

Multi-Level Intrusion Detection System and Log Management in Cloud Computing

Ibebuogu C.C Ph.D

Department of Computer Science, Imo State University, Owerri
krischynwe@yahoo.com

Dr. Alphonsus Agbakwuru

Head, Department of Computer Science, Imo State University, Owerri
alphonsus1010@yahoo.com

Chinagorom Oluchi Maureen

Imo State University Owerri
chinagorom337@gmail.com

DOI: 10.56201/ijcsmt.v9.no2.2023.pg75.84

Abstract

The aim of this project is to design a cloud based intrusion detection system that will help detect cyber-attack. Cloud computing is increasingly being used by many organizations and individual users for their computing activities; hence the increased susceptibility to threats of the cloud provided services and resources, and poor log management system of the large number of cloud logs. Existing intrusion systems use more resources than necessary while preventing threats, hence having reduced resources left to allocate to users, also they use the same intrusion detection system for all level of services available on the cloud environment, lastly they provide platform for users to monitor their activity logs but with limited control over submission of suspected threats. A model for the system was designed with the use of diagram, sequence diagram, activity diagram and collaboration diagram. The database of the system was designed using MySQL database running on Apache Server in order to simulate a central database and have direct connection with a cloud environment. A cloud environment was simulated using a web environment to enable testing of the system locally on the computer during the implementation process, using html, and PHP for the backend code. A multi-level intrusion detection and log management system in the cloud-computing environment was designed and developed to ensure and achieve effectiveness and efficiency of using cloud resources without causing a trade-off between them, and enable users monitor their logs efficiently thereby black listing suspected threat IP address. The simulated system made use of an intrusion detection system that uses minimum resources to enable verified cloud users to use the resource on the cloud without fear of threats or intrusion, after passing the different security levels and blocks unauthorized users from the cloud environment.

Keywords Cloud computing: *the practice of using a network of remote servers hosted on the internet to store, manage, and process data, rather than a local server or personal computer*

Log: *this is the process of gaining access into an identifying data, as a username or password, into a database, mobile device or computer*

Log management (LM): *comprises an approach to dealing with large volumes of computer generated log messages (also known as audit records, audit trails, event-logs, etc.). Log Management generally covers: Log collection, Centralized log aggregation, Long-term log storage and retention.*

Intrusion Detection: *An intrusion detection system (IDS) is a device or software application that monitors a network or systems for malicious activity or policy violations.*

INTRODUCTION

The term cloud is analogical to “Internet”. The term cloud computing is based on cloud drawings used in the past to represent telephone networks & later to depict internet (Voorsluys, Broberg, and Buyya, 2011). Cloud computing is internet based computing where virtual shared servers provide software, infrastructure, platform devices and other resources and hosting to customer as a service on pay-as you-use basis. Users can access these services available on the “internet cloud without having any previous know-how on managing the resources involved. Cloud users do not own the physical infrastructure; rather they rent the usage from a third- party provider. They consume resources as a service and pay only for resources that they use. What they only need is a personal computer and internet connection. Cloud computing has revolutionized the IT world with its services provisioning infrastructure, less maintenance cost, data & services availability assurance, rapid accessibility and scalability (Karthik et. al., 2015).

Intrusion Detection System (IDS) is a security system that acts as a protection layer to the infrastructure (Bray R., 2008). Throughout the years, the IDS technology has grown enormously to keep up with the advancement of computer crime. Since the beginning of the technology in mid-80’s, researches have been conducted to enhance the capability of detecting attacks without jeopardizing the network performance. (Kemmerer, Vigna, 2002).

IDS is the high-tech equivalent of a burglar alarm. A burglar alarm configured to monitor access points, hostile activities, and known intruders. IDS is a specialized tool that knows how to read and interpret the contents of log files from routers, firewalls, servers, and other network devices (Debar, Dacier and Wespi, 1999). An IDS often stores a database of known attack signatures and compare patterns of activity, traffic, or behavior it sees in the logs it is monitoring against those signatures to recognize when a close match between a signature and current or recent behavior occurs. At that point, the IDS can issue alarms or alerts, take various kinds of automatic action ranging from shutting down internet links or specific servers to launching back traces, and make other active attempts to identify attackers and actively collect evidence of their nefarious activities. IDSs can be software based or can combine hardware and software (in the form of preinstalled and preconfigured stand-alone IDS devices). Often, IDS software runs on the same device or server where the firewall or other services are installed monitors those devices tend to

operate at network peripheries, IDSs can detect and deal with insider attacks as well as external attacks.

Cloud computing has evolved through a number of implementations. Moving data into the cloud provides great convenience to users. Cloud computing is a collection of all resources to enable resource sharing in terms of scalable infrastructures, middleware and application development platforms, and value-added business applications.

A cloud is subject to several accidental and intentional security threats, including threats to the integrity, confidentiality and availability of its resources, data and infrastructure. Also, when a cloud with large computing power and storage capacity is misused by an ill-intentioned party for malicious purposes, the cloud itself is a threat against society. Intentional threats are imposed by insiders and external intruders. Insiders are legitimate cloud users who abuse their privileges by using the cloud for unintended purposes and we consider this intrusive behavior to be detected. An intrusion consists of an attack exploiting a security flaw and a consequent breach which is the resulting violation of the explicit or implicit security policy of the system. Although an intrusion connotes a successful attack, IDSs also try to identify attacks that don't lead to compromises. Attacks and intrusions are commonly considered synonyms in the intrusion detection context. The underlying network infrastructure of a cloud, being an important component of the computing environment, can be the object of an attack. Grid and cloud applications running on compromised hosts are also a security concern. We consider attacks against any network or host participating in a cloud as attacks against that, since they may directly or indirectly affect its security aspects. Cloud systems are susceptible to all typical network and computer security attacks, plus specific means of attack because of their new protocols and services (Hassan et. al., 2012)

An intrusion detection system (IDS) is a **data mining tool used to identify cyber attacks**. Besides quickly identifying attacks, it has many other benefits such as enabling the collection of intrusion information, recording malicious events, generating reports, and alerting system administrators by raising an alarm.

Intrusion Detection System (IDS) is a security system that acts as a protection layer to the infrastructure (Rebecca, and Peter 2001). Throughout the years, the IDS technology has grown enormously to keep up with the advancement of computer crime. Since the beginning of the technology in mid-80, researches have been conducted to enhance the capability of detecting attacks without jeopardizing the network performance. In this paper we hope to provide a critical review of the IDS technology, issues that transpire during its implementation and the limitation in the IDS research endeavors. Lastly we will proposed future work while exploring maturity of the topic, the extent of discussion, the value and contribution of each research to the domain discussed. At the end of this paper, readers would be able to clearly distinguish the gap between each sub-area of research and they would appreciate the importance of these research areas to the industry.

During the late 1980's, with a growing number of shared networks, enterprise system administrators all over the world began adopting Intrusion Detection Systems. However, IDS presented a couple of problems (Bace R., and Peter M. 2003).

First, it could only alert on known issues that had been categorized as threats on a signature list; zero day attacks could compromise a network's security. Second, the constant scanning and

updating of a signature list was cumbersome and significant resource drain. In the 1990's, IDS technology improved to address the increasing number and sophistication of network attacks. This new method, named anomaly detection, relied on identifying unusual behavioral patterns on the network, and provided alerts for any identified abnormality. Unfortunately, the inconsistent nature of networks through the 1990's and early 2000's resulted in a high number of false positives, and many administrators thought IDS to be unreliable, and headed for a slow death. The advent of cloud computing, however, has brought new relevancy to IDSs, resulting in a surge in the IDS market. An essential component of today's security best practices, IDSs are designed to detect attacks that may occur, despite preventive measures. In fact, IDS is now one of the top selling security technologies, and predicted to continue to gain momentum, after all, security-cloud security in particular is far too complex to be monitored manually.

The logic and tactics IDS uses are more relevant today than ever before. With cloud computing, IDS has truly found an environment where it can thrive and be most effective. With cloud computing, the infrastructure has caught up with the IDS technology. The consistent nature of servers in the cloud lends itself perfectly to IDS technology. As such, IDS is able to build stronger and more accurate baselines than were possible on the erratic on-premise network infrastructures on the past. Big data also plays an important role in the growth and importance of Intrusion Detection today (Roberto and Luigi V. 2008). The world's data doubles every 20 months, and as cloud hosted databases expand exponentially, it's no wonder IDS is more important than ever.

RELATED WORK

Cloud computing gets its name as a metaphor for the Internet. Typically, the Internet is represented in network diagrams as a cloud. The cloud icon represents "all that other stuff" that makes the network work. It's kind of like "etc." for the rest of the solution map. It also typically means an area of the diagram or solution that is someone else's concern, so why diagram it all out? It's probably this notion that is most applicable to the cloud computing concept.

Cloud Computing is a fused-type computing paradigm which includes Virtualization, Grid Computing, Utility Computing, Server Based Computing(SBC), and Network Computing, rather than an entirely new type of computing technique (JaeHyuk Jang, 2010). Cloud computing has evolved through a number of implementations. Moving data into the cloud provides great convenience to users. Cloud computing is a collection of all resources to enable resource sharing in terms of scalable infrastructures, middleware and application development platforms, and value-added business applications (Enisa C. 2009).

Intrusion Detection System

An intrusion detection system (IDS) examines system or network activity to find possible intrusions or attacks. Intrusion detection systems are either network-based or host-based; vendors are only beginning to integrate the two technologies (Hassan et. al., 2013). Network based intrusion detection systems are most common, and examine passing network traffic for signs of intrusion. Host-based systems look at user and process activity on the local machine for signs of intrusion (Kendall, 1998). Since each type has specific strengths and weaknesses, we will cover each type of tool in the following sections.

You might ask, “how does an IDS determine what is suspicious?” This is a good question. There are, generally speaking, three kinds of commercially available analysis engines:

- Event or Signature-based Analysis
- Statistical Analysis
- Adaptive Systems

The event, or signature-based, systems function much like the anti-virus software with which most people are familiar. The vendor produces a list of patterns that it deems to be suspicious or indicative of an attack; the IDS merely scan the environment looking for a match to the known patterns. The IDS can then respond by taking a user-defined action, sending an alert, or performing additional logging (Amirreaza, 2012). This is the most common kind of intrusion detection system. A statistical analysis system builds statistical models of the environment, such as the average length of a telnet session, and then looks for deviations from “normal”. After over 10 years of government research, some products are just beginning to incorporate this technology into marketable products. The adaptive systems start with generalized rules for the environment, then learn, or adapt to, local conditions that would otherwise be unusual. After the initial learning period, the System understands how people interact with the environment, and then warns operators about unusual activities. There is a considerable amount of active research in this area.

Technical Summary

The various types of IDS tools provide a wide range of capabilities for identifying or analyzing potential threats to computer networks. The type of analysis and the time between analysis and intervention will control decisions regarding type of tool to select. Certain organizations may find that they have a need for each type of product in a complementary security implementation on large networks. The common thread throughout these five categories is “human capabilities.” The organization must have expertise in-house (or hire a service) that can evaluate the legitimacy of any given intrusion warning. Any of these products can produce significant false positive rates; this requires investigative expertise within the organization.

What intrusion detection systems and related technologies can and cannot do

Every new market suffers from exaggeration and misconception. Some of the claims made in marketing materials are reasonable and others are misleading. Here with, a primer on how to read intrusion detection marketing literature.



*First Name:

 *Middle Name:

 *Last Name:

 *Email ID:

 *Contact No (1):
Maximum of 10 digits only and no special characters.

 *Contact No (2):
Maximum of 10 digits only and no special characters.

 Profile picture: No File chosen

What are you doing, ping get from image only.

 *Address:

LOGIN MONITOR						
EMAIL	PASSWORD	IP ADDRESS	HOST	SIGN TIME	STATUS	ACTION
emp@csmt@gmail.com	admin	11	Emp@csmt	05-28-2019 07:10 PM	Success	<input type="button" value="Details"/>
emp@csmt@gmail.com	admin	11	Emp@csmt	05-28-2019 07:15 PM	Success	<input type="button" value="Details"/>
emp@csmt@gmail.com	admin	11	user	05-28-2019 01:14 PM	Success	<input type="button" value="Details"/>
emp@csmt@gmail.com	12345678	11	user	05-28-2019 01:15 PM	Failed	<input type="button" value="Details"/>
emp@csmt@gmail.com	admin	11	user	05-28-2019 01:15 PM	Success	<input type="button" value="Details"/>
emp@csmt@yahoo.com	password12	11	user	05-28-2019 01:57 PM	Failed	<input type="button" value="Details"/>
emp@csmt@gmail.com	admin	11	user	05-28-2019 02:18 PM	Success	<input type="button" value="Details"/>
emp@csmt@gmail.com	admin	11	user	05-28-2019 03:11 AM	Failed	<input type="button" value="Details"/>
emp@csmt@gmail.com	admin	11	user	05-28-2019 03:11 AM	Success	<input type="button" value="Details"/>

Secured Address Book Management System



Avatar	First Name	Last Name	Contact No/ID	Email	Actions
	Amelia	Shanta	7744750034	ameliash@gmail.com	View Edit Delete
	Chakraborty	Utsavkumar	8188427182	ampanmcc201@gmail.com	View Edit Delete
	Chakraborty	Shanta	805222188	mushid@msu.edu.com	View Edit Delete
	David	Seetharam	775218699	seetharam@aravira.com	View Edit Delete
	Deepika	Radhika	888881182	deepika@rediffmail.com	View Edit Delete
	Deepika	Radhika	0102202022	deepika@rediffmail.com	View Edit Delete
	Deepika	Radhika	8188427182	ampanmcc201@gmail.com	View Edit Delete

Advantages of the Proposed System

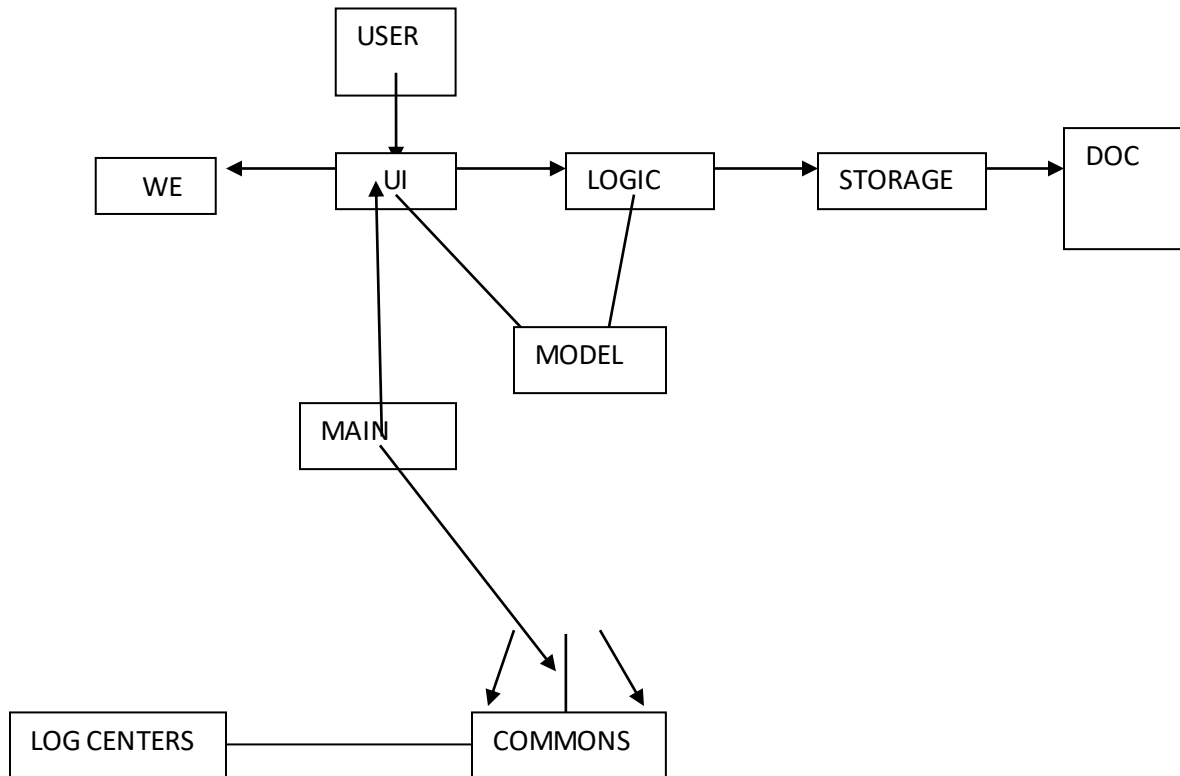
The advantages of the proposed system include;

- **Minimizing the cost:** The proposed system minimize the cost of installation from one system to an existing system
- **Stronger Security:** It provides far better security when compared to the existing system.
- Another major advantage of implementing the new system is that you do not need to be going around from city to city with your computer because the application you want to make use of is there waiting for it to be launched.

Justification of The Proposed System

The major disadvantage of the present system is that it cannot be used without the presence of good internet connections. So if a user is in an area where there is no internet service then he will experience some difficulties. Lack of large and central database for storage of terror related acts which can be retrieved when needed.

High level model of the Proposed System

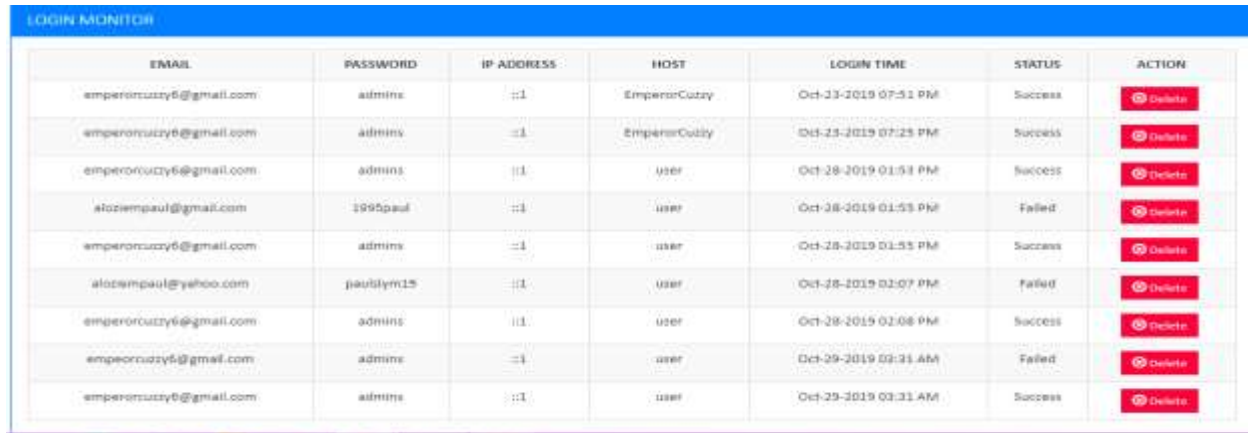


The **Architecture Diagram** given above explains the high-level model of the present system. Given below is a quick overview of each component

- **Log centers:** used by many classes to write log messages to the application log file and also manages the application logins of the users
- **UI:** the user interface of the present system
- **Logic:** the command executor
- **Model:** Holds the data of the present system in the memory
- **Storage:** reads data from and writes data to the hard disk

Each of the components defines its API in an interface with the same name as the component and exposes its functionality.

Image showing terror related input by the user



EMAIL	PASSWORD	IP ADDRESS	HOST	LOGIN TIME	STATUS	ACTION
emperorcuzzy6@gmail.com	admins	::1	Emperorcuzzy	Oct-23-2019 07:51 PM	Success	Delete
emperorcuzzy6@gmail.com	admins	::1	Emperorcuzzy	Oct-23-2019 07:23 PM	Success	Delete
emperorcuzzy6@gmail.com	admins	::1	user	Oct-28-2019 01:51 PM	Success	Delete
alozempaul@gmail.com	1995paul	::1	user	Oct-28-2019 01:53 PM	Failed	Delete
emperorcuzzy6@gmail.com	admins	::1	user	Oct-28-2019 01:53 PM	Success	Delete
alozempaul@yahoo.com	paulblm15	::1	user	Oct-28-2019 02:07 PM	Failed	Delete
emperorcuzzy6@gmail.com	admins	::1	user	Oct-28-2019 02:08 PM	Success	Delete
emperorcuzzy6@gmail.com	admins	::1	user	Oct-29-2019 03:31 AM	Failed	Delete
emperorcuzzy6@gmail.com	admins	::1	user	Oct-29-2019 03:31 AM	Success	Delete

Summary

Multi-level IDS and log management method is based on consumers behavior for applying IDS effectively to the cloud system. They assign a risk level to users behaviors based on analysis of their behavior over time. By applying Differentiated levels of security strength to users based on the degree of anomaly Increasing the effective usage of resources. Their method proposes the classification of generated logs by anomaly level. This is so that the system Administrator analyses logs of the most suspected users first. Also the data Traffic in the cloud is minimized and security is enhanced.

5.3 Conclusion

Cloud Computing technology provides human to advantages such as economical cost reduction and effective resource management. However, if security accidents occur, ruinous economic damages are inevitable. Our project proposed Multi-level IDS for effective resource and log management. Proposed method provides how we decrease the rule-set size of IDS and manages users' logs.

REFERENCES

- Amirreza Z. (2012). Research on Internet Intrusion Detection System Service in a Cloud, appear in *International Journal of Computer Science Issues*, Vol. 9, Issue 5.
- Bace R., and Peter M. (2003). *NIST Special Publication on Intrusion Detection Systems*.
- Debar H., M.Dacier and A.Wespi, *Towards a Taxonomy of Intrusion Detection System*, *Int'l J. Computer and Telecommunications Networking*, vol. 31, no.9, pp. 805-822, 1999.
- Enisa C. (2009). *Cloud Computing Risk Assessment*.
- Jae Hyuk Jang (2010). Cisco, *Cloud Computing: Drive Business Paradigm Shift*.
- Kemmerer, D., Vigna, G.: *Intrusion Detection: A brief history and overview*. *Computer* 35(4), 27- 30 (2002).
- JaeHyuk Jang, Cisco, *Cloud Computing: Drive Business Paradigm Shift*, 2010.
- Karthik, V., Schulte, A., Westphall, C.B., And Westphall, C.M., *Intrusion Detection for Cloud Computing*. 2015
- K. Kendall, "A Database of Computer Attacks for the Evaluation of Intrusion Detection Systems". Master's Thesis Massachusetts Institute of Technology, 1998
- Rebecca Bace and Peter Mell, *NIST Special Publication on Intrusion Detection Systems*, 2001.
- Roberto D. P, and Luigi V. (Jan. 2008) *Intrusion Detection Systems*, Springer.
- Voorsluys, W., Broberg, J. and Buyya, R. 2011 "*Introduction to cloud computing*).
- Wikipedia, http://en.wikipedia.org/wiki/Cloud_computing.
- (*The Best Firewall Book Period, 2003 pages 111-124*).
- (Cloud Security Alliance, *Security Guidance for Critical Areas of Focus in Cloud Computing*. Dec. 2009).