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*

[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.