East African Journal of Arts and Social Sciences
eajass.eanso.org
Volume 4, Issue 1, 2019
ISSN: 1743-6254

EAST AFRICAN NATURE & SCIENCE ORGANIZATION

Original Article

UNDERSTANDING THE ARCHITECTURE, BENEFITS, AND SHORTCOMING OF CLOUD-BASED SERVICES

Justin Mulwa

Machakos University

Article history:

Received: 17 Aug 2019
Accepted: 22 Sep 2019
Published: 26 Sep 2019

Keywords:

Cloud Computing, Cybersecurity, Information, Cloud Based Services

ABSTRACT

With the inception on internet technology, information and communication industry has extensively been advanced. Cloud computing technology is on the reckoning force in ICT and an indispensable tool used in daily operations of organizations and institutions. Many corporations are striving to ensure their services and information is cloud based as the tech makes operations more efficient. The primary objective of this paper shall be to evaluate the architecture of cloud-based systems, the challenges, and remedies to cyber security and privacy issues among other uncertainties associated with the technology.

INTRODUCTION

Since the inception of internet technology, man has significantly relied on the use of internet in carrying out of his daily activities. The Internet has substantially changed the information technology and computer world. Internet technology has advanced very fast from parallel computing to distribution of data, information, and application through cloud computing (Ali, et al., 2015). Cloud computing can define as an environment where multiple computers are linked together via the internet enabling different parties from different locations to access data and information from parties at various places. Chen & Zhao (2012) on the other hand defines cloud computing as a model capable of permitting convenient on-demand access and sharing of information from a common pool of configured computing resources such as servers which can quickly be provisioned and disseminated with least management efforts and service provider interactions. Cloud computing gave rise to a common phrase among the internet users known as "the internet never forgets" meaning that billions of data can be stored in the cloud forever.

Butterfield, et al. (2016) points out that cloud-based technologies and services are extensively being used in many fields stemming from business to public administration, social life to media and communication agencies and much more. It provides a remarkable opportunity in providing its users with cost efficient and robust services that are also easy to manage and source. Nevertheless, despite the many advantages drawn from the cloud-based technology, there come considerable challenges that are extremely concerned about security and privacy issues (Kshetri, 2013).

The greatest concern to internet users and cloud-based application are centered on safety and

confidentiality issues. Data security and confidentiality protection concerns are the primary limitation of cloud computing services. The filled with people with malicious intents, internet hackers being the most daunting sources of internet breaches and insecurities (Chang, et al., 2016; Puthal, et al., 2015). Lack of a robust and consistent internet security protocols makes cloud computing much less credible as compared to the traditional systems such as paper filling (Rittinghouse & Ransome, 2016). The primary objective of this article shall provide a current update of cloud computing architecture, potential challenges and threats in internet services, and the probable remedies to the shortcomings.

Cloud computing has many potential benefits to the users as well as drawbacks. Despite the challenges, many businesses, and public institutions are all striving in making their services digitalized as they acknowledge the benefits that accrue from keeping their data and application in the cloud. The adoption of cloud-based services and application have led to improving efficiency and effectiveness in the development and deployment organization strategies more so a reduction in the costs of purchasing and maintenance of infrastructure (Butterfield, et al., 2016). The Internet has revolution information and communication technology, through the system people can learn so much from the web, the data stored in the cloud has become the readily available source of references and knowledge.

One property about cloud computing is the ability to handle large volumes of work with easy as customers, employees, and stakeholder's information is stored on the organization's websites permitting quick access and delivery of services. Through the internet, a person can access a wide array of information and services that have made life quite simpler. Companies and institutions that have embraced this technology attest escalated customer satisfactions, reductions costs, and easy management of inventories and business assets (Puthal, et al., 2015). Cloud computing has become the most reliable means of conducting business, accessing public and private services, is has come a hallmark center for research and education. People depend on nearly everything on the technology (Jadeja & Modi, 2012).

As much as the web users enjoy it, as earlier stated the imminent obstacle to the widespread adoption of cloud computing are security and privacy issues. A considerable of people, corporation, public institutions and research organizations are very reluctant to trust cloud computing technology thus are adamant in shifting their digital assets to third party service providers. The reasons behind their reluctance cannot be overlooked and dismissed. Web services are infested with insecurities. It is of fundamental importance to undertake strict security measures in protecting the company assets and customers privacy (Zissis & Lekkas, 2012). Various studies attest to cyber insecurities and attacks to be the prime limitation of the magnificent technology. According to Ali, et al. (2015) robust security measures must be taken to safeguard the data stored in cloud server at all cost.

According to Butterfield, et al. (2016), the success of any cloud-based services rests in the aptness of the decision-making the process at every step of the systems life cycle as per the organization's strategic plans. Throughout the entire lifecycle of the clouded based applications many stakeholders are involved hence, it is critical to have certain organizational, legal and ethical policies pertaining the management and use of the services (Kshetri, 2013). Cloud computing has become a dream come true in the paradigm of computing utility that has been providing reliable and resilient infrastructure to users. The decision-making process has enabled users to store data remotely and use on demand the web applications and services. It has mitigated the burden of local storage of data and reduction of costs on outsourcing of resources as well as maintenance. Besides the online security threats, cloud computing also faces a dire challenge from loss of data through lapses in physical control as well as possession of the data (Chang, et al., 2016).

Architecture of Cloud Computing

Cloud computing design is based on interconnected and configured internet networks which do not require the users to have special knowledge about the concepts and details of the technology. The cloud-based resources can either be externally owned such as public cloud servers powered by Google and Amazon or internally owned referred as private Cloud. The public Clouds offers access of

general public users through a pay-as-you-use basis while the private Clouds enable access to users within an enterprise without any charge as the services are paid in advance (Jadeja & Modi, 2012). The challenges encountered in the management of cloud architecture comprise of user interfaces, task distribution, and coordination.

Jadeja & Modi (2012, pp. 887-888) describes the characteristics of cloud computing that shall help in the analysis of its architecture and properties. First, it is prudent to acknowledge web users can browse and access data and information from anywhere regardless of the device they are using. The third party service providers enable users to access the internet from their computerized gadgets. In addition, minimal its skills are required for the implementation of the technology as individuals can surf with minimal skills, at most basic computer skills are sufficient (Puthal, et al., 2015; Masud & Huang, 2012). The design of web-based application also provides reliable services for multiple sites feasible for large institutions and markets; however traffic issues can slow down the use of the system. Tennace of the systems is easier as they need not be installed on the every user's' computer. Pay-as-you-use billing properties permit regulation and measurement of the usage of services per a client or user. The performance of the systems can be monitored hence it is scalable. The security of critical data is much more secure with appropriate and coherent measures (Zissis & Lekkas, 2012).

Having looked at the characteristics and properties of cloud computing, they provide a credible front of the architecture. The technology can be divided into two distinct categories: the front end and the back end explains Jadeja & Modi (2012, p. 888). The front end is basically the user interface while the back end is the entire cloud system (encompassing computers, servers as well as data storage) that enable the user to perform his/her efficiently commands. The two sections are interconnected via a network, using the internet. Basing on the definition of cloud-based systems, the computers are interconnected and configured to a central computer/server that manages the monitor's traffic, aid in te administration of the system and management of the client's demands. Despite the system being user-friendly and efficient, its efficacy is guided by the rules put in play for its operation such as protocols and special software is known as middlewares that allow computers to communicate to each other (Patterson & Hennessy, 2013; Puthal, et al., 2015).

Between the users and the client, some layers and services facilitate the server user interface. There are applications, web platforms and infrastructures enabling the web interactions. The layers shall be analyzed from the front to the back end. At the front end are the cloud clients which encompass the computer hardware and software that depend on cloud computing for service delivery (Patterson & Hennessy, 2013). A cloud application concerns the provision of Sofware as a service (SaaS) on the web eliminating the need for installation and running of the software of the each user's computer system. The networks and connection capabilities are managed from a central point allowing the clients to access the information and data remotely through the internet. For instance, through Google App, people can access huge sums of information about an institution without necessarily physically visiting the organization's offices. IBM, Oracle, Netsuite, and Microsoft besides Google apps are some of the commonly used SaaS (Jadeja & Modi, 2012).

The application work well under specific [latorms which as referred as Platform as a service (PaaS). The platform services provide a computing podium that enables users to use the cloud infrastructure. The system has all the necessary applications and software enabling efficient the interaction between the users and the servers. The platforms eliminate the necessity of the users purchasing and installing the applications into their computers. Some of the platforms include GAE and Microsoft's Azure which have been developed with sufficient attributes that facilitate its operation in its entire life cycle. On the other hand, the Infrastructure as a Service (IaaS) provides the necessary infrastructure needed for the servers. It also eliminates the necessity of the users to purchase servers, network resources as well as data centers. They include GoGrid, Layered Technologies, Masso just to name a few. Servers sums up the layers and services of a cloud computing system, they store and disseminate information and data to all the computers linked to it via the platforms and applications (Jadeja & Modi, 2012).

Cloud computing can be deployed through different mechanisms; however there are three primary ways of implementing the services: public cloud, hybrid cloud, and the private cloud. All the needs of an organization such as governance data, risk management, policies and guidelines, company databases, monitoring, and controlling among others are all directed to the cloud and captured by the designated cloud (Jadeja & Modi, 2012).

The public clouds allowed access to the cloud through the use of web browsers under the pay-as-you-use paradigm. As earlier stated, the private clouds are own by particular organization or institutions permitting access of data designed for purely for the internal use. They are easier to manage, control, and upgrade as compared to public clouds as it has a limited number of users and can be managed by the organisation. The hybrid clouds consequently combine the private and public clouds. It is designed in a manner that allows the linking of private clouds to one or more public servers. It is more efficient and secure compared to the former two. The design and adoption the cloud computing depends on the objectives of the organization or institution. It is essential for the organization to undertake a critical evaluation of the design and architecture of the system they want to use and which can yield the maximum benefits as well as more secure (Masud & Huang, 2012; Jadeja & Modi, 2012).

The security of cloud-based application are also determined by the data life cycle, a process ranging from data generation to destruction. The process is divided into seven phases: production, transfer, use, share, storage, archival and destruction (Erl, et al., 2013). Data generation aspects pertain the ownership of data; the owners oversee the management of data. Data transfer involves the transmission of data within the boundaries of access capabilities. Confidential data is managed by a particular group of authorized personnel; employees have a limited grant to access information. Data use refers to the approval to acquire and manipulate the stored information, the data is often not encrypted to allow ease utilization and elimination of problems that may lead to indexing and query complications (Butterfield, et al., 2016). The sharing phase pertains the expansion of the spheres of data dissemination as well as data permission for critical data. The storage steps involve the redirection of information to a particular location for future use; the data can either be stored in an Iaas or PaaS environment. The archival stage permits offsite storage of data for long duration; it also involves storage of very critical data prone to risks of insecurity (Almutairi, et al., 2012). Finally, destruction phases are the destruction of irrelevant data, however, data deleted is restorable hence can lead to immense security issues is disclosed.

Security and Data Confidentiality Issues

The topic of cloud computing is inconclusive without the discussion of security and privacy issues. Both organizations and clients value the privacy of their information. In the recent past, problems with web insecurities and cyber attacks have been incredibly rampant. Security and confidentiality protection concerns are grave importance. According to Chen & Zhao (2012) the openness and multi-user property of the cloud has brought substantial impacts to the field of information security. Lack of definite cloud infrastructure and safety boundaries are escalated due to the dynamic scalability of the technology, service abstractions and storage transparency features that make it difficult to a particular threaten or compromised resource. Another imminent shortcoming of services provided by cloud technologies emanated from the ownership of the servers. Multiple parties own most of the servers; it is often difficult to harmonize security protection issues and coming up with unified security measures whenever the parties have a conflict of interest (Sen, 2013).

The multi-user property of the tech also poses a grave impediment in ensuring the protection of information. The system is very open, and the virtualized sharing of resources can allow a user to access unauthorized data in the disguise of the accredited party. Some of the cyber breaches occur within the organization where an employee can gain access to logins of their superiors allowing them to access unaccredited data (Butterfield, et al., 2016; Sookhak, et al., 2015). The greatest drawback of the technology results from the large volumes of data directed to the cloud servers. The extensiveness of the data poses a grave shortcoming

in the storage and access of data. Whenever large quantities of data access concurrently by several users, it causes internet traffic leading to very clumsy access of the information (Wang, et al., 2012).

The virtualized environment of cloud computing equally has introduced its set of vulnerabilities and risks which include malicious cooperations stemming from virtual machines (VMs) to VM escapes. Using the virtualized networks such as VM image sharing, malicious people can share images containing malware which once uploaded into a user computer it grants the person access hence allowing them manipulate and corrupt confidential information as well as leaking critical information to the public. The cloud models such as PaaS, Iaas, and SaaS dependency also causes a grave insecurity concern (Modi, et al., 2013; Wang, et al., 2012). For instance, in an intruder manages to gain access and control of other of the models, the other models are compromised. None of the models can operate independently hence, an attacker may only attack one model which will cripple the entire system. Besides data privacy and security issues, legal matters pertaining cloud computing also induces considerable challenges in the management of the system. Under different areas of jurisdiction, cloud owner encompasses conflicting legalizations and policies creating problems of which laws to apply or adhere to (Ali, et al., 2015; Ahmed & Hossain, 2014; Kshetri, 2013). Such cases have the potential of leading to risks of privacy breaches.

Remedies to Cloud Computing Issues and Challenges

There are several solutions noted in literature to aid in combating of cyber insecurities and privacy breaches. One of the most discussed remedies is trust; it has been extensively researched in the field of computer science more so on the security and access control issues, computer networking as well. The guiding principle trust states the "*Am entity A is considered to trust another entity B when entity A believes that entity B will behave exactly as expected and required*" (Zissis & Lekkas, 2012). Trust nevertheless depends extensively on the deployment models used, the governance, outsourced applications and delegation of the servers control protocols (Zissis & Lekkas, 2012). Trusted Third Parties (TTP) are considered to be viable and ideal enhancers of web security. Besides the TTP, it is vital for cloud owners to deploy an application for security identification of threats, such standards help in early detection and prevention of potential malware and threats such as Trojan horses and worms (Sen, 2013).

Security can also enhance by the use of multiple data protection protocols such as firewalls, IPS, IDS, Virtual LAN, use of antivirus software, encrypted access permissions among others (Sen, 2013; Chen & Zhao, 2012). The standards help in reduction of leakage of customers data through VM networks. Advanced Cloud Protection Systems (ACPS) have been advocated to provide significant cloud resources and services security (Modi, et al., 2013). It shields the cloud from attacks directed to users from networks as they monitor VMs running on the host platform. CyberGuarder is another vital security tool. It works on the principles of VM isolation by use of the virtual private networks (VPN) that bridges the layer-two tunnels. They monitor network traffics and provides additional security through the application integrity verification as well as monitoring of the system calls that have been invoked by applications. These with many other cyberattack countermeasures can de deploy to ensure cloud computing is sustainable protecting organisations and customers privacy (Ullah & Khan, 2014).

CONCLUSION

Cloud computing as discussed in an indispensable tool in the current digital age where almost every aspect of information and communication has been integrated to cloud technology. Users gain considerable benefits such as reduced maintenance costs in outsourcing of resources, quick access to data as it is centralized, access of information from any location just to name a life. Cloud-based services have taken over the traditional information systems and had extensively been embraced by many people, private and public corporations and institutions. Notwithstanding, the benefits the technology should not bar its users from visiting its limitations. Despite the many opportunities and benefits, the system has a substantial shortcoming. Security and privacy protection concerns are the most critical inhibitors of the adoption of the

technology. Data transmitted and stored in the cloud do not provide a hundred percent security. Cybercrimes, attacks and breaches have been on the rise, therefore, all third-party service providers and the users should take great efforts in ensuring their systems are well secure. The paper has listed some of the countermeasures that can be used.

REFERENCES

Ahmed, M. & Hossain, M. A., 2014. Cloud computing and security issues in the cloud. *International Journal of Network Security & Its Applications,* 6(1), 25-31.

Ali, M., Khan, S. U. & Vasilakos, A. V., 2015. Security in cloud computing: Opportunities and challenges. *Information Sciences*, 305, 357-383.

Almutairi, A. et al., 2012. A distributed access control architecture for cloud computing. *IEES Software*, 29(2), 36-45.

Butterfield, R. et al., 2016. Towards Modelling a Cloud Application's Life Cycle. *Proceedings of the 6th International Conference on Cloud Computing and Services Science (CLOSER 2016)*, 1, 310-319.

Chang, V., Kuo, Y. H. & Ramachandran, M., 2016. Cloud computing adoption framework: A security framework for business clouds. *Future Generation Computer Systems*, 57, 24-41.

Chen, D. & Zhao, H., 2012. Data Security and Privacy Protection Issues in Cloud Computing. *International Conference on Computer Science and Electronics Engineering (ICCSEE)*, 1, 647-651.

Erl, T., Puttini, R. & Mahmood, Z., 2013. *Cloud computing: concepts, technology, & architecture*. Pearson Education.

Jadeja, Y. & Modi, K., 2012. Cloud Computing - Concepts, Architecture and Challenges. International Conference on Computing, Electronics and Electrical Technologies, 887-880.

Kshetri, N., 2013. Privacy and security issues in cloud computing: The role of institutions and institutional evolution. *Telecommunications Policy*, 37(4), 372-386.

Masud, M. A. & Huang, X. 2012. An e-learning system architecture based on cloud computing. *System*, 10(11).

Modi, C. et al., 2013. A survey on security issues and solutions at different layers of Cloud computing. *The Journal of Supercomputing*, 63(2), pp. 561-592.

Patterson, D. A. & Hennessy, J. L. 2013. *Computer organization and design: the hardware/software interface*. Newnes.

Puthal, D., Sahoo, B. P., Mishra, S. & Swain, S., 2015. Cloud computing features, issues, and challenges: a big picture. *International Conference on Computational Intelligence and Networks (CINE)*, 116-123.

Rittinghouse, J. W. & Ransome, J. F., 2016. *Cloud computing: implementation, management, and security*. CRC Press.

Sen, J., 2013. Security and privacy issue in cloud computing. *Architectures and Protocols for Secure Information Technology Infrastructures*, 1-45.

Sookhak, M. et al., 2015. *Remote data auditing in cloud computing environments: A survey, taxonomy, and open issues*. ACM Computing Surveys (CSUR, 47(4).

Ullah, K. & Khan, M. N., 2014. Security and Privacy Issues in Cloud Computing Environment: A Survey Paper. *International Journal of Grid and Distributed Computing*, 7(2), 89-98.

Wang, C. et al., 2012. Toward secure and dependable storage services in cloud computing. IEEE Transactions on Services Computing, 5(2), 220-232.

Zissis, D. & Lekkas, D., 2012. Addressing cloud computing security issues. Future Generation Computer systems, 28(3), 583-592.