GSJ: Volume 10, Issue 12, December 2022
ISSN 2320-9186

GSJ: Volume 10, Issue 12, December 2022, Online: ISSN 2320-9186
www.globalscientificjournal.com

SECURITY IN CLOUD COMPUTING USING AN IMPROVED MULTI-LEVEL INTRUSION DETECTION AND LOG MANAGEMENT SYSTEM

Rimdans Victor Zwalmak
fisho4jos@yahoo.com **+2348061574069**
Department of Mathematics/Statistics/Computer Science, University of Agriculture, Makurdi, Nigeria

Abstract - Cloud Computing is a new type of service which provides large scale computing resource to each customer. Cloud computing systems can be easily threatened by various cyber-attacks, because most of the cloud computing systems provide services to so many people who are not proven to be trustworthy. A common issue of intrusion detection and management of large loads of data affecting security and performance in a cloud computing system need attention of a strong balance between IDS security level and system performance. If the IDS provide stronger security service using more rules or patterns, then it needs much more computing resources in proportion to the strength of security. To resolve these kinds of issues, an improved multi-level ID'S and log management system is developed which will detect various type of attacks and provide suitable level of security by examining attackers data record observed in processes on the virtual machine and send sms and email to the administrator. A spiral research methodology is adopted throughout this research. The implementation shows that, cloud computing system can achieve both effectiveness of using the system resource and strength of the security service without trade-off between them. Tools used are PHP, Atom and MySql in developing the web applications.

Keywords - Intrusion Detection Systems, Log Management System, Host-Based IDS, Network-Based IDS, Software as a Service (SAAS), Platform as a Service (PAAS), Infrastructure as a Service (IAAS)

I Introduction

The term cloud is synonymous to "Internet". Cloud computing can be described as designs formally used to represent telephone networks and also to represent internet. 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, [1]**.** Several firms and corporations have began looking for ways to minimise IT cost and surpass the economic down-turn been experience in recent years. Cloud Computing service is the latest computing era in which users only need to pay for the use of services without cost of purchasing physical hardware. As a result of this, Cloud Computing has been hugely developed along with the trend of IT services. Users find cloud computing more easy and cost saving as they can always access services they need from Cloud Computing provider. In fact, Cloud Computing has been recently more spotlighted than other computing

GSJ: Volume 10, Issue 12, December 2022
ISSN 2320-9186

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 it is easily threatened by attackers. Especially, system administrators potentially can become attackers.

Hence, the need for Cloud Computing providers to protect the systems safely against both insiders and outsiders using Intrusion Detection Systems (IDSs,) which is the widely accepted device for protecting Cloud Computing systems from various types of attack. An IDS observes the traffic from each Virtual Machine (VM) and generates alert logs, it can manage Cloud Computing globally. Logs management in Cloud Computing systems generate huge amount of data, therefore, system administrators should decide to which log should be analysed first [2].

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. 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, application development platforms, and value-added business applications. Cloud computing is characterised to be virtual, scalable, efficient, and flexible. In cloud computing, three kinds of services are provided: Software as a Service (SaaS) systems, Infrastructure as a Service (IaaS) providers, and Platform as a Service (PaaS). In SaaS, systems offer complete online applications that can be directly executed by their users; In IaaS, providers allow their customers to have access to the entire virtual machines; and in SaaS, it offers development and deployment tools, languages and APIs used to build, deploy and run applications in the cloud [3].

Cloud computing 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, it becomes 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 behaviour 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 do not lead to compromises. Attacks and intrusions are commonly considered synonyms in the intrusion detection context [4].

There are three ways to report the detection results, notification, manual response and automatic response. Notification response system, IDS only generates reports and alerts. Manual response system IDS provides additional capability for the system administrator to initiate a manual response and automatic response system IDS immediately respond to an intrusion through auto response system [5]. Thus what is needed to complement the works of others is to develop an application that will secure cloud resources by detecting various types of attacks and provide suitable level of security by examining attacker data record observed in processes on the virtual machine without consuming much system resources that will have adverse impact on resource allocation to client services.

II Literature Review

State of the Art of Intrusion Detection Systems

The importance of Cloud computing and its future you can predict on the basis of that almost all big-players in the software industry are deploying their cloud services. The future of any technology depends upon the condition that how much industrialization is going on for that technology [6]. Multiple research activities were introduced to address the issue of intrusion detection within cloud computing environments. These activities can be classified as those to detect intrusions against the cloud itself and those to detect attacks that target individual machines inside the cloud. Our study is on the latter type of the two. More specifically, it will cover the service-based or subscription-based intrusion detection; which is a field that did not

GSJ: Volume 10, Issue 12, December 2022
ISSN 2320-9186

receive as much attention as the classical intrusion detection activities.

Intrusion Detection Systems

Intrusion detection system and Intrusion prevention systems are the two most common technologies for monitoring a network for violations of the security notion. The IDS is for grouping a technology consisting of various representations into one classification. If IDS is placed on the HOST then it is referred as Host based IDS and if it is a stand-alone node inside the network, then it is called as network based IDS. Computer Security Threat Monitoring and Surveillance introduced the basic concept of IDS [7].

Intrusion detection for grid and cloud computing

Cloud and Grid computing are the most vulnerable targets for intruder's attacks due to their distributed environment. For such environments, Intrusion Detection System (IDS) can be used to enhance the security measures by a systematic examination of logs, configurations and network traffic. Traditional IDSs are not suitable for cloud environment as network based IDSs (NIDS) cannot detect encrypted node communication, also host based IDSs (HIDS) are not able to find the hidden attack trail. [8] have proposed an IDS service at cloud middleware layer, which has an audit system designed to cover attacks that NIDS and HIDS cannot detect. The architecture of IDS service includes the node, service, event auditor and storage. The node contains resources that are accessed through middleware which defines access-control policies. The service facilitates communication through middleware. The event auditor monitors and captures the network data, also analyzes which rule / policy is broken. The storage holds behavior-based (comparison of recent user actions to usual behavior) and knowledge-based (known trails of previous attacks) databases. The audited data is sent to IDS service core, which analyzes the data and alarm to be an intrusion. The authors have tested their IDS prototype with the help of simulation and found its performance satisfactory for real-time implementation in a cloud environment. Although they have not discussed the security policies compliance check for cloud service provider and their reporting procedures to cloud users.

Intrusion detection in the cloud

Intrusion detection system plays an important role in the security and perseverance of active defense system against intruder hostile attacks for any business and IT organization. IDS implementation in cloud computing requires an efficient, scalable and virtualization-based approach. In cloud computing, user data and application is hosted on cloud service provider's remote servers and cloud user has a limited control over its data and resources. In such case, the administration of IDS in cloud becomes the responsibility of cloud provider. Although the administrator of cloud IDS should be the user and not the provider of cloud services. [9] proposed an integration solution for central IDS management that can combine and integrate various renowned IDS sensors output reports on a single interface. The intrusion detection message exchange format (IDMEF) standard has been used for communication between different IDS sensors. The authors have suggested the deployment of IDS sensors on separate cloud layers like application layer, system layer and platform layer. Alerts generated are sent to "Event Gatherer" program. Event gatherer receives and convert alert messages in IDMEF standard and stores in event data base repository with the help of Sender, Receiver and Handler plug-ins. The analysis component analyzes complex attacks and presents it to user through IDS management system. The authors have proposed an effective cloud IDS management architecture, which could be monitored and administered by the cloud user. They have provided a central IDS management system based on different sensors using IDMEF standard for communication and monitored by cloud user.

Log Management System

So many people would use Cloud Computing service, so the huge logs arise from transaction between systems, user information update, and mass data processing and so on. Therefore, it is very difficult to analyze using the logs in emergency. Log generation and storage can be complicated by several factors, including:

- A high number of log sources;
- Inconsistent log content;
- Lack of structure among generated logs;
- Formats;
- Timestamps among sources;
- Increasingly large volumes of data;

GSJ: Volume 10, Issue 12, December 2022
ISSN 2320-9186

- Not calculating the proper events per second (EPS); and
- Losing logs due to saturation.

To make analyzing log better, [10] propose the method that divides log priority according to security level. The auditing priority of the logs is also decided by the anomaly level of users. It means the logs generated by user who have most high anomaly level are audited with top priority. On the other hand, logs of low-level users are audited at last. So our method can efficiently cope with potential attacks from the relatively more dangerous users than others.

Security Issues/threats in Cloud Computing

Since the advent of the computer, people have been trying to find ways to exploit hardware and software bugs and mis-configurations for pride and profit as ideological, political and theological reasons. The first boot sector virus appeared in 1981 till manifested to the present threat environment of multi vector worms, blended threats, flash worms and distributed denial of service. The quantity, variety and potential disruptiveness of known attack techniques have been on the rise dramatically, particularly in recent years [11].

In March 1994, the Computer System Laboratory Bulletin has identified the basic 9 common threats such as Errors and omissions, Fraud and theft, Disgruntled Employees, Physical and Infrastructures, Malicious Hackers, Industrial Espionage, Malicious Code, Malicious Software and Threats to Personal Policy. Computer crimes are defined in many forms, all of which can have equally serious consequences where a business is concerned. This can include the alteration, destruction or misappropriation of data, the introduction of viruses or other malicious code, and the importation of pornographic, or other inappropriate material, into the organization and its dissemination. With so many business critical processes now deeply entrenched in networks, databases and computer storage, the threat posed by computer crime has become very real [12]. There is now a growing realization that a significant fraud threat comes from inside, and not outside, the organization [13].

Categorize of Security Threats

i. Cloud data confidentiality issue

Confidentiality of data over cloud is one of the glaring security concerns. Encryption of data can be done with the traditional techniques. However, encrypted data can be secured from a malicious user but the privacy of data even from the administrator of data at service provider's end could not be hidden. Searching and indexing on encrypted data remains a point of concern in that case. Above mentioned cloud security issues are a few and dynamicity of cloud architecture are facing new challenges with rapid implementation of new service paradigm [14].

ii. Network and host Based Attacks on Remote Server

Host and network intrusion attacks on remote hypervisors are a major security concern, as cloud vendors use virtual machine technology. DOS and DDOS attacks are launched to deny service availability to end users [15]**..**

iii. Cloud security auditing

Cloud auditing is a difficult task to check compliance of all the security policies by the vendor. Cloud service provider has the control of sensitive user data and processes, so an automated or third party auditing mechanism for data integrity check and forensic analysis is needed. Privacy of data from third party auditor is another concern of cloud security [16].

iv. Lack of data interoperability standards

It results into cloud user data lock-in state. If a cloud user wants to shift to other service provider due to certain reasons it would not be able to do so, as cloud user's data and application may not be compatible with other vendor's data storage format or platform. Security and confidentiality of data would be in the hands of cloud service provider and cloud user would be dependent on a single service provider [17].

v**. Threat cause by insiders**

The internal security threat encompasses a broad range of events, incidents and attacks, all connected by being caused by organization's own staff, its authorized IT users. This threat area covers user errors and omissions, negligence and deliberate acts against the company [18]**.**

vi. Poor security lead to internal threat damage on the system

The internal threat is predominantly the result of poor user security behaviour such as forgetting to apply security procedures, taking inappropriate risks because of not appreciating

GSJ: Volume 10, Issue 12, December 2022
ISSN 2320-9186

or believing the level of risk involved such as leaving the PC unattended in an open office without logging off. Deliberate acts of negligence consist of users knowingly failing to follow essential security processes, and deliberate attacks by the technically literate abusing their positions in order to commit fraud like users purposefully acting against the organization's interests [19].

Methods of Solving Fraud

Practically, there are two methods of containing any kind of fraud; Prevention and Detection. Prevention focuses on controls designed to reduce the opportunity for unauthorized use of corporate resources. Detection controls designed to alert the appropriate personnel of the fraud detected. Thus we intend to develop an application that will secure cloud resources by detecting various types of attacks and provide suitable level of security by examining attacker data record observed in processes on the virtual machine without consuming much system resources that will have adverse impact on resource allocation to client services. [20] demonstrated the use of a hybridized machine learning models with the expectation of showing the capability to the job of intrusion detection in a computer network. The research used the training and testing versions of the NSL-KDD datasets in other to illustrate the effectiveness of the model against known and unknown entries in the model. This work made use of Neural Network (NN) and Support Vector Machine (SVM) algorithms for the supervised learning, K-Means algorithm for the unsupervised learning and PCA and GFR for feature selection on the datasets.

III Methodology

This paper investigates the use of multi-level IDS based on logs using the spiral development model. These logs are from a cloud based system with respect to the behaviour of a guest. This system will strengthen the security in cloud computing systems. To achieve the multi-level IDS which will secure cloud computing systems, we adopted the method by [21]. This method was adopted because it has proved to be very effective for detecting intrusions in the cloud. However, our proposed method will perform investigations on a cloud computing system compared to the one used by [22] and handle different logs. This method will furthermore bind users to different security group in accordance with the degree of anomaly.

System Architecture

The proposed system architecture

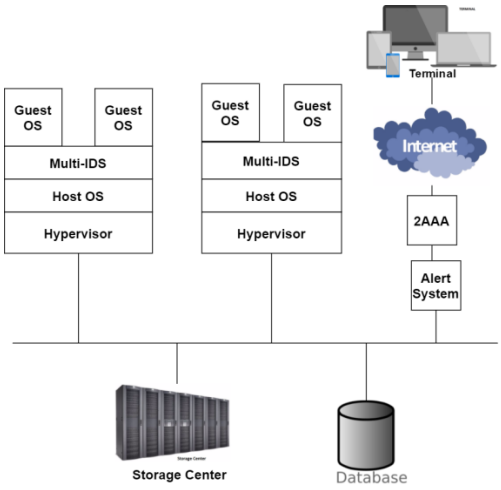

Figure 1: Multi-Level ID'S Architecture

2AAA is a management module for two level authentication, authorization and accounting. When a user tries to access Cloud Computing system, the 2AAA checks the user's authentication information. If the user is authenticated, then 2AAA gets the user's anomaly level, which has been most recently generated, by inspecting the user's information in the database. After that, 2AAA chooses suitable IDS which have the security level correspondent to the user's anomaly level. Then 2AAA requests the host OS, in which the chosen IDS is installed, to assign guest OS image for the user. Database stores and manages user information, system log, transaction of user and system. System managers can quickly cope with the non-predictable situation in Cloud Computing system through the assistance of the database that periodically intercommunicates with 2AAA and host OS.

The alert system was designed to recognize a variety of events that occur in the monitored space and notifies users of the system in real time. It was implemented to show the credibility and reliability of the system. Storage center stores private data of users. All users' data is logically isolated, so nobody can access the data except owners of the data and users who have been given access right by owner. After a user is assigned a guest OS, the connection between the guest OS and data owned by the

GSJ: Volume 10, Issue 12, December 2022
ISSN 2320-9186

user in storage center is then established. In this paper, security level is divided in to High, Medium and Low for effective IDS construction, High-level is a group which apply patterns of all known attacks and a portion of anomaly detection method when needed, for providing strong security services. Medium-level is a group of middle grade which apply patterns of all known attacks to rules for providing comparatively strong security service. Low-level is a group for flexible resource management which apply patterns of chosen malicious attacks that occur with high frequency and that causes fatally to the system.

In Multi-level IDS scheme, an IDS consumes more resource when providing higher level security, because higher level security apply more rules than lower level. On the other hand, if an IDS provides lower level security policy, then the amount of resource usage is decreased although the detecting power of attacks also drops. The assignment of VM to a user is determined in accordance with security level. The grade of VM is proportional to user criteria of anomaly level. Anomaly levels of users are estimated by their behaviours during the usage of service based on saved user anomaly level in the system.

For instance, when a user access Cloud Computing system first time, Multi-level IDS judges anomaly level of user using the following: the user's IP coverage, vulnerable ports to attack, the number of ID/PW failure. The most important element for estimating anomaly level is how fatal it is. The rest of judgment criteria are possibility to attack success, possibility to attack occurrence, etc. The fatal grade of an attack is the degree of impact to systems of the attack, which includes from personal information extortion to system control and destruction. Possibility to attack success is an experimental value which indicates the probability of success for an attack. Possibility to attack occurrence is a value based on the frequency of specific attack. The data in table 1 shows user risk level.

Table 1: User Risk Level

	Business Impact				
Possibility of incident situations	**Very low**	**Low**	**Medium**	**High**	**Very high**
Very low	0	1	2	3	4
Low	1	2	3	4	5
Medium	2	3	4	5	6
High	3	4	5	6	7
Very high	4	5	6	7	8

Source: Lee *et al.,* 2011

Database Design

An entity relationship diagram (ERD) is a data modeling technique that graphically illustrates an information system's entities and the relationships between them. The entity relationship diagram of the propose system is shown in Figure 2:

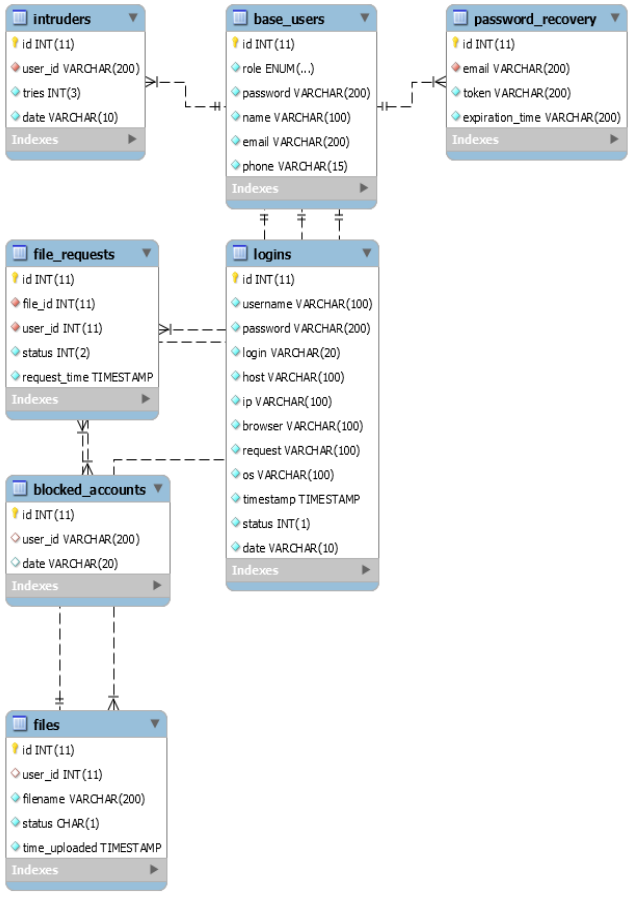

Figure 2: ERD of the Proposed System

Alert System Algorithm

i. START
ii. LOGIN
iii. CHECK FOR THREAT
iv. IF THREAT DETECTED
v. VERIFY THREAT
vi. IF ALARM IS FALSE
GOTO VII
ELSE
ALERT ADMINISTRATOR

GSJ: Volume 10, Issue 12, December 2022
ISSN 2320-9186

```
                EXIT
vii. PROCESS LOGIN CREDENTIALS
viii. IF CREDENTIALS ARE CORRECT
                GRANT ACCESS
        ELSE
                DENY ACCESS
ix. EXIT
```

IV Results

Intrusion detection systems (IDS) are one of the most popular applications for protecting cloud computing systems from various types of attack. IDS can observe the traffic from each virtual machine (VM) and generate alert logs and can manage cloud computing globally. Since cloud infrastructures have enormous network traffic, traditional IDSs are not efficient enough to handle such a substantial data flow. A common issue is intrusion detection and management of large loads of data. There needs to be a strong balance between IDS security level and system performance. Multi-level IDS method leads to effective resource usage by applying differentiated level of security strength to users based on the degree of anomaly.

This paper has three (3) components/modules which are implemented in this system: CSP (Content Service Provider) module, TPA (Third Party Administrator) module, and USER(s) module. You can only access them if you are a registered user through the login and Confirmation code page (Two factor authentication) as it shown Figure 3.

Two Factor Authentication

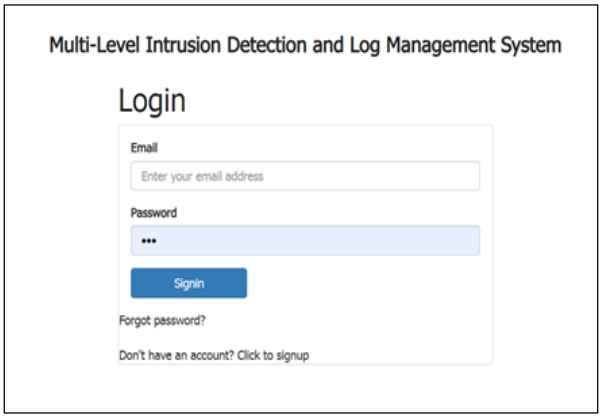

Figure 3: Login Page

Figure 4: Confirmation Code Page

Once the system detect any malicious activity, it set an alternative path to all users trying to gain unauthorized access to the cloud, and send SMS alert, e-mail to the system administrator, informing him/her about the attacker in order to take immediate actions.

CSP (Content Service Provider) provides access to view system logs that is a comprehensive record of all attempted logins into the system, whether it was successful or not as it flows in the hierarchy of the proposed system. Also, it displays a list of all intruder activity (failed logins into registered users account) on the system and list of all registered users respectively.

TPA (Third Party Administrator) displays a list of all uploaded files yet to be accepted or declined by the Third Party Administrator, all processed files and information about all the files a user requested for.

USER'S module provide a form from which a user can upload a file to the system, this file has to be approved by the TPA in other for other users to have access to it and displays the account information (Name, phone, email) of the user. From this module, the user can also have access to a form that will enable him/her update the account information. The user can also update his/her password from this page too.

[23] method increases resource availability of Cloud Computing system and handle the potential threats by deploying Multi-level IDS and managing user logs per group according to anomaly level. Suppose that VMs have equal quantity of resource, then host OS can assign less guest OS with IDS, because IDS use much resource. On the other hands, he assign more guest OS with Multi-level IDS, because medium level and low-level IDS use less resource. The users classified as high-level group are potentially dangerous user, therefore a high-level IDS consumes much resource to detect all of anomalous behaviors. However, a low level IDS consumes less resource, because the user classified as low-level group are judged, that

GSJ: Volume 10, Issue 12, December 2022
ISSN 2320-9186

they are normal users. As a result, low-level IDSs maintain little rules for managing effective resource, so it can assign more guest OS than high and medium-level. His method also supports classifying the logs by anomaly level, so it makes system administrator to analyze logs of the most suspected users first.

By adding the alert system to the existing system proposed by [24] it can be observed that, the system administrator can tackle any security bridge by an intruder immediately, since the alerting system notify or alert the administrator immediately when there is an attempt by an attacker in the cloud, where as in the existing system the administrator will only know about an attack when he/she login into the system and check the system logs for possible attack. Therefore our method provides high speed of detecting attacks over the previous work.

In the previous work, the system administrator has to login to analyze logs of the most suspected users first base on the anomaly level. But in the proposed security in cloud computing using an improved intrusion detection and log management system, the administrator can easily analyze level of an attacker behavior through the alert received from the system unlike in the previous system.

V Conclusion

In this paper, we used an improved Multi-level intrusion detection and log management system method based on consumer behavior to applying IDS effectively to the cloud system. They assign a risk level to user behavior based on analysis of their behavior over time. By applying differentiated levels of security strength to users based on the degree of anomaly, increases the effective usage of resources. Their method proposes the classification of generated logs by anomaly levels, so that the system administrator analyses logs of suspected users first. Also, the data traffic in the cloud is minimized and the security level is enhanced.

References

[1]Parag, K. S., Sneha, S. and Gawande, A. D. (2012). Intrusion Detection System for Cloud Computing. *International Journal of Scientific & Technology Research,* 1 (4): 2277-8616.

[2]Lee, H. J., Min, W. P. and Jung, H. E. (Feb.2011). Multi-level Intrusion Detection and Log Management in Cloud Computing. Institute of Electrical Electronic Engineers (*IEEE) Computer Society,* 5(4): 552-555.

[3]Parag, K. S., Sneha, S. and Gawande, A. D. (2012). Intrusion Detection System for Cloud Computing. *International Journal of Scientific & Technology Research,* 1 (4): 2277-8616.

[4]Debar, H., Dacier, M. and Wespi, A. (1999). Towards a Taxonomy of Intrusion Detection Systems. *International Journal of Computer and Telecommunications Networking*, 31(9): 805–822.

[5]Prema, J. and Ashwin, K. (2014). Ensuring Security in Cloud with Multi-Level IDS and Log Management System. *International Journal of Recent Advances in Engineering & Technology (IJRAET),* 2(5): 2347-2812.

[6]Mohammed, Y. Getu, H. and Shahnawaz, H. (2017) *State of the Art Study of Intrusion Detection System for Cloud Computing.* Samara, Ethiopia: Samara University. Pp 336-339.

[7]George, R. (2009). *Cloud Application Architectures.* 1st edition. O'Reilly Media. Pp. 345-348.

[8]Vieira, K., Schulter, A. Westphall, C. B. and Westphall, C. M. (2010). Intrusion Detection for Grid and Cloud Computing. Institute of Electrical Electronic Engineers (*IEEE) Computer Society,* 12 (4): 38 – 43.

[9]Schulter, A. and Carlos, B. (2008). Intrusion Detection for Computational Grids, *Procedia 2nd Internal Conference New Technologies, Mobility, and Security*, Institute of Electrical Electronic Engineers (IEEE) Press, 5(3): 1–5.

[10]Prema, J. and Ashwin, K. (2014). Ensuring Security in Cloud with Multi-Level IDS and Log Management System. *International Journal of Recent Advances in Engineering & Technology (IJRAET),* 2(5): 2347-2812.

[11]Kropp, T. (2006). System Threats and Vulnerabilities (Power System Protection), Institute of Electrical Electronic Engineers (*IEEE) Power and Energy Magazine,* 4(2): 46– 50.

[12]Rao, K. V., Pal, A. and Patra, M. R. (2009). A Service Oriented Architectural Design for Building Intrusion Detection Systems.

GSJ: Volume 10, Issue 12, December 2022
ISSN 2320-9186

International Journal of Recent Trends in Engineering, 1(2): 11-14.

[13]Foster, I., Zhao, Y. Raicu, I. and Lu, S. (2008). Cloud Computing and Grid Computing 360-Degree Compared, *Grid Computing Environments Workshop*. 611pp.

[14]Kento, S., Hitoshi, S. and Satoshi, M. (2009). A Model-based Algorithm for Optimizing I/O Intensive Applications in Clouds using VM-Based Migration, *9th IEEE/ACM International Symposium, Cluster Computing and Grid,* 7(4): 98.

[15]Kento, S., Hitoshi, S. and Satoshi, M. (2009). A Model-based Algorithm for Optimizing I/O Intensive Applications in Clouds using VM-Based Migration, *9th IEEE/ACM International Symposium, Cluster Computing and Grid,* 7(4): 98.

[16]Kento, S., Hitoshi, S. and Satoshi, M. (2009). A Model-based Algorithm for Optimizing I/O Intensive Applications in Clouds using VM-Based Migration, *9th IEEE/ACM International Symposium, Cluster Computing and Grid,* 7(4): 98.

[17]Kento, S., Hitoshi, S. and Satoshi, M. (2009). A Model-based Algorithm for Optimizing I/O Intensive Applications in Clouds using VM-Based Migration, *9th IEEE/ACM International Symposium, Cluster Computing and Grid,* 7(4): 98.

[18]Kento, S., Hitoshi, S. and Satoshi, M. (2009). A Model-based Algorithm for Optimizing I/O Intensive Applications in Clouds using VM-Based Migration, *9th IEEE/ACM International Symposium, Cluster Computing and Grid,* 7(4): 98.

[19]Thakar, U. (2005). Honey Analyzer – Analysis and Extraction of Intrusion Detection Patterns & Signatures Using Honeypot. *The second International Conference on Innovations in Information Technology, Dubai UAE, (*September), 4(3): 26-28.

[20]Perez, D. Astor, M. A. Abreu, D. P. and Scalise, E. (2017). *Intrusion Detection in Computer Networks Using Hybrid Machine Learning Techniques.* Caracas, Venezuela: Central University of Venezuela. Pp 765-769.

[21]Lee, H. J., Min, W. P. and Jung, H. E. (Feb.2011). Multi-level Intrusion Detection and Log Management in Cloud Computing. Institute of Electrical Electronic Engineers (*IEEE) Computer Society,* 5(4): 552-555

[22]Lee, H. J., Min, W. P. and Jung, H. E. (Feb.2011). Multi-level Intrusion Detection and Log Management in Cloud Computing. Institute of Electrical Electronic Engineers (*IEEE) Computer Society,* 5(4): 552-555

[23]Lee, H. J., Min, W. P. and Jung, H. E. (Feb.2011). Multi-level Intrusion Detection and Log Management in Cloud Computing. Institute of Electrical Electronic Engineers (*IEEE) Computer Society,* 5(4): 552-555

[24]Lee, H. J., Min, W. P. and Jung, H. E. (Feb.2011). Multi-level Intrusion Detection and Log Management in Cloud Computing. Institute of Electrical Electronic Engineers (*IEEE) Computer Society,* 5(4): 552-555