International Journal of Research
IJR
International Journal of Research
Available at
https://edupediapublications.org/journals
p-ISSN: 2348-6848
e-ISSN: 2348-795X
Volume 04 Issue 06
May 2017

An Improved Automated Multi Level Intrusion Detection and Log Management System In Cloud Computing.

ALABI O. A[1]
DEPARTMENT OF COMPUTER SCIENCE
UNIVERSITY OF PORT HARCOURT, NIGERIA
UWALAKA C. S[2]
DEPARTMENT OF ENGINEERING
NIGERIAN NAVAL ENGINEERING COLLEGE, SAPELE

ABSTRACT

Information and Communications Technology (ICT)] has come to stay. As a result, most of our institutions have decided to move their important files to the cloud and do online transactions – allocation of resources to reviewer, proper storage of the big data from hackers. Cloud also involves multi-mesh distributed and service oriented paradigms, multi-tenancies, multi-domains, and multi-user autonomous administrative infrastructures which are more vulnerable and prone to security risks. Cloud computing service architecture combines three layers of inter-dependent infrastructure, platform and application; each layer may suffer from certain vulnerabilities which are introduced by different programming or configuration errors of the user or the service provider. A cloud computing system can be exposed to several threats including threats to the integrity, confidentiality and availability of its resources, data and the virtualized infrastructure which can be used as a launching pad for new attacks. The problem becomes even more critical when a cloud with massive computing power and storage capacity is abused by an insider intruder as an ill-intention party which makes cloud computing a threat against itself.

INTRODUCTION

It is efficient and cost economical for consumers to use computing resources as much as they need or use services they want from Cloud Computing provider. Especially, Cloud Computing has been recently more spotlighted than other computing services because of its capacity of providing unlimited amount of resources. Moreover, consumers can use the services wherever Internet access is possible, so Cloud Computing is excellent in the aspect of accessibility. Cloud Computing systems have a lot of resources and private information, therefore they are easily threatened by attackers (Enisa, 2009). Especially, System administrators potentially can become attackers. Therefore, Cloud Computing providers must protect the systems safely against both insiders and outsiders.

Intrusion Detection Systems (IDSs) are one of the most popular devices for protecting Cloud Computing systems from various types of attack. Because an IDS observes the traffic from each VM and generates alert logs, it can manage Cloud Computing globally (Roberto et al, 2008). Another important problem is log management. Cloud Computing systems are used by many people, therefore, they generate huge amount of logs. So, system administrators should decide to which log should be analyzed first.

Cloud Computing is a service that assigns virtualized resources picked from a large-scale resource pool, which consists of distributed computing resources in a Cloud Computing infra, to each consumer. Cloud Computing is a fused-type computing paradigm which includes Virtualization, Grid Computing, Utility Computing, Server

Based Computing(SBC), and Network Computing, rather than a entirely new type of computing technique [JaeHyuk, 2010].

An Intrusion Detection System (Commonly referred to IDS) is a system that replaces the typical task of system administrators of constantly reviewing the log files in attempt to spot any abnormal records. And by abnormal we mean any records that indicate a malicious activity by the user. These malicious activities include a wide variety of actions that usually tend to attack and/or damage the system being the target. This method was enough for monitoring the activities of small group of people within a private organization.

But with the expanded usage of computing system and by the development of complex interconnected networks, this is no longer an applicable method. Automated methods were needed to make the task faster and easier [Kemmerer and Vigna,(2002]. This was the first step towards the Generally, IDs can be defined as the tools, methods, and resources that help to identify, assess, and report unauthorized or unapproved network activities. The intrusion detection part of the name is a bit of a misnomer, as an IDS system doesn't actually detect intrusions. It rather detects activities in traffic that may or may not be an intrusion. Intrusion detection is usually part of an overall security architecture that is installed around a system or device [Foster et al, 2008)

Materials and methods

This project work is based on Multi-level intrusion detection and log management in cloud computing is an embracing topic in the determinant of how applications are developed and installed on a server, intrusion detection systems which acts as an antivirus is also installed to fight against cyber-attacks. For the purpose of this research work, the researcher shall be limited to developing an address book application (software) which will be installed on a server for us to be able to test the strength of multilevel intrusion and log management in cloud computing.

[Gruschka and Jensen, 2010]: work on cloud attack policy. The interface between a service instance and an user can be considered as a client-to-server interface, that is vulnerable to all types of attacks that are possible in common client-server architectures, including SQL injection, buffer overflow, privilege escalation, SSL certificate spoofing, phishing attacks, and flooding attacks.

[Thomas and Narayanaswamy, 2011]: work on intrusion detector system that detect attacks in the incoming traffic, the IDSs are typically parameterized by a threshold T. The IDS uses a theoretical basis for decidingg the thresholds for analysing the network traffic to detect intrusions. Changing this threshold allows the change in performance of the IDS. If the threshold is very low, then the IDS tends to be very aggressive in detecting the traffic for intrusions. However, there is a potentially greater chance for the detections to be irrelevant which result in a large number of false alarms. A large threshold on the other hand will have an opposite effect; being a bit conservative in detecting attacks. However, potential attacks may get overlooked by this method.

Yee et. al (2012): have proposed an intrusion detection system designed specifically to detect certain attacks against web services. The Web Service they proposed cannot be controlled by users and aims at protecting the web services themselves. Therefore, we can consider this as an intrusion detection system designed to protect the cloud itself which is usually the location where web services are hosted.

Bosin et. al. [2014]: have proposed a model for a new generation of intrusion detection systems. The new Web Service, which is designed for security managers, is mainly designed to enable the access to intrusion detection services whenever needed. The Web Service doesn't specify the intrusion detection service itself, but rather focuses on the composition of interoperable intrusion detection (ID) services and aims to promote the reuse of ID tools and systems already available at network nodes and/or supplied by different vendors. The model however assumes the existence of already configured intrusion detection services. It also doesn't allow the clients within the cloud of network to determine the protection requirements but rather use the ID service from one vendor and replaces it if it doesn't suit their demands.

Methods of achieving Goal

We proposed a Two protection level to solves the trends in intrusion detection system. The first is the Host-Based Protection (HIDS), and the second is the Network-Based Protection (NIDS).

Host-Based IDS

This is where the intrusion detection system is intended to protect a single host. This is usually achieved using a special software running on the host and utilize fire-wall like strategies to intercept traffic and analyze it to report any malicious traffic.

Network-Based IDS

This type of IDS is usually used to protect a complete network segment. In order for them to be able to do this task, they are typically placed on the network perimeter in a place that allows it to read all the exchanged traffic with the protected network segment

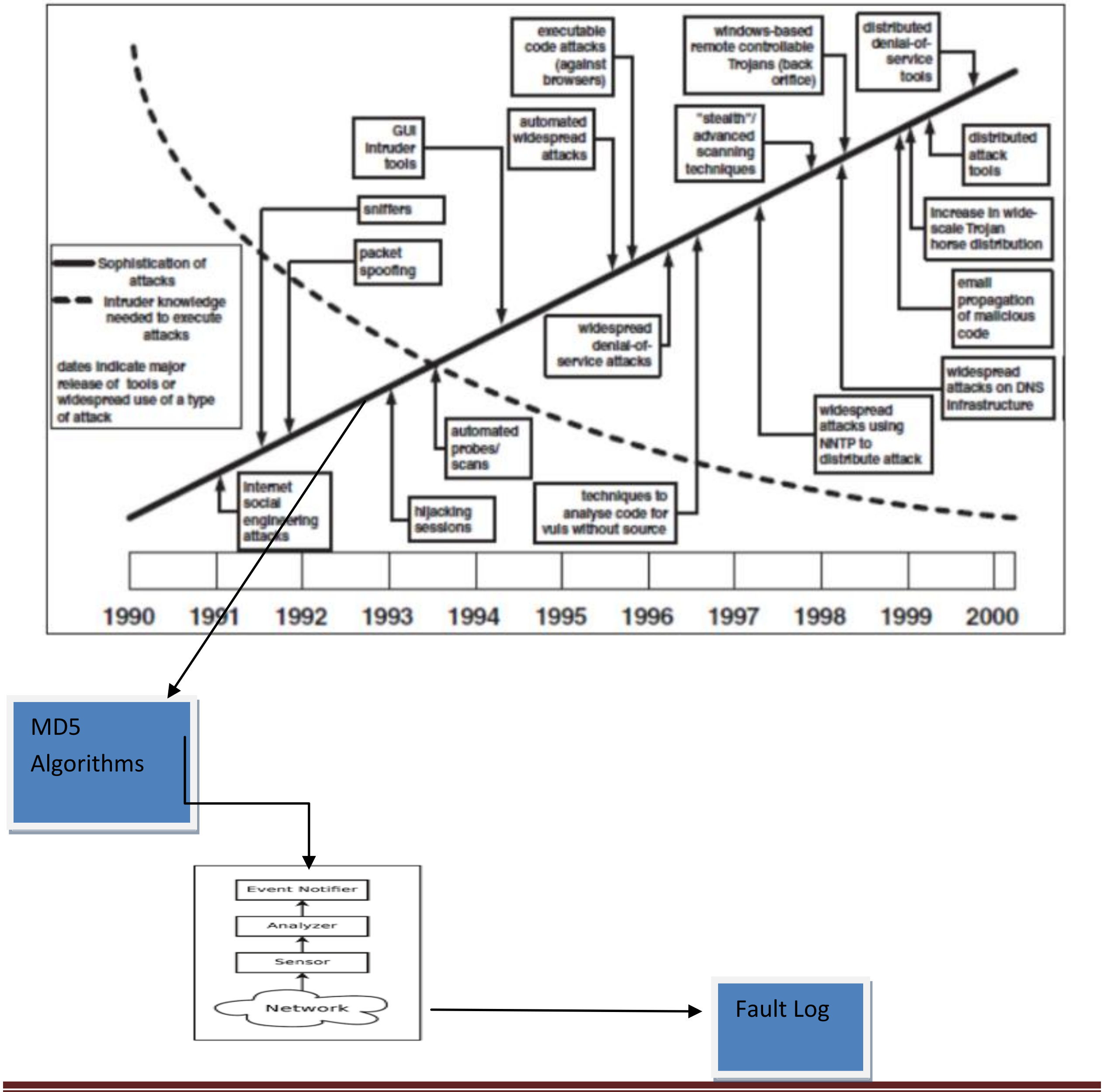
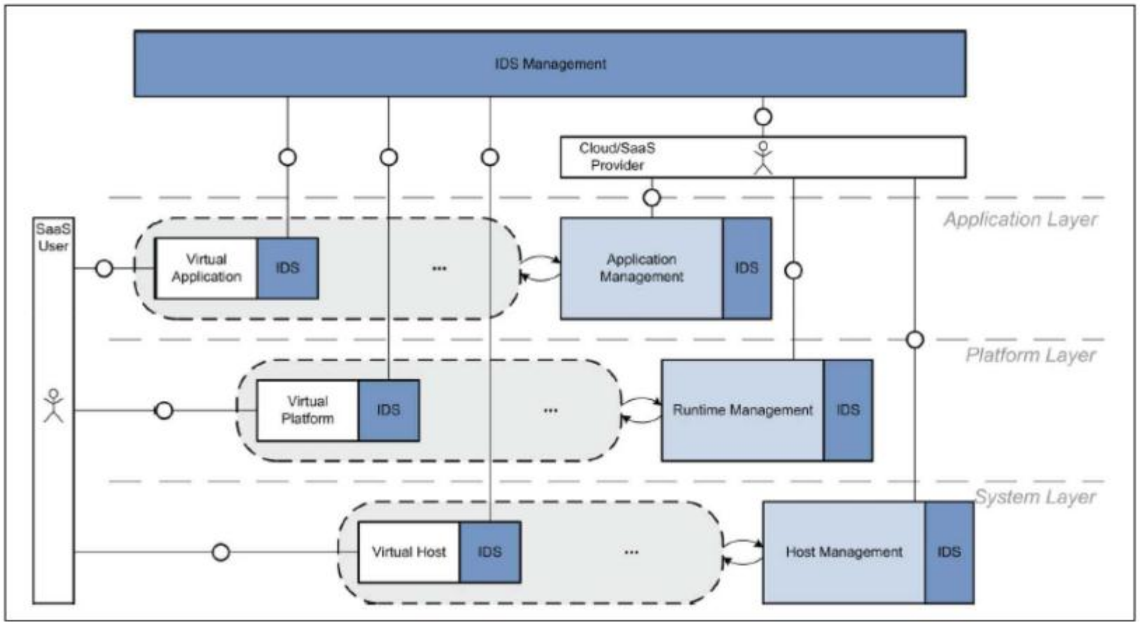

executable code attacks (against browsers)
windows-based remote controllable Trojans (back orifice)
distributed denial-of-service tools
GUI intruder tools
automated widespread attacks
"stealth"/ advanced scanning techniques
distributed attack tools
sniffers
Increase in wide-scale Trojan horse distribution
packet spoofing
Sophistication of attacks
Intruder knowledge needed to execute attacks
dates indicate major release of tools or widespread use of a type of attack
email propagation of malicious code
widespread denial-of-service attacks
widespread attacks on DNS infrastructure
automated probes/ scans
widespread attacks using NNTP to distribute attack
Internet social engineering attacks
hijacking sessions
techniques to analyse code for vuls without source
1990
1991
1992
1993
1994
1995
1996
1997
1998
1999
2000
MD5 Algorithms
Event Notifier
Analyzer
Sensor
Network
Fault Log

Fig. 1 The Architecture of the Proposed System

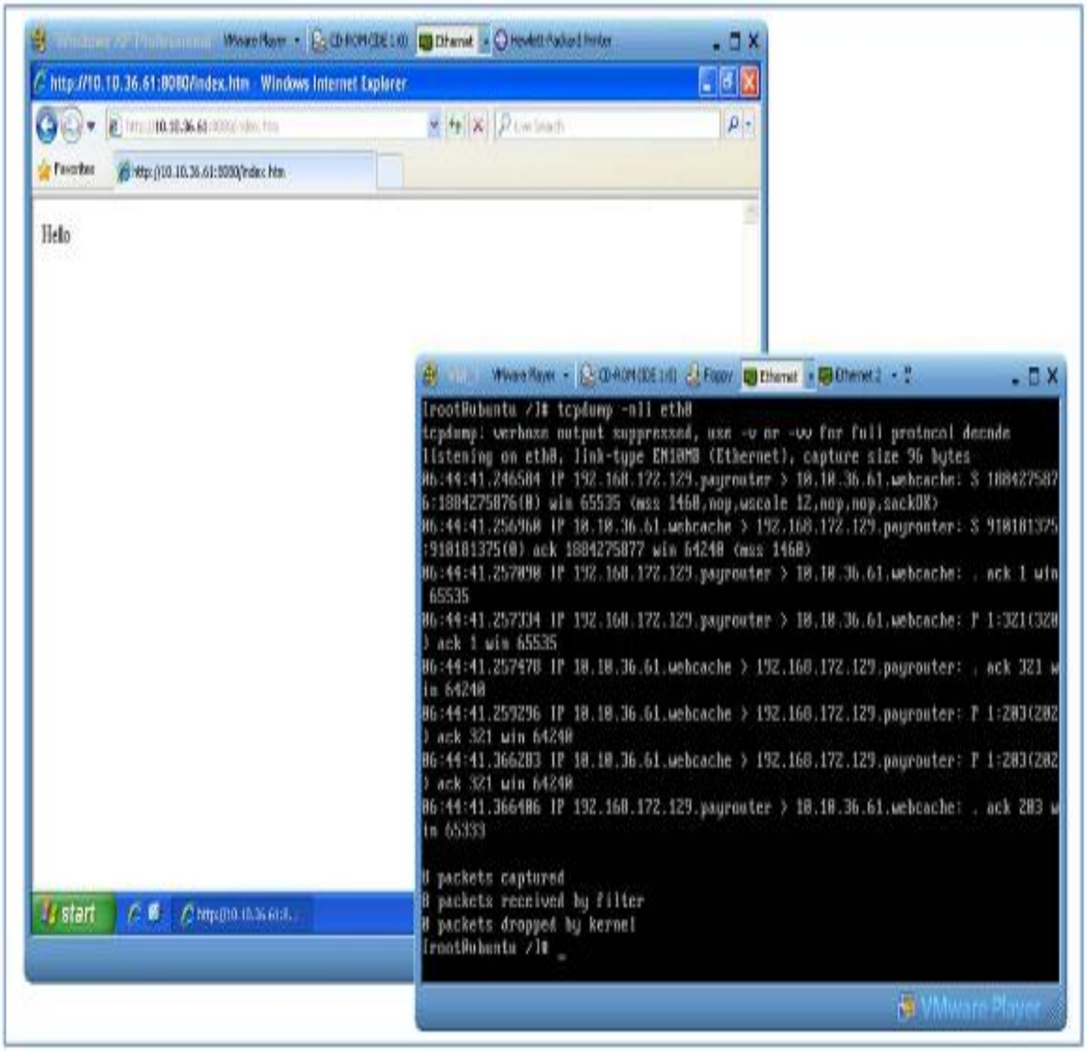
MD5 (Message Digest 5) Algorithms will be used to secure this line of internet because MD5 is a security algorithm that secure information from a sender to the Receiver . in this project work we will used Anomaly Detection (The main advantage of anomaly detection systems is that they can detect previously unknown attacks. By defining what's normal, they can identify any violations, whether it is part of the threat model or not. In actual systems however, the advantage of detecting unknown attacks is paid for in terms of high false-positive rates. Anomaly detection is also difficult to train in highly dynamic environments.) and Misused Detection (The misuse-based intrusion detection systems attempt to model the abnormal behavior, any occurrence of which clearly indicates system abuse. For example, an HTTP request referring to the cmd.exe file may indicate an attack.

The main disadvantage of misuse detection systems is that they can detect only known attack for which they have a predefined signature. These techniques require the modeling and development of new signatures for each newly discovered attack. These signatures must then be added to the published signature database



IDS in cloud (signatures to monitor the traffic originating from or destined to the other virtual machines).

This should not be allowed to happen since it violates a basic principal of information security, i.e. confidentiality.



```
[root@ubuntu /]# tcpdump -nll eth0
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 96 bytes
06:44:41.246504 IP 192.168.172.129.payrouter > 10.10.36.61.webcache: S 188427587
6:1884275876(0) win 65535 <mss 1460,nop,wscale 12,nop,nop,sackOK>
06:44:41.256960 IP 10.10.36.61.webcache > 192.168.172.129.payrouter: S 910181375
:910181375(0) ack 1884275877 win 64240 <mss 1460>
06:44:41.257090 IP 192.168.172.129.payrouter > 10.10.36.61.webcache: . ack 1 win
 65535
06:44:41.257334 IP 192.168.172.129.payrouter > 10.10.36.61.webcache: P 1:321(320
) ack 1 win 65535
06:44:41.257470 IP 10.10.36.61.webcache > 192.168.172.129.payrouter: . ack 321 w
in 64240
06:44:41.259296 IP 10.10.36.61.webcache > 192.168.172.129.payrouter: P 1:203(202
) ack 321 win 64240
06:44:41.366203 IP 10.10.36.61.webcache > 192.168.172.129.payrouter: P 1:203(202
) ack 321 win 64240
06:44:41.366406 IP 192.168.172.129.payrouter > 10.10.36.61.webcache: . ack 203 w
in 65333

8 packets captured
8 packets received by filter
0 packets dropped by kernel
[root@ubuntu /]# _
```

Figure 3- 2: network packets being read by one virtual machine

Figure 5-2 displays the results obtained when measuring the process size for each of the two cases. As clearly visible in the figure, the process size for using the CIDS to protect multiple networks is very similar to using “Snort” for protecting a single network. his behavior stays the same despite the number of subscribed signatures. The architecture of CIDS Web Service is expected to give such result since the only addition difference is length of the same number of signatures. The remaining process components are all the same. The process size overhead is very small compared to the original snort process size.

This overhead is negligible because we are comparing the case of protecting a single network and the case of protecting multiple networks

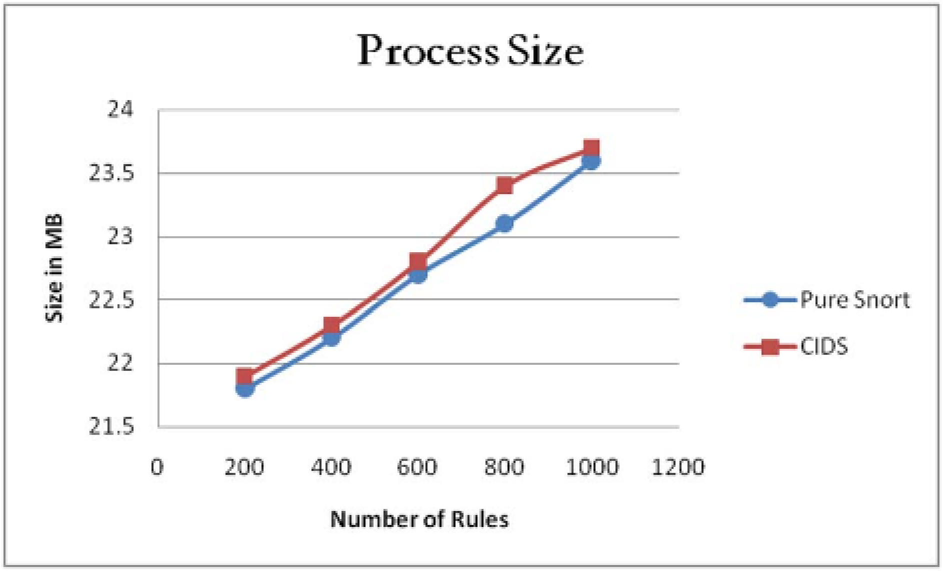


Figure 5- 2: Process size in (MB) for using CIDS and standard "Snort"

We now measure the detection rate of heavy and hostile traffic. Figure 5-3 shows the obtained results for the effective attack detection rate for the two cases mentioned earlier. As the figure illustrates, the average attack detection rate is very high for the two cases.

Despite the degradation in performance for the CIDS compared to the pure "Snort" implementation, the detection rate is still very high since we are dealing with CIDS protecting multiple networks. This result also proves that the CIDS is very effective when it comes to detecting attacks in real-time.

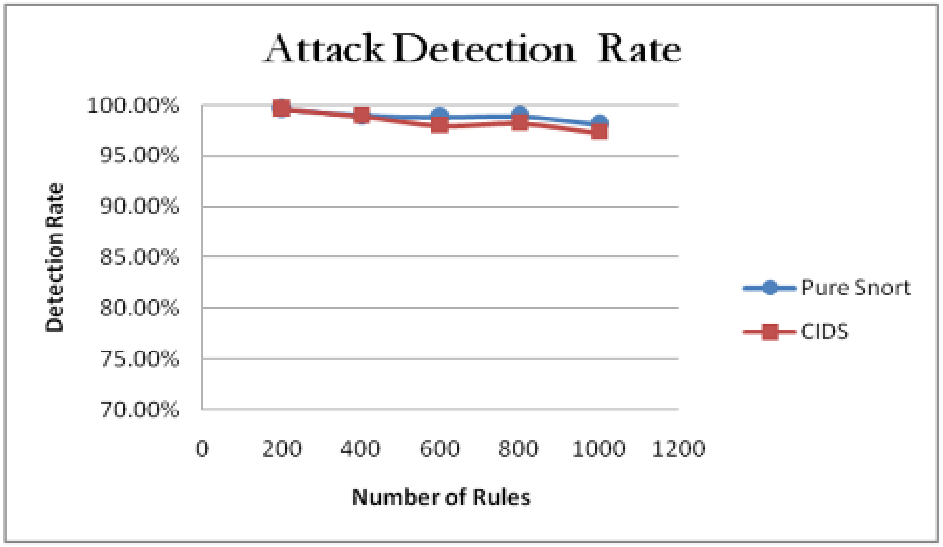


Figure 5- 3: Attack detection rate in (%)

Conclusion

As a final conclusion, the CIDS have been a successful Web Service for managing intrusion detection systems in cloud networks and provide it as a service to the cloud clients. The system component of the CIDS is very scalable and extremely effective in memory utilization, and supports large volumes of traffic

Reference

A. Bosin, N.Dessì, and B. Pes,(2012): "Service Based Approach toa New Generation of Intrusion Detection Systems "in Sixth European Conference on WebServices,Dublin,pp.215-224.

Enisa H.Y, 2009: Efficient Cloud Computing with Secure Data Storage using AES, International Journal of Advanced Research in Computer and Communication Engineering Vol. 4, Issue 6, 23-34

I. Foster, Y.Zhao, Raicu ,and S.Lu, (2008): "Cloud Computing and Grid Computing 360-Degree Compared, "in Grid Computing Environments Workshop, GCE.

JaeHyuk A.T, 2010: “Data Partitioning Technique to Improve Cloud Data Storage Security”, International Journal of Computer Science and Information Technologies, Vol. 5 (3) , 2014, 3347-3350

R.A. Kemmerer and G. Vigna,(2002) "Intrusion Detection: A Brief History and Overview, "IEEE Security and Privacy Magazine, vol.35, no.4, pp.27-30.

S.Roschke,F. Cheng, and Ch. Meinel,(2014): "Intrusion Detection in the Cloud," in Eighth IEEE International Conference on Dependable, Autonomic, And Secure Computing,pp.729-734