Sub-Sahara African Academic
Research Publications
December, 2020, Editions

JPAS
Journal of Pure and Applied Science
Vol..17, No.9, ISSN 2318-9315

CLOUD COMPUTING AND THE IMPROVEMENT STATUS OF CLOUD SECURITY

OFUALAGBA MAMUYOVWI HELEN
Department of Computer Science, Delta State Polytechnics Otefe, Oghara, Delta State.

ABSTRACT
Cloud computing is an Internet-based computing service provided by the third party allowing share of resources and data among devices. It is widely used in many organizations nowadays and becoming more popular because it changes the way of how the Information Technology (IT) of an organization is organized and managed. It provides lots of benefits such as simplicity and lower costs, almost unlimited storage, least maintenance, easy utilization, backup and recovery, continuous availability, quality of service, automated software integration, scalability, flexibility and reliability, easy access to information, elasticity, quick deployment and lower barrier to entry. While there is increasing use of cloud computing service in this new era, the security issues of the cloud computing become a challenges. Cloud computing must be safe and secure enough to ensure the privacy of the users. This paper focus on the architecture (software and hardware requirement of the cloud computing, then discuss the most common security issues of using cloud and some solutions to the cloud security issues since security is one of the most critical aspect in cloud computing due to the sensitivity of user's data. And also the Improvement Status of Cloud Security.

Keywords: *cloud, computing, information technology, security, internet, data,*

INTRODUCTION
Cloud security, also known as cloud computing security, consists of a set of policies, controls, procedures and technologies that work together to protect cloud-based systems, data, and infrastructure. These security

measures are configured to protect cloud data, support regulatory compliance and protect customers' privacy as well as setting authentication rules for individual users and devices. From authenticating access to filtering traffic, cloud security can be configured to the exact needs of the business. And because these rules can be configured and managed in one place, administration overheads are reduced and IT teams empowered to focus on other areas of the business.

The way cloud security is delivered will depend on the individual cloud provider or the cloud security solutions in place. However, implementation of cloud security processes should be a joint responsibility between the business owner and solution provider. For businesses making the transition to the cloud, robust cloud security is imperative. Security threats are constantly evolving and becoming more sophisticated, and cloud computing is no less at risk than an on-premise environment. For this reason, it is essential to work with a cloud provider that offers best-in-class security that has been customized for your infrastructure. More and more organizations are realizing the many business benefits of moving their systems to the cloud. Cloud computing allows organizations to operate at scale, reduce technology costs and use agile systems that give them the competitive edge. However, it is essential that organizations have complete confidence in their cloud computing security and that all data, systems and applications are protected from data theft, leakage, corruption and deletion.

REVIEW OF RELATED LITERATURE

According to Mall & Grance, 2011 on 'cloud computing' Aside from this a cloud environment must also be available over the network, capable of resource pooling and capable of being measured. This means that a cloud environment must contain mechanics for monitoring, reporting and controlling.

(Chen & Zhao, 2012) on 'Data privacy and integrity ' Ensuring that your data is kept private and secure from unauthorized users as well as free from malicious or unintentional modifications is no easy task. When managing these aspects of security one main issue is the lack of control a cloud user has over the actual server the data is stored on

Al-Anzi, Yadav & Soni (2014) suggest a security model for CC comprising governance, risk management and compliance. CC security requirements vary quite significantly from traditional environments because of its dynamic nature and customer ownership. It is pertinent to mention that this model can be applied to each type of cloud, e.g. private, public, hybrid and community.

BRIEF OVERVIEW OF CLOUD SECURITY

Cloud security is a pay-per-use model for enabling convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction

There are numerous security issues and challenges in cloud computing because it encompasses many technologies such as networks, databases, operating system, virtualization, resource scheduling, transaction management, concurrent control and memory management (Eria, 2018). This is very important because the cloud service provider must ensure that the users is not facing any serious problem like data loss and data theft which may cause a great loss depending on the sensitivity of the data stored in cloud. A malicious user may pretend to be the legitimate users and infecting the cloud.

Security Issues of Cloud That Can Be Address

1. Data theft

Dave and Frieed (2015) stated that data at rest is the major issues in cloud computing because users may store all their common, private, or even sensitive data in the cloud which can be accessed by anyone anywhere. Data theft is a very common issues that are facing by the cloud service providers nowadays. Besides, some cloud service providers even don't provide their own server because of the cost effectiveness and flexibility. There are also incidents like data loss which might be also a serious problem for the users. For example, the server is suddenly shut down and causes data loss of the users. Furthermore, natural disaster might also cause data to be damaged or corrupted. Therefore, physical data location can be considered one of the security issues in cloud computing.

2. Privacy issues

The cloud computing service provider must enforce their own policies to ensure the safety of the data users stored in their cloud model. They must make sure that they realize who is actually accessing the data stored in the cloud and only the authorized person can maintain the cloud service model (Lee, 2019). The security of cloud computing should be done on the provider side and also the user side. Cloud service provider should provide a good layer of security protection for the users while the users should not tampered with the other user's data. The cloud computing is a good way to reduce the cost and provide more storage if and only if the security is done by both provider and user.

Yang (2015) claimed that regulatory reform is essential to protect sensitive data in the cloud since one of the most challenging aspect in cloud computing is to ensures that the consumer have trust in privacy and security of their data.

3. Application issues

Darius (2017) stated that monitoring and maintenance should be done by the cloud service provider frequently to ensure that the cloud is secure and not infected by the malicious code that have been uploaded to the cloud by the hackers or attackers with the purpose of stealing sensitive information or even damaging the information of certain users.

Lede (2017) stated that there are lots of security issues regarding the cloud computing that have been widely used nowadays. The top threat that have been mentioned in various researches are:

Data Breaches: Data that stored to the cloud by the users might be important and sensitive. The data store in cloud might be stole by the unauthorized users and that might poses some level of danger to the users under attack. It is the top threat to threat to the cloud computing because hackers or attackers can easily access to the data of the users which store in the cloud. The cloud stored a pool of confidential information of many users. The cloud service users should also ensure the quality, reliability and performance of the cloud service providers through Service Level Agreements (SLAs) negotiated between providers and users (Umar, 2012). Therefore, data breaches are the worst problem that the cloud computing service faces.

Data Loss: Data stored in cloud might be damaged or corrupted due to some reasons such as shut down of server because of financial or legal problem, natural disaster like earthquakes and fire (Uriam, 2013). Data might not be able to recover because back up is not done well and the data of the users will be lost forever if there are no extra copies of that information.

Account Hijacking: Yang (2015) explained that the user's account is stolen or hijacked and the hackers might impersonate he user to perform malicious and unauthorized activities which might also harm the user For example, the hackers might manipulate the data, provide false information and eavesdropping on transactions using the stolen account. In addition, no native APIs are used for login and anyone can register as a cloud service user hence the chances of the account being hijacked is high

Insecure APIs: Software Interface for the users to interact with the cloud services is also crucial to ensure the security of the cloud model. The API from the authentication and access control to the encryption and activity monitoring should be well implemented to protect against both accidental and malicious attack.

Malicious Insiders: Dave and Frieed (2015) also added that an employee of the company might also be a big threat. They might be the attacker themselves or a partner of the hacker who have the better chances of stealing or tampering the data of the cloud model with intention. These activities cause the sensitive or confidential data of the users leak to the others which might harm the targeted users.

Studies by Eria, (2018) reveals that password and other confidential data can be easily obtained by malicious insiders of cloud service providers. He also addressed the problems of malicious insiders where they claimed that it should be studied in two context which are insider threat in cloud provider (i.e. insider is malicious employee working for cloud provider) and insider threat in cloud outsourcer (i.e. employee of an organization which sourced its infrastructure to the cloud).

CLOUD COMPUTING ENABLING TECHNOLOGIES

Several technologies are related to cloud computing, and the cloud has emerged as a convergence of several computing trends. It seeks to address

certain key aspects that may have been lacking in each of these trends, individually.

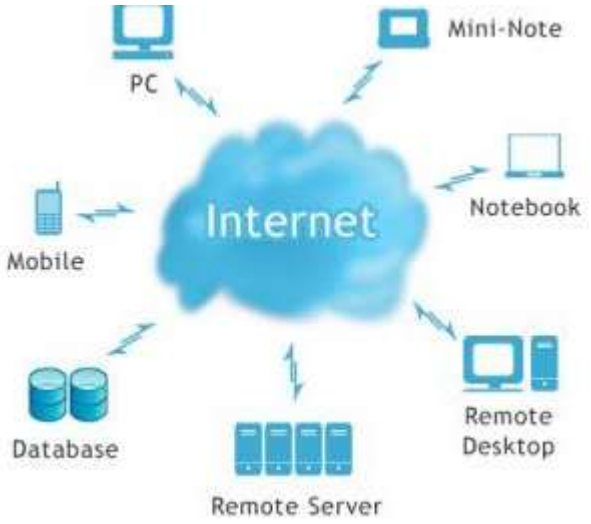

Fig 1: Cloud Computing (google image)

Yang (2015) detailed that clouds extend the capabilities of other domains with the specific goal to achieve scalability/ elasticity, availability with optimal resource utilisation, which is as such only partially addressed in other domains. Specifically, clouds belong to the wider areas of Internet of Services (including Web Services, Web3.0, Service Oriented Architecture (SOA) etc.) and Utility Computing (including Grid, Virtual Organisations etc.) and implicitly inherit multiple aspects from these domains, such as virtualisation and outsourcing.

Eria (2016) stated that depending on usage, they may extend these characteristics, in particular by adding a new business model. What is important to stress again in this context is that not all cloud characteristics exclusively belong to the cloud domain; extrinsic features that generally belong to other domains enable service and utility computing are naturally taken over in clouds.

Characteristics exclusive to the Cloud (intrinsic features)

Characteristics belonging to other domains but having to be adapted in order to meet the cloud relevant specifics (extrinsic extended)

Characteristics that belong to other domains and just act as enablers to cloud systems, that is, do not have to be extended (extrinsic inherited)

Fig 2: cloud security(Google image)

Cloud Deployment Models

Uriam, (2013) stated that cloud services are provisioned in different ways, this are referred to as deployment models. They include;

Public Cloud: The cloud infrastructure is available to the general public.

Private Cloud: The type of the cloud, that is available solely for a single organization.

Community Cloud: In this type of cloud deployment model, the infrastructure of the cloud is shared by several organizations and supports a specific community with shared concerns.

Hybrid Cloud: This is a cloud infrastructure that is a composition of two or more clouds that is, private, community or public

IMPROVEMENT STATUS OF CLOUD SECURITY

The cloud computing have become more popular because many users start to realize its benefits. It allows the user to easily shrink the operation and also help to save cost. However, with the increased adoption rate of the cloud service, the security issues and risk have been increased as well (Kells, 2019).

Prikash, (2018) stated that in order to make cloud computing a better option to increase the user storage capacity and save their confidential information securely, there are few solutions and practice that helps.

Vulnerability shielding: The cloud service provider should improve the patch management. They should check the vulnerability of their cloud service frequently and always update and maintain the cloud to limit the possible access point and reduce the risk of attack of the cloud by the hackers. The cloud service provider might also use the Intrusion Detection System (IDS) to make sure the cloud service provided is secure and safe.

Trusted cloud service provider: The user should make sure that they find the right cloud service provider. Each cloud service provider have different approaches on data management in the cloud. Well established and experienced cloud service provider is more trust worthy and better choice. Besides, the standards and regulations of the cloud service provider is also

very important. Examples of trusted clouds service providers are Amazon Web Services (AWS), IBM, Google and Microsoft.

Jason and Gloibe (2018) suggested the following cloud security solutions:

Security check events: The users should have clear contract with the cloud service provider so that the users can claim if any accidents or breaches of the sensitive data stored in the cloud. The users must have clear agreement with the cloud service provider before using the cloud services provided by that particular cloud service provider. The users should ensure that the cloud service provider give enough details about fulfilments of promises, break remediation and reporting contingency.

Data storage regulations: The architecture of the cloud environment is an important aspect to ensure the security of the data stored in the cloud. The users must understand the concept of the data storage regulations which the cloud service provider follows.

Facilities for recovery: Cloud service provider should take the responsibility to recover the data of the users if there is any data loss due to certain issues. Cloud service provider should make sure that they have proper backup and can retrieve and recover the confidential data of the users that might be costly.

Fig 2: cloud security (Google image)

SUMMARY

Cloud computing is a paradigm shift to computing that sees and delivers computing as a service rather than as a resource. And cloud security is improving significantly, because it provides lots of benefits such as simplicity and lower costs, almost unlimited storage, least maintenance, easy utilization, backup and recovery, continuous availability, quality of service, automated software integration, scalability, flexibility and reliability, easy access to information, elasticity, quick deployment and lower barrier to entry.

CONCLUSION

Conclusively, cloud security is fast improving with modern technology. Because cloud computing is a model that helps to speed up and increase the flexibility of data management with reduced cost. It is undeniable that cloud computing has brings us lots of benefits and becoming more popular nowadays. Many large companies start using cloud service in their business. While the cloud computing is widely used, the security becomes a concern to everyone who use cloud services. There is a lot of security arises continuously while there are improvement as well on the security model of the cloud service provided. Despite the increasing use of the cloud service, the user should use the cloud service provided wisely in a way that always ensure good security practices so that this technology have the potential to bring the information technology to the next level. Cloud computing might help us to separate software from the hardware as more technologies are used as service using cloud and software might have a highly abstract space with the computer hardware.

REFERENCES

Darius, J. (2017). Cloud Computing: New Wine or Just a New Bottle? IT Professional, 15-17.

Dave, J. and Frieed I. (2015). Cloud Computing and Grid Computing 360-Degree Compared. IEEE Grid Computing Environment Workshop (GCE „08), pp 1-10.

Eria, C. (2018). The Anatomy of the Grid: Enabling scalable virtual organization. The International Journal of High Performance Computing Applications, vol. 15(3), pp. 200-222.

Jason, C. and Gloibe, T. (2018). The Physiology of the Grid: An Open Grid Services Architecture for Distributed Systems Integration. Globus Project.

Kells, R. (2019).Cloud Computing: An Overview. Journal of Theoretical and Applied Information Technology, vol. pp. 71-79. www.jatit.org.

Lede, S. (2017) "Cloud Computing‟s Effect on Enterprises", Dept of Informatics, Lund University Unpublished Master‟s Thesis 1-89.

Lee, T. (2019).Grid Basics. In: Stanoevska-Slabeva, K., Wozniak, T., and Ristol, S., Grid and Cloud Computing A Business Perspective on Technology and Applications. Springer Berlin Heidelberg,

Prikash, J. (2018): Advances in Clouds: Research in Future Cloud Computing, Expert Group Report. Information Society and Media, European Union, Belgium.

Uriam, H. (2013) Grid Computing fürvirtualisierteInfrastrukturen. In: Barth T, Schüll A (eds) Grid Computing: Konzepte, Technologien, Anwendungen, pp. 1-15. Vieweg+Teubner, Wiesbaden.

Yang, X. H. (2015).Evolution of Grid Computing Architecture and Grid Adoption Models. IBM Syst. J. 43(4):624-644.