



## A Survey on Cloud Based Intrusion Detection System

P. Praveen Kumar<sup>1</sup>, K. Bhaskar Naik<sup>2</sup>

Department of Computer Science

Sree Vidyanikethan Engineering College, Tirupati, INDIA.

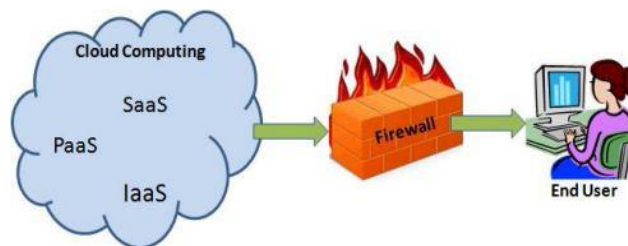
**Abstract:** Cloud Computing is becoming popular day by day as many enterprise applications and data are moving into cloud based platforms. Because of the distributed nature, cloud computing environments are aim for intruders looking for possible vulnerabilities to exploit. However, with the increasing use of cloud computing, security issues are came out on a growing scale. It is needful to solve these security issues to contribute to the wider applications of cloud computing. Security is an important issue in cloud computing environment. Therefore, some Intrusion Detection Systems (IDSs) needed in Cloud computing system for protecting each virtual machine against intruders. There is a trade-off between the system performance and security levels of Intrusion Detection Systems. If the IDS provide stronger security services using more rules or patterns, then it needs much more computational resources in directly proportion to the strength of security. Another difficulty in Cloud Computing is that, it is not easy to analyze extensive amount of logs by system administrators. The main objective of the paper is to propose a model that makes Cloud Computing System to achieve both effectiveness of using the system resources and capability of the security service.

**Keywords:** Intrusions, cloud security, vulnerabilities, anomaly detection, IDS.

### I. Introduction

In these times cloud computing is developing rapidly and is an innovative computing method that carry out convenient, on-desired, network access to a configurable computing resources (e.g. servers, storage, applications, etc) 'as a service' through the Internet for satisfying computing demand of clients. As shown in below Fig. 1, it carries out services in variety forms: Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as Service (IaaS).

**Figure 1 General architecture of Cloud computing.**



Enabling security in a distributed system environment requires more than user verification with passwords and confidentiality in information transmission. The Cloud Computing Intrusion Detection System combines behavior and knowledge analysis to find intrusions. Because of their distributed environment nature, cloud computing environments are easy aim for intruders searching for possible vulnerabilities to exploit. As Cloud services and applications are delivered over the Internet; privacy and security of Cloud resources and services are the major concerns. According to the International Data Corporation (IDC) survey, security is the major challenge of Cloud computing environment [2]. Cloud suffers from conventional attacks such as Distributed Denial of Service (DDoS), IP spoofing, DNS poisoning, Address Resolution Protocol (ARP) spoofing, Routing Information Protocol (RIP) attack, port scanning, man-in-the-middle attack, Insider attack, Denial of Service (DoS) etc. These attacks affect the availability, confidentiality and integrity of Cloud resources and services. To address such attacks, Cloud providers uses the firewall, as shown in Fig. 1. Firewall is acts as the first line of defense and it protects the front access points of system. The major drawback of firewall is it can sniffs the packets only at the network boundaries, insider attacks cannot be detected by it. some DoS or DDoS attacks are too difficult to detect using conventional firewall. So, use of only conventional firewall to block all the intrusions is not an effective solution. Another solution is to combine network intrusion detection system (NIDS) in Cloud computing.

There are two types of methods used in NIDS:

- 1) One is signature based detection method that can find known attacks efficiently and

2) Another is anomaly detection that finds whether a given behavior is exploiting or not.

## II. Attacks In Cloud Computing

Cloud intrusions classification is given as follows:

### A. Unauthorized Access:

It is may possible by obtaining the user's password through guessing, stealing, cracking, or the careless influence by the user himself. There may be another possibility of attacking the authentication service and it may result in attack trails left at the service side.

### B. Misuse:

This may be a influence of an unauthorized access by a legitimate user. The misuse of cloud resources are depends on the pre-defined policies or rules or patterns.

### C. Cloud Attack:

Attacks performed with the help of tools that aims at vulnerabilities existing in cloud services, protocols and applications. Attacks may be appear in the form of denial-of-service (DOS) attacks and worms.

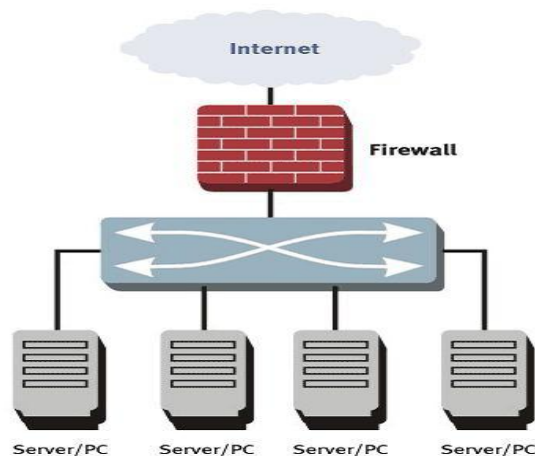
### D. Data Security:

Cloud data is stored in different locations, in several parts of the Earth. Data security is most difficult to get protection.

## III. Firewalls: Traditional Approach For Intrusions

Firewall is acts as the first line of defense. Firewalls [9] are used to allow or deny protocols, ports or IP addresses. It turns away incoming packets according to predefined policies or rules.

**Figure 2 Basic Firewall Installation.**



In Table 1, we presented different firewalls used in network for security purpose.

**Table I Various firewalls used in network**

| Firewall Type                      | Summary                           |
|------------------------------------|-----------------------------------|
| Static packet filtering Firewall   | Inspecting header information     |
| Stateful packet filtering firewall | Used in client-server environment |
| Stateful inspection firewalls      | Used for apps like FTP            |
| Proxy Firewalls                    | Analyze Protocol Syntax           |

#### IV. Dealing With Intruders

Intruders may be external or insiders. External intruders are hackers or crackers and internal intruders are most common and dangerous.

Security policies should state what steps will be taken to handle intrusion activities,

##### A. *Prevent and ignore:*

It is the simplest way to handling intrusions. Prevent the intruder and address the vulnerable activity and don't take any further action.

##### B. *Prevent and investigate:*

Prevent/block the intruder and report the vulnerability, Collect evidence and try to determine intruder's identity and finally investigate about possibility of attack.

##### C. *Honey pot (bait the intruder):*

Allow the attacker to access a part of your network. Try to catch the intruder while he explores it. This is a potentially dangerous approach attackers may become interested in your site.

#### V. Types of Intrusion Detection System

Based on the audit information used by each IDS, the IDSs may be classified into Host-based IDSs, Distributed IDSs and Network-based IDSs.

##### A. *Host-based IDSs:*

Host- based Intrusion Detection System Uses OS auditing and monitoring/analysis mechanisms to find malware. It can execute full static and dynamic analysis of a program and monitor shell commands and system calls executed by user applications and system programs. It has the most comprehensive program info for detection, thus accurate. There are few Problems against the HIDS, it is user dependent: install/update IDS on all user machines. If attacker takes over machine, can modify audit logs. It is Possible Only local view of the attack.

##### B. *Distributed IDSs:*

It gathers audit data from multiple hosts and possibly the network that connects the hosts and detects attacks involving multiple hosts.

##### C. *Network-Based IDSs:*

Use network traffic as the audit data source, cause to the burden on the hosts that usually provide normal computing services. It detects attacks from network. At the early stage of the worm only limited worm samples. It inspecting the network traffic by watching for violations of protocols and unusual connection patterns and look into the packet payload for malicious code. It may be easily defeated by encryption, but can be make less severe with encryption only at the gateway/proxy.

##### D. *Host-based vs. Network-based IDS:*

IDS systems are classified by their intended locations. A network-based IDS monitors all traffic on a network segment, it can detect intrusions that cross a specific network segment, administrators sometimes place one inside and one outside of a firewall and it will not see traffic that passes between LAN computers.

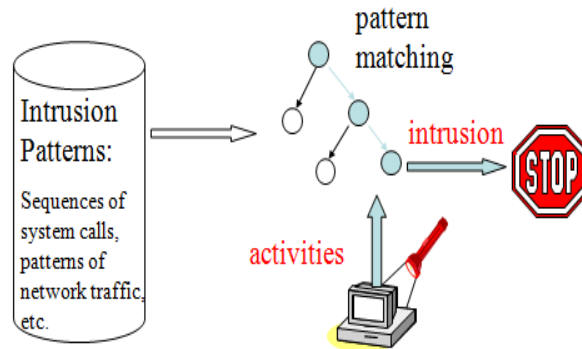
Host-based IDS examines all traffic and activity for a particular machine. It can examine system log files as well as inbound and outbound packets and each system requires its own IDS. Best choice is to use both network-based and host-based IDS in an organization.

#### VI. Intrusion Detection Techniques:

Misuse detection technique identifies the intrusions most accurately. But here the rules are pre-defined, based on known attacks intrusions are being detected. The major limitation is it cannot detect new attacks.

##### 1. *Misuse Detection Systems (MDSs):*

The concept behind the MDSs is that there are ways to represent attacks in the form of a pattern or a signature so that even variations of the same attack can be detected. They can detect many or all known attack rules, but they are of little use for unknown attack methods. Misuse detection systems try to recognize known "bad" behavior as shown in figure 3.

**Figure 3 Misuse detection Technique.**

Example: if (traffic contains “x90+de[^\r\n]{30}”) then “attack detected”

#### A. Expert systems:

These are modeled in such a way as to separate the rule matching phase from the action phase. The expert system misused detection component encodes known scenarios and attack patterns.

#### B. Key Stroke Monitoring:

This is a very simple technique that monitors keystrokes for attack patterns. Features of shells in which user definable aliases are present defeat the technique unless alias expansion and semantic analysis of commands is taken up. Operating systems do not offer much support for keystroke capturing, so the keystroke monitor should have a hook that analyses keystrokes before sending them to their intended receiver. An improvement would be to monitor system calls by application programs as well.

#### C. Pattern Matching:

This model encodes known intrusion signatures as patterns that are then matched against the audit data. The implementation makes transitions on certain events called labels, and Boolean variables called guards can be placed at each transition.

### 2. Anomaly Detection:

Based on the normal behavior of a subject, sometime assume the training audit data does not include intrusion data. Any action that significantly deviates from the normal behavior is considered intrusion. Based on audit data collected over a period of normal operation, when a noise (intrusion) data in the training data, it will make a miss-classification. Relatively high false positive rates and anomalies can just be new normal activities.

In table 2, we mentioned major IDS techniques and its advantages and limitations.

**Table 2. Various IDS Techniques**

| IDS techniques            | Advantages                                | limitations                |
|---------------------------|-------------------------------------------|----------------------------|
| Signature based detection | Identifies intrusions by pattern Matching | Cannot detect new attacks. |
| Anomaly detection         | Identifies known attacks.                 | High false alarms rate.    |

## VII. Conclusion

This survey talks about several intrusions which can violate integrity, confidentiality and availability of Cloud services. One of the existing solution is firewall may not be enough to solve Cloud security issues. The paper stressed the usage of alternative options to unite intrusion detection techniques into Cloud. Recent research findings uniting IDS specifically in Cloud have been discussed and their merits and limitations have been highlighted. This paper finally identified many security challenges and issues that need to be solved by the cloud research community.

## References

- [1] P. Mell, T. Grance, The nist definition of cloud computing (draft), NIST, [http://csrc.nist.gov/publications/drafts/800-145/Draft-SP-800-145\\_cloud-definition.pdf](http://csrc.nist.gov/publications/drafts/800-145/Draft-SP-800-145_cloud-definition.pdf) (2011).
- [2] Google apps, Website, <http://www.google.com/apps/business> (2011).
- [3] Google app engine, Website, <http://code.google.com/appengine/> (2011).
- [4] Azure services platform, Website, <http://www.microsoft.com/azure> (2011).
- [5] Amazon web services, Website, <http://aws.amazon.com> (2011).
- [6] Eucalyptus, Website, <http://eucalyptus.cs.ucsb.edu/> (2011).
- [7] Y. Chen, R. Sion, On securing untrusted clouds with cryptography, In WPES '10, 2010, pp. 109–114.
- [8] S. Beg, U. Naru1, M. Ashraf, S. Mohsin, Feasibility of Intrusion Detection System with High Performance Computing: A Survey, International Journal for Advances in Computer Science.
- [9] Firewall, Telecom-Network Tech, <http://teleconetwork.blogspot.com/> (2011).
- [10] Firewall, Telecom-Network Tech, <http://teleconetwork.blogspot.com/> (2011).
- [11] Denial-of-service attack, Website, [http://en.wikipedia.org/wiki/Denial-of-service\\_attack](http://en.wikipedia.org/wiki/Denial-of-service_attack) (2011).
- [12] T. Dutkevych, A. Piskozub, N. Tymoshyk, Real-Time Intrusion Prevention and Anomaly Analyze System for Corporate Networks, 4th IEEE Workshop on Intelligent Data Acquisition and Advanced Computing Systems:Technology and Applications, 2007. IDAACS 2007, 2007, pp. 599- 602.