A Study Of Intrusion Detection System For Cloud Network

Nishika, Kamna Solanki, Sandeep Dalal

Abstract: Information security is a vital issue about data transmission in a cloud-computing environment, along with possessing potential challenges. Cloud services play a significant role in offering Information Technology (IT) services. However, security challenges will remain a serious threat to such services. The Intrusion Detection System (IDS) plays a central role in the protection of network security by detecting the occurrence of an attack. The rising incidences of the cyber-attacks have raised the demand for an efficient IDS security system. Detecting accuracy and stability are the two key indicators to evaluate the efficiency of IDS. In this paper, the authors presented an inclusive framework to explore the surveys that notify the researchers of the novel mechanisms and techniques being developed for IDS. Types of intrusions and relative effects that have been studied until now are presented in the paper. An examination was conducted to enlighten better perspectives to have available research in the future.

1 INTRODUCTION

In the current scenario, Internet development and computer system usage have been an essential concern in electronic transmission of data, which has several problems, such as privacy, security, and discreetness of information. Considerable progress has been seen in the improvement in terms of computer system security [1]. Security problems and the privacy issues of electronic systems are the key challenges existing with the computer systems. Though there is no 100% secure system present in the world. It was noted that there are massive cases of attacks. In general, if a novel signature detected in the signature database, then the behavior is to be deemed to be an attack. The vulnerabilities of computer systems could accomplish with recognized and non-recognized users. In this regard, several tools have implemented to get rid of the attack that helps in security assistance, and IDS is considered as one of the best tools that assist in examining information and network system. It identifies intrusions and is significant for breaking norms such as integrity, non-repudiation, and accessibility [2]. With the dawn of computer networking, IDS played a significant role in insurance of a safe network for each user, though the form of role has changed since last year. Essential intrusion detection components are described below

i. Data Pre-processor: It is accountable for the provision and the collection of audit data in an exact format to the subsequent analyzer or the component to developing some decision. The data is known as an Audit log.

ii. Analyzer (Intrusion Detector): It is the significant component that examines the audit log for the detection of an attack.

iii. Different pattern matching, data mining, statistical techniques, and machine learning methods could be utilized as Intrusion detectors — the system strength measured in terms of the analyzer’s ability for intrusion detection.

iv. Response Engine: It is accountable for the control of the reaction method and also establishes the responsibilities of the occurrence of an attack. The attack relies on pre-defined security strategies.

The description of varied IDS components is given below [3]:

i. Data gathering device: It is accountable for the collection of data using a monitored system.

ii. Detector engine: It examines the data amalgamated from the sensors for the identification of intrusive activities.

iii. Knowledgebase: It has information amalgamated by the sensors but for the pre-processed format. Security experts and network experts generally give information.

iv. Configuration device: It gives the information for the existing IDS state.

v. Response component: It starts with the actions when the intrusion is detected. It could be either by human interaction or automated interaction.

The general architecture of IDS has been illustrated in Fig. 1 and is defined as follows

![Fig. 1. Basic IDS architecture](image-url)

---

- Nishika is currently pursuing Research Scholar program in UIET, Rohtak, India. E-mail: nishika510@gmail.com
- Kamna Solanki is currently working as an assistant professor in UIET, MDU, Rohtak, India. E-mail: kamna.mdurohtak@gmail.com
- Sandeep Dalal is currently working as an assistant professor in UIET, MDU, Rohtak, India E-mail: sandeepdalal.80@gmail.com
1.1 Motivation

The structure and services of clouds become fully open as a more attractive target for probable entrants. It deals with multimesh parameters and services aimed at the services that are more vulnerable and multi-user administrative independent administrative infrastructures that are more susceptible to a security threat. The architecture of cloud services consists of applications, viz. infrastructures, platforms, and interdependent applications. Every layer experienced some vulnerability that adds different configuration or programming errors to the service providers. Cloud might be acknowledged to different threats because of the confidentiality, reliability with the accessibility of its resources, virtual infrastructure, and the data that could be utilized being a new attack initiation pad. It has resulted in a significant critic when cloud storage ability and enormous computing power are neglected by the intruder that intimidates the cloud. The lack of overall control of the consumer infrastructure of cloud services is a significant concern in these scenarios. It values the IDS role in defending consumer cloud computing information assets. This manuscript examines the claims and the concerns that prohibit the advanced IDPs expansion in the cloud computing environment. It intends to attract esteemed authors for probable solutions in building IDPS with current dissimilar study together for delivering secure current widespread resources and services in the cloud. Besides, it analyses the required IDS concern for the cloud and has proposed significant training implications.

1.2 Research Boundaries & Limitations

The existing IDS prevention and detection system include the study of each system that judges more feature of the explanation and mechanism in this manuscript. A couple of authors have aimed at specific Intrusion Detection and prevention systems or a particular attack that aimed at reducing false-positive rates. Since cloud computing is a promising field, the manuscript tried to emphasize current research topics being published in these years to reap advantage from modern and advanced system. Prevention is considered as a very recent IDS feature. Hence, there are merely some existing works with this feature. However, this research has contemplated current work on IDS as they are a flexible accumulation of prevention part, and this boundary has set a limit for this research by the traditional work. As the cloud has been accepted globally; consequently, there are some systems for detecting possible and experimental intrusions established in the real world.

2 CURRENT STATE OF THE ART OF IDS

IDS includes monitoring of the network for malicious activities like detection of an attack, malicious software, and unauthorized access to the system. IDS try to monitor an intruder penetrating in the system by exploiting genuine resources of user’s system while the IDS have been executed to work better on some massive networks, Cloud deployment is a demanding issue and based on Cox work in 2012, IDS could be placed at any VM, every node (hypervisor or host) or conventional network [1][2]. It can be placed on the traditional network, which is the Cloud system access point. The permits Cloud to detect external attacks. It cannot assist in detecting internal attacks [3]. In the virtual environment of the cloud, virtualization is required to communicate between the VMs (on all host systems) and, consequently, to the network traffic monitoring that flows through the virtual passage. Additionally, it is necessary to provide security and performance, as well. Hence, efficient mechanisms have to be utilized for the reduction of false observant and guarding their performance. It can involuntarily manage more data flow with no human intercession. Several vulnerabilities in the hypervisor led to the impossibility and control of an attacker’s VMs [4][5]. Hence, these vulnerabilities permit the attacker to allow IDS to compromise on VMs. The methods used to detect the intervention should have a lower computing cost than the IDS that executes in an authentic period. The sensor and even the warning co-relation modules influence scalability and performance after working together to detect interference of these modules. It can defend itself from unauthorized attacks and access. It confirms network devices and protects their data. Roschke et al. have observed VM-IDS structure, which collects malicious events in the IDS sensor and event database [6]. The investigation component (user-config.d) log into the database of event and then examines them. The IDS sensor detects malevolent events and transmits them to an event collector. As with any VM filter deployed on a network attack, this approach provides VMs with malicious activity. Though, with increasing VM cases, IDS patterns are also increasing. An agile method based on MA (Mobile Agents) detects interference was giving by Dastgerdi et al. [7]. The research has utilized an MA for the prevention of VMs slight the architecture. Attack confirmation from each attacked VMs is composed of MA for subsequent assessment and audit. Therefore, this method corresponds to the definition of intrusion in the VM outside the organization. Nevertheless, when the VMs enhances, more of the traffic removes. Another approach of agent basis by Lo et al. and Ram et al. has deployed the IDS sensor in every cloud section [8][9]. This method avoids the cloud from a DDoS attack. Bakshi and Yaqash installed IDS in a virtual passage to notice a DDoS attack on the VM. IDS includes virtual traffic control / virtual network traffic in the database [10]. Each zombie machines (DDoS attack victims) are blocked-up. So, the DDoS attack could be stopped up by this method. It only finds identified attacks. Mazzariello et al. placed SNORT to find the intrusions on the open-source Eucalyptus Cloud Controller with Physical Machines (PMs) [11]. This placement resolves the issue of developing different IDS patterns. Gul and Hussein have proposed third party IDS architecture that uses multi-threaded techniques for the improvement of detection speed [12]. Dhage et al. have proposed the IDS framework that offers a user with a mini-IDS sample when logged in to Cloud Server (centralized) Cloud services. Mini-IDS observe user activities (network traffic) and transfers the session notes to the IDS controller [13]. Khalid et al. have presented a novel architecture, namely, Cloud-based IDS (CIDS) with two IDS detectors for every node, viz. HIDS and CIDS [14]. Node participates in identifying interference by recognizing information about security breaches and other information. Network-based IDs for the detection of interventions in the virtual environment given by Gupta et al. [15]. Idrees et al. had considered the cloud IDS framework. In this, network interruptions in the DMZ network are detected, and system attacks on critical machines (or servers) are detected [16].

3 INTRUSION DETECTION IN CLOUD ENVIRONMENT
Different detection methods are being introduced in the cloud for identifying the flooding attack. In this recognition architecture, various Intrusion detection systems are interconnected. Also, the IDS compose of two components, viz., alarm system, and an analyzer [4]. The steps of detection in HIDS (Host-Based Intrusion Detection System)-based architecture begin by collecting data by system logs with an event handler. The classification of intruded data is done with the two methods either by knowledge base or by behavioral methods. The primary technique being utilized in the detection is ANN (Anomaly Neural Network) approach. The following method recognizes merely the known attacks. When the attack occurs, an alarm system notifies another node. Additionally, a HIDS-based technique has been utilizing for the detection of known and unknown attacks. Though, no insider attack can be detected inside VMs. A VM-compatible IDS architecture has been proposed. The architecture of HIDS is shown in Fig. 2. This architecture consists mainly of two parts, IDS sensor, and IDS management [5]. The original part has four parts, namely, events gatherer, an analysis component, events database, and events database. In the case of VM compatible architecture, an attack includes steps, like primary, IDS sensors have caught up with malevolent behavioral events and the transfer of data to the events and the searcher’s stores in the database events. Subsequently, the examination of these events is with the analyzing components (intended users) to depict the behavior of malicious nodes. Even, communication among IDS sensors and IDS-VMs is led as per the remote controller IDS. The main task of IDS sensors is the identification of the malicious nature of the VMs and transferred them for searchers events.

**Fig. 2. HIDS Based Environment**

Additionally, the sensors could be a NIDS (Network-Based Intrusion Detection System) that is provided with the IDS remote controller. Accordingly, a novel sensor could be solved as per directly linking the sender/receiver towards the event gatherer. NIDS architecture is shown in Fig. 3 [6].

**Fig. 3. NIDS Based Environment** [6]

DIDS (Distributed IDS) has different IDS (such as, HIDS, NIDS, etc.) in an infinite structure, each of which interfaces one another, or has focal server licenses are viewed. Parts of the impedance territory obtained data structure and changed it to a systematic shape passed to the focal analyzer [7]. The combination of diversity from the standards and base ID-based systems is utilized for the purpose of the examination. DIDS could be utilized to view identified and cloud ambulances because they require focal reasons for both NIDS and HIDS. Fig. 4 shows the employment of DIDS, and Table 1 summarizes the strengths and challenges of various types of IDS.

**Fig. 4. DIDS Based Environment**

<table>
<thead>
<tr>
<th>IDS Types</th>
<th>Strengths</th>
<th>Challenge</th>
<th>Positioning in cloud</th>
<th>Deployme nt and monitoring authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>HIDS [20]</td>
<td>It finds the intrusions with the Host File System (HFS) monitoring.</td>
<td>It has to be installed on every machine. It should monitor the attacks</td>
<td>On every VM/HS (Host System)</td>
<td>Cloud users on VMS and Cloud providers on the hypervis or.</td>
</tr>
</tbody>
</table>

**TABLE 1**

**IDS Types OUTLINE**
There is no need for extra hardware.

It finds the intrusions with monitoring the network traffic. It should be placed on the exact network. It may examine various systems on time.

It is hard to distinguish the intrusions on the encrypted traffic. It assists with the detection of external intrusions. It is difficult for the detection of network intrusion in the Virtual network.

On virtual network Cloud provider

4 IDS ATTRIBUTES

A number of preferred attributes for IDS are identified and described below:

i. Prediction performance

In IDS, an easy parameter of performance like prediction accuracy is not enough. To have better performance, IDs should gratify the two criterions: (i) it should accurately recognize the intrusions and (ii) it should not recognize the legitimacy of the system environment as intrusion [8]. Standard measures include checking the IDS predictive performance, such as the false alarm rate and the detection rate, as described in Table 2.

### Table 2

<table>
<thead>
<tr>
<th>Actual connection label</th>
<th>Predicted connection label</th>
</tr>
</thead>
<tbody>
<tr>
<td>Normal connection</td>
<td>Normal</td>
</tr>
<tr>
<td></td>
<td>Intrusions/Attacks</td>
</tr>
<tr>
<td>Normal</td>
<td>TN (True Negative)</td>
</tr>
<tr>
<td></td>
<td>FA (False Alarm)</td>
</tr>
<tr>
<td>Intras/Attacks</td>
<td>FN (False Negative)</td>
</tr>
<tr>
<td>Correctly Detected</td>
<td>TP (True Positive)</td>
</tr>
</tbody>
</table>

ii. Time Performance

It communicates to the overall time for the detection of intrusion by IDS. It includes propagation and processing time. Processing time relies on the processing speed as the processing audit event rate [9]. When the rate is not that high, then the possibility of security events is less. The propagation time is considered as the time needed for the executed information to propagate the analyst. It should take less time to execute so that security analysts could get the time to respond to the attack before more damage and for halting the attacker to modify the IDs. The proportion by which the attacks can be identified accurately is the detection rate. The connection that has been misclassified like attack with the total...
standard connection is a false alarm or false positives. It became very tricky to analyze the measures as it is not probable to have knowledge of every attack. The false alarm and the detection rate are diverse, so, IDS can be implemented by means of ROC (Receiver Operating Characteristics) [10]. The effectiveness of IDS could be because of the ROC closeness to the left corner to the graph that is the point that equivalence to the zero percent as a false alarm and a hundred percent as detection rate.

iii. Fault Tolerance
One of the most evident features of any IDS mechanism is fault tolerance. This parameter examines the stamina of the network over the incoming faults. How much effect a fault can make into the processing architecture and till what point the network can bear the load of fault is defined as fault tolerance. It can be evaluated in terms of packet error, load, or even by any other Quality of Service (QoS) parameter.

iv. Accuracy
It is defined as the prediction accuracy of the correct detections of the Intrusion Detection System. It is the ratio of the total number of correct detections to the total number of detections. High prediction accuracy refers to the high identification rate and precise detection mechanism.

v. QoS Evaluation
This section lightens up the existing work for IDS in the cloud to consider the best algorithm/technique/method in the future for the enhancement by means of Accuracy measure. We have analyzed the work of three researchers for prediction performance in terms of ROC and accuracy [17-19].

Fig. 5 shows a receiver operating characteristic (ROC) curve resulting from two systems in an IDS test in terms of false alarm. Lippmann and Zissman had shown that IDS could be activated at any region on the curve. The systems under study were network-based IDS, and for the measurement purpose, the unit was defined as the total packets that are broadcast over the network. The authors had concluded that A-SYSTEM showed more significant potential to get customized to various operating points as compared to B-SYSTEM. This is due to the fact the other system possesses a single functional point. The study was based on the assumption that at the awful case, IDS results in 1-alert/packet and, at best, will be equal to the number of packets transmitted [17].

Fig. 6 depicts the work by Singh et al., that has introduced a detective control mechanism in IDS. COIDS (Cuckoo optimization-based IDS) has been proposed with COFS (Cuckoo Optimization-based feature selection) to enhance the accuracy of IDS. As depicted in the fig., the researcher has considered varied feature selection algorithms like IGFS (Information gain feature selection), CSFS (Chi-square Feature Selection), and GRFS (Gain Ratio based feature selection) with ORFS (OneR feature selection). It has been seen that the performance of proposed COFS is better as contrasted to other feature selection algorithm with an average value of 71.689 [18].

CONCLUSION
The privacy, accessibility, and integrity of a computer system

Fig. 5. ROC Curves for intrusion detection techniques [17]

Fig. 6. Accuracy examination [18]
are verified with IDS. Because of the expanding growth of cloud users, IDS are in immense demand. As more and more modern computing infrastructure moving to the cloud, intrusion detection has become a more significant piece of the research landscape. For the protection of infrastructure, the associations around the world are considering a lot of information on IDS in the cloud. The concept is even varying, and the novel techniques fit in cloud computing. The significant pros in using IDS virtualization is the segregation of a monitored environment that gives an extra security layer that stops the threats with user information access or for disabling the system protection. An examination has been shown of existing research to understand the future perspective to conduct better research.

6 REFERENCES


