International Journal of Scientific Engineering and Research (IJSER)
www.ijser.in
ISSN (Online): 2347-3878, Impact Factor (2014): 3.05

Mitigating Security Threats in Virtualized Environments

Bashir Aliyu Yauri[1], Joshua Abah[2]

[1] Department of Computer Science and Information Technology, Kebbi State University of Science and Technology Aliero, PMB 1144, Kebbi State, Nigeria

[2] Department of Computer Engineering, University of Maiduguri, PMB 1069, Maiduguri, Borno State, Nigeria

Abstract: ***This paper reviews and provides clarification to the meaning and concept of cloud computing with particular reference to Infrastructure as a Service (IaaS) and its underlying virtualization technologies. The categories of cloud computing and key characteristics of cloud environment are also discussed. A review of virtualization technologies and approaches is presented with key vulnerabilities to security threats and mitigation strategies and countermeasures are also presented. This knowledge is imperative in making virtual Information Technology (IT) environment more secure and robust and can help improve the operational efficiency of Virtual Machines (VMs)in such a manner that organizations can benefit from virtualization technology in particular and the cloud computing systems in general.***

Keywords: Cloud Computing, Hypervisor, Security, Threats, Virtualization, Virtual Machines.

1. Introduction

Hitherto a lot of audience and spectators in the Information Technology (IT) industry tend to see the term "Cloud Computing" as a 'mumbo jumbo'. The lack of agreed upon single working definition of the term revealed this fact. This perception underscores the presentation of this paper which is intended to clear the air by restating the definition of Cloud Computing in a more concise number of ways.

According to [1], Cloud Computing is a model for enabling 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's interaction.

Jack [2] defines Cloud Computing as the ability to access data, software applications, storage, communications capabilities, and computer processing power from the "Cloud" of online resources.

In the context of cloud computing according to [2], the term "Cloud" is used to denote those computing resources that are remotely located. This concept of the Cloud dates back to the early days of the Internet; this makes the cloud computing to also be referred to as Internet Computing by some researchers and technology experts. Cumulus Cloud is used by the Engineers to represent an abstraction of a network whose topology is too complex to be sketched [2].

For better understanding, this paper is organized in the following manner; section one introduced the paper, section two: literature review with clear discussions on the architecture, categorization and characteristics of cloud computing environment, service and deployment models. Sub-section 2.2 focused on virtualization and its approaches, hypervisors and its types, Virtualized Environment and its Associated Security Issues and countermeasures. Section three gives the summary and finally, section four is the conclusion to this paper.

2. Literature Review

To better understand the concept of Cloud Computing; the Architecture, Categorization and Characteristics of Cloud Computing environment, several approaches and models are adopted. Todd in [3] classified Cloud computing into two models namely; the Service Stack model and the Deployment model. Five key characteristics of Cloud environment were also identified.

2.1 Cloud Computing Service Models

The cloud computing service models consists of three stacks of functionalities; Infrastructure as a Service (IaaS**)**, Platform as a Service (PaaS**)** and Software as a Service (SaaS**)**. Like the conventional computer System in which the Users application seats on the Operating System which in turn seats on the Systems' Hardware, in the service stack model the IaaS is the underlying Hardware, on which the PaaS seats on, and the SaaS seats on the Provisioned PaaS[3].This service stack model is as illustrated in Fig. 1.

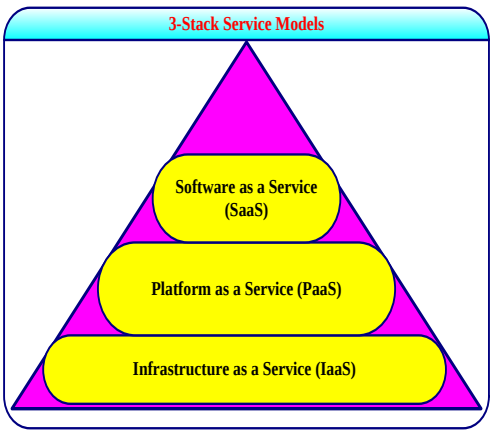

Figure 1: The Three-stack service Model of the Cloud

Licensed Under Creative Commons Attribution CC BY

2.2 Cloud Deployment Models

According to [1] there are four deployment models of the Cloud namely;

1) Private Cloud: the infrastructure is provisioned to be utilized by a single corporate entity
2) Public Cloud: the infrastructure is provisioned for general public utilization
3) Community Cloud: the infrastructure is provisioned to cater for consumers that have shared concerns.
4) Hybrid Cloud: the infrastructure is a mixture of two or more distinct cloud infrastructures (private, public and community) that remain unique entities but, are bound together by standardized or proprietary technology that enables data and application portability.

2.3 Characteristics of Cloud Environment

As stated in[4], [3], [1] the five essential characteristics of Cloud environment are; Measured Service, Elasticity, Resource Pooling, On Demand Self Service and Broad Network Access, these are illustrated in Fig. 2.

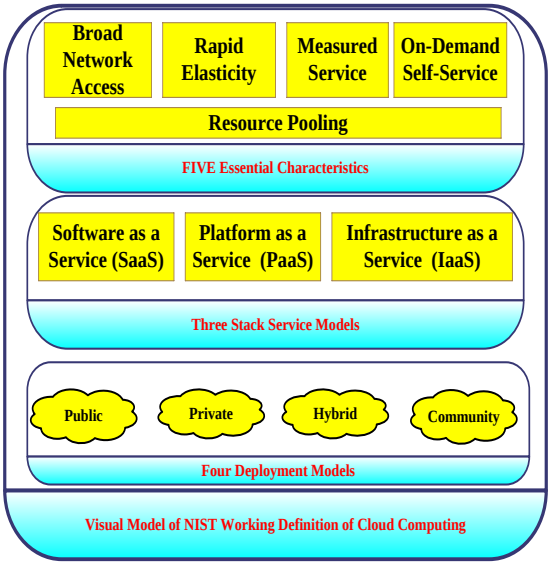

Figure 2: A Visual Model of NIST Working Definition for Cloud Computing [4].

2.3 Virtualization

The concept of virtualization stems from IBM Corporation in the mid-1960s[6] where virtualization at this time was synonymous with *time sharing* systems. As at that time, multiple computer programmers can seat at their designated terminals to access the same underlying hardware that is, the Mainframe Computer without having to wait for a time slice in order to gain access to the peripheral**.** Therefore, virtualization got its root from this concept. Consider Fig. 3 as a typical illustration of a virtual environment.

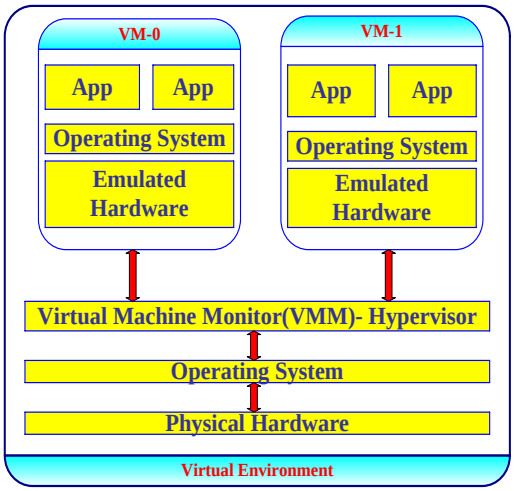

Figure 3: Illustration of a virtual environment [4].

Virtualization technology has today taken the center stage of Cloud Computing. From earlier predictions of Gartner which indicated that by 2012, fifty percent of servers would be virtualized worldwide [12], this has become more realistic today as more and more small to medium scaled businesses are adopting the technology.

In a lucid form, Virtualization is the underlying technology that lays in-between the physical platform or machine and the host Operating System (OS) that is, the interface between the underlying hardware and the OS.This includes the guest OS or Virtual MachineMonitor (VMM) together with the associated applications running on top of it that produces the software abstraction layer (SAL)[4]. The Virtualization Special Interest Group defines virtualization as the logical abstraction of computing resources from physical constraints [5]. One common abstraction is referred to as a virtual machine, or VM, which takes the content of a physical machine and allows it to operate on different physical hardware and/or along with other virtual machines on the same physical hardware. In addition to VMs, virtualization can be performed on many other computing resources, including operating systems, networks, memory and storage [5].

To make virtual IT environments more secure and robust, adequate knowledge of virtualization technologies is mandatory for the installation and audit of virtual systems. Basic audit techniques coupled with proper control over the unique aspects of virtualization technologies can help mitigate the security risks of virtual IT systems. The audit guideline provided can assist in identifying and fixing the weaknesses of virtual IT systems and can help improve the operational efficiency of VMs in such a way that organizations could benefit from virtualization technologies[12].

2.4 Approaches to Virtualization

There are basically three approaches to creating Virtual Systems [7].Although the implementation to these approaches differs, there exist certain traits that are common to all.The three approaches are namely;

1) Full virtualization
2) Para virtualization and
3) Operating System level virtualization.

Licensed Under Creative Commons Attribution CC BY

The physical server is called the *host* while the virtual server is called the *guest*. The *guest* behaves like the *host* but it is being hosted on the physical server meaning that the *guest* runs like any other applications on the physical server (*host).*

To attain full virtualization, special kinds of software known as *Hypervisors* are used. A hypervisor in its specialty has the ability to interact directly with the physical systems resources, such as the CPU, Network channels, I/O devices and Disk spaces. It provides a platform on which the virtual system's OS seats. Multiple Virtual Servers (*guests*) can co-exist on a single physical machine. They Run independently and are even unaware of the existence of one another except when they need to interact or communicate in some sort. The ability of a *host* to host or house multiple *guests* is enabled by the Hypervisor[7].Interestingly, the *guests* need not run the same OSs, the *guests* which are virtual servers can be running different OSs such that one is running UNIX and another Windows [7].

The operation of the Hypervisor as explained by [7] is such that it monitors and manages the physical server's resources. As virtual servers run applications, the hypervisor relays resources from the physical machine to the appropriate virtual server. A fundamental issue of concern here is that some of the physical servers' processing power and resources are consumed by the hypervisor itself, which means that the physical server must reserve some processing power and resources to run the hypervisor application. This hinders the overall server's performance and slows down the amount of resources that could be available to run applications and the virtual servers [7].

Paravirtualization approach is slightly different. Unlike Full virtualization, the guest servers are aware of the existence of each another in Para virtualization technique. A Para virtualization hypervisor requires less processing power to manage the guest's operating systems, as each OS is already aware of the demands the other operating systems are placing on the physical server. The whole system works together as a cohesive entity.

The technique of virtualization is entirely different in Operating System level virtualization technique as it requires no hypervisor at all[7]. In view of the hypervisor, the virtualization capability is integrated as part of the host OS, which performs all the functions of a fully virtualized hypervisor. One major drawback of this approach is that it is required that all guest servers must run on a homogenous OS. Even though each virtual server remains independent from each other, their respective OS cannot be mixed and matched among the different independent running virtual machines [7].

2.5 Hypervisors

Hypervisor is a hardware virtualization technique that allows multiple *guest* OSs to run on a single physical (*host)* system concurrently [7]. The *guest* OSs shares the hardware of the *host* computer, such that each OS appears to have its own processor, memory and other hardware resources. A hypervisor is also known as Virtual Machine Manager or Monitors (VMM)[4]. The term hypervisor stems from IBM in the mid-1950s to refer to software programs distributed with IBM RPQ for the IBM 360/65.

The sharing of the computer's memory became possible as a result of the hypervisor program installed on the computer [4].When installed on the server hardware, the hypervisor controls the guest operating system running on the host machine. The hypervisor is responsible for catering for the needs of the guest operating system and effectively managing it such that the instances of multiple operating systems do not interfere with one another.

2.6 Types of Hypervisors

There are two basic categories of hypervisors namely TypeI and Type II hypervisors. The Type I also known as native or bare-metal hypervisors run directly on the *host* computer's hardware to control the hardware resources and to manage *guest* operating systems.

Examples of Type 1 hypervisors include VMware ESXi, Citrix XenServers and Microsoft Hyper-V hypervisors. Type II also known as hosted hypervisors runs within a formal operating system environment from where it runs as a distinct second layer while the operating system runs as a third layer above the hardware.

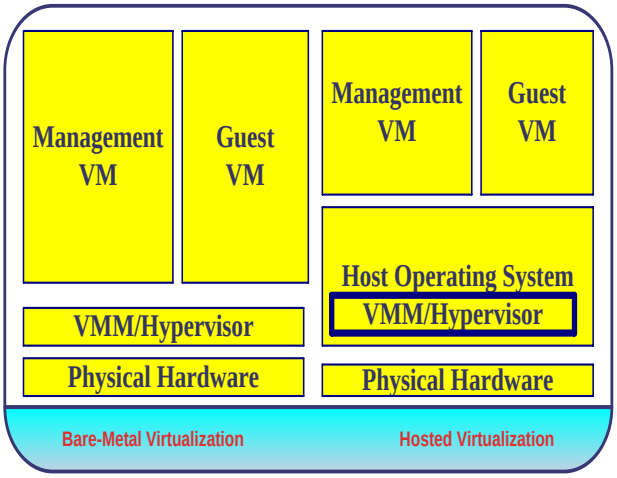

Figure 4: Types of Virtualization Architectures [4].

2.7 Security Issues of Virtualized Environment

One of the greatest set back to the adoption of virtualization technology is the inherent fear of the inherent security risks associated with it as pointed out by several IT industry spectators [8]. Despite the advancement in the way and manner this technology have been deployed over the years, there exist the likelihood that virtual systems are still deployed insecurely[8].

With the increasing adoption of virtualization technologies by different scales of businesses, and the continued existence of this likelihood, security breaches are a potential risk that could impede the rate of adoption in a considerable manner if not properly tackled. According to Kaspersky Lab [8] 69% of companies in the U.S are currently implementing or have already implemented server virtualization, while 46% plan to implement virtual desktop infrastructure and 51% plan to go for virtualized data storage.This shows that the perception of virtual security risks among businesses

Licensed Under Creative Commons Attribution CC BY

worldwide is alarmingly unsound. It is believed that virtual infrastructure has to be treated with the utmost attention in terms of security, and failure to do so could result in significant damage. Therefore, addressing the security risks associated with virtualization technologies will motivate and assures potential businesses in their adoption bid.

2.8 Vulnerabilities of Virtualization Technologies

Cox [9] identified Virtualization technology as a core feature where top Cloud Computing threats occur. He identified four areas of threat to Virtualization, these are reviewed as follows:

1) Trojanized Prebuilt Virtual Machines (VM)/virtual appliances that is, VM containing malicious codes;
2) Improperly Configured Virtual Firewalls or Networking;
3) Improperly Configured Hypervisors and
4) Data leakage through offline images

The need for the building of defense strategies to counter virtualization security risks cannot be over emphasized as the concept though trivial but often overlooked. The hypervisor and its guests are really one big pile of code in one physical box. There is no guarantee that the hypervisor is more secure or less buggy than any other software of comparable size unless evaluated and analyzed based on some criteria like the United State Government Department of Defense (DoD) Trusted Computer System Evaluation Criteria[9].Undertaking critical analysis about security threats on virtual systems can no longer be leveraged upon the security features that used to exist at physical isolation/separation level , as such isolation/separation seized to be on virtual systems[9].

2.8.1 Trojanized Virtual Machines/Virtual Appliances

The top virtual environment security risks that should be addressed are checking the presence of untrusted virtual machines or Trojanized virtual appliances[9].The untrusted VM will manifest itself in public clouds that is multitenant, this scenario open up loophole that is capable of bringing up a malicious system that will attempt to identify proximity related vulnerabilities. The threats are created because the VM is either running on the same hypervisor or within the same cloud, and the cloud provider has created some level of "trust" between the virtual machines that the consumer is not aware of. If those vulnerabilities exist, the likelihood of exploit increases significantly[9].

Malicious virtual appliances (an appliance in this sense is anything that is pre-packaged which is downloadable and could be run as a VM) would be a threat in public or private cloud environments. Since these appliances could be downloaded, installed and used, there is an element of trust bestowed to them. The malicious system would then attempt to find vulnerabilities through its "trust" and exploit them. Once an attacker has a compromised machine in the environment, the intrusion and subsequently the attack will succeed. An instance of this scenario is the Amazon's experience where their Elastic Compute Cloud (EC2) customers were notified that they had identified compromised Amazon Machine Images (AMI) in its community set of AMIs which is stacks of software created to help users deploy servers quickly in EC2. The notification reminded users about the danger of compromised AMIs. Amazon realized that a compromised "appliance" or "build image" provides a trusted foothold in obtaining critical information, such as credentials for further exploit.

Counter Measures

The key to mitigating these threats are to use only verified and tested appliances/images, and have assurance that your cloud provider has properly configured hypervisor and networking configurations that do not create unintended proximity trust while keeping in mind the nature of physical isolation/separation in the virtualized environment and configure systems accordingly. In addition, users of these appliances should verify that a program running on the cloud is executing properly. This amounts to a guarantee that no malicious code is interfering with the programs execution [13].The same system also protects the data used by applications running in the cloud, cryptographically ensuring that the user won't learn anything other than the immediate results of the requested computation.

2.8.2 Improperly Configured Virtual Firewalls or Networking

In the conventional setting, it is the networking team that does all the configurations of networking devices and firewalls. They have the professional knowledge on the intricacies of security and implication of VLANs, tagging, routing, stateful connections, how inbound vs. outbound apply to interfaces etc. This may or may not be true for many host administrators. In a virtual environment, many of the host administrators are now configuring and managing these network security devices. If these devices are not configured correctly, one can have traffic meant for one VM being seen or delivered to another VM or an outside entity.

While tools exist to do this right, it is primarily a "people issue" in that administrators are being asked to manage security devices they do not understand. Overlooking this will amount to security vulnerability that could be exploited by attackers.

Counter Measures

The key to minimizing this security risk in a virtualized environment is to have the network team handle the networking in the virtual environment, even though the virtual networking devices are not physical pieces of networking equipment. Alternatively customers should be provided with sets of configuration offers to select from the one that best suit their purpose. If these are not convenient, then training the host administrator in the security aspects of network configurations is the next best mitigation strategy.

2.8.3 Improperly Configured Hypervisors

The security of a hypervised environment is directly linked to the security of the hypervisor itself; any unauthorized access to the hypervisor compromises the environment. The main threat here is in access rights, permissions and privileges; a lack of control to limit who can gain access, and once in, what permissions they have to do what and to what extent. These are pretty straightforward threats in that allowing unrestricted access to hypervisors, especially one that can be reached from an untrusted network (e.g., the Internet) increases the threat of attacks. Secondly, if restrictions are not placed as to who and what legitimate

Licensed Under Creative Commons Attribution CC BY

users can access once they authenticate, it will become a vulnerability that could be exploited to carry out attacks.
The first vulnerability, according to [9]is easy to deal with by restricting what systems can get access to the management functions (GUI, API, login, etc.). The second is not quite as easy, because a robust access control mechanism to allow access/management of the user's VMs (workloads), but not to the host is needed. Furthermore, it is likely that one want to allow certain operations on the host to some users, but not all operations. The underlying access control mechanism must be able to support this. Since many cloud providers (e.g., Amazon) are building hypervisors almost from the ground up, getting the necessary access control mechanisms is difficult.

Counter Measure
The key to minimizing this threat is the use of a more granular role-based access control mechanisms to the hypervisor and management applications [9].

2.8.4 Data Leakage through Offline Images
When guest images are suspended, unlike physical systems that would need physical access to pull data out of memory, the memory "footprint" now is in a file, and for all intents, searchable. Take an application securing Social Security or credit card numbers for instance, the VM may be solid and secured, however, when the system is suspended, any information put in memory is likely not protected and assumed to be volatile. The problem arises when the image suspends and writes that memory to disk. Also, with migration, information states that would never have existed before now exist which must also be protected [9].

Counter Measures
The nice thing about virtual security is that if there is a good security program in general, there will likely be a secure virtual environment as well. The fact is that if old system administration practices (as they relate to security) are applied to virtual environments, there will be better chances to minimizing virtualization security risks and a secure environment [9].

Although Malware for hypervisors are rare, they could have a significant effect on the trustworthiness of a system [10]. For hypervisor malware to increase in occurrence, it is likely that criminals would need to find ways to more easily monetize attacks on the hypervisors [10]. However, given the high level of access that could be gained by compromising a hypervisor, these types of attacks is one of several virtualization security concerns that are likely to increase in occurrence and could cause significant disruptions, such as denial-of-service (DoS) attacks or the compromise of sensitive data.

Also, some hypervisors are vulnerable to malware attacks because of the platform they run on. Microsoft Hyper-V, Virtual PC and certain versions of VMware, run on top of Windows, and other hypervisors are Linux-based systems. The Linux or Windows server components could be attacked to compromise the security of the virtual infrastructure[10] but as we all know, Linux systems provides better security than Windows platforms.

Apart from the methods specified by researchers at North Carolina State University and the IBM, new approaches exists that could be used to prevent malware from infecting hypervisors [10]. These approaches include isolating the management interfaces of, and connections to the hypervisor to only the systems that need access, not running un-trusted code on the hypervisor, such as software not provided by the hypervisor vendor and keeping the hypervisor software up to date. This excludes security measures applicable to the guest OSs in the virtual infrastructure to ensure the guests cannot be used to attack the hypervisor.

2.9 New Generation Fire Walls as a Countermeasure

The list of the various threats/risks associated to this age long technology of virtualization is unending therefore there is no single solution to mitigate threats. However the use of New Generation Fire Walls (NGFW) is proposed as against the traditional firewall, which does not give a high level of granularity to the security controls.

The IT Project Center[11] gave the operational framework of NGFW. Firewalls are like bouncers or doormen. They stand at the entrance to coordinate network traffics, deciding what traffic comes in or out and what traffic gets prevented from doing so based on a set of rules. The traditional firewall uses port-based rules, blocking traffic to most ports, but allowing traffic in (and out) to specific ports for specific types of traffic. This approach was fine in the past, but the rise of Web 2.0 applications has highlighted a problem with port-based firewalling. Many Web applications especially social networks such as Facebook for example, run over port 80 (http) or port 443 (https). To block employees from using Facebook applications, ports 80 and 443 have to be blocked. And blocking ports 80 and 443 would not only block access to Facebook application but will also block the entire Web.

A next generation firewall provides far greater granular control over traffic coming in and out of the network. It provides standard firewall capabilities such as packet filtering, NAT, stateful protocol inspection and VPN capabilities, but in addition it offers application awareness with full stack visibility. This implies that a next generation firewall gives the capability to inspect exactly which applications are being used on the network. This may include previously undetected, bandwidth intensiveapplications such as streaming video and audio services and even peer-to-peer file sharing applications, which may be illegal.

More importantly, the next generation firewall also provides control to application usage by identifying the applications and enforcing network security policy at the application layer independent of port and protocol. For instance, one can

1) Allow Facebook but not Facebook applications such as Candy Crush Saga
2) Allow Skype for voice-over-IP but not for file sharing
3) Allow webmail attachment downloads but not attachment uploads
4) Simply apply application blacklists or whitelists

Next generation firewalls can also use external intelligence sources such as reputation systems to enhance blocking

Licensed Under Creative Commons Attribution CC BY

decisions. Most next generation firewalls integrate with corporate directories such as Active Directory which help one to apply firewall rules to some groups of employees but not to others. For example, one can create a rule allowing sales and marketing staff to use a certain set of Web applications, while contractors or temporary staff can only use a subset of those. At the same time, one can give board members unfettered Internet access.

Next generation firewalls typically go beyond firewall functionalities by including a range of other security features. These can usually be enabled or disabled as appropriate. Some next generation firewalls include all the functionalities in the base price, while others offer a more flexible approach by including the basic firewall functionalities in the base price with additional functionalities available for an added license fee.

In this respect next generation firewalls share many characteristics with all-in-one security appliances, often called unified threat management devices or security gateways. The key features that distinguishes a next generation firewall apart from the application awareness is the integration of all these security functions into the firewall core, so that they can all be carried out at high speed in a single pass as traffic flows through the firewall.

By contrast, unified threat management devices generally combine a number of security functions in one box, with software that integrates the management of these functions to a greater or lesser extent. But each of these security functions is performed separately and in series, leading to performance that is generally lower than a true next generation firewall.Even so, enabling additional features such as IPS or even malware scanning in a next generation firewall can make a significant difference to the throughput capability of the device. A next generation firewall that is rated as having a maximum 1Gbps throughput may only be able to handle 500Mbps or less when all the security services are enabled.

Other additional security features that next generation firewalls offers include:

Intrusion Prevention
Early next generation firewalls offered fairly rudimentary IPS capabilities, but more recent ones generally offer IPS on a par with standalone solutions.

Anti-malware Scanning
This involves centralized scanning of all traffic coming in to the network. This should not be seen as an alternative to endpoint anti-virus software; however, malware that passes undetected through the firewall may be spotted by endpoint software during a routine scan a few days later once anti-virus signatures have been updated to detect that particular piece of malware.

Secured Socket Layer (SSL) Inspection
Encrypted traffic can be a blind spot for many organizations. Next generation firewalls solve this problem using homomorphic cryptography and by issuing self-signed certificates to endpoints. By this, they can then work as a "man in the middle", intercepting SSL transactions, decrypting them, inspecting the traffic and then re-encrypting them and sending them on to their destination[11].

3. Summary

Virtualization is the underlying technology of Cloud Computing which has given the small scale firms in the IT industry the opportunity to rapidly setup and grow and relieving them of the burden of infrastructural acquisition as utilization of this pool of resources is measured, metered and paid for on a pay as you use basis. With the various security risks envisaged in the technology, it is believed by IT Professionals that the security risks in a virtual environment are significantly lower than those for physical infrastructure. While many are still skeptical about the adoption of the cloud system for fear of threats and attacks, it is noteworthy that the perceived vulnerabilities of virtualized environments could be mitigated with proper security measures and controls.

4. Conclusion

Cloud computing has come to stay as the computing technology of the next century with virtualization as its realization tool. In this paper, cloud computing with its underlying virtualization technology has been reviewed and possible security vulnerabilities that present threats in virtualized environment with countermeasures have been identified and discussed. The pace at which virtualization technology is being embraced by organizations can be a cause of concern if robust security features are not applied to the virtual IT systems. To make virtual IT environments more secure and robust, adequate knowledge of virtualization technology is mandatory for the installation and audit of virtual systems. Basic audit techniques coupled with proper control over the unique aspects of virtualization technology can help mitigate the security risks of virtual IT systems. The audit guideline provided can assist in identifying and fixing the weaknesses of virtual IT systems and can help improve the operational efficiency of VMs so that organizations benefit from virtualization technology optimally in trust without perceived threats of security risks.

References

[1] NIST (2014). *Cloud computing program*. Retrieved September 06, 2014from http://www.nist.gov/itl/cloud/
[2] Jack, S. (2011). What is cloud computing? *Dynasis*. Retrieved September 10, 2014 from http://www.dynasis.com/wp-content/uploads/2011/08/dynasis_what_is_cloud_computing.pdf
[3] Todd, S. (2012). An introduction to securing a cloud environment. *SANS Institute*
[4] Fatma, B., Yeun C. Y., Mohamed J. Z., (2012). State-of-the-art of virtualization, its security threats and deployment models. IJISR , 2, (3/4), 335-343. Retrieved from http://www.infonomics-society.org/IJISR/Paper%201.pdf
[5] Virtualization Special Interest Group (2011). Information supplement: Pcidss virtualization guidelines.*PCI Security Standards Council*

Licensed Under Creative Commons Attribution CC BY

[6] Cory, J. (2014). What does hypervisor mean? *Techopedia*. Retrieved June 10, 2014from http://www.techopedia.com/definition/4790/hypervisor
[7] Strickland, J. (2008). How server virtualization works. *HowStuffWorks*. Retrieved June 21, 2014 from http://computer.howstuffworks.com/server-virtualization.htm
[8] Jennifer, L. (2013).Managing security risks in a virtual environment. *Lumension*. Retrieved September23, 2014 from http://blog.lumension.com/6413/managing-security-risks-in-a-virtual environment/
[9] Philip, C. (2011). Top virtualization security risks and how to prevent them. pp 3-6. Retrieved from
[10] http:// www.searchsecurity.com
[11] Nick, L. (2010). Virtualization security concerns: the threats of hypervisor malware. Retrieved June 20, 2014 from http://searchsecurity.techtarget.com/answer/Virtualization-security-concerns-The-threat-of-hypervisor-malware
[12] IT Project Center (2013). Introduction to new generation firewalls. *QuinStreet*. Retrieved April 22, 2014 from http://www.eweek.com/project-center/next-generation-firewall
[13] Abhik, C., Solms, S., H., Dipanwita, C., (2011). Auditing security risks in virtual IT systems. ISACA Journal Vol1, pp1-10. Retrieved September 30, 2014 from http://www.isaca.org/Journal/Past-Issues/2011/Volume-1/Documents/jpdf11v1-auditing-security-risks.pdf
[14] Massachusetts Institute of Technology Science Daily(2013). New system allows cloud customers to detect program-tampering.Retrieved October 27, 2014 from www.sciencedaily.com/releases/2013/09/130911114737.htm

Author Profile

Joshua Abah received a B.Tech (Hons) in Computer Science from Abubakar Tafawa Balewa University Bauchi, Nigeria in 2005, and MSc. in Computer Science from Bayero University Kano, Nigeria in 2011. He is at present a Ph.D fellow in Computer Science at the Federal University of Technology Minna, Nigeria. He is currently working in the academia where he has been for the past eight years. His research interests include Mobile Cloud Computing Security, Network Security, Cloud Computing, Virtualization, Scheduling Algorithms, QoS and Computer Education. He has published many journals in both national and international scene and has authored and co-authored many textbooks.

Bashir Aliyu Yauri Obtained a B.Sc. degree in Computer Science from Usmanu Danfodiyo University Sokoto, Nigeria in 1999, and M.Sc. in Computer Science from Bayero University Kano, Nigeria in 2011. He has a decade of IT professional experience in the IT Division in the Nigerian Banking Sector. Currently a Lecturer at the Department of Computer Science and Information Technology, Kebbi State University of Science and Technology Aliero, Nigeria. His current research interests include; Networking, security of virtualized systems, cloud computing and cloud security.

Licensed Under Creative Commons Attribution CC BY