CLOUD COMPUTING AND SECURITY: VULNERABILITY ANALYSIS AND PREVENTIVE SOLUTIONS

Musa Ahmed Zayyad

Department of Computer Studies, Hassan Usman Katsina Polytechnic, Katsina
E-mail: zayyad19@yahoo.com +2348063440008(Nigeria) and +905428726723(Cyprus).

Abstract
In the past few decades, Cloud Computing has risen from relatively unknown field to become one of the most popular and fastest growing segments of the Information and Communication Technology (ICT) industry. Its success and popularity lies heavily on the fact that Internet has become part of people's daily life, enabling individuals and organizations to become enlightened about the benefits that Cloud Computing could provide. Everyday more and more information and data of people are being deployed on the cloud, services and resources are also placed in the cloud system by cloud service providers, which are then accessed by people who have access to the internet at a minimal cost or free in some cases. However, despite the publicity and successes surrounding the cloud computing technology, individuals and organizations are still reluctant to establish their businesses and personal data in the cloud system. The reason being that security is one of the main issues that reduce the growth of cloud computing as well as complications with data privacy and data protection continues to affect the system. This paper describes the security threats involved in using the cloud computing as a web service and how these threats can be overcome.
Keywords: Cloud computing, nodes, security, system, virtualization

Introduction

Cloud computing has risen from relatively unknown field to become one of the most popular and fastest growing segment of the Information and Communication Technology (ICT) sector. Its success and popularity lies heavily on the fact that Internet has become ubiquitous, this enable individuals and organizations to become enlightened about the benefits that cloud computing could provide (Wyld, 2009). Everyday more and more information and data of people are being deployed on the cloud, services and resources are also placed in the cloud system by cloud service providers (Song *et al*, 2011), which are then accessed by people who have access to the internet at a minimal cost or free in some cases.

Farhan & Sajjad (2011) define cloud computing as accessing a set of services and resources through the use of internet. That means cloud computing can simply be regarded as internet computing. Although, a question may be asked; what is the reason behind naming the system cloud computing? According to Sakr (2010) *"The Cloud means the Datacenter hardware and software that the service providers use to offer the computing resources and services, while cloud computing represents both the 'cloud' and the services provided"*.

Kim et al (2009), describe cloud computing as a service that enables users to use a Web browser to receive computing services by connecting to the Internet. The users would normally pay for the services they actually use. Due to the popularity of the internet, it appears that a wide implementation of cloud computing in the foreseeable future is unavoidable, and its adoption will bring about a massive change in the pricing and distribution practices for both software and hardware.

However, despite the publicity and successes surrounding the cloud computing technology, individuals and enterprises are still reluctant to rely heavily on the cloud system. The reason being that security is the major threat that reduces the growth of cloud computing as well as complications with data privacy and data protection continues to affect the system (Nabil, 2010).

Literature review

Vouk (2008) describes cloud computing as a technology that lets you use files and applications over the internet without physically having access to the computing resources. Cloud computing enables consumers to access resources online through the use of internet, from wherever and at any time, without having to worry about the technical or physical management and maintenance issues of the original resources.

Buyya et al., (2008) also describe cloud computing as a dynamic, cost-effective and proven delivery platform for providing business or consumer IT services over the Internet. The cloud technology provides access to computing resources, such as networks, servers, storage, applications and services, which can be rapidly provisioned and released with minimal management effort or service provider interaction.

Won (2009) defines cloud computing as a system that enable access to data, information, programs, files and 3rd party resources and services that are hosted by millions of web servers through the use of internet via web browsers. He opined that these services and resources are being used at a very minimal cost or sometimes even free.

Cloud computing is considered as the most significant IT development in recent years, presently it has brought many changes to IT in general and how IT-enabled services are used all over the world (Zissis & Lekkas, 2010). Cloud computing has successfully brought a new concept to computing in general. From the way enterprise businesses run their organizations, and the manner in which individuals use their personal computers to access services over the internet (Reddy *et al*., 2009). The emergence of Cloud Computing technology has changed the way IT services are developed, deployed, used, maintained, and paid for (Marston *et al*, 2010). Some of the advantages offered by cloud computing includes the ability of companies and organizations to increase their capacities or add their capabilities dynamically without having to invest in new infrastructure, or train new personnel, or purchasing new licensing software. In other words, cloud computing has greatly

reduced the cost of doing business (Subashini & Kavitha, 2010).

Despite what some researchers and IT providers pointed out, the significant advantages of Cloud Computing solution and the impressive business values companies can accomplish cannot be over-emphasized, other researchers has also forecasted a decline in the adoption of the Cloud solution because of its possible risks (Benlian & Hess, 2011). Due to the numerous opportunities offered by Cloud Computing system, it has become one of the fastest growing segments of the IT industry, and has attracted so many interests from both the academia and analyst. Enterprises have been set to lower the computing rates and started to bring IT operations together and use virtualization technologies (Schmidt, *et al*., 2010).

Cloud Computing is one of the new technology that helps for the goodness of the enterprises for which it demands to take it to a new level that will permit them to lower the costs to a greater extent through improved utilization, reduced administration and infrastructure cost and faster deployment cycles (Anwar & Albazzaz, 2013). Cloud Computing can best be described as both a platform and type of application. As a platform, it provides access to servers; also these servers can be physical machines or virtual machines. Cloud Computing provides applications that can be accessible through the Internet, for this reason large Datacenters and powerful servers are used to host web applications and web services (Khajeh-Hosseini *et al*., 2010). Cloud computing offer three different services, namely SaaS (Software as a Service), IaaS (Infrastructure as a Service) and PaaS (Platform as a Service). These services are shown in the diagram below (Lombardi & Roberto, 2010):
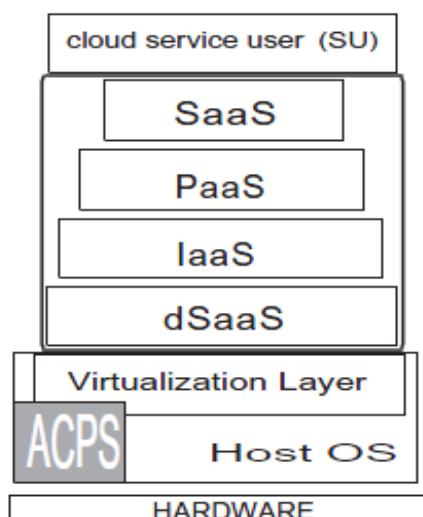
Fig 1: Cloud computing services

The diagram above shows the types of services that are provided by the cloud computing system; SaaS provides access to software programs through the internet in a form of service. IaaS provides virtual hardware with no software stack. PaaS provides virtualized servers, OS, and applications. The dSaaS delivers basic storage capability over the network. Advanced Cloud Protection System (ACPS) is a system that increases the security of cloud nodes, which transparently monitors cloud components in order to recover from attacks.

Security threats in cloud computing
Security is the major stumbling block in cloud computing technology, individuals and organizations are still skeptical about relying heavily on the cloud system (Yu & Zhu, 2012). Although, cloud computing system is, in principle, subject to all or most of the security threats that exist in every single subject in computing, such as:
- Account hacking
- Virus attack
- Data loss
- Data leakage
- Insecure interfaces and APIs
- Malicious insiders
- User's Authentication
- Wrong usage of cloud computing services
- Hijacking of sessions while accessing data

Solution to cloud computing security threats

The main issue in the adoption of cloud computing system is security; many analysts and experts have carried out a great deal of research in acknowledgement of the security threats that are inherent in the cloud system. However, basic network security is not effective at the moment, because even with modern protocols, hackers and worms can attack a system and create havoc within a few hours (Zhifeng & Yang, 2013). Within the Cloud system, the prospects for attack are many, this implies that architectures and applications must be protected and security must be appropriate.

The following are the solutions to some of the cloud computing security threats outlined above:
i. Account hacking
    The threat posed by hackers has always been a serious concern in the field of Information and Communication Technology (ICT). Hackers are always on the lookout for weak systems in order to attack. Therefore, both the loud service providers and the cloud users should be aware of the activities of hackers in order to take the necessary measurement for their own safety.
ii. VM-Level attacks
    The cloud computing system is designed based on virtual machine technology. In order to implement the cloud system, a virtual machine monitor known as hypervisor is used, which sometimes affects the performance of the system.

Examples of hypervisor include Microsoft virtual PC, Xen, VMWare, etc. This type of security threat can be overcome by monitoring the virtual machine through IDS (Instruction Detection System).

iii. Data loss or leakages

Data may be lost due to unforeseen circumstances, such as weak authentication, insecure encryption key and unauthorized access. This security threat can be overcome by strong authentication, making the encryption key more secure and safe from unauthorized access.

iv. Insecure interfaces and APIs

Interaction with the cloud computing system is through APIs (Application Program Interfaces). However, if the software is weak, it may expose organizations to various security threats, such as unauthorized access, and stealing of user's passwords. This security threat can be overcome by implementing strong authentication process and access controls.

v. Wrong usage of cloud computing services

This security threat is as a result of poor registration system in the cloud computing environment. Usually people use their credit card to register and make use of the service, this makes the system to be vulnerable to attacks by hackers, spammers and other criminals who are always on the lookout for weak systems. This threat can be overcome by making the registration to be very strict and more vigilant.

vi. Malicious insiders

This security threat arises due to lack of knowledge about cloud service provider programs and processes. Enterprises should have more information about the cloud vendors and their guidelines. This would enable the users to follow strict instructions outlined by the suppliers.

Conclusion

In conclusion, this paper describes the security threats faced by the cloud computing technology and proffer solutions to the threats in a bid to make it more safe and reliable. Although there are numerous advantages in using the cloud computing system, there are yet many practical problems that are yet to be resolved. Cloud computing is a technology with immense implications not only for Internet services but also for the ICT sector as a whole. There are still many researches going on in a bid to make it safer.

References

Anwar, J., & Albazzaz, J. M. (2013). Cloud Computing: an overview. *International Journal of Advanced Research in Computer and Communication Engineering* (IJARCCE), 2(9), 3522-3525.

Benlian, A. & Hess, T. (2011). Opportunities and risks of software-as-a-service: Findings from a survey of IT executives. *Journal of Decision Support Systems* 52(1), 232-246.

Buyya, R., Yeo, C. S., Venugopal, S., Broberg, J., & Brandic, I. (2008). Cloud computing and emerging IT platforms: Vision, hype and reality for delivering computing as the 5th utility. *Journal of Future Generation Computer Systems* (FGCS), 25(2009), 599-616.

Farhan, B. S., & Sajjad, H. (2011). "Security Threats in Cloud Computing" 6th International Conference on Internet Technology and Secured Transactions, 214 – 219, Abu Dhabi, UAE.

Khajeh-Hosseini, A., Greenwood, D., & Sommerville, I. (2010). Cloud Migration: A Case Study of Migrating an Enterprise IT System to IaaS. Symposium on Cloud Computing (SOCC 2010), Submitted to IEEE CLOUD 2010.

Kim, W., Kim, S. D., Lee, E., & Lee, S. (2009). Adoption Issues for Cloud Computing. 7th International Conference on Advances in Mobile Computing and Multimedia, 2-5.

Lombardi, F., & Roberto, D. (2010). Secure virtualization for cloud computing. *Journal of Network and Computer Applications* (JNCA), 34(2011), 1113-1122.

Marston, S., Li, Z., Bandyopadhyay, S., Zhang, J., & Ghalsasi, A. (2010). Cloud Computing – The business perspective. *Journal of Decision Support Systems* (DSS), 51, 176 – 189.

Nabil, S. (2010). Cloud Computing for Education: A new dawn? *International Journal of Information Management*, 30(2010), 109-116.

Reddy, B.K., Paturi, R.V. & Rakshit, A. (2009). Cloud Security Issues. IEEE International Conference on Services Computing, Bangalore,India. 517-520.

Sakr, M. F. (2010), "Introduction to Cloud Computing" Carnegie Mellon, Doha Qatar.

Schmidt, M., Fallenbeck, N., Smith, M. & Freisleben, B. (2010). Efficient Distribution of Virtual Machines for Cloud Computing. 18th Euromicro Conference on Parallel, Distributed and Network-based Processing Pisa Italy. 567-574.

Song, J., Yao, J., & Wu, C. (2011). "Cloud Computing and its Key Techniques", International Conference on Electronic & Mechanical Engineering and Information Technology Heilongjiang, China 320-324. 12th – 14th August, 2011.

Subashini, S., & Kavitha, V. (2010). A survey on security issues in service delivery models of cloud computing. *Journal of Network and Computer Applications* (JNCA), 34(2011), 1-11.

Vouk, M. A. (2008). Cloud computing – issues, research and implementations, *Journal of Computing and Information Technology* 16 (4), 235–246.

Won, K. (2009). Cloud Computing: Today and Tomorrow. *Journal of Object Technology* (JOT), 8(1), 65-72.

Wyld, D.C. (2009). The Utility of Cloud Computing as a New Pricing and Consumption Model for Information Technology. *International Journal of Database Management Systems* (IJDMS), 1(1).

Yu, T. & Zhu, Y. (2012). "Research on Cloud Computing and Security", 11th International Symposium on Distributed Computing and Applications to Business, Engineering & Science, 314-316.

Zhifeng, X., & Xiao, Y. (2013). Security and privacy in cloud computing. IEEE Communications Surveys & Tutorials, 15(2), 843-859.

Zissis, D. & Lekkas, D. (2010). Addressing Cloud Computing Security Issues. *International Journal of Future Generation Computer Systems* (JFGCS), 28(2012), 583-592.