NATIONAL INNOVATION AND RESEARCH ACADEMIA
International Journal of Computing, Engineering and Information
ISSN: 2713-4677. Volume 6, Issue 1. Pages 01- 07. October, 2019
Double Blind Peer Reviewed International Research Journal
editornirajournals@gmail.com

Sustainability and Efficiency of Data Security in Cloud Computing. A Review

Muhammad Moruma Lawan
Department of Computer Engineering, Ramat Polytechnic Maiduguri, Nigeria | Email: engrmorumalawan@gmail.com

Bukar Baba Aji (PhD)
Department of Computer Science and Information Technology, Olabisi Onabanjo University, Nigeria | Email: bukarbabaaji@gmail.com

Muhammad Alkali Abbo
Department of Electrical and Electronic Engineering, Ramat Polytechnic Maiduguri, Nigeria | Email: muhammadalkaliabbo@gmail.com

Abubakar Mustapha Kura
Department of Electrical and Electronic Engineering, University of Maiduguri, Nigeria | Email: akurah4u@yahoo.com

Abstract: *Cloud computing is an on demand service in which shared resources, information, software and other devices are provided according to the clients requirement at specific time. The study reviewed the sustainability and efficiency of data security in cloud computing, To achieve this, numerous academic papers were reviewed and concluded that; to improve the sustainability and security in cloud computing, it is vital to provide authentication, authorization and access control for data stored in cloud. Furthermore, cloud computing has the potential to become a frontrunner in promoting a secure, virtual and economically viable IT solution in the future. Also, a security solutions should have the intelligence to be self-defending and have the ability to provide real-time detection and prevention of known and unknown threats.*

Keywords: *Cloud, Computing, Data, and Security*

Introduction

Cloud computing has created substantial interest in both academia and industry; nevertheless it's still a developing paradigm. Fundamentally, it aims to consolidate the economic utility model with the evolutionary expansion of many prevailing approaches and computing technologies, including distributed services, applications, and information infrastructures containing of pools of computers, networks, and storage resources. Confusion exists in IT communities about how a cloud varies from prevailing models and how these differences affect its implementation. Some understand a cloud as a novel technical revolution, while others consider it a natural development of technology, economy, and culture (Takabi et al.2010).

Nevertheless, cloud computing is a significant paradigm, with the potential to significantly decrease costs through optimization and increased operating and economic competences (Catteddu and Hogben, 2009). Moreover, cloud computing could significantly improve partnership, agility, and scale, therefore, allowing a truly global computing model over the Internet infrastructure. However, without suitable security and privacy solutions designed for clouds, this potentially transforming computing paradigm could develop a enormous failure. Numerous surveys of potential cloud adopters indicate that security and privacy is the primary concern hindering its implementation (Bruening and Treacy, 2009).

Despite the tremendous business and technical benefits of the cloud, the security and privacy concern has been one of the key hurdles preventing its widespread implementation (Shahzad, 2014). Particularly for outsourced data services, the owners exclusive control over their data is ultimately surrendered to the CSPs (Li et al. 2013). As a result, from the data owners point of view, whenever their outsourced data contain sensitive personal information, such as financial and medical records, and social network profiles, it can no longer be considered as private as before. On the other hand, although in reality CSPs typically impose data security through mechanisms like firewalls and virtualization, these actions do not fully guard against threats of unauthorized data access from insiders, outsiders, or other cloud tenants due to the non-bug-free deployment and low degree of transparency. Infamous data breach incidents occur from time to time, such as the recent Sony PlayStation data breach (Edwards and Riley, 2011).

Cloud computing is an on demand service in which shared resources, information, software and other devices are provided according to the clients requirement at specific time. It's a term which is usually used in case of Internet. The whole Internet can be viewed as a cloud. Capital and operational costs can be cut using cloud computing. With traditional desktop computing, we run copies of software programs on our personal computer. The documents we make are stored on our own PC. Though documents can be retrieved from other computers on the network, they cannot be retrieved by computers outside the network. If a computer crashes, the software is still accessible for others to use. Similar goes for the documents one create; they are stored on a collection of servers accessed through the Internet. Everyone with permission can not only access the documents, but can also edit and cooperate on those documents in real time.

According to Hogan and Sokol, (2013) there are 5 key actors in cloud computing based on their participation as shown in Fig. 1. Cloud consumer or cloud service consumer (CSC) is the one who gets the service from a cloud provider and pays for the service as per the use. Cloud provider or cloud service provider (CSP) is the one who provides the cloud services to the CSC. Cloud auditor is the one who conducts an independent assessment of cloud services, information system operations, performance and security of the cloud implementations. Cloud broker is the one who interacts between CSP and CSC to make the business happen. Cloud carrier is the one who provides the connectivity and cloud services from CSP to CSC (Hogan and Sokol, 2013).

Figure 1. Cloud Computing Model (Gurjeet and Mohita, 2018

Based cloud computing model comprises of four cloud deployment models, three service delivery models and five vital characteristics. A Cloud can be deployed as Private, Public, Community and Hybrid clouds. Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS) and Software-as-a-Service (SaaS) are the three service delivery models have become widely recognized and formalized. Rapid Elasticity, Measured Service, Resource Pooling, Broad Network access and On-Demand Self Service are the 5 vital features of cloud computing (Hogan and Sokol, 2013; Brunette and Mogul, 2009; & Xiao and Xiao.2012). Other researchers [Aldossary, and Allen, 2016; Catteddu and Hogben, 2009; & Reed et al. 2011) states that multi-tenancy is also an important characteristic of cloud computing. The following table 1 shows that a cloud computing delivery model can offer 9 services, namely Application, Data, Runtime, Middleware, Operating System, Virtualization, Server, Storage and Networking which are the components in the traditional computing (Ludwig. 2011; Sookhak, et al. 2014, Aldossary, and Allen, 2016).

Models of Cloud Computing

Cloud Computing can be accessed through a set of cloud computing service models such as Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS). In SaaS the service providers offer the services and customers make use of these services to run applications on a cloud infrastructure. These applications can be accessed over web browsers. PaaS is a way to rent hardware, operating systems, storage and network capacity over the internet. The service delivery model allows the customer to rent virtualized servers and associated services for running prevailing applications or evolving and testing new ones. In IaaS, the consumer is provided with power to control process, manage storage, network and other essential computing resources which are helpful to manage arbitrary software (Rao & Selvamani, 2015)..

Data Security Challenges

As one moving into internet based cloud model, it needs great emphasis on Data Security and Privacy. Data loss or Data leakage can have severe influence on business, brand and trust of an organization. In Fig. 2. Data leak prevention is considered as most significant issue with 88% of Critical and Very vital challenges. Similarly, Data Segregation and Protection has 92% effect on security challenges (Rao & Selvamani, 2015).

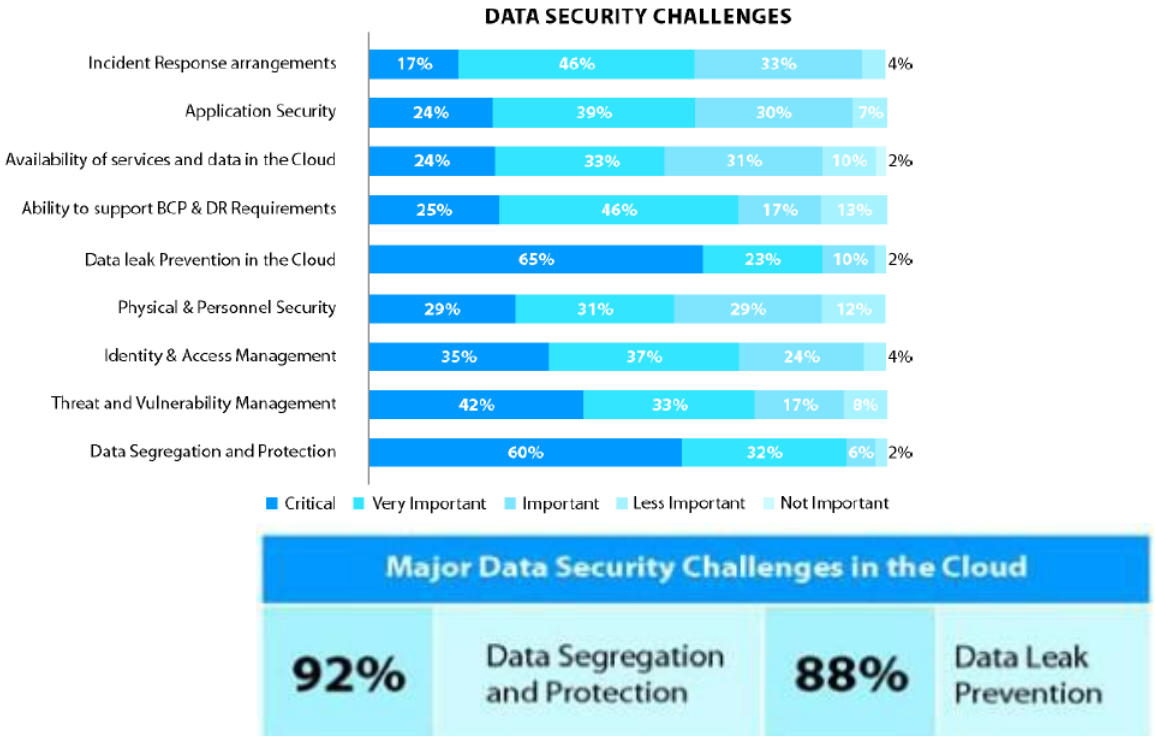

Figure 2: Data Security Challenges. (Source: (Rao & Selvamani, 2015)

When numerous organizations share resources, there is a risk of data misuse. Therefore, to evade risk it is essential to secure data repositories and the data that includes storage, transit or process. Protection of data is the most significant tasks in cloud computing. To improve the security in cloud computing, it is vital to provide authentication, authorization and access control for data stored in cloud. The 3 main areas in data security are; Confidentiality, its the top vulnerabilities to be checked to ensure that data is protected from any attacks. Therefore, security test has to be done to protect data from malicious user such as Cross-site Scripting, Access Control mechanisms (Rao & Selvamani, 2015). The second one is Integrity: to provide security to the client data, thin clients are used where only few resources are available. Users should not store their personal data such as passwords so that integrity can be assured. Thirdly, *Availability*; availability is the most significant issue in numerous organizations facing downtime as a major issue. It depends on the agreement between vendor and the client (Rao & Selvamani, 2015).

.

Data Security and Cloud Computing Models Implementation

Essentially, the deployment of a cloud is managed in house (Private Cloud) or over a third-party location (Public Cloud). Although, for several reasons, it is deployed as an integrated private-public cloud (Hybrid Cloud) (Armbrust et al. 2010; Zissis. and Lekkas, 2012). A "Community Cloud" is a fourth type of cloud implementation models, where the infrastructure spreads over numerous organizations and is accessed by a specific community (Zissis. and Lekkas, 2012). The different cloud implementation models are shown in Figure 2. In private cloud configuration, an organization may have control over its infrastructure or delegate that to a third party, being physically on-site or off-site

(Armbrust et al. 2010; Zissis. and Lekkas, 2012). Securing the in-house cloud infrastructure is manageable and requires no need for extra trust mechanisms. While having a third-party service provider running the private cloud is prone to numerous doubts (Zissis. and Lekkas, 2012). Users adopt a private cloud implementation to increase the security level. Furthermore, operating over a secure virtual private network is an option to segregate the private cloud hosted by a third party. Despite the benefits of a private cloud, numerous issues need attention as unbalanced resources utilization (Jamil and Zaki, 2011).

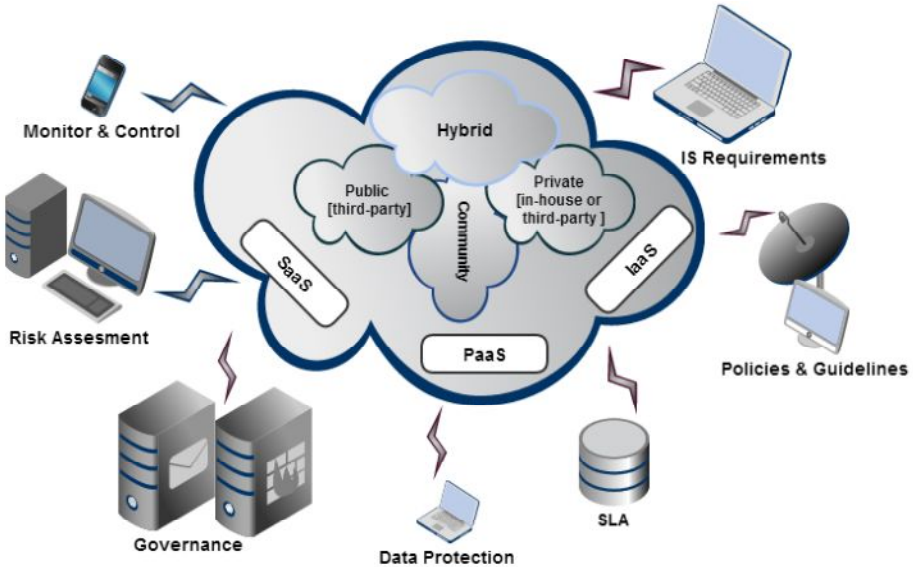

Figure 3. Cloud implementation model **(**Zissis and Lekkas 2012 and Ramgovind et al. 2010)

A data security model comprises of authentication, data encryption and data integrity, data recovery, user protection has to be designed to improve the data security over cloud. To avoid access of data from other users, applying encryption on data that makes data totally unusable and normal encryption can complicate availability. Before uploading data into the cloud the users are suggested to verify whether the data is stored on backup drives and the keywords in files remain unchanged. Calculate the hash of the file before uploading to cloud servers will ensure that the data is not altered. This hash calculation can be used for data integrity but it is very difficult to maintain it. Distributed access control architecture can be used for access management in cloud computing. To identify unauthorized users, using of credential or attributed based policies are better. Permission as a service can be used to tell the user that which part of data can be accessed. Fine grained access control mechanism enables the owner to delegate most of computation intensive tasks to cloud servers without disclosing the data contents. A data driven framework can be designed for secure data processing and sharing between cloud users. Network based intrusion prevention system is used to detect threats in real-time (Rao & Selvamani, 2015).

.

Conclusion

Cloud computing is the new developing technology that offerings a good number of benefits to the users. However, it faces lot of security challenges. Therefore, this paper

reviewed sustainability and efficiency of data security in cloud computing and following conclusions were drawn

1. To improve the sustainability and security in cloud computing, it is vital to provide authentication, authorization and access control for data stored in cloud
2. Before uploading data into the cloud, the users are suggested to verify whether the data is stored on backup drives and the keywords in files remain unchanged.
3. Cloud computing has the potential to become a frontrunner in promoting a secure, virtual and economically viable IT solution in the future.
4. The main drawback of the existing cloud service implementations is their inability to provide an accredited high security level
5. A security solutions should have the intelligence to be self-defending and have the ability to provide real-time detection and prevention of known and unknown threats

References

Aldossary, S., and Allen, W. (2016) Data Security, Privacy, Availability and Integrity in Cloud Computing: Issues and Current Solutions. *International Journal of Advanced Computer Science and Applications,* 7 (4).

Bruening P.J., and Treacy, B.C. (2009) "*Cloud Computing: Privacy, Security Challenges*," Bureau of Nat'l Affairs.

Brunette, G., and Mogul, R. (2009) Security Guidance for Critical Area of Focus in Cloud Computing 2(1), *Cloud Security Alliance* (CSA), 1-76.

Catteddu, D., and Hogben, G. (2009) Cloud Computing: Benefits, risks and recommendations for information security, *European Union Agency for Network and Information Security* (ENISA), 1-125.

Edwards, C., and Riley, M. (2011) *Sony data breach exposes users to years of identity-theft risk*. 05-03.

Gurjeet S., and Mohita G., (2018) Data Security In Cloud Computing: A Review*. International Journal Of Computers & Technology.*17 (2)

Hogan, M., and Sokol, A. (2013) NIST Cloud *Computing Standards Roadmap Version 2. NIST Cloud Computing Standards Roadmap Working Group*, NIST Special Publications 500-291,

Kumar, P. R., Raj, P. H., & Jelciana, P. (2018). Exploring data security issues and solutions in cloud computing. *Procedia Computer Science*, *125*, 691-697.

Jamil, D., and Zaki, H. (2011) "Cloud Computing Security," *International Journal of Engineering Science and Technology*, 3(4): 3478-3483.

Li, M., Yu, S., Ren, K., Lou, W., Hou, Y. (2013) Toward privacy-assured and searchable cloud data storage services. *Network, IEEE*; 27(4):56–62.

Ludwig. S. (2011) Cloud 101: *What the heck do IaaS, PaaS and SaaS companies do*? Venture Beat.

Ramgovind S., Elo, M., and Smith, E. (2010) "The Management of Security in Cloud Computing," *Information Security for South Africa*, Sandton. 1-7.

Rao, R. V., & Selvamani, K. (2015). *Data security challenges and its solutions in cloud computing. Procedia Computer Science*, 48, 204-209.

Reed, A., Rezek, C., and Simmonds. P. (2011) Security Guidance for Critical Area of Focus in Cloud Computing. *Cloud Security Alliance* (CSA) 1-177.

Sarddar, D., Sen, P., and Sanyal, M. K. (2016) "*Central Controller Framework for Mobile Cloud Computing,*" Int. J. Grid Distrib. Comput., 9 (4): 233–240.

Shahzad, F. (2014). State-of-the-art survey on cloud computing security Challenges, approaches and solutions. *Procedia Computer Science*, *37*, 357-362.

Sookhak, M., Talebian, H., Ahmed, E., Gani, A., Khan. M. K. A. (2014) Review on remote data auditing in single cloud server: Taxonomy and open issues. *Journal of Network and Computer Applications,* 43:121-141

Takabi, H., Joshi, J. B., & Ahn, G. J. (2010). Security and privacy challenges in cloud computing environments. *IEEE Security & Privacy*, *8*(6), 24-31.

Xiao, Z., and Xiao.(2012) Security and Privacy in Cloud Computing, *IEEE Communications Surveys & Tutorial*, 15(2): 843- 859.

Zissis, D., and Lekkas, D. (2012) "Addressing Cloud Computing Security Issues," *Future Generation Computer Systems*, 28(3). : 583-592.