Threat Handling and Security Issue in Cloud Computing

[a,c]Akinola Kayode E., [b]Odumosu Adesola A.

[a]*Computer Science Department*, ***Abraham Adesanya Polytechnic***, *Ijebu-Igbo, Ogun State, Nigeria.*
[b]*Computer Science Department*, ***Abraham Adesanya Polytechnic***, *Ijebu-Igbo, Ogun State, Nigeria.*
[c]*Department of Computer Science*, *Babcock University*, *Ilishan Remo Ogun State Nigeria*, *Nigeria.*

email address: *kayodewale87@yahoo.com (Akinola, K. E); kayodewale87@gmail.com (Akinola K. E.),*

Abstract - Clouds provide a powerful computing platform that enables individuals and organizations to perform variety levels of tasks on the internet. It has been developed to provide information technologies services on demand to individuals as well as organization. However, as good and flexible as cloud Computing is, there are lots of threat from hackers to security of data passing through it day in day out. Therefore, cloud security have to be strong and consistent, so that the flexibility and advantages that cloud computing has to offer will be reliable. This paper presents a review on the cloud computing threats as well as security issues and how to handle them in the context of cloud infrastructure.

KEYWORDS
Cloud computing, cloud service, cloud security, threat, attacks, security issues.

1.0 Introduction

Cloud Computing is a computer model that provides services in the form of on-demand services, it's accessible for everyone, everywhere and every time , including clouds referring to the internet and the web (Y. Ghebghoub, S. Oukid, and O. Boussaid, 2013). Clouds provide a powerful computing platform that enables individuals and organizations to perform variety levels of tasks such as: social networking, buying and selling of goods, online storage space, training, development of customized computer software, and creation of a "realistic" network environment. With each passing years, the number of people using cloud services has dramatically increased and lots of data has been stored in cloud computing environments. In addition, Cloud computing enables ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g. networks, servers, storage,

applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction (Hashizume et al., 2013). In the meantime, data breaches to cloud services are also increasing every year due to hackers who are always trying to exploit the security vulnerabilities of the architecture of cloud (D. Jamil and H. Zaki , 2011).

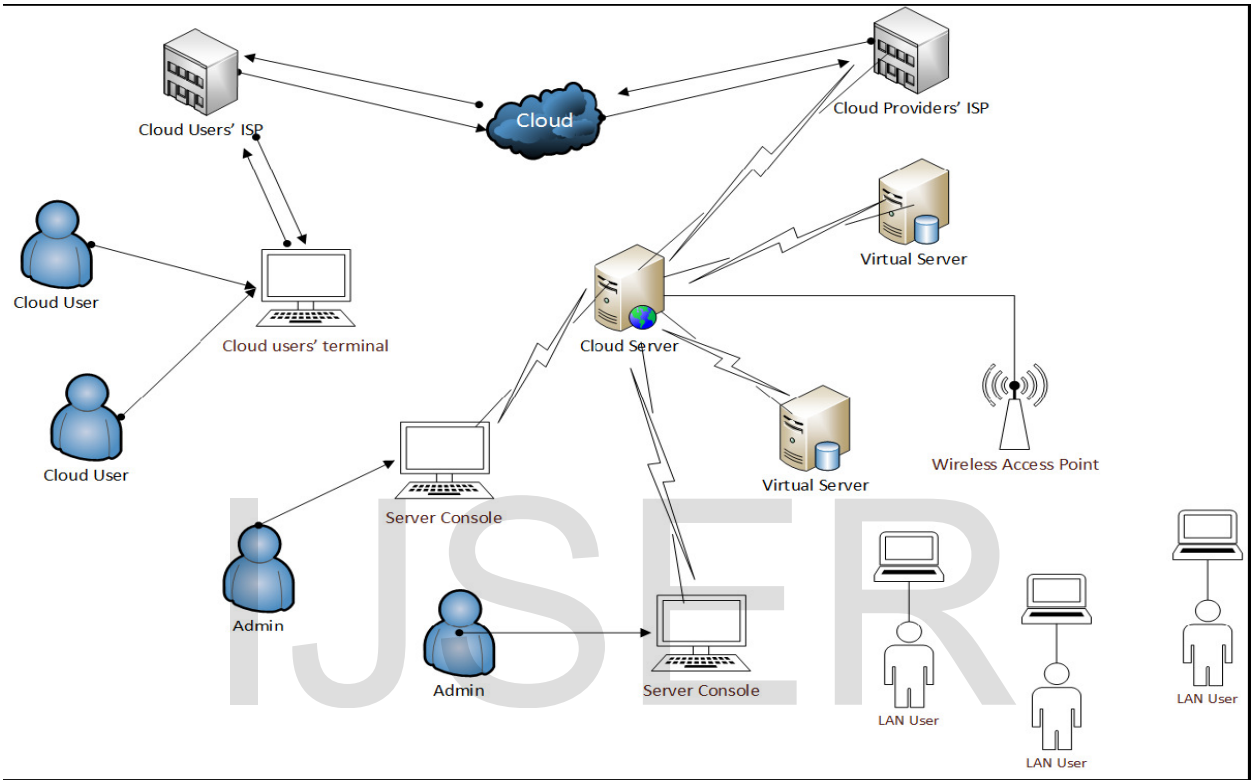

Figure 1: A Typical Cloud Architecture

The illustration of cloud architecture in figure 1 is a simplest one, where we can see: the cloud, cloud user ISP, virtual server, cloud server and cloud user. The purpose of the illustration is to establish the arrangement that makes the visualized concept of cloud computing a tangible one. The network architecture is self-explanatory with the identification of cloud users when considered in-line with the discussion of the cloud computing idea presented earlier (Monjur Ahmed and Mohammad Ashraf Hossain, 2014).

1.2 SECURITY THREAT ON THE CLOUD

Threat: is an actor who wants to attack assets in the cloud at a particular time with a particular goal in mind, usually to inflict his own financial gain and consequentially financial loss of a customer.

Vulnerability: is a flaws in a system that can be exploited by the attacker for his own personal gain. A flaw can be present in software, environments and systems which allows an attack to be successful.

Security attacks through cloud computing have proliferated in recent years. These attacks can be grouped into two types: the active and passive attacks. The active attacks include masquerading, replay attack, modification of messages and denial of service. Passive attacks include traffic analysis. These attacks are likely to happen when the stream of information leaves the client network to the Cloud network.

The attacks on the cloud have become both more prolific and easier to implement because of the ubiquity of the internet and the pervasiveness of easy-to-use operating systems and development environments. There are multiple penetration points for attacks to take place in a cloud system, which can be grouped under these three models: Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS).

1.3 IPS (INFRASTRUCTURE, PLATFORM AND SOFTWARE) MODELS IN CLOUD COMPUTING

Three models are typically used, in order of decreasing enterprise control: Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS).

• **Infrastructure as a Service (IaaS)** - In IaaS, generally the service provider offers a VM platform and underlying infrastructure with CPU, memory, storage, bandwidth and networking. Enterprises then deploy their VMs into this environment. The enterprise retains control of operating systems (OS), storage data, and applications. In the IaaS model, the enterprise does not control the underlying hardware or hypervisor, but retains significant control over security on the VM level. With IaaS many users are available to use available resources.

• **Platform as a Service (PaaS**) - In PaaS, the enterprise retains control of applications and limited control over application hosting environment configurations. Otherwise, the enterprise relies on the service provider to provide security.

• **Software as a Service (SaaS)** - In SaaS, the enterprise retains control of only limited user- specific application configuration settings. In SaaS models, the enterprise relies on the service provider to provide security.

Figure 2. Unauthorized access of data within the Cloud

The figure 2 above describes the scenario where the data of the local network resides within the cloud, where the local network and the authorized users can access their data physically in the Cloud. At that instant of time, there exists a possibility for unauthorized users to enter and access the data in the Cloud.

To prevent unauthorized access, the virtual machines are allotted to users of the Cloud. These machines have valid logins. However, these logins can be abused and cracked. The data may also be accessed in other perverted ways.

There is no doubt that security has been the major barrier in the adoption of the cloud by organizations as the thought of running your software and storing sensitive data on someone else's hard disk is rather frightening. According to a 2009 IDC Survey, security was rated as the greatest factor for holding back organizations from implementing it.

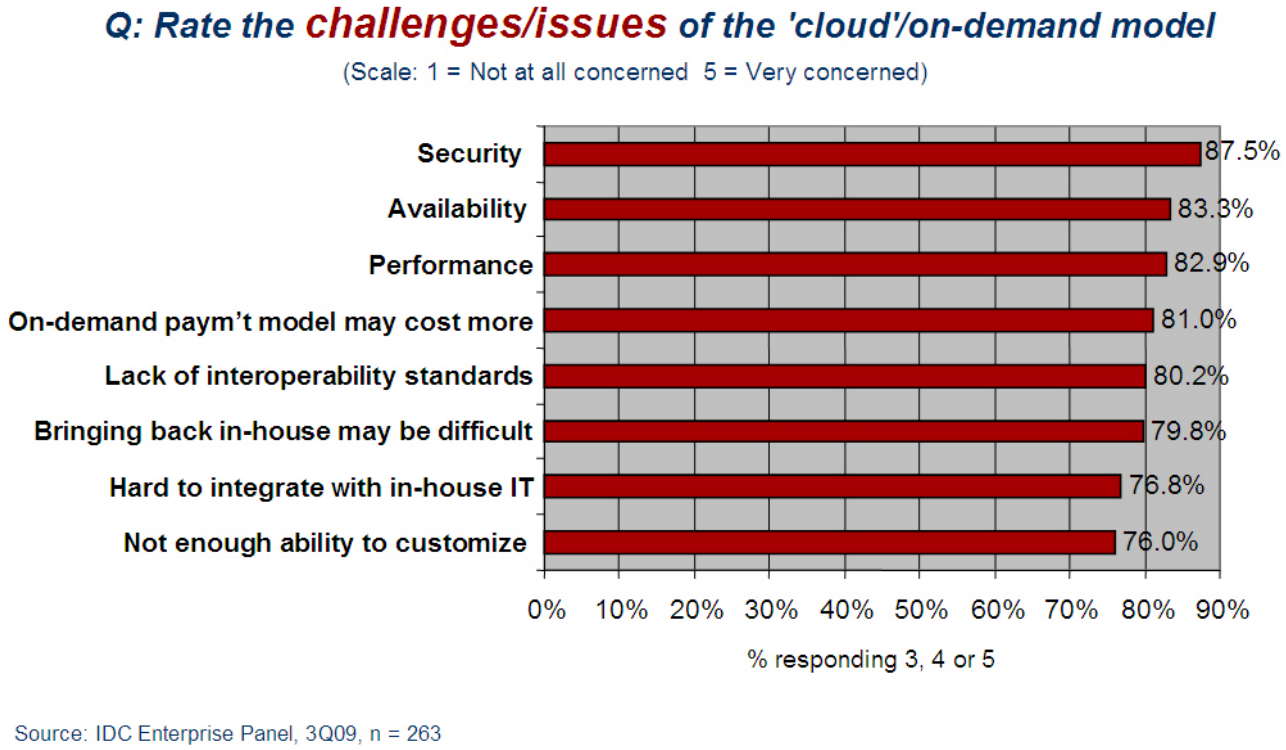

Figure 3. IDC Survey rating the challenges of cloud computing

There are numerous security issues that are associated with cloud computing because it encompasses various technologies which include networks, databases, operating systems, virtualization, resources scheduling amongst many others (K. Hamlen, M. Kantarcioglu, L. Khan, & B. Thuraisingham, 2010). In light of this, it is expedient for organizations to apply security measures that will cater for the delivery method they adopt since threats differ from layer to layer (S. O. Kuyoro, A. A. Omotunde, C. Ajaegbu, F. Ibikunle, 2012).

2.0 EXISTING SECURITY THREATS & ATTACKS IN CLOUD COMPUTING

2.1 MALICIOUS INSIDERS

Employees working at cloud service provider could have complete access to the company resources. Therefore cloud service providers must have proper security measures in place to track employee actions like viewing a customer's data. Since cloud service provides often don't follow the best security guidelines and don't implement a security policy, employees can gather confidential information from arbitrary customers without being detected.

2.2 DNS ATTACKS

A Domain Name Server (DNS) server performs the translation of a domain name to an IP address. Since the domain names are much easier to remember. Hence, the DNS servers are needed. But there are cases when having called the server by name, the user has been routed to some other evil cloud instead of the one he asked for and hence using IP address is not always feasible. Although using DNS security measures like: Domain Name System Security Extensions (DNSSEC) reduces the effects of DNS threats but still there are cases when these security measures prove to be inadequate when the path between a sender and a receiver gets rerouted through some evil connection. It may happen that even after all the DNS security measures are taken, still the route selected between the sender and receiver cause security problems (Philip Wik, 2011).

2.3 SNIFFER ATTACKS

These types of attacks are launched by applications that can capture packets flowing in a network and if the data that is being transferred through these packets is not encrypted, it can be read and there are chances that vital information flowing across the network can be traced or captured. A sniffer program, through the NIC (Network Interface Card) ensures that the data/traffic linked to other systems on the network also gets recorded. It can be achieved by placing the NIC in promiscuous mode and in promiscuous mode it can track all data, flowing on the same network. A malicious sniffing detection platform based on ARP (address resolution protocol) and RTT (round trip time) can be used to detect a sniffing system running on a network (Zouheir Trabelsi, Hamza Rahmani, Kamel Kaouech, Mounir Frikha, 2004) .

2.4 ISSUE OF REUSED IP ADDRESSES

Each node of a network is provided an IP address and hence an IP address is basically a finite quantity. A large number of cases related to re-used IP-address issue have been observed lately. When a particular user moves out of a network then the IP-address associated with him (earlier) is assigned to a new user. This sometimes risks the security of the new user as there is a certain time lag between the change of an IP address in DNS and the clearing of that address in DNS caches. And hence, we can say that sometimes though the old IP address is being assigned to a new user still the chances of accessing the data by some other user is not negligible as the address still exists in the DNS cache and the data

belonging to a particular user may become accessible to some other user violating the privacy of the original user.

2.5 SECURITY CONCERNS WITH THE HYPERVISOR

Cloud Computing rests mainly on the concept of virtualization. In a virtualized world, hypervisor is defined as a controller popularly known as virtual machine manager (VMM) that allows multiple operating systems to be run on a system at a time, providing the resources to each operating system such that they do not interfere with each. As the number of operating systems running on a hardware unit increase, the security issues concerned with those that of new operating systems also need to be considered. Because multiple operating systems would be running on a single hardware platform, it is not possible to keep track of all and hence maintaining all the operating systems secure is difficult. It may happen that a guest system tries to run a malicious code on the host system and bring the system down or take full control of the system and block access to other guest operating systems (Daniel Petri, 2009).

If a hacker is able to get control over the hypervisor, he can make changes to any of the guest operating systems and get control over all the data passing through the hypervisor. Various types of attacks can be launched by targeting different components of the hypervisor (Berman, M., 2009). Based on the learning of how the various components in the hypervisor architecture behave, an advanced cloud protections system can be developed by monitoring the activities of the guest VMs and inter-communication among the various infrastructure components (Flavio Lombardi, Roberto Di Pietro, 2011; Hanqian Wu, et al., 2010).

2.6 DENIAL OF SERVICE ATTACKS

A DoS attack is an attempt to make the services assigned to the authorized users unable to be used by them. In such an attack, the server providing the service is flooded by a large number of requests and hence the service becomes unavailable to the authorized user. Sometimes, when we try to access a site we see that due to overloading of the server with the requests to access the site, we are unable to access the site and observe an error. This happens when the number of requests that can be handled by a server exceeds its capacity. The occurrence of a DoS attack increases bandwidth

consumption besides causing congestion, making certain parts of the clouds inaccessible to the users. Using an Intrusion Detection System (IDS) is the most popular method of defence against this type of attacks (K. Vieira, et al., 2010).

2.7 COOKIE POISONING

It involves changing or modifying the contents of cookie to make unauthorized access to an application or to a webpage. Cookies basically contain the user's identity related credentials and once these cookies are accessible, the content of these cookies can be forged to impersonate an authorized user. This can be avoided either by performing regular cookie cleanup or implementing an encryption scheme for the cookie data (D. Gollmann, 2008).

2.8 BACKDOOR AND DEBUG OPTIONS

A common habit of the developers is to enable the debug option while publishing a web-site. This enables them to make developmental changes in the code and get them implemented in the web-site. Since these debug options facilitate backend entry to the developers, and sometimes these debug options are left enabled unnoticed, this may provide an easy entry to a hacker into the web-site and let him make changes at the web-site level (Zouheir Trabelsi et al., 2004).

2.9 DISTRIBUTED DENIAL OF SERVICE ATTACKS

DDoS may be called an advanced version of DOS in terms of denying the important services running on a server by flooding the destination sever with an umpteen number of packets such that the target server is not able to handle it. In DDoS the attack is relayed from different dynamic networks which have already been compromised unlike DOS. The attackers have the power to control the flow of information by allowing some information available at certain times.

Thus the amount and type of information available for public usage is clearly under the control of the attacker (Ruiping Lua and Kin Choong Yow, 2011). The DDoS attack is run by three functional units: A Master, A Slave and A Victim. Master being the attack launcher is behind all these attacks causing DDoS, Slave is the network which acts like a launch pad for the Master. It provides the platform to the Master to launch the attack on the Victim. Hence it is also called as co-ordinated attack.

Basically a DDoS attack is operational in two stages: the first one being Intrusion phase where the Master tries to compromise less important machines to support in flooding the more important one. The next one is installing DDoS tools and attacking the victim server or machine. Hence, a DDoS attack results in making the service unavailable to the authorized user similar to the way it is done in a DoS attack but different in the way it is launched.

2.10 MALWARE INJECTION ATTACK

Malware which is short for **malicious software** is any software used to disrupt computer operations, gather sensitive information or gain access to private computer including cloud. The malware injection attack has become a major security concern in cloud computing systems. It can be prevented by using File Allocation Table (FAT) system architecture (M. Jensen et al., 2011). From the FAT table, the instance (code or application) that a customer is going to run can be recognized in advance. By comparing the instance with previous ones that had already been executed from the customer's machine, the validity and integrity of the new instance can therefore be determined. Another way to prevent malware injection attacks is to store a hash value on the original service instance's image file (K. Zunnurhain and S. Vrbsky, 2010). By performing an integrity check between the original and new service instance's images, malicious instances can be identified.

For XML signature wrapping attacks on web services, a variety of techniques have been proposed to fix the vulnerability found in XML-based technologies. For example, XML Schema Hardening technique is used to strengthen XML Schema declarations (S. Gajek, M. Jensen, L. Liao, and J. Schwenk, 2009).

3.0 HANDLING EXISTING SECURITY ISSUES IN CLOUD COMPUTING

3.1 Security Testing

Organizations should know how often security procedures are audited and should have information to meet regulatory breach notification requirements. Review the cloud provider's own disaster recovery and be sure it aligns with the requirements of your business enterprise. Business continuity plans should also address compliance limitations.

3.2 Protect data at rest

Data kept in one place can become an easy target Figure 4. Even though it is encrypted it is not always safe; physical security and authentication scheme should be put in place to prevent insider attacks. Organization should perform a personal inspection of cloud service providers and look at the physical structure. Find out who has access to the data center. Are there armed guards, barbed wire, and other security safeguards?

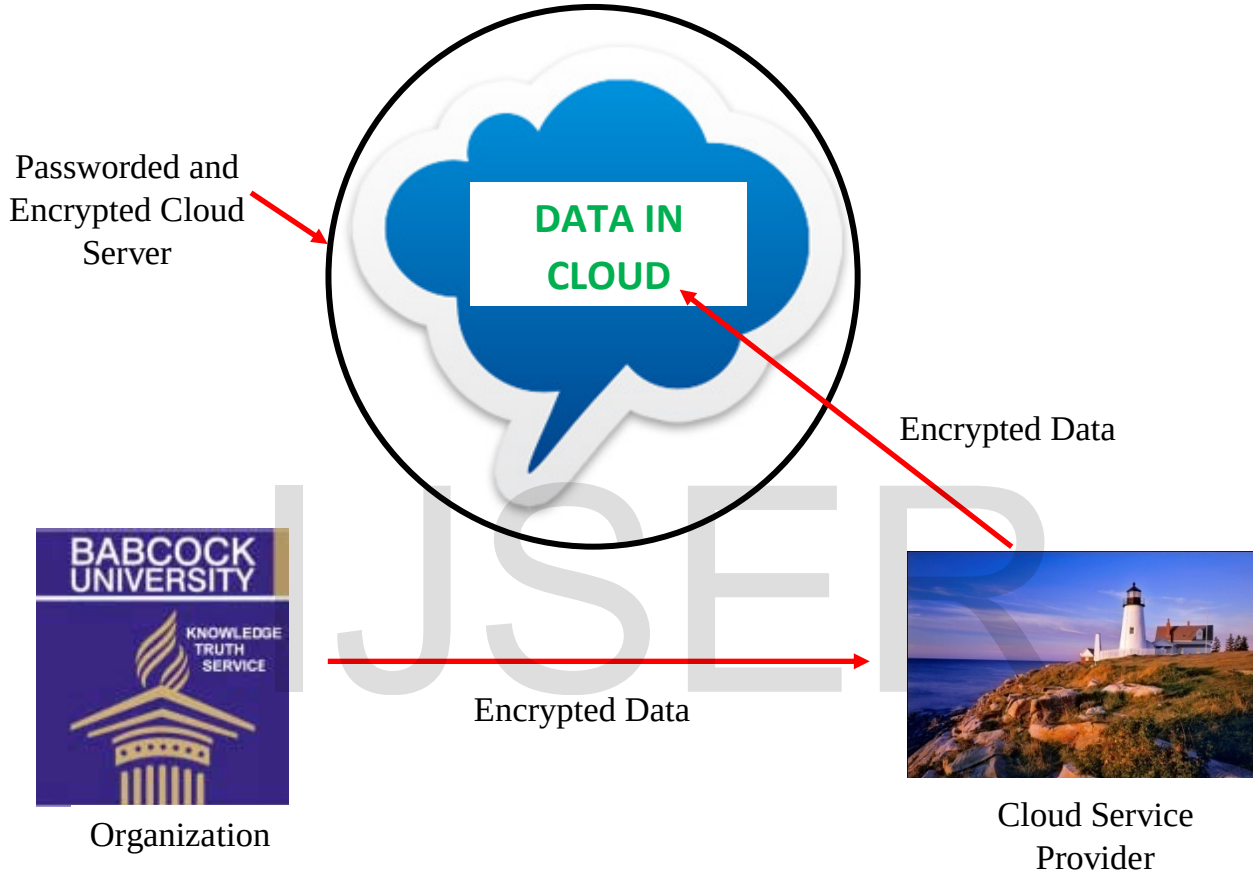

Fig 4. Encrypted Data in the Cloud

3.3 Network Level Security

Networks are classified into many types like: shared and non-shared, public or private, small area or large area networks and each of them have a number of security threats to deal with. To ensure network security following points such as: confidentiality and integrity in the network, proper access control and maintaining security against the external third party threats should be considered while providing network level security. The outdated network level security policies allow only the authorized users to access the specific IP address. With the technological advancement, these security policies have become obsolete as there have been instances when the system's security has been

breached, having accessed the system in the disguise of a trusted user. With the recent technological advancements, it's quite possible to imitate a trusted user and corrupt entire data without even being noticed. Problems associated with the network level security comprise of: DNS attacks, Sniffer attacks, issue of reused IP address, Denial of Service (DoS) and Distributed Denial of Service attacks (DDoS) etc.

3.4 Application Level Security

Application level security refers to the usage of software and hardware resources to provide security to applications such that the attackers are not able to get control over these applications and make desirable changes to their format. Now a days, attacks are launched, being disguised as a trusted user and the system considering them as a trusted user, allow full access to the attacking party and gets victimized. Hence, it is necessary to install higher level of security checks to minimize these risks. The traditional methods to deal with increased security issues have been to develop a task oriented device which can handle a specific task providing greater levels of security with high performance (Scalable Security Solutions, Check Point Open Performance Architecture, Quad-Core Intel Xeon Processors, "Delivering Application-Level Security at Data Centre Performance Levels," Intel Corporation, 2008. http://download.intel.com/netcomms/technologies/security/320923.pdf). The threats to application level security include XSS attacks, Cookie Poisoning, Hidden field manipulation, SQL injection attacks, DoS attacks, Backdoor and Debug Options etc resulting from the unauthorized usage of the applications.

Table 1 summarizes some important security issues in cloud computing and their possible defense mechanisms.

Table 1. Cloud computing threats and suggested defense mechanisms for these threats

S/NO.	SECURITY THREATS	POSSIBLE DEFENSE MECHANISMS
1	Malicious Insiders	Authentication Protect secrets Don't store secrets
2	DNS Attacks	Using Domain System Security Extension (DNSSEC). Authentication Protect secrets Don't store secrets
3	Sniffer Attacks	Encryption Scheme Using Packet Sniffer Program
4	Distributed Denial of Service (DDOS)	Authentication Using Intrusion Detection System like SNORT on virtual machine
5	Cookie Poisoning	Regular cookie clean up
6	Backdoor and Debug Option	Debug option should be left disabled
7	Denial of Service (DoS)	Authentication Using Intrusion Detection System e.g SNORT
8	Malware Injection Attacks	Using File Allocation Table (FAT) Architecture Run with least privilege

4.0 CONCLUSION

Threats in cloud computing is multi-facet and many vulnerability in clouds still exists , hackers continue to exploit these security holes. In order to provide better quality of service to cloud users, security flaws must be identified in order to provide effective defensive mechanism. Auditing of the cloud at regular intervals needs to be done by cloud service providers to safeguard the cloud against external threats. In addition to this, cloud service providers must ensure that all the service level agreements (SLA's) are met and human errors on their part should be minimized to enabling smooth functioning. Finally, threat to cloud computing is too numerous to mention and in diverse form, and it requires different approaches to tackle properly.

REFERENCES

Berman, M. (2009). "Virtualization Audit 101: The top 5 risks and recommendations for protecting your virtual IT," Computer Technology Review, Feb. 4, 2009.http://www.wwpi.com/.

Daniel Petri (2009). "What You Need to Know About Securing Your Virtual Network," Jan. 8, 2009.http://www.petri.co.il/what-you-need-to-know-about-vmware-virtualization-security.htm/.

D. Gollmann (2008). "Securing Web Applications," Information Security Technical Report, vol. 13, issue. 1, 2008, Elsevier Advanced Technology Publications Oxford, UK, DOI: 10.1016/j.istr.2008.02.002.

D. Jamil and H. Zaki (2011). "Security Issues in Cloud Computing and Countermeasures," International Journal of Engineering Science and Technology, Vol. 3 No. 4, pp. 2672-2676, April 2011.

Flavio Lombardi, Roberto Di Pietro (2011). "Secure Virtualization for Cloud Computing," Journal of Network and Computer Applications, vol. 34, issue 4, pp. 1113- 1122, July 2011, Academic Press Ltd. London, UK.

Hanqian Wu, Yi Ding, Winer, C., Li Yao (2010). "Network Security for Virtual Machines in Cloud Computing," 5th Int'l Conference on Computer Sciences and Convergence Information Technology, pp. 18-21, Seoul, Nov. 30-Dec. 2, 2010. ISBN: 978-1-4244-8567-3.

K. Hamlen, M. Kantarcioglu, L. Khan, & B. Thuraisingham. (2010) "Security Issues for Cloud Computing" International Journal of Information Security and Privacy, 4(2), 39-51.

K. Hashizume, David G Rosado, Eduardo Fernández-Medina and Eduardo B Fernandez

(2013). An analysis of security issues for cloud computing. Journal of Internet Services and Applications 2013, 4:5 http://www.jisajournal.com/content/4/1/5

K. Vieira, A. Schulter, C. B. Westphall, and C. M. Westphall (2010). "Intrusion detection techniques for Grid and Cloud Computing Environment," IT Professional, IEEE Computer Society, vol. 12, issue 4, pp. 38-43, 2010.

K. Zunnurhain and S. Vrbsky, "Security Attacks and Solutions in Clouds," 2nd IEEE International Conference on Cloud Computing Technology and Science, Indianapolis, December 2010.

Monjur Ahmed and Mohammad Ashraf Hossain (2014). Cloud Computing and Security issues in the Cloud. International Journal of Network Security & Its Applications (IJNSA), Vol.6, No.1, January 2014 DOI : 10.5121/ijnsa.2014.6103 25

Philip Wik (2011). "Thunderclouds: Managing SOA-Cloud Risk", Service Technology Magazine. 2011-10. Retrieved 2011-21-21.

Ruiping Lua and Kin Choong Yow (2011). "Mitigating DDoS Attacks with Transparent and Intelligent Fast-Flux Swarm Network," IEEE Network, vol. 25, no. 4, pp. 28-33, July-August, 2011.

Scalable Security Solutions, Check Point Open Performance Architecture, Quad-Core Intel Xeon Processors, "Delivering Application-Level Security at Data Centre Performance Levels," Intel Corporation, 2008. http://download.intel.com/netcomms/technologies/security/320923.pdf.

S. O. Kuyoro, A. A. Omotunde, C. Ajaegbu, F. Ibikunle. (2012) Towards building a Secure Cloud Computing Environment. International Journal of Advanced Research in Computer Science, 3(4), 166-171.

S. Gajek, M. Jensen, L. Liao, and J. Schwenk (2009). "Analysis of Signature Wrapping Attacks and Countermeasures," IEEE International Conference on Web Services, pp. 575–582, Miami, Florida, July 2009.

Te-Shun Chou (2013). Security threats on cloud computing vulnerabilities. International Journal of Computer Science & Information Technology (IJCSIT) Vol 5, No 3, June 2013

Y. Ghebghoub, S. Oukid, and O. Boussaid (2013). A Survey on Security Issues and the Existing Solutions in Cloud Computing. *International Journal of Computer and Electrical Engineering, Vol. 5, No. 6, December 2013*

Zouheir Trabelsi, Hamza Rahmani, Kamel Kaouech, Mounir Frikha (2004). "Malicious Sniffing System Detection Platform", Proceedings of the 2004 International Symposium on Applications and the Internet (SAINT'04), pp.201-207, 2004, ISBN: 0-7695-2068-5.