*Recent Developments in Electronics and Communication Systems*
*KVS Ramachandra Murthy et al. (Eds.)*


*doi:10.3233/ATDE221315*

# Securing Cloud Using Intrusion Detection Systems: A Review

Vishnu Balaji Eepari[a], Ch. Govind Raju[b], P. Dileesh Sai[c], K Govindaraju[d], B.S.Kiruthika Devi[e,1]
[a,b,c] *U.G Student, Department of CSE, Aditya Engineering College (A), Surampalem, A.P, India*
[d] *Associate Professor, Department of CSE, Aditya Engineering College (A), Surampalem, A.P, India*
[e] *Research Mentor, CL Educate Ltd., New Delhi, India*

**Abstract.** Cloud computing consists of technologies like distributed computing, grid computing, virtualization, utility computing, network computing, and the web. There are several threats in the cloud, such as man-in-the-middle attacks, port scans, DoS/DDoS attacks, IP spoofing, and phishing. One of the most serious threats today is denial-of-service attacks, because they affect the availability of critical resources. The primary goal of this paper is to analyze the intrusion detection systems (IDSs) that can identify intrusion attempts in distributed systems as well as virtualized environments. This paper discusses various types of systems such as anomaly, signature, hybrid, hierarchical, and collaborative IDS. The systems are studied and the various methodologies, tools, datasets, operating layers, and accuracies of the IDS are compared and contrasted.

**Keywords.** Intrusion Detection System, Cloud Computing, Denial of Service attack, Signature Based, Anomaly Based, Hybrid, Hierarchical, Collaborative IDS.

## 1. Introduction

A cloud computing technology is a technology that provides on-demand access to computer resources, primarily for information storage and computation, without the need for severe management control by the clients. Cloud services, which are provided by companies, enable users to store their files, applications, and data on remote servers and then access them via the Internet. It is a collection of source information that allows for the distribution of data. It is highly coordinated with its computing facilities that deliver its response to a request from a customer. The consumer is not required to buy any facilities, devices, applications, or other resources that would lead to significant financial outlay. In general, clouds provide services through a third party rather than directly to the end user. A large number of users access the cloud's services for a wide range of reasons that are not based on solid foundations, making the cloud vulnerable to attacks. By finding many applications on the cloud, there are huge chances of susceptibility and attacks in the cloud [1].

[1] Corresponding Author, B.S.Kiruthika Devi, Research Mentor, CL Educate Ltd., New Delhi, India; E-mail: kiruthika.devi@accendere.co.in

IDSs detect unnecessary activities on networks and systems, mainly from the Internet, and can also be implemented to detect the various attacks on a network/cloud to preserve its security. Methodologies for intrusion detection and prevention (IDP) are primarily divided into two categories, such as misuse and anomaly detection. Misuse approaches are widely used because they can identify intrusions based on well-known trends such as network packets, related sender and receiver addresses, ports, keywords in the payload, and so on. This scheme has a limitation in that it must be updated frequently with attack specifics. The attacks that have been already stored in the database will be discovered. However, it does have a benefit in that it does have a lower rate of false positives. The anomaly system works by detecting deviations from normal behavior and issuing notifications in the event of a potential unknown attack that has not been previously identified. It has a higher rate of false alarms than the misuse method, but it is capable of detecting unknown attacks and searching for deviations in a random direction [20], unlike the misuse technique. An organized attack on the availability of services of a specific target that is indirectly launched by multiple computers associated with the network is referred to as a Distributed Denial of Service Attack (DDoS). Attackers exploit software vulnerabilities in the system and then use the server's RAM or CPU to their advantage, causing the system to crash. These types of attacks command multiple agents to send a stream of packets to a victim, and as a result, they can reduce the quantity of assets the victim has while the attack is ongoing [2].

## 2. Related Work

In the year 2012, a framework that is capable of detecting intrusion attempts in a cloud computing environment as well as safeguarding the cloud from possible security infringements is proposed. This proposed system consists of cloud architecture and various kinds of risks such as privacy risks, security risks, and risks in the cloud. It has collected information on data integrity, data segregation, data security, and the tabulated form of security mechanisms of service providers [1]. Ken and Theng shared different types of intrusion systems that are affected by the cloud. The techniques used in this method are signature, anomaly-based, and hybrid [2]. A Hypervisor based Cloud Intrusion Detection System (HCIDS) is proposed to address some of the challenges in traditional intrusion systems and cloud environments. They gathered data on workload, activities, and attacks; used an attack analysis approach for detecting attacks [3]. Several machine learning algorithms [4] for detecting DDoS attacks are analyzed in order to select the optimal model using real-world attack sets of data. They studied supervised ML techniques for detecting attacks and applied several ML and supervised ML algorithms for the purpose [23]. This research studies denial of service attacks and their defenses. It explains the denial of sustainability, network security, and system security. It discusses the adversary effect of DoS attacks as one of the most significant obstacles to ensuring sustainable and secure systems [5].Using artificial neural networks [6], a system for the detection of known and unknown DDoS attacks was proposed. They have used a trained artificial neural network algorithm [22] to detect TCP, UDP, and ICMP attacks based on patterns that distinguish legitimate traffic from DDoS attacks. A hybrid statistical technique in a cloud computing environment provides a cloud infrastructure for studying DDoS attacks. They proposed their heuristic as well as various approaches such as the covariance matrix, Kendall's Tau, and entropic schemes [7]. Christina Enache established a system by trying to implement an enhanced bat-algorithm for attack

detection in a computer. They investigated a variety of Swarm Intelligence (SI) algorithms and their prominence, which have been implemented in a variety of applications over the past couple of years. The standard BBA was used in conjunction with a combined binary version and SVM [8] [21] to pick an input variable for the model.

## 3. Methodology Used

The methodology refers to various functionalities involved in the intrusion detection system. There are various intrusion detection systems that can be used for detecting attacks in the cloud, which are anomaly, signature, collaborative, hierarchical, and hybrid.

### *3.1. Anomaly based IDS*

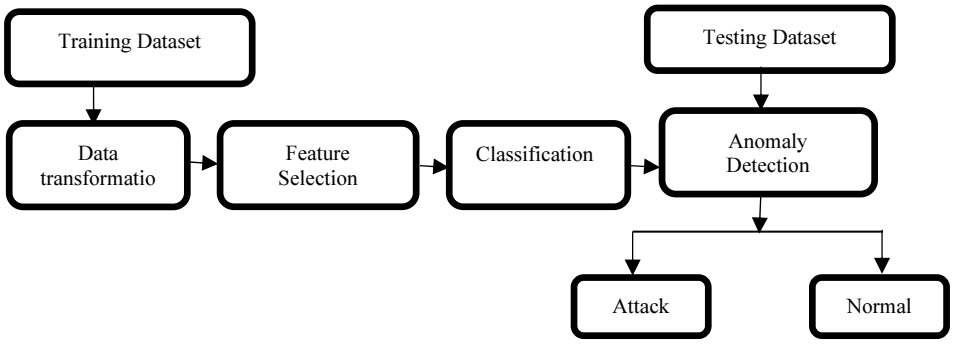


**Figure 1.** Anomaly based IDS

The anomaly model includes data transformation, data normalization, feature selection, and classification, which is shown in Figure 1 [9]. A data preprocessing phase is a time-consuming process, but it is very vital in the data mining process. The data collected from a variety of portals is inconsistent, inadequate, and repetitive in their ways of acquiring information. Outliers and redundant samples are removed, and data transformation is performed in this work [19]. The pre-processing stage in this work also includes data transformation. The process of transforming data from a high dimension to a low dimension space is called reduction. High-dimensional spaces can be unproductive for a variety of reasons, not the least of which is that raw data is frequently split as a result of the anomaly of dimension. After the features are selected, the anomaly detection categorizes the data into normal and attack.

### *3.2. Signature Based Intrusion Detection System*

Signature-based detection [17] is generally utilized to recognize existing attacks and is therefore the most effective method. It operates on the basis of a pre-programmed list of known risks and a clear indication of compromise associated with each threat (IOC). The data related to the user identification, which consists of an id, password, and IP address. It can read the protocols of specific IP addresses as well as port numbers in incoming requests [10]. The process involves matching the captured packets against a set of rules in the knowledge base to find any correlation. In the event of any attack, it determines the nature of the attack and sends the warning message as an alert to the alert system. The working process on the rules, which can be written in any language, so that the rules

can be read and modified easily [11]. The solution developed by signature-based IDS is used to find the sequences and patterns that match a particular attack signature, usually employed to scan the system files for any malicious activity [18].

### *3.3. Hybrid Based Intrusion Detection System*

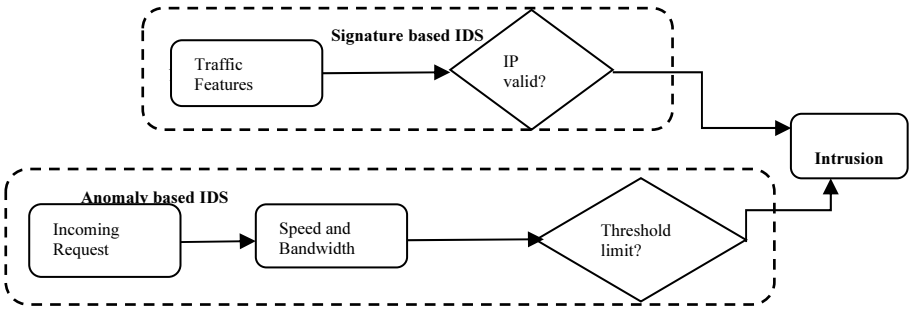


**Figure 2.** Hybrid IDS

A Hybrid IDS is a combined one that is derived from more than one kind of IDS. Here, we considered two IDSs, which are signature-based and anomaly-based as shown in Figure 2. In execution, both the intrusion systems will result in an intrusion condition if the condition or requirements are not satisfied. The process is continued with the input signal or incoming request from the user, which may have some physical quantities, say speed and bandwidth. If the incoming request's speed or bandwidth crosses the threshold limit, the system detects or results in an intrusion. In the same way, if any signature or IP address is mismatched, then the IDS also detects the intrusion. Traffic features include email id, password, physical address, protocol, and port number of the incoming request for signature matching. An incoming request is taken as an input for the anomaly basis, which contains speed and bandwidth to compare with the threshold values. If it exceeds, then there is an intrusion in the network.

### *3.4. Hierarchical Intrusion Detection System*

The proposed cloud IDS is an architecture that consists of six different layers in which each layer performs a specified function. The Physical Layer is the lowest level that defines the physical specifications of the cloud [13]. The Hypervisor and Cloud services provide system security functions such as isolation, inspection, and management of their components. In the virtualization layer, VMs are mapped onto their physical cores. The Alert includes HIDS, NIDS, and Data Driven Semi-Global Alignment (DDSGA). Integration and Reporting layer generates the alerts from the local host and the network. It uses the IDMEF format. It also handles a large number of integrated alerts and reports them to the next layer. The Web Interface Layer offers the central location to the administrator and manages the IDS components by handling the web pages [12].

### *3.5. Collaborative Network Intrusion Detection System*

Network intrusion in the cloud is detected by integrating an NIDS module on the front-end of the system. The Virtual Machine Monitor (VMM) back end identifies insider and external attacks. Cloud-based virtual machines are designed to deal with these attacks as

efficiently as possible [17]. Packet sniffing collects the in-bound and out-bound network packets. Tools like Wireshark are used in packet sniffing. These packets are verified by a signature-based technique. The Alert system generates alerts about intrusions which are determined either by SNORT or Anomaly-based IDS. Alerts are stored in the alert system and passed further to the central log database for intrusion detection [16]. The SVM algorithm used for anomaly detection. NIDS sensors change their bases in response to alerts that are recorded in the central database. The signature-based system, as a result, can be used to detect any additional intrusions with relative ease. This lowers the computation complexity of NIDS while simultaneously increasing its accuracy [11].

## 4. Results and Discussions

Table 1 describes the techniques used with respect to the OSI reference model in the computer networks. The accuracy of the techniques is compared and contrasted.

**Table 1.** Comparison of various techniques implemented in the cloud

| S.No | Techniques Used | Tools used | Dataset | Layer | Input | Output | Accur -acy |
|---|---|---|---|---|---|---|---|
| **1** | Anomaly Based Detection [3] | MYSQL, DBMS, PHP, Open-Stack | KDD 1999, NSL-KDD | Network | Bandwidth, Speed, Incoming request | Thresh-old limit, | 98.10% |
| **2** | Signature Based Detection [18] | SNORT IDS | KDD'99 , ISCX, UNSW-NB15 | Network/ Transport | Traffic features, IP addresses, Port, Protocol, | Request status | 97.52% |
| **3** | Hybrid IDS [7] | SQL, NOSQL | NSL-KDD | Network, Host | Incoming request, | Checksu m | 99.98% |
| **4** | Collaborative IDS [11] | Trinoo, Shaft, Trinity | DARPA | Transport | Traffic Parameters | Alert | 97.40% |
| **5** | Hierarchical IDS [13] | Cloud Servers, | DARPA | App -lication | Traffic parameters | Alert | 99.42% |

## 5. Conclusion and Future Work

This paper provides a detailed study of various intrusion systems for detecting DDoS attacks. The IDS architecture and its efficiency against attacks are compared and contrasted. Anomaly-based IDSs are light in nature and create false alarms compared to other systems. Signature-based IDSs are suitable for large-sized networks so that they may have overheads in updating the intrusion in matching signatures. By combining the two IDSs, a hybrid IDS is designed and it gives relatively high accuracy. Collaborative and hierarchical IDSs are much more time-consuming systems due to their layered or module approach, but they are highly efficient and produce more accuracy and a lower false alarm rate.

## References

[1] Dhage SN, Meshram BB, Rawat R, Padawe S, Paingaokar M, Misra A. Intrusion detection system in cloud computing environment. InProceedings of the International Conference & Workshop on Emerging Trends in Technology 2011 Feb 25 (pp. 235-239).

[2] Kene SG, Theng DP. A review on intrusion detection techniques for cloud computing and security challenges. In2015 2nd International Conference on Electronics and Communication Systems (ICECS) 2015 Feb 26 (pp. 227-232). IEEE.
[3] Nikolai J, Wang Y. Hypervisor-based cloud intrusion detection system. In2014 International Conference on Computing, Networking and Communications (ICNC) 2014 Feb 3 (pp. 989-993). IEEE.
[4] Bindra N, Sood M. Detecting DDoS attacks using machine learning techniques and contemporary intrusion detection dataset. Automatic Control and Computer Sciences. 2019 Sep;53(5):419-28.
[5] Zlomislić V, Fertalj K, Sruk V. Denial of service attacks, defences and research challenges. Cluster Computing. 2017 Mar;20(1):661-71.
[6] Saied A, Overill RE, Radzik T. Detection of known and unknown DDoS attacks using Artificial Neural Networks. Neurocomputing. 2016 Jan 8;172:385-93.
[7] Girma A, Garuba M, Li J, Liu C. Analysis of DDoS attacks and an introduction of a hybrid statistical model to detect DDoS attacks on cloud computing environment. In2015 12th International Conference on Information Technology-New Generations 2015 Apr 13 (pp. 212-217). IEEE.
[8] Enache AC, Sgarciu V. An improved bat algorithm driven by support vector machines for intrusion detection. InComputational Intelligence in Security for Information Systems Conference 2015 Jun 15 (pp. 41-51). Springer, Cham.
[9] Dwivedi S, Vardhan M, Tripathi S. Defense against distributed DoS attack detection by using intelligent evolutionary algorithm. International Journal of Computers and Applications. 2022 Mar 4;44(3):219-29.
[10] Rajendran PK, Rajesh M, Abhilash R. Hybrid intrusion detection algorithm for private cloud. Indian Journal of Science and Technology. 2015 Dec;8(35):1-0.
[11] Al Haddad Z, Hanoune M, Mamouni A. A collaborative framework for intrusion detection (C-NIDS) in Cloud computing. In2016 2nd International Conference on Cloud Computing Technologies and Applications (CloudTech) 2016 May 24 (pp. 261-265). IEEE.
[12] Gundabathula G, Kunda P, Nandan D, Kumar S. Implementation of Cloud Based Traffic Control and Vehicle Accident Prevention System. InICCCE 2020 2021 (pp. 1125-1134). Springer, Singapore.
[13] Schueller Q, Basu K, Younas M, Patel M, Ball F. A hierarchical intrusion detection system using support vector machine for SDN network in cloud data center. In2018 28th International Telecommunication Networks and Applications Conference (ITNAC) 2018 Nov 21 (pp. 1-6). IEEE.
[14] Karan BV, Narayan DG, Hiremath PS. Detection of DDoS attacks in software defined networks. In2018 3rd International Conference on Computational Systems and Information Technology for Sustainable Solutions (CSITSS) 2018 Dec 20 (pp. 265-270). IEEE.
[15] Alzahrani S, Hong L. Detection of distributed denial of service (DDoS) attacks using artificial intelligence on cloud. In2018 IEEE World Congress on Services (SERVICES) 2018 Jul 2 (pp. 35-36). IEEE.
[16] Priya BJ, Kunda P, Kumar S. Design and Implementation of Smart Real-Time Billing, GSM, and GPS-Based Theft Monitoring and Accident Notification Systems. InProceedings of International Conference on Recent Trends in Machine Learning, IoT, Smart Cities and Applications 2021 (pp. 647-661). Springer, Singapore.
[17] Kumar V, Sangwan OP. Signature based intrusion detection system using SNORT. International Journal of Computer Applications & Information Technology. 2012 Nov;1(3):35-41.
[18] Santoso BI, Idrus MR, Gunawan IP. Designing Network Intrusion and Detection System using signature-based method for protecting OpenStack private cloud. In2016 6th International Annual Engineering Seminar (InAES) 2016 Aug 1 (pp. 61-66). IEEE.
[19] Rezvani M. Assessment methodology for anomaly-based intrusion detection in cloud computing. Journal of AI and Data Mining. 2018 Jul 1;6(2):387-97.
[20] Dong S, Abbas K, Jain R. A survey on distributed denial of service (DDoS) attacks in SDN and cloud computing environments. IEEE Access. 2019 Jun 12;7:80813-28.
[21] Jyothi KD, Sekhar MS, Kumar S. Applications of Statistical Machine Learning Algorithms in Agriculture Management Processes. In2021 6th International Conference on Signal Processing, Computing and Control (ISPCC) 2021 Oct 7 (pp. 237-241). IEEE.
[22] Rozendaal K, Mailewa A. Neural Network Assisted IDS/IPS: An Overview of Implementations, Benefits, and Drawbacks. International Journal of Computer Applications.;975:8887.
[23] Unnisa A N, Yerva M, MZ K. Review on Intrusion Detection System (IDS) for Network Security using Machine Learning Algorithms. International Research Journal on Advanced Science Hub. 2022 Mar 29;4(3):67-74.