East African Scholars Journal of Engineering and Computer Sciences
Abbreviated Key Title: East African Scholars J Eng Comput Sci
ISSN: 2617-4480 (Print) & ISSN: 2663-0346 (Online)
Published By East African Scholars Publisher, Kenya

Volume-3 | Issue-5 | May-2020 | DOI: 10.36349/easjecs.2020.v03i05.09

Research Article

Cloud-Based Software Engineering, Network Security, and Performance Evaluation

Dr. Ogala, Emmanuel*[1]& Rose O. Akor[2]

[1]Federal University of Agriculture, Makurdi, Department of Maths/ Stat/ Computer Science, Benue State, Nigeria
[2]Kogi State University, Anyigba.Kogi State, Nigeria

Article History
Received: 08.04.2020
Accepted: 25.05.2020
Published: 30.05.2020

Journal homepage:
https://www.easpublisher.com/easjecs

Quick Response Code

Abstract: The cloud computing technology has improved the traditional data usage in our generation, which has more computing power, analysis capabilities of software engineering and storage capabilities, the Internet technology and computer technology to effectively combine the transformation of computer information technology in software engineering, The security of data gendering need more attention on daily bases. This paper systematically explains the concept of cloud-based software engineering, its security and general performance evaluation using the concept of network speed analysis, the uptime and downtime in relation to the native engineering, which is outside the scope of internet access.

Keywords: Ogala, Cloud, Computing Technology, Security, Software Engineering., Data and Network Performance.

INTRODUCTION

The IT Industry and its commentators are abuzz with the phrase "cloud computing" and most of people still have no idea what this latest terminology means or what technology are they referring to. This section starts by addressing the question – "what is cloud computing, and provides an understanding of the technology". Then out of the hundreds of definitions of cloud computing, some widely accepted ones are presented. Cloud computing is then related to technologies that have been around for ages. Finally, it is explained that cloud computing is the same old networking technology, but with the integration to the Internet a lot can be done differently with wider implications. So, what is cloud computing?

Cloud security refers to set of policies interims of technologies, applications, and controls utilized in order to protect virtualized internet protocol (IP) for data, applications, services, and the associated infrastructure of cloud computing environs. It is a sub-domain of computer security in data manipulation in the cloud…

"The most widely used definition of the cloud computing model is introduced by NIST (Almorsy, M. *et al.*, 2016) as "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 interaction."

Cloud security computing is an Internet-based service that is related to the increase, use and delivery models that are generally used for data manipulation over the Internet to dynamically scale and provide virtual resources. Cloud security computing is more capable than traditional computer computing in soft ware engineering, and it reaches 12 trillion operations per second. Therefore, it is widely used to predict weather software engineering changes, simulate nuclear explosions and market trends of data usage over the cloud. The need of software engineering in cloud security arises because of higher rate of demand in user requirements and environment on which the software is working with in the data application in cloud. Software engineering is so important because software is needed in every area industry, Education for example undergraduate result computation and in every business. It becomes more important in our dally activities. The most important aspect of the software engineering are:

a) Reduces complexity
b) To minimize software cost
c) To decrease time
d) Handling big projects
e) Reliable software and
f) Effeteness

Therefore the role of software engineering cannot be over emphasis over cloud security in computing environment. Cloud computing has the capacity to solves some of the major challenges in the software engineering of large or medium software systems. With the look of infinite capacity with the ability to scale at the same speed as the traffic changes, the performance of software engineering will become redundant. Many industries might think that the need for future plans for developing a new software application, to optimize, or to worry about efficient operation. The aim of this paper argues that cloud computing is an area where performance of software engineering must be applied and customized.

Cloud Network Security Issues

The development of computer, internet and other mobile devices, the issues of cloud network security is becoming more important. In recent years across the globe, many cyber security incidents have been launched by international hacker in industries and cyber terrorist organizations. In June 2014, the information of 10,000 users of internet in Nigeria loss a lot of economic value as result of cloud network hackers.

Taxpayers in the United States were stolen, resulting in a direct economic loss of 50 million U.S. dollars. In June, the Japanese government's pension information system was hacked, revealing 1.25 million personal information; in October, the British telecom operator talk was hacked, resulting in the disclosure of 4 million user information. This shows that computer network security is related to personal, business, social and national information security. At present, under the wave of Internet economy, various computer software and mobile phone APPs emerge in an endless stream, and the speed of upgrading is very fast. Some of these software and mobile phone APP itself has many flaws but it is recommended to install and use. Therefore, in the course of using the network security problems often appear (Zhou, Y., & Tang, Y. 2018, April).

The most common issue for many industries is that even when they have the best cyber security solutions, they might not have enough man power in place to properly manage those solutions. When this happens it course cloud security challenges alerts and this may get missed, and successful attacks landing may not be eliminated in time to minimize damage on time. Therefore there is a need for enough internal IT (information Technology) cloud security team in conjunction with software engineer to manage any organization data flow over the cloud.

Cloud Security Performance Evaluation

Cloud security computing resources must be well-matched, high performance and authoritative. High performance is one of the cloud security network load advantages which must be suitable for each service, Performance evaluation of services and everything related to cloud- base security network have an influence on users and service providers. Hence, performance evaluation for cloud base security network providers and users is important. The following method can be use for performance and evaluation of cloud base security network.

1. Evaluation based on criteria and characteristics
2. Evaluation based on simulation

A different type of evaluating cloud base security network performance can be classified with three layers of cloud services evaluation.

In software engineering evaluation assurance and performance testing is in general practice performed to determine a system capability in terms of responsiveness, speed, reliability and stability under a particular workload on a network. It can also use to investigate, the measure, the validation or to verify other evaluation attributes of the system, such as scalability, resource usage and reliability. Performance evaluation is a subset of performance software engineering, in cloud security practice which strives to build performance standards into the implementation, design and architecture of a computer system. It is important to specify performance specifications (requirements) and input them in any performance evaluation plan. In an ideal world, this is done during the requirements development phase of any project development, before any design effort.

Though, performance evaluation is normally not performed against a specification; for example. No one will have spoken what the maximum satisfactory response time for a given populace of users should be. Performance evaluation is frequently used as fraction of the process of performance outline tuning. The idea is to recognize the "the security performance” here is inevitably a part of the system which, if it is made to react faster, will result in the overall system running quicker. It is sometimes a difficult task to recognize which part of the system represents this important path, and some examination tools include (or can have add-ons that provide) instrument that runs on the server (agents in the cloud) and reports operation times, database access times, security network overhead, and other server monitors, which can be analyzed jointly with the raw performance figures. Without such instrumentation one might have crouched over some operating system Task Manager at the server to see how much the central processing unit load the performance evaluation are generating (for example Windows system is under evaluation).

Performance evaluation can be performed all over the web and even worked in different parts of the country, since the response times of cloud security itself vary from one region to another. It can evaluate in-house though routers would then need to be configured to bring in the cover that would characteristically occur on public networks.

As a result, consumers must understand the division of responsibilities and trust that the CSP meets their responsibilities. Based on our literature searches and analysis efforts, the following list of cloud-unique and shared cloud/on-premise vulnerabilities and threats were identified. The figure below also details the threat picture for cloud computing platforms Timothy Morrow (Timothy Morrow. 2018).

The Cloud-Base Architecture and Its Security Implications

Cloud-Base Architecture refers to the various mechanisms in terms of databases, software capabilities; applications and engineering the leverage that power the cloud resources to solve business tribulations. Cloud architecture defines the mechanisms as well as the associations between them.

The Cloud-base model has three examine delivery models and main three deployment models which are:

(1) Private cloud: a cloud platform that is dedicated for an organization,

(2) Public cloud: a cloud platform that is available for public users to register and use the infrastructure, and

(3) Hybrid cloud: a cloud that combine the function of private and public. That is, a private cloud that can make bigger use of resources in public clouds. Public clouds are the most susceptible deployment model because they are available for public users to host their services who may be malevolent users. The cloud-base service delivery architectural models are presented below.

a. Infrastructure-as-a-service (IaaS): where cloud providers convey computation resources, storage and network as an internet-based services. This service model is based on the virtualization technology. Amazon EC2 is the most familiar IaaS provider.

b. Platform-as-a-service (PaaS): where cloud providers deliver platforms, tools and other business services that enable customers to develop, deploy, and manage their own applications, without installing any of these platforms or support tools on their local machines. The PaaS model may be hosted on top of IaaS model or on top of the cloud infrastructures directly. Google Apps and Microsoft Windows Azure are the most known PaaS.

c. Software-as-a-service (SaaS): where cloud providers deliver applications hosted on the cloud infrastructure as internet-based service for end users, without requiring installing the applications on the customers' computers. This model may be hosted on top of PaaS, IaaS or directly hosted on cloud infrastructure. SalesForce CRM is an example of the SaaS provider.

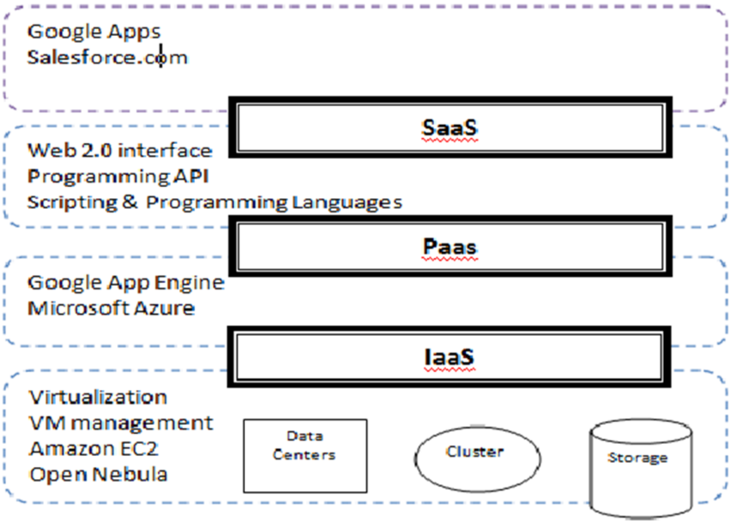

Fig. 2. *Present the three layer of cloud architecture (Source:* https://www.researchgate.net/figure/Layered-Cloud-Architecture_fig1_239949848*)*

Every service delivery model has many ways of possible implementations, as in figure 2, which difficult for the development of standard security model for each service delivery model. Furthermore, these service delivery models may exist in one cloud platform leading to further complication of the security management process.

Software Engineering Architecture

Software Engineering Architecture refers to the basic structures of a software system and the authority of creating such structures and systems; It functions as a plan for the system and the mounting project, laying out the necessary tasks to be executed by the design teams as presented in figure 3.

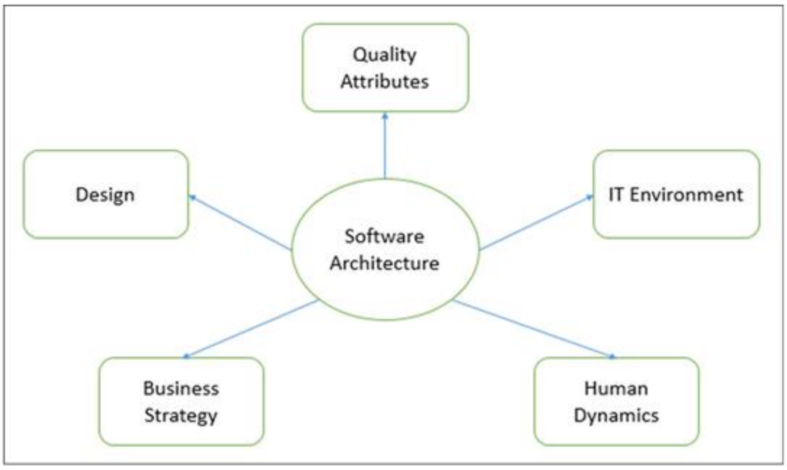

Fig. 3. *Present the software engineering architecture*
(Source: https://en.wikipedia.org/wiki/Software_architecture*)*

We can separate Software Engineering Architecture into two different phases: Software Architecture and Software Design. In Architecture, nonfunctional decisions are shed and separated by the functional requirements. In Design, functional requirements are accomplished (Emmanuel, O., & Ali, O.S. 2020).

Conclusion

Cloud-Base computing is a new computational paradigm that offers an innovative business model for organizations to adopt IT without upfront investment. Despite the potential gains achieved from the cloud computing, the model security is still questionable which impacts the cloud model adoption. The security problem becomes more complicated under the cloud model as new dimensions have entered into the problem scope related to the model architecture, multi-tenancy, elasticity, and layers dependency stack. In this paper we introduce a detailed analysis of the cloud security problem. We investigated the problem from the cloud architecture perspective, the cloud offered characteristics perspective, the cloud stakeholders' perspective, and the cloud service delivery models perspective. Based on this analysis we derive a detailed specification of the cloud security problem and key features that should be covered by and proposed security solution.

References

1. Almorsy, M., Grundy, J., & Müller, I. (2016). An analysis of the cloud computing security problem. *arXiv preprint arXiv:1609.01107*.
2. Zhou, Y., & Tang, Y. (2018, April). Application of Cloud Computing Technology on Computer Secure Storage. In *2018 3rd International Workshop on Materials Engineering and Computer Sciences (IWMECS 2018)*. Atlantis Press.
3. Timothy Morrow. (2018). 12 Risks, Threats, & Vulnerabilities in Moving to the Cloud, software engineering institute.
4. Emmanuel, O., & Ali, O.S. (2020). Performance Evaluation of Fingerprint against Auto-pin andPassword in Cloud Computing. *11 (1) January 2020. pp. 586 – 594 at www.Ijser.org*
5. ENISA, "Cloud computing: benefits, risks and recommendations for information security,"2009, http://www.enisa.europa.eu/act/rm/files/deliverables/cloudcomputing-risk-assessment, Accessed On July 2010.
6. Cloud Security Alliance (CSA). (2010). Available: http://www.cloudsecurityalliance.org/
7. Balachandra , R. K., Ramakrishna, P., & Atanu, R. (2009). "Cloud Security Issues," inProceedings of the 2009 IEEE International Conference on Services Computing, pp. 517-520.
8. Kresimir, P., & Zeljko, H. (2010). "Cloud computing security issues and challenges," in The Third International Conference on Advances in Humanoriented and Personalized Mechanisms, Technologies, and Services, pp. 344-349.
9. Jensen, M., Schwenk, J., Gruschka, N., & Iacono, L. L. (2009, September). On technical security issues in cloud computing. In *2009 IEEE*

International Conference on Cloud Computing (pp. 109-116). Ieee.

10. Grobauer, B., Walloschek, T., & Stocker, E. (2010). Understanding cloud computing vulnerabilities. *IEEE Security & privacy*, *9*(2), 50-57.
11. Subashini, S., & Kavitha, V. (2011). A survey on security issues in service delivery models of cloud computing. *Journal of network and computer applications*, *34*(1), 1-11.
12. Ristenpart, T., Tromer, E., Shacham, H., & Savage, S. (2009, November). Hey, you, get off of my cloud: exploring information leakage in third-party compute clouds. In *Proceedings of the 16th ACM conference on Computer and communications security* (pp. 199-212).
13. Microsoft. (2006, October, 2010). Multi-Tenant Data Architecture. Available: http://msdn.microsoft.com/en-us/library/aa479086.aspx
14. Amazon. (October, 2010). Amazon EC2 SLA. Available: http://aws.amazon.com/ec2-sla/
15. Holstein, D. K., & Stouffer, K. (2010, January). Trust but verify critical infrastructure cyber security solutions. In *2010 43rd Hawaii International Conference on System Sciences* (pp. 1-8). IEEE.
16. Zhang, W. (2010, April). Integrated security framework for secure web services. In *2010 Third International Symposium on Intelligent Information Technology and Security Informatics* (pp. 178-183). IEEE.
17. Bin, W., Yuan, H. H., Xi, L. X., & Min, X. J. (2009, October). Open identity management framework for SaaS ecosystem. In *2009 IEEE International Conference on e-Business Engineering* (pp. 512-517). IEEE.
18. Fong, E., & Okun, V. (2007, January). Web application scanners: definitions and functions. In *2007 40th Annual Hawaii International Conference on System Sciences (HICSS'07)* (pp. 280b-280b). IEEE.
19. NIST. (October 2010). National Vulnerability Database (NVD). Available: http://nvd.nist.gov/home.cfm