International Journal of Engineering & Technology, 9 (2) (2020) 454-457

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

Security of cloud computing: belongings for the generations

Jahangir Jabbar [1] *, Hussain Mehmood [1], Hassaan Malik [1, 2]

[1] *Department of Computer Science, National College of Business Administration & Economics, Multan, 66000, Pakistan*
[2] *School of Systems and Technology, University of Management & Technology, Lahore, 60000, Pakistan*
**Corresponding author E-mail: jahangir2002@hotmail.com*

Abstract

Cloud computing plays an important role in Information Technology (IT) management. Consequently, various cloud computing developers and users experience different benefits and similarly challenges to its use and potential opportunities in driving the Fourth Industrial Revolution. Despite the increasing benefits of cloud computing, including increased speed of data processing and reduced costs compared to traditional computing, issues of security and privacy risk remain one of the greatest concerns in cloud computing. Through a systematic literature review, the evolution and developments in technology and issues of security and privacy from many years are examined to establish the trends in the threats; and thereby, provides a projection on the future of security of cloud computing. This paper presents the cloud computing aspects (types/aspects, and categories such as Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS). The paper dwells on the challenges of cloud computing going into the future with some solutions that have potential to work.

Keywords: *Cloud Computing; IT Management; Internet; Security.*

1. Introduction

Cloud computing, a technique used to store and access programs or data through the internet [[1]], is a core technological component in this digital era and the Fourth Industrial Revolution (4IR). In IT management, cloud computing continues to be a major boost and a breakthrough in the provision of efficient computing. Some of the associated provisions of cloud computing include centralizing data reposition, processing of data as well as information measures [**Error! Reference source not found.**] [[2]].
John McCarthy's speech at MIT in 1960 indicated that computing can also be sold as utility just like water and electricity, and since then computing has met with evolution [[3]]. Starting from Salesforce Company in 1999, to Amazon Web Service in 2002, there has been continuous provision and improvement of cloud computing. The emergence of cloud computing and subsequent growth in popularity and continued appreciation in IT management can be associated with the ability to manage a huge number of operations without service interruptions and within the cloud transparently [[4]].
There are different aspects of cloud computing worth appreciating; (a) a cloud made available to the public based on only pay-as-you-go system is called Public Cloud [[4]], and (b) a cloud infrastructure that is operated for the sole business or an independent organization is called Private Cloud [[4]]. Otherwise, a combination between a Private Cloud and that of a Public Cloud is called Hybrid Cloud. [[5]][[6]]

Public Cloud	Hybrid Cloud	Private Cloud
• Public cloud makes resources such as virtual machines and applications for storage available. • The services are offered by third party provides • They are available for sale or for free to anyone • Clients can pay based on • Storage • CPU cycles. bandwidth consumed • They can save companies costs of purchase, maintenance, and management	• A mix of the private and the public cloud computing characteristics • Offer greater flexibility but at a reduced cost • Offering a hybrid cloud requires the following to be available • Public Infrastructure as a Service (IaaS) such as Google Cloud Platform or Amazon Web services • Adequate Wide Area Network (WAN) • Hosted private cloud provider	• Private cloud is offered to individual organizations through private infrastructure • It is managed through internal resources • Allows for greater elasticity and scalability as well as control and adaptation. • Ideal for companies that have to conform with strict data processing and security

Hybrid cloud computing brings together all the aspects of both public and private cloud computing Some of the main components of cloud computing include systems software, hardware and the applications that are offered, processed or delivered over the internet. For example, a cloud computing system commonly used by various organizations and individuals include E-Mail, where organizational email typifies

the Private Cloud and Gmail or Yahoo mail for Public Cloud. Other examples of Cloud Computing include Google Cloud, where Google App provides a search engine (or platform) for the development of web applications.

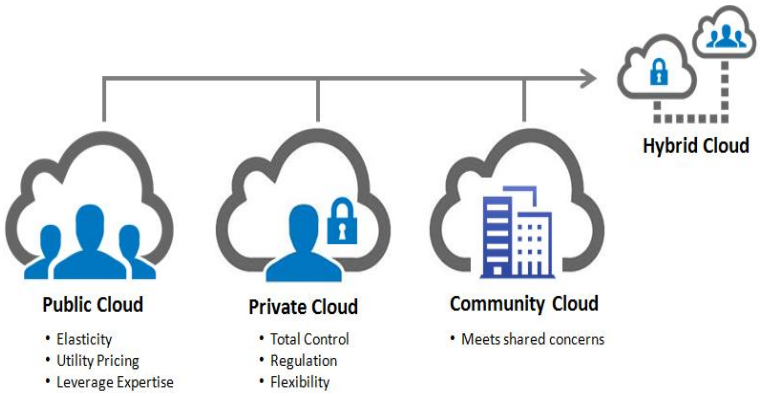

Fig. 1: Main Characteristics of Each of the Three Aspects of Cloud Computing.

The cloud providers are grouped into various categories. Accordingly, Gilliam and Nick indicate that cloud providers include

1) Infrastructure as a Service (IaaS)
2) Platform as a Service (PaaS)
3) Software as a Service (SaaS) [[4]].

Infrastructure as a Service offers web-based access to the computing power as well as storage; PaaS gives the developers tools that are used to build and even host web-based applications; and SaaS are applications that can be accessed by and from several client devices through a web browser [[4]] [[7]].

Platform Type	Common Examples
SaaS	Google Apps, Dropbox, Salesforce, Cisco WebEx, Concur, GoToMeeting
PaaS	AWS Elastic Beanstalk, Windows Azure, Heroku, Force.com, Google App Engine, Apache Stratos, OpenShift
IaaS	DigitalOcean, Linode, Rackspace, Amazon Web Services (AWS), Cisco Metapod, Microsoft Azure, Google Compute Engine (GCE)

Fig. 2: Examples of Cloud Computing for Each Platform.

Overall, the underlying differences between cloud computing and the traditional computing solutions include aspects such as: cloud computing being built upon a scalable and flexible infrastructure; the underlying software and associated infrastructure is offered and abstracted as a service; data and information can be shared over the Internet using any device; and users pay for the computing services and resources used without any upfront commitment by those users [[7] - [9]].

There are various characteristics of cloud computing, indicating the existing challenges, implications for the use, and potential use at present and in future IT management and 4IR. The common characteristics of the cloud computing services include the security offered, the license type, cloud users, adherence to standards and the payment systems among others [[7]]. Some of these characteristics, such as the provision of open-source software platforms, security and privacy and licenses to use the platforms, play a critical role in offering the infrastructure and platform in which the future generations may realize the benefits of cloud computing. It is worth appreciating the past and present attempts to ensure proper security and privacy of the data shared or processed through cloud computing platforms. Notably, there are country-specific or regional laws, such as the EU's data protection laws, which are meant to protect the end-users of the cloud computing platforms. However, there still exist various challenges concerning security and privacy challenges; which create even a bigger challenge and threat to the use and appreciation of cloud computing in the future. For example, recent developments on the exploitation of public data on platforms such as E-Mails and Facebook by Cambridge Analytic are some of the evident challenges, which may even complicate future security and privacy for the future cloud computing users.

Based on these eminent challenges in cloud computing, the primary aim of this study was to investigate the current challenges with the security and privacy risks associated with cloud computing and thereby project the findings to the future generations in terms of security implications of cloud computing in businesses and the general public. Moreover, with the recent developments on security and privacy breaches involving cloud-computing users, this study examine the potential threats that may interfere with the progression of cloud computing in the future, which may limit and entirely ruin moving to the cloud.

2. Cloud computing challenges

There are five major categories of challenges in cloud computing that pose serious challenges to future generations in social and economic uses of the technology. These are availability and reliability, performance, interoperability, portability and performance [[10]].The following challenges directly or indirectly fall into one or more of the five categories above. Security and privacy are at the heart of many of the challenges associated with cloud computing.

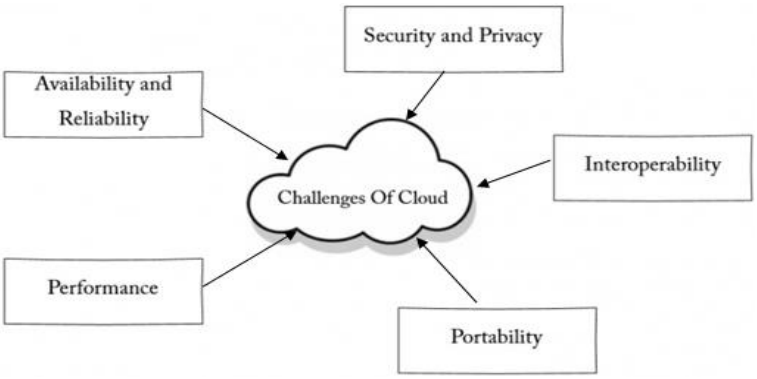

Fig. 3: Basic Categories into Which Challenges of Cloud Computing Fall.

The threat of account and service hijacking is real in cloud computing. Attackers or hackers still pose the threat of gaining unauthorized and malicious entry into a web service in a website hosted in a cloud server or whose service providers rely on cloud computing. Hackers still have great powers to install their control software in cloud infrastructures. Since future generations will be increasingly reliant on cloud computing, it means that plentiful more data (personal and private) will require to be dealt with through cloud computing and hence the need to address service hijacking and many other security issues.

Abuse and malicious use of cloud computing is also a major challenge going into the future. Hackers can install malware and spam to gain access and commit fraud and theft. In the same category are cross-site scripting, denial of service attacks and insecure programming of applications. Additionally, data breaches, hacked interfaces, and APIs, broken authentications and compromised credentials are also concerns for many people [[11]]. All these and more security concerns have pushed many people to be wary of cloud computing and limited its application and usage to issues that pose relatively low security concerns.

Cloud computing poses the challenge in costs and containment. Cloud computing can save businesses money by eliminating the costs incurred in installation and maintenance of hardware. However, due to the scalable and on-demand nature of cloud computing services it becomes difficult to predict costs and quantities. Organizations are also placing more workloads on clouds thereby requiring the cloud service providers to keep up with various tools and plenty of expertise.

Governance and control of the cloud computing is also a significant challenge that borders on security issues and organizational goals. Proper governance of IT systems requires that assets are used and implemented in accordance with some agreed procedures and policies to ensure proper control and maintenance of the assets in a manner that supports and business goals and strategies of specific organizations. However, that is not the case with many cloud-computing systems and organizations have to fit in with the cloud's services allowing only slight customizations.

Cloud computing also faces challenges in compliance [[11]]. Whenever organizations especially those in profitable businesses move their data from their internal storage to have it in a cloud they face challenges with industry compliance regulations and laws. For instance, healthcare organizations in the US have to comply with the Health Insurance Portability and Accountability Act (HIPAA) of 1996 while public traded companies have to comply with the Sarbanes-Oxley Act of 2002. Failure to comply with industry regulations places an organization at risk and exposes it to lawsuits and security lapses against which it cannot be covered or protected by laws or industry regulations.

There are a number of challenges in cloud computing that are related to performance. These include longer downtime and reduced service provider reliability. When companies are reliant on crowded cloud computing providers, they risk facing lengthy and loss-ridden downtimes for which they have little control over [[10]]. There is a security risk of interference during downtimes. Technicians from cloud computing companies may not always be available when users need them.

Cloud computing services have issues integrating smoothly with on-premise IT hence raising problems with interoperability and portability. Businesses ought to have the leverage of migrating from the cloud and to various providers without lock-in periods that they face with cloud computing.

3. Analysis on cloud computing security

Cloud computing is at the heart of new generation technology. However it should be noted that there is no infrastructure that is invulnerable to security threats [[12]]. Failure to provide adequate security measures and protection of privacy will result in catastrophic outcome along with potential loss and high costs that could eliminate all the potential benefits of cloud technologies.

Cloud security refers to a set of cloud-based policies and technologies that are adapted to regulatory compliances as well as improving the functionality of cloud technology infrastructure [[14]].

When planning for cloud security going into the future it is advisable that analysts and organizations follow this plan. The first step is to analyze the sensitivity they have to risks or exploring the areas where they are vulnerable [11]. Secondly, they need to train all personnel to be careful and watchful in handling cloud-computing technologies to avoid creating loopholes that can be exploited by hackers and all unauthorized persons. Thirdly, ought to be the type of cloud that an organization chooses. The other issue should be having the users try to gain an understanding of data storage and transfer mechanisms.

Cloud security controls can fall into four main categories- preventive, detective, corrective and deterrent controls. Preventive controls refer to measures of strengthening systems against attacks and incidents by eliminating possible vulnerabilities. Detective controls are meant to detect and react appropriately and instantly to incidents. Deterrent controls give warnings as a way to reduce threats. Corrective controls on the other hand come in when some threat has had broken into a system and it reduced the impacts of such incidents by controlling or limiting damages. As such, the major points that one ought to adopt in securing cloud data include auditing, access control, authorization, and authentication.

4. Solutions to cloud computing challenges

Numerous solutions are coming up to address various security concerns and challenges facing cloud-computing technologies. Improvements are continuously sought by Cloud Service Providers (CSPs) in augmenting their cloud infrastructure with technologies, architectures, resources, organization designs, processes, and workflows [[15]]. These result in better delivery of cloud services, security against attack, and accommodation of human error. To begin with, organizations and individuals using cloud computing need to verify that that the SaaS provider has secure user authentication, identify management and that secure access control mechanisms are in place. It is also important for users to verify the database security and privacy laws that the cloud service provider subscribes. It is also important that going into the future, the cloud computing service providers cover as much ground as they can in compliance with laws and regulations from various industries or sectors [[11]].

There are a number of tools that can be used for analyzing cloud computing. One of the best is Weka- a java-based machine-learning tool that uses C 4.5 algorithm for its decision tree implementation. Weka can be used in data mining processes and applied from one's java code or applied directly to a dataset. It is a whole package with the tool being used for regression, data pre-processing, classification, association, clustering, and visualization [[11]]. In the pre-processing phase, Weka enables the user to select a file from the local machine or from a URL – where the user can select the data file from different locations.

Trusted Third Party service providers are ideal in offering integrity, confidentiality, and authenticity. They are entities that facilitate secure interactions between two parties that trust the third party. The TTP provide information systems that offer end-to-end security services, which are scalable, based on specialization sectors, geographical areas and useful domains across various domains.

5. Conclusion

There is no doubt that cloud computing will become the future's key computing paradigm. It is the practice of using remote servers hosted on the internet to manage, store and also process data instead of using local servers or personal computers. Cloud computing is advantageous, dynamic, and can deliver the processing power of super computers without procuring one physically. In addition, cloud providers such as Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS) have ensured the ease of offering new services in various forms. With its compelling influence and convenience of use, many sectors are eager to adopt the usage of the technology.

Despite the vast advantages and dynamism that could be achieved with cloud computing, challenges such as availability and reliability, performance, interoperability, portability and performance have been the accompanying drawback. More importantly, security threats is on the high alert as it could ironically be regarded as the limiting factor that result to potential loss that could diminish all the dominance of cloud technologies. However, security measures should be a non-compromising requirement for cloud computing environment. While there are numerous ways to deal with the accompanying problems of cloud computing. It is a worthwhile observation that tools such as Weka have been conveniently used for regression, data pre-processing, classification, association, clustering, and visualization. Addressing all of these challenges also assist in dealing with security challenges. Regardless on the kind of challenges, it can be concluded that there is the need to adopt some major measures such as auditing, access control, authorization, and authentication in all areas be they preventive, detective, corrective and deterrent controls, to deal with the shortcomings of cloud computing.

References

[1] Singh, Vaishali, and S. K. Pandey. "Research in cloud security: problems and prospects." International Journal of Computer Science Engineering and Information Technology Research (IJCSEITR) 3, no. 3 (2013): 305-314.

[2] Gorelik, Eugene. "Cloud computing models." PhD diss., Massachusetts Institute of Technology, 2013.

[3] Srivastava, P., Khan, R.: "A Review Paper on Cloud Computing." International Journal of Advanced Research in Computer Science and Software Engineering, 8(6), (2018). https://doi.org/10.23956/ijarcsse.v8i6.711.

[4] Gillam, Lee, and Nick Antonopoulos, eds. Cloud computing: principles, systems, and applications. Springer, 2017. https://doi.org/10.1007/978-3-319-54645-2.

[5] Erl Thomas; Puttini Ricardo & Mahmood Zaigham. Cloud Computing: Concepts, Technology & Architecture. Prentice Hall. 2013.

[6] Buyya Rajkumar; Broberg James &Goscinski. Cloud Computing: Principles and Paradigms. John Wiley & Sons. 2010. https://doi.org/10.1002/9780470940105.

[7] Höfer, C. N., and Georgios Karagiannis. "Cloud computing services: taxonomy and comparison." Journal of Internet Services and Applications, 2(2), 81-94 (2011). https://doi.org/10.1007/s13174-011-0027-x.

[8] Alam, Md Imran, Manjusha Pandey, and Siddharth S. Rautaray. "A comprehensive survey on cloud computing." International Journal of Information Technology and Computer Science (IJITCS) 7, no. 2 (2015): 68. https://doi.org/10.5815/ijitcs.2015.02.09.

[9] Núñez, Alberto, Jose L. Vázquez-Poletti, Agustin C. Caminero, Gabriel G. Castañé, Jesus Carretero, and Ignacio M. Llorente. "iCanCloud: A flexible and scalable cloud infrastructure simulator." Journal of Grid Computing 10, no. 1 (2012): 185-209. https://doi.org/10.1007/s10723-012-9208-5.

[10] NedalTurab, Anas Abu Taleb and Shadi R Masadeh. "Cloud Computing Challenges and Solutions." International Journal of Computer Networks and Communications. (2013). Vol.5, No.5. https://doi.org/10.5121/ijcnc.2013.5515.

[11] Siani Pearson, George Yee. Privacy and Security for Cloud Computing. Springer Science and Business Media. 2012. https://doi.org/10.1007/978-1-4471-4189-1.

[12] Yadav, R. Sharma, A.: "A Critical Review of Data Security in Cloud Computing Infrastructure. "International Journal of Advanced Studies of Scientific Research, 3(9), (2019).

[13] W3 Schools. Cloud Security Challenges. Retrieved 23 August 2019 from https://www.w3schools.in/cloud-security-challenges/.

[14] Isaca Information Systems Audit and Control Association. IT Control Objectives for Cloud Computing: Controls and Assurance in the Cloud. 2011.

[15] Yousif, M.: "Cloud Computing Reliability – Failure is an Option" in IEEE Cloud Computing, 5(3), 4-5 (2018). https://doi.org/10.1109/MCC.2018.032591610.