3, pp. 1133–1151, 2013, doi: 10.1007/s11227-011-0608-2.

[21] S. Das and M. J. Nene, "A survey on types of machine learning techniques in intrusion prevention systems," *Proc. 2017 Int. Conf. Wirel. Commun. Signal Process. Networking, WiSPNET 2017*, vol. 2018-Janua, pp. 2296–2299, 2018, doi: 10.1109/WiSPNET.2017.8300169.

[22] A. Patel, M. Taghavi, K. Bakhtiyari, and J. Celestino Júnior, "An intrusion detection and prevention system in cloud computing: A systematic review," *J. Netw. Comput. Appl.*, vol. 36, no. 1, pp. 25–41, 2013, doi: 10.1016/j.jnca.2012.08.007.

AUTHORS BIOGRAPHIES

Vaneeta did her MCA from Kurukshetra University, Kurukshetra in the year 2012 and qualified UGC NET in 2019. She is pursuing her Ph.D. from Punjabi University, Patiala. And is currently working in Patel Memorial National College, Rajpura. She has a total of 7 years of experience in teaching.

Sangeeta Rani is currently working as an Assistant Professor in the Mata Gujri College, Fatehgarh Sahib (Punjab), India, with an overall experience of 14 years in the academia and research fields of computer science and IT. She received her Ph.D. degree from Punjab Technical University, Jalandhar, India. She is an avid researcher having guided dissertations of many PG students and she is currently guiding Ph.D. scholars. Her research interests include mobile phone security and network security.