IOSR Journal of Computer Science (IOSR-JCE)
e-ISSN: 2278-0661, p-ISSN: 2278-8727
PP 33-39
www.iosrjournals.org

Comparative Study and Analysis of Ids Implementation In Cloud Computing Environment

Swapnil Shinde[1], Ashwini Bangar[2], Manali Tawde[3]
[1]*Lecturer, Dept. Information Technology, RAIT, Nerul*
[2,3]*Dept. Information Technology, RAIT, Nerul*

ABSTRACT :*Intrusions have been a major problem in terms of computing resources such as grid computing, ubiquitous computing ,cloud computing, distributed computing and so on. Intrusions are hard to detect but there has been a lot of work done on detecting and removing the intrusions .The focus of intrusion detection should be mainly on detecting the intrusions at the system resources and at the network level for a predefined network. This paper mainly focuses on cloud computing a method which is infrastructure less and provides free system resources to the users. As clouds are distributed in nature , it becomes an easy target for the intruders to exploit the vulnerabilities of the network. The solution proposed for years is the use of intrusion detection system at various levels depending on the applications for which the detection is to be provided. The paper covers the study of intrusion detection system implemented in cloud environment for dealing with various security issues related to cloud. The various parameters considered for comparison are detection technique, types of attacks addressed, advantages, disadvantages and performance.*

KEYWORDS: *CIDSS, Cloud Computing, Flow matrix, IDS, KF Sensor, Log management.*

I. INTRODUCTION

Cloud computing is a paradigm evolved from many traditional computing models which provides organizations with much sophisticated services and related functions and aspects without heavy investment and with much lower Total Cost of Ownership(TCO)[3]. The various models include Private , Public , Community and Hybrid Cloud[1][2]. Each model has security issues that has to be dealt with by applying some or the other techniques. Some of the security issues related to cloud are Authentication and Identity management , Access control and accounting, Trust Management and Policy Integration, Secure service management, Privacy and data protection, Organizational and security management[10]. All these security issues can be addressed by implementing well proven technique called Intrusion Detection System (IDS).

1.1. IDS can be broadly classified into three main types:

a. Network Intrusion Detection System (NIDS)
b. Host-based Intrusion Detection System (HIDS)
c. Stack-based Intrusion Detection System (SIDS)

a. Network Intrusion Detection System (NIDS)

NID[6]S is a detection system that monitors the network traffic and packets over the network to determine the intrusions.

b. Host-based Intrusion Detection System (HIDS)

Host based IDS[6] are installed on local host machines making them more reliable and versatile. They generate timely reports of intrusion and update the clients with a central pattern file.

c. Stack-based Intrusion Detection System (SIDS)

This is the newest IDS[11] technology that varies from host to host, so it’s an evolution of HIDS. Stack-Based IDS works integrating closely with the TCP/IP stack allowing packets to be monitored as they traverse their way up the OSI Layer and work in non-promiscuous mode.

1.2. Detection Techniques in IDS

a. Signature or Misuse Based detection

Signature based IDS[15] monitors’ traffic over the network and detects the malicious content based on patterns or signatures from the database. Pattern matching can be performed very quickly on modern system saving time.

b. Anomaly Based detection

Anomaly detection is based on the network behavior used widely to detect unknown attacks. The engine works on the rules defined for protocols at each layer and detects the intrusions for different types of networks. Defining of rules is the only problem [15].

c. Specification Based detection

The system defines a set of constraints that describe the correct operation of a program or protocol. Then, it monitors the execution of the program with respect to the defined constraints. The constraints depend on the area where intrusion detection is to be performed.

1.3. IDS Architectures

There are many different types of architecture design that are used to design an IDS, the four main architectures that are followed on the network are.

a. Standalone IDS

In this type, the IDS run on separate machine and they are independent of other machines. There is no co-operation, no data exchange between two nodes .

b. Hierarchical IDS

This is an extended form of distributed and collaborative IDS, where it follows a multilayered architecture. This architecture proposes use of multilayered infrastructure for designing where the network is divided into clusters.

c. Distributed and Collaborative IDS

The distributed and collaborative architecture is one in which every node in the ad hoc network must participate in intrusion detection and response by having an IDS agent running on them [15].

II. RELATED IDS ARCHITECTURES IN CLOUD

Cloud computing is a platform for the users to access various system resources and services; here security becomes a major concern. Some of the security issues are discussed above and IDS is one of the solutions suggested. The review of this paper is based on the architectures of IDS which includes multi-level, hybrid, distributed etc.

2.1. Layered-Integrated IDS

The job of cloud intrusion detection system is to analyze the data present at the nodes, networks and verify whether it is a possible intrusion or not. This intrusion detection is carried either with the help of available signature patterns or they are anomalies. The major concerns associated with cloud computing are, first the cost required to fix the security problems, second difficulty faced by the system to analyze huge logs and finally desirable resource distribution to the customers on demand. However, the current IDS model fails to provide protection against wide range of intrusions that may appear in the system. Let us now understand the proposed solution to help us get rid of the issues discussed above.

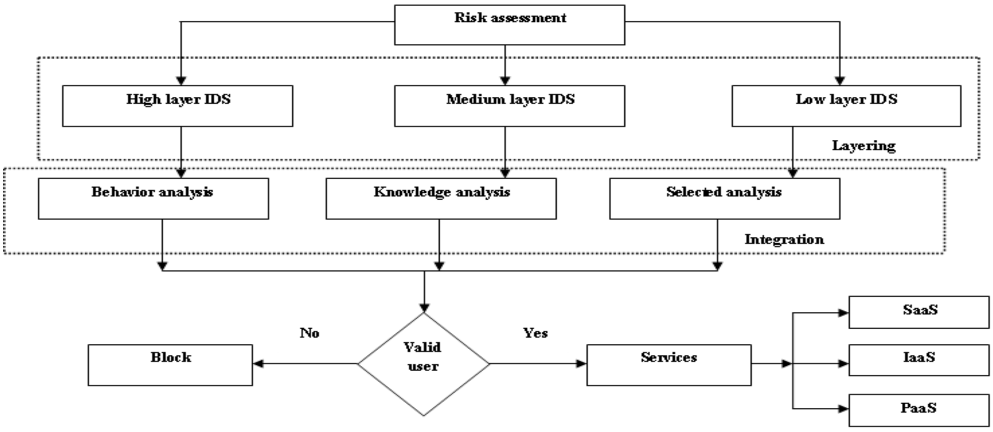


Figure 1.Proposed Layered Integrated Model

The layered-integrated model, as the name suggests is the combination of two IDS techniques namely integrated IDS and Layered IDS[5]; hence this model incorporates the working mechanism of both these techniques. This model was mainly proposed to solve two major concerns related to cloud computing, that are log management and high performance intrusion detection. The incoming data is first analyzed by risk assessment. After data is analyzed it becomes easy to distribute the data in different layers corresponding to their anomaly levels provided through risk assessment. This distribution is done within security core which implements feed forward artificial neural network which is capable of quick information processing, has self learning capabilities, and can tolerate small behavior deviations. [4]. Corresponding to their segregation the data is then passed to integrated model which implements one of the three analysis which can be behavior ,knowledge or selected patterns. Once the user along with its data gets authenticated he is provided with requested services.

2.2. Internet IDS in Cloud

Amirreza Zarrabi et al[6] proposed a Cloud Intrusion Detection System Service (CIDSS) to overcome and secure the cloud user from cyber attacks. The architecture consists of mainly three components: Intrusion Detection Service Agent, Cloud Computer Service Component (CCSC), and Intrusion Detection Service Component (IDSC) as shown in Fig 2. Intrusion Detection Service Agentmainly consists of a single purpose equipment known as Agent, may be hardware or software, situated inside the user network for collecting the important data. CIDSS[6] could protect a segment of the network or the whole network depending on the location of the agent. Depending upon the rule-sets and network traffic, agents can be grouped for better efficiency and protection.

Cloud Computer Service Component (CCSC) collects the messages from the agent, format it on the basis of grouping constraints defined and pass it on to IDSC. Passing the messages is the most critical and important task, so there must be a secure connection between CCSC[6] and the agent such that the system behavior is not violated by external intrusion. Intrusion Detection Service Component (IDSC) component mainly focuses on intrusion detection. It itself consists of four sub components playing a major role. Collector reads all the information received by CCSC, sort them according to the interest and pass on to the analysis engine. Analysis Engine consists of sophisticated decision and pattern matching algorithm. Event Publisher is a standard form of making reports which gives a unified view of results provided by the analysis engine as it can be an independent process implemented using any IDS, e.g. Snort. Intrusion Detection Message Exchange Format (IDMEF)[6] can be used as the standard format for giving alerts. IDS Controller is responsible for remote configuration and control of all agent groups. It has access to IDSC configuration for fine tuning its operation based on user demands.

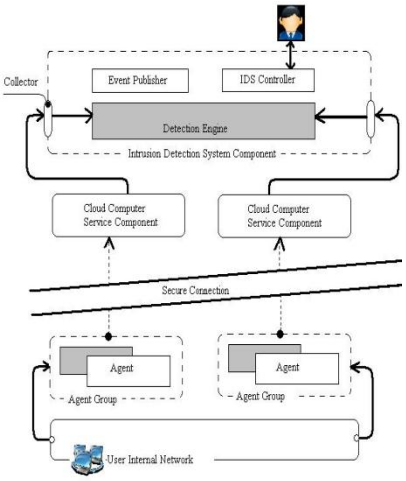


Figure 2. Internet Based Cloud IDS

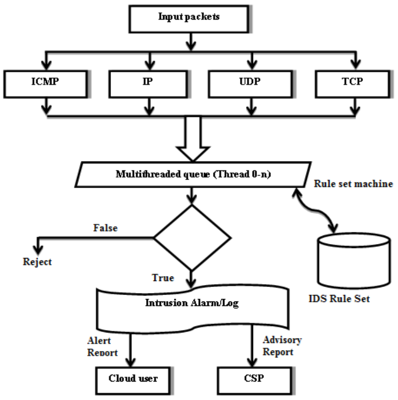


Figure 3. Flowchart for Proposed Model

2.3. Distributed IDS

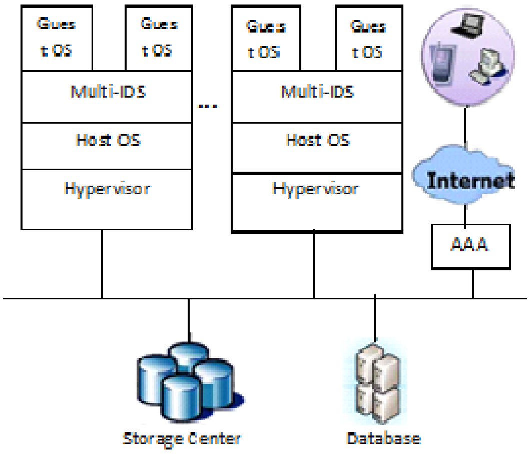
In Cloud computing, massive amount of data is generated due to high network access rate, therefore IDS must be robust against noise data & false positives. Cloud infrastructure has enormous network traffic the traditional IDSs are not efficient enough to handle such a large data flow. Most known IDSs are single threaded and due to rich data flow, there is a need of multi-threaded IDS in Cloud computing environment, hence the distributed IDS[9] was proposed by Irfan Gul and M. Hussain also called as multi-threaded IDS[9] shown in Fig 3. Distributed IDS is an efficient and effective Cloud IDS which uses multi-threading technique for monitoring the network traffic and the malicious packets. The system then sends intrusion alarms to a third party monitoring service, which can provide instant reporting to cloud user organization management system with an advisory report for cloud service provider.

Distributed IDS is based on three modules: Capture and queuing module receives the data packets. The captured data packets are then sent to shared queue for analysis. Analysis and process module receives the data packets from the shared queue and analyzes them against predefined rule set. With the help of an efficient matching and analysis technique the process module detects the bad packets and then the alerts are generated. Reporting module reads the alerts and produces the alert reports for the cloud user and an advisory report for the cloud service provider.

2.4. Multi-Level IDS in Cloud

Reducing the number of resources required for IDS implementation is main concern so a new system based on multilevel concept is proposed by M.Kuzhalisai et al.[7] which deals with effective use of system of resources. The proposed system binds user in different security groups based on degree of anomaly called anomaly level. Refer Fig 4.

It consists of AAA module which is responsible for authentication, authorization and accounting. When user tries to access the cloud the AAA checks the authentication of the user and based on it, it gets the recently updated anomaly level. Security is divided into three levels viz. high, medium and low. High Level applies patterns of all known attacks and a portion of anomaly detection when it needs for providing strong security service. Medium Level applies patterns of known attacks to rules providing strong security service. Low Level has flexible resource management and applies patterns of chosen malicious attacks that can occur at high frequency which affect more fatally.



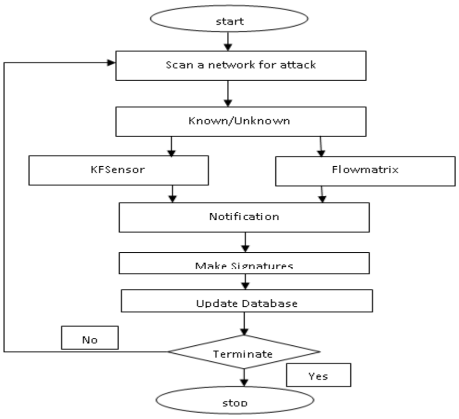


Figure 4. Multilevel Proposed Model

Figure 5. Flowchart for Hybrid IDS

2.5. Improved Hybrid IDS for Cloud

There are many IDS proposed based on signature detection and anomaly detection techniques. Signature based will detect only known patterns of signatures and other will go undetected, where as anomaly detects behavior based malicious activity that leads to high false positive alarms. Many Hybrid based systems are also proposed which are combination of signature and anomaly, network IDS and Anomaly detection and third proposed hybrid system based on biological immunology and mobile agent. Advancement in technology has lead to many new attacks which results in failure of hybrid IDS so Ajit Kumar Gautam et al.[8] proposed improved Hybrid IDS. The Improved hybrid IDS is combination of anomaly based detection and honey pot technology with KFSensor and Flowmatrix as shown in Fig 5.

Proposed system of Honey pot technology and Anomaly based IDS: Honey pot attracts more and more attackers, the detection obtained can be used to create new signatures and update the database. Finally anomaly can be used to detect unknown attack in the whole network. KF Sensor is a host based IDS which works on the honey pot based technology, it adds the definitions of that attacker to the database for the next time and restrict the entry of that attacker or intruder to the main network of the organization. Flow Matrix is based on Anomaly based detection methodology. It compares the samples from the normal traffic with the regular samples obtained from the network and the moment it finds the difference between the normal and the regular sample it gives an alert.

1. Comparison Table

Proposed Models Parameters	Layered-Integrated IDS	Internet IDS	Distributed IDS	Multi-level IDS	Hybrid IDS
Architecture	Layered, Integrated	Internet Based	Distributed	Multi-level	Hybrid
Detection Technique	Anomaly, Signature	Signature, Anomaly	Signature	Anomaly, Signature	Anomaly, Honey pot
Attacks Addressed	Log Management,	Cyber Attacks	Distributed Denial of	Log Management,	False Alarms

	Resource Utilization		Service (DDOS)	Resource Utilization	
Type of IDS used	Host	Network	Host, Network	Host	Network
Advantage	Scalable, Compatible, Efficient	Securing from Cyber Attacks	Improved Performance, Reduced Packet Loss	Increased Resource Availability, Increase in Attack Detection	Reduction in False Alarms, Improved Detection
Disadvantage	High Resource Utilization	Collision, Speed	Time consuming	Security Compromised	-
Application	IBM Open cloud architecture, Oracle SOA suite	Detection of cyber attacks like spoofing, sniffing.	MANET(Mobile Adhoc Netwrk Environtment)	Detection of Syn and DOS attacks	Used in Large and complex networks
Solutions	Improve efficiency of detection	adding a hub inline, network TAP, a SPAN	Utilize resources properly	Use of security features in cloud	Addition of Signature based detection

2. Analysis

The techniques discussed above are based on IDS architecture which has their own pros and cons. The layered-integrated IDS deals with the problem of efficient log management and optimum system resource utilization. Internet IDS has different components namely agent component, cloud computer service component and intrusion detection component among which agent plays a vital role. Multilevel IDS assigns different anomaly levels depending on the level of security assigned to the users. Hybrid IDS is combination of honey pot technology and anomaly detection where the problem of false alarm is completely removed by using honey pot concept. Distributed IDS is a multithreaded IDS which deals with the problem of handling both the network traffic as well as the transfer of data packets resulting in reduced loss of data packets.

III. CONCLUSION

The study of various IDS architectures explained in this paper, leads to a conclusion that hybrid and distributed IDS are the best solutions for cloud environment. In this paper, we have studied a multi-threaded cloud IDS which can be administered by a third party monitoring service which provides a advisory report to the cloud service provider and an alert report to the cloud user for a better optimized efficiency and transparency for the cloud user. Hybrid IDS combines anomaly detection and honey pot to reduce false alarms and improve performance.

References

Introduction to Cloud Computing white paper Dialogic , 2010

Sanjay Ram M , Velmurugan N and Thirukumaran S, "Effective Analysis of Cloud Based Intrusion Detection System" , IJCAIT, Vol 1-issue 2, September 2012.

Thoran Rodrigues, "Cloud Security: Technology, Processes, Responsibility", The Enterprise Cloud, May 29,2012.

M. Sudha and M. Monica, "Investigation on Efficient Management of Workflows in Cloud Computing Environment", IJCSE, Vol. 2, No. 05, 2010.

Soumya Mathew and Ann Preetha Jose, "Securing Cloud from Attacks based on Intrusion Detection System", IJARCCE, Vol. 1, Issue 10, December 2012.

Amirreza Zarrabi and Alireza Zarrabi, "Internet Intrusion Detection System Service in Cloud", IJCSI, Vol. 9, Issue 5, No. 2, September 2012.

M. Kuzhalisai and G. Gayathri, "Enhanced Security in Cloud with Multi-Level Intrusion Detection System", IJCCT, Vol. 3, Issue 3, 2012.

Ajeet Kumar Gautam, Dr. Vidushi Sharma, Shiv Prakash and Manak Gupta, "Improved Hybrid Intrusion Detection System (HIDS): Mitigating False Alarm in Cloud Computing", JCT, 2012.

Irfan Gul and M. Hussain, "Distributed Cloud Intrusion Detection Model", IJAST, Vol. 34, September, 2011.

Hassan Takabi, James B. D. Joshi and Gail-Joon Ahn, "Security and Privacy Challenges in Cloud Computing Environments", IEEE, November/December 2010.

Pradeep Kumar Tiwari and Dr. Bharat Mishra ," Cloud Computing Security Issues, Challenges and Solution " ,IJETAE, Volume 2, Issue 8, August 2012.

Chirag Modi, DhirenPatel, BhaveshBorisaniya, HirenPatel , Avi Patel , MuttukrishnanRajarajan, "A survey of intrusion detection techniques in Cloud ", JNCA, 2013.

Krunal Patel, "Security Survey For Cloud Computing: Threats &Existing IDS/IPS Techniques", International Conference on Control, Communication and Computer Technology, 24th, March 2013.

Áine MacDermott, Qi Shi, Madjid Merabti, and Kashif Kifayat, "Detecting Intrusions in the Cloud Environment", RCCICTP, 2008.

Swapnil Shinde and Vanita Mane , "Study of Distributed Intrusion Detection System in Adhoc Networks" , ICCSIT,2012.