NEO Research

An Introduction to Cloud Computing

An overview on the cloud computing structure, usage, benefits and drawbacks

Written by:
Laurie Prélot
Yanik Kipfer

An Introduction To Cloud Computing

Laurie Prélot & Yanik Kipfer
NEO Research, Zurich, Switzerland
laurie@neonetwork.ch
yanik@neonetwork.ch

Abstract

Cloud computing has become a cornerstone in modern IT infrastructure. It provides copious amounts of beneficial services to individuals, small and big firm alike. However, as with any technology it also faces many non-neglectable challenges concerning security, regulatory compliance and accountability. This paper gives a short overview on the cloud computing structure, its usage and reviews the benefits and drawbacks of cloud computing. Then we propose solutions to address the challenges in cloud computing use.

Keywords

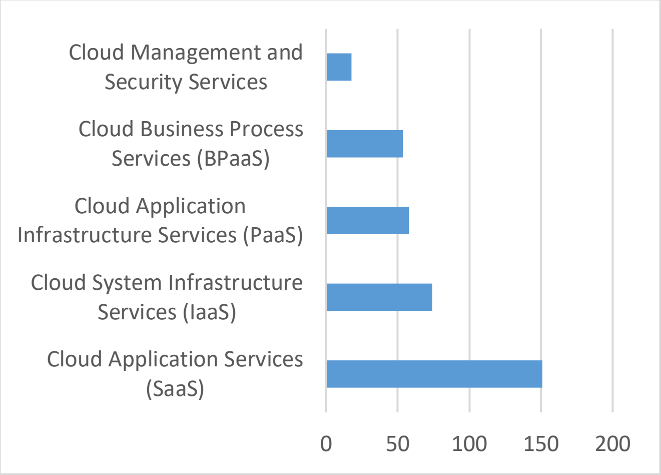
Cloud Computing, Technology, Regulation, Privacy

1 INTRODUCTION

From its emergence in the mid 90's, cloud computing has evolved to become a cornerstone of modern IT infrastructure. Both governments and businesses alike are increasingly adopting cloud computing services, to reduce their in-house IT costs. Looking at Switzerland alone, a study conducted by the ETH and the FHNW in 2016 concluded that around 30% of swiss firms are already, to some extent, using cloud computing services [1].

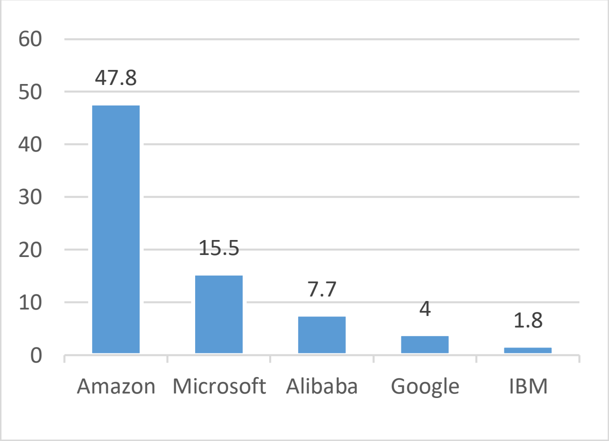
According to Gartner, worldwide public cloud revenue is expected to grow by 17% in 2020 and reach a whooping of 356 billion USD by 2022 [2]. Amongst all cloud services, the "Software as a Services", with an expected revenue of 151 billion dollars in 2022, is forecasted to be the most lucrative cloud computing service in the following years.

Figure 1: Worldwide Public Cloud Service Revenue Forecast, 2022 (Billions of U.S. Dollars) [2].



It is, therefore, not surprising that big tech firms have long since recognized that cloud technologies have a potential impact on our societies. Therefore, they have bet on cloud computing and are seeking to dominate this market. Currently, Amazon with its Amazon Web Services (AWS) is the leading provider of Infrastructure as a Service [3].

Figure 2: Worldwide IaaS Public Cloud Market Share (in %), 2018 [3].



The increasing importance of cloud computing services in our economy comes together with challenges. Thus, an inquisitive study of the issues that follow the use of this technology is needed. Amongst the main concerns frequently brought are the issues with security, privacy and regulation in cloud computing.

This paper will first give a short introduction to cloud computing and, secondly, provide an overview of the main advantages and disadvantages of cloud computing services, as well as suggest potential solutions aimed at remedying the aforementioned shortcomings.

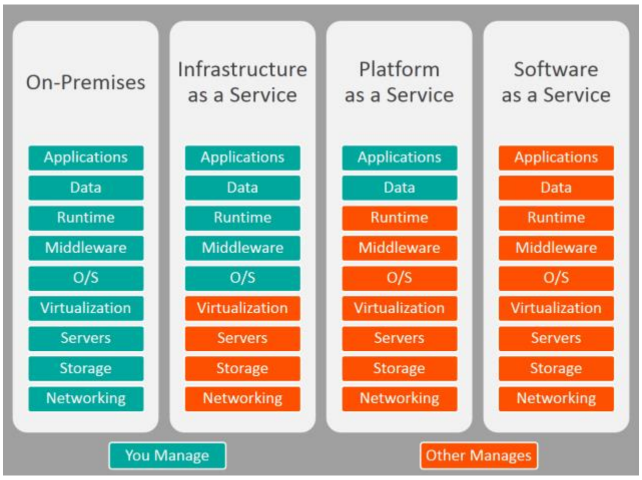
2 DEFINITION

Cloud computing can be described as the provision of computer system resources, like data storage, software and servers, through a network such as the internet or a Virtual Private Network (VPN). Stated simply, cloud computing allows companies to outsource their data processing tasks. The services provided by cloud computing allow firms to access and use a third party's software and computational power via a network, making it possible for them to rent servers, software and applications instead of buying and maintaining their own. Most cloud computing service providers charge for usage through a pay-per use subscription model. The pay-per use model of pricing allows customers the flexibility to adjust their need for computing resources as they see fit.

2.1 Services provided by cloud computing

The National Institute of Standards and Technology (NIST) identifies Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS), as the three main service models associated with cloud computing [4]. These three service models are mainly distinguished by the amount of control the consumer has over the cloud infrastructure and software. Figure 3 provides an overview of the three different service types and the amount of costumer control.

Figure 3: Main cloud service models from a consumer's perspective [5].



2.1.1 Infrastructure as a Service

Through IaaS the service provider makes its hardware (e.g. servers, storage and routers) available to consumers by renting out virtual machines (VM) [6]. The VM, provide the user with administrational control over the accessibility and runtime of the VM, the installation of software and applications, as well as the management and supervision of the operating system (OS). IaaS is, thus, highly scalable, since it provides the consumer with the option of increasing and decreasing his computational power "on the go". The underlying cloud infrastructure, however, is solely controlled and maintained by the provider. Examples of IaaS are Amazon Web Services, Microsoft Azure and Google Compute Engine.

What is a Virtual Machine?

The term "virtual machine" simply refers to software that pretends to be a stand-alone computer, with the advantage that you can switch between different operating systems with a few mouse clicks.

Virtual machines offer numerous advantages over installing operating systems and software directly on the physical hardware. Isolation ensures that applications and services running within a VM do not interfere with the host OS or other VMs. Virtual machines can be easily moved, copied and reallocated between host servers to optimize hardware resource utilization. Administrators can also take advantage of virtual environments for easy backups, disaster recovery, new deployments, and basic system administration tasks.

Thus, overall virtual machines allow for an easy and effective way of pooling and sharing computational hardware resources.

2.1.2 Platform as a Service

The PaaS provides the consumer with a computing platform, containing the OS, software, servers, middleware and computing environment [6]. The main idea behind PaaS lies in the delivery of a complete application development environment, containing all the needed hardware and software. Developers can thereby concentrate on the creation of application and do not need to worry about acquiring and maintaining the infrastructure needed for application development. Examples of PaaS are AWS Elastic Beanstalk, Windows Azure and Google App Engine.

2.1.3 Software as a Service

SaaS consist in the delivery of applications in the form of web-based services [6]. Prominent examples of this service model are Google Apps and Dropbox. The primary advantage of SaaS is that it reduces the workload of in-house IT. It removes the need to install software separately on each computer and, additionally, updating of software and hardware fall into the responsibility of the service provider. However, of all three service model types, this model is the one in which the consumer has the least amount of control.

3 ADVANTAGES AND DISADVANTAGES OF CLOUD COMPUTING

As seen in the previous section, the different service models address the needs of different consumers and, thereby, provide a distinct set of benefits to its customers. However, cloud computing services as a whole also offer broader perspectives. The following section will take a look at the potential of cloud computing services, together with the challenges that they are faced with.

3.1 Main Advantages

- *Cost reduction* [6,7]: The most striking benefit provided by cloud computing is, inevitably, its ability of reducing in-house IT costs. Be it IaaS, PaaS or SaaS, all service models have in common, that they allow firms to outsource their IT infrastructure to cloud service providers. This is especially advantageous for small firms, who often struggle to finance a fully equipped in-house IT outfit. Additionally, providers of cloud computing services can rely on economy of scale to vastly increase their own efficiency in comparison to the IT infrastructure of in-house IT departments.

- *Scalability* [6,7]: Cloud computing services grant firms the ability to easily and quickly increase or decrease their computing power and IT infrastructure through pay-per use subscription services. Thus, increasing or decreasing IT capabilities can be done by a simple and swift change of the subscription plan. In addition to saving costs, this also allows firms to respond to changes in the market in a quicker and more efficient way.

- *Data Backup* [*6,7*]: In the digital age of today, data backup has become paramount for every type of business. Natural disasters, human error or malicious attack can all lead to the loss of essential data. Cloud computing, in specific the provision of storage through cloud technology, allow firms to store their data offsite. Additionally, the data can be store in different server at different geographical locations, thereby, vastly decreasing the chance of total data loss in the event of a catastrophic event.

3.2 Main Disadvantages

- *Security [8]*: As with any computer based service, cloud computing services are prone to malicious attacks, technical faults and human error. Broadly speaking, security threats can be divided into two categories. Threats affecting the service provider and threats affecting the costumer. The primary threats faced by the service provider are related to infrastructure issues (e.g. software bugs, hardware damage, etc.) which might lead to data loss or data breaches, as well as malicious attacks both from within the provider's organization as well as from outside. On the costumer's side, main risks are security breaches caused by human error and malicious insiders, both of which can lead to the firms cloud account to become compromised.

- *Regulatory Compliance* [8]: Regulation in the firms home country might prevent data to be stored outside of the country or in countries which do not fulfil certain regulatory specifications. An example of how regulatory compliance might be an issue in the provision of cloud computing services is the case of the European Union's General Data Protection Regulation (GDPR). Firms seeking to store costumer data in servers located in countries which do not comply with the EU's privacy law will face significant regulatory difficulties and might even be banned from doing so. Additionally, firms in the financing or healthcare sector might face additional restrictions related to the use of sensitive personal data. Furthermore, a gradual fragmentation of the internet, with attempts at creating "domestic internet" in countries such as Iran, Russia and China, has taken place over the recent years and can be expected to increase pressure in regulatory conflicts.

- *Accountability and Data Control* [7,8]: In all of the above mentioned service models, the data is stored on servers owned and controlled by the providers. Firms do not have the knowledge of whether the providers are accessing their confidential data or not. Moreover, if the servers are located outside of the firm's home country, the firm might even be unable to use national laws to force the provider to comply with their desired data policy. Therefore, firms need to carefully consider what type of data they choose to save on the servers and which service provider they should choose.

- *Interoperability & Data-Lock In* [6,7]: A major concern for cloud users is the fact that once they commit on using the services of a particular provider, they might not be able to easily change providers again, should the need arise. The main reason for this, is that cloud providers might not offer export functionalities within their services, making it virtually unable to move data from one provider to the next. Additionally, the software employed by the different providers might also create a barrier for data migration.

4 SOLUTIONS

Having taken a look at the main disadvantages of cloud computing, we will now propose potential ways of mitigating these shortcomings. We identify two categories of potential solutions: regulatory solutions and technical solutions.

4.1 Regulatory Solutions

Regulation would primarily be able to solve the issues of regulatory compliance, accountability and data control. There are two means of regulating cloud service: government regulation and standards and conventions.

On the one hand, government regulation would ensure the broadest and the most easily enforceable form of regulation. Cloud service providers would be obliged to follow the laws and requirements set forward by the governing bodies or face punitive consequences. Government regulation provides a greater guaranty of accountability and control over one's own data and can force providers to implement transparency of their actions. Costumers of cloud service providers would have the backing of the national government, in disputes concerning data handling and breaches of confidentiality by the provider. Thus, government regulation would shift the responsibility of compliance and data safety from the costumer to the provider. However, government regulation would increase issues of regulatory compliance. Providers would only be able to provide access to servers in countries sanctioned by the national law and costumers dealing with sensitive data would need to carefully assess whether a firm complies with all the requirement to avoid being made liable.

On the other hand, standards and conventions provide a means of regulating the cloud industry on an international scale, instead of a solely national level. Standard and conventions allow cloud service providers to regulate themselves. Contrary to government regulation, standards and conventions rely mostly on consent and self-enforcement. The ability to self-regulate, allows for a less intrusive form of regulation, thereby, decreasing the risk of significant market distortions, which might hamper further innovations in the industry. It creates the ability of both industry and consumer associations to voice their concern and work toward finding a solution which is agreeable to both. However, enforceability of standards and conventions is significantly lower than that of government regulation.

4.2 Technical Solutions

Ensuring a good encryption of the data is the primary solution to prevent security issues and data breaches. Therefore, data should not only be encrypted when being stored, but also while being transferred. The provision of specially secured transfer channels for highly sensitive data, such as medical data, could further increase security and even allow firms working in these fields to more freely use cloud services.

Moreover, Interoperability between different cloud providers should be more widespread. From a purely economic standpoint, cloud service providers might oppose greater interoperability for fear of losing costumers, however, from an industry standpoint, the ability to freely and easily change between providers would raise trust in the industry and, thereby, increase further adoption of cloud services. Also, the ability to fully be able to follow who and when data was accessed or restrict access to data to certain countries would further increase trust, transparency and accountability. This could be either done through notifications every time someone accesses the data or through the creation of a protocol which records the time and place of accesses.

5 CONCLUSION

This paper set out to give an overview of the definitions, benefits and disadvantages of cloud computing, as well as suggest possible solutions to the most common challenges found within the cloud industry.

Cloud computing can significantly decrease IT infrastructure costs of companies, through the provision of efficient and scalable services. It is, therefore, not surprising that cloud computing is increasingly being used by private companies and governments who seek to outsource their IT needs.

However, cloud services also face substantial challenges which need to be addressed if the adoption of this type of technology is to further increase. The main disadvantages of cloud computing identified where issues concerning the security and safety of data storage and handling, regulatory compliance of cloud services with national data protection laws, accountability and control over data and the lack of interoperability and migration of data between cloud providers.

Both regulatory and technical solutions are available to solve these issues. From a regulatory standpoint government regulation, as well as standards and conventions could be used for problems involving accountability and compliance. While government regulations are better enforceable than standards and conventions, they are also is more disruptive for the industry.

Technical solutions are best suited for issues of security and interoperability. Better encryption of data in storage as well as during transfer, would decrease the risk of breaches. Furthermore, the creation of specially secured channels for highly sensitive data would further increase security and allow for adoption of cloud services in industry sector dealing with these types of data. Lastly, the adoption of greater interoperability and ease of data migration between providers would enhance trust in the industry and, thereby, increase adoption of cloud technology in business and society.

To conclude, cloud computing holds the promise to significantly reshape government bodies' and private firms' IT infrastructure and investments. While, the technology has already been widely adopted by various private and public institutions, the further spread of cloud computing services and technology is largely dependent on if and how the industry manages the solve the challenges mentioned within this paper.

6 REFERENCES

[1] S. Arvanitis, G. Grote, A. Spescha, T. Wäfler, M. Wörter, Digitalisierung in der Schweizer Wirtschaft: Ergebnisse der Umfrage 2016. Eine Teilauswertung im Auftrag des SBFI, KOF Studien, 2017. https://doi.org/10.3929/ethz-b-000167666.

[2] Gartner, Gartner Forecasts Worldwide Public Cloud Revenue to Grow 17% in 2020, Gartner. (2019). https://www.gartner.com/en/newsroom/press-releases/2019-11-13-gartner-forecasts-worldwide-public-cloud-revenue-to-grow-17-percent-in-2020 (accessed January 26, 2020).

[3] Gartner, Gartner Says Worldwide IaaS Public Cloud Services Market Grew 31.3% in 2018, Gartner. (2019). https://www.gartner.com/en/newsroom/press-releases/2019-07-29-gartner-says-worldwide-iaas-public-cloud-services-market-grew-31point3-percent-in-2018 (accessed January 26, 2020).

[4] P. Mell, T. Grance, The NIST Definition of Cloud Computing, (2011) 7.

[5] S. Watts, M. Raza, SaaS vs PaaS vs IaaS: What's

The Difference and How To Choose – BMC Blogs, (2018). https://www.bmc.com/blogs/saas-vs-paas-vs-iaas-whats-the-difference-and-how-to-choose/ (accessed January 26, 2020).

[6] M.K. Gourisaria, A. Samanta, A. Saha, S.S. Patra, P.M. Khilar, An Extensive Review on Cloud Computing, in: K.S. Raju, R. Senkerik, S.P. Lanka, V. Rajagopal (Eds.), Data Engineering and Communication Technology, Springer, Singapore, 2020: pp. 53–78. https://doi.org/10.1007/978-981-15-1097-7_6.

[7] A. Mikail, Big Data, Law and Policy: Cloud Computing in Europe, (n.d.) 23.

[8] K. Abouelmehdi, L. Dali, E. Abdelmajid, H.E.E. Fatiha, B. Abderahim, Classification of Attaks over Cloud Environment, in: 2015.