APSEI 2020-21

Assignment 3

Subject: **Cloud Computing versus On Premise**
Context: **Individual work to be carried out in the framework of APSEI 2020-21 under the supervision of Prof. Manuel de Oliveira Duarte**

Author: **Mário Silva nºmec 93430**
Date: **20/06/2021**

Index

1 Framework

In today's society, the popularity of cloud computing has increased so much, due to all the advantages it offers, from cost savings, flexibility, agility, scalability, and many others... However, on-premise software, that is installed on a company's infrastructures and behind their firewall is and has always been a reliable way for deploying a service for organizations. They allow for these companies to maintain a higher level of control, management, security, and others... when compared to the cloud. For these reasons, it is necessary to think very thoroughly when deciding the hosting strategy.

2 Objectives

Taking into consideration the context of the framework above, this assignment has the objective of defining Cloud Computing and what it offers, and do the same for the traditional on-premise approach, then compare these two approaches advantages and disadvantages and finally explain with use cases the thought process and decision making of the approach, accordingly to the requirements of each use case.

3 On-Premise

3.1 Definition

On-premise is the traditional approach in which all the required software and infrastructure for a given application reside in-house. On a larger scale, this could mean the business hosts its own data center on-site.

Running applications on-site includes buying and maintaining in-house servers and infrastructure. Apart from physical space, this solution demands a dedicated IT staff qualified to maintain and monitor servers and their security.

Many companies opt for on-premise because it does not require third-party access, gives owners physical control over the server hardware and software, and does not require them to pay month after month for access.

On-premises software is located and operated within a user's data center. As such, it uses the user's computing hardware rather than that of a cloud provider. Also known as "shrinkwrap", on-premises programs are among the most commonly used enterprise and consumer applications that require licenses per server or computer. Vendors are no longer responsible for their security and overall management but do provide after-sales technical support.

4 Cloud Computing

4.1 Definition

Cloud computing is an umbrella term that refers to computing services via the internet. By definition, it is a platform that allows the delivery of applications and services. These services include computing, storage, database, monitoring, security, networking, analytics, and other related operations.

The key characteristic of cloud computing is that the user pays for what it uses. The cloud service provider also takes care of maintaining its network architecture, giving it the freedom to focus on your application.

Most cloud providers offer much better infrastructure and services than what organizations set up individually. Renting rack space in a data center costs only a fraction of what it would to set up and maintain the in-house infrastructure at such a scale. Also, there are considerable savings on technical staff, upgrades, and licenses.

Essentially, cloud computing has enabled the use of a wide range of resources from third parties companies over the internet that can be provided quickly and easily. All the trouble needed to build and manage a static IT infrastructure is thus avoided.

Many cloud providers offer different deployment models for such resources: Public Cloud, Private Cloud, and Hybrid Cloud.

- ***Public cloud*** is the provision of computing services over the public internet by a third-party provider. Public cloud services are available to anyone who wants to use them and can be free or paid to use and are offered by providers such as Google, IBM, Amazon, Microsoft, and others.
- ***Private cloud*** is the provision of computing services for single organization access over the internet or a private internal network. A private cloud can be managed internally or by a third-party provider.
- ***Hybrid cloud*** is the provision of computing services through a combination of public cloud and private cloud deployments. This type of deployment allows the sharing of data and applications between both cloud environments.

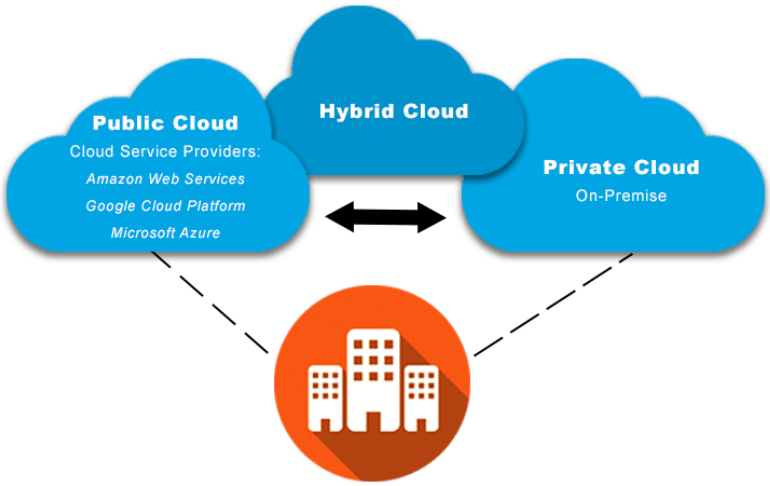

Figure 1: Cloud Computing Types

Apart from those models, cloud-based resources are commonly classified into three categories:

- ***Infrastructure as a Service*** **(*IaaS*)**: Offers services, such as Pay as You Go, and allows users to access processing, storage, networks, and other fundamental computing resources, to be used for any purpose.
- ***Platform as a Service*** **(*PaaS*)**: Is usually used to create and deploy applications. Resources like servers and storage can be managed by the enterprise or other 3rd Party providers, while developers can focus on the management of applications. Examples: *Heroku*, *OpenShift*, etc.

- ***Software as a Service*** **(*SaaS*)**: Allows users to use third-party software that runs on Cloud infrastructure. Frequently it is used when Companies do not want to spend time on installing, managing, or upgrading software. Examples: *Dropbox*, *Cisco WebEx*, etc.

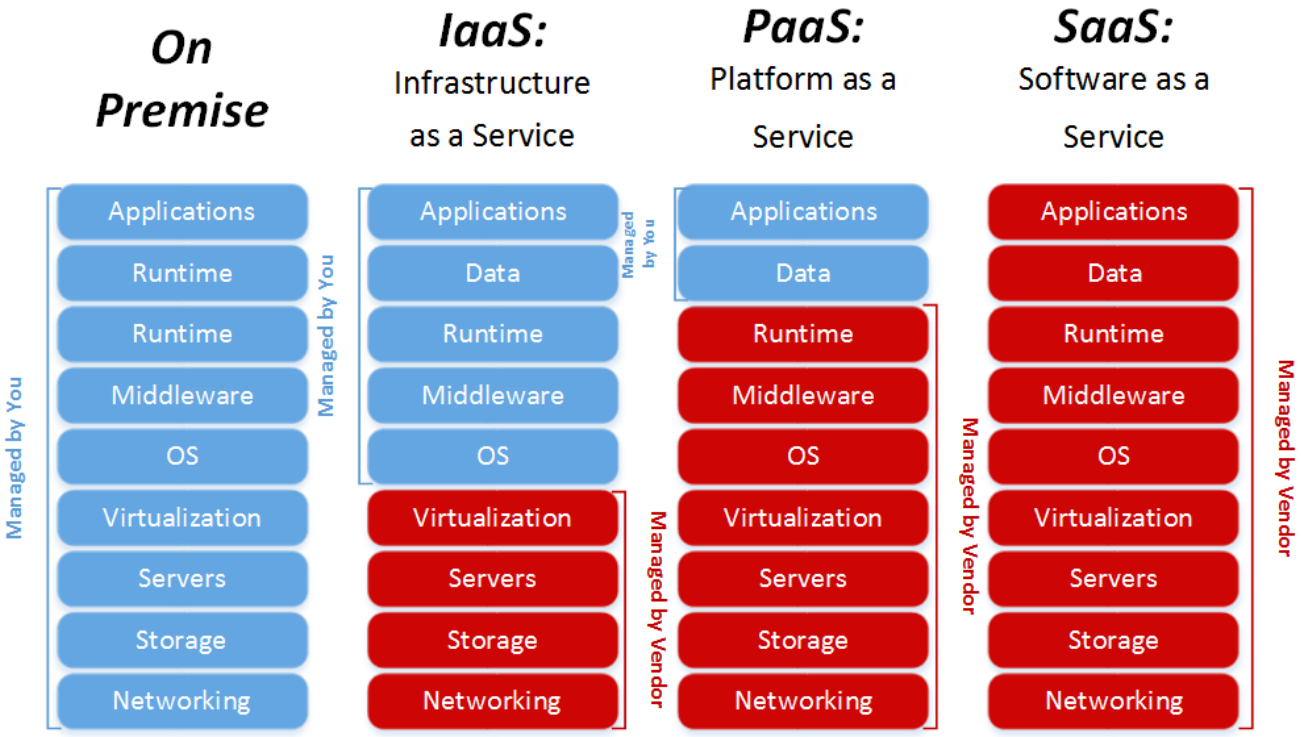

Figure 2: Cloud Computing Types

5 On-Premises versus Cloud Computing: Key Differences

Much has changed since organizations valued on-premise infrastructure as the best option for their applications. Nowadays, most companies are moving towards off-premise possibilities such as cloud or colocation.

There is no clear winner between on-premise vs. cloud computing solutions that cover all business purposes. Each organization must look into its architecture and make application-specific decisions, giving each application individual assessments.

When deciding on whether to go for a cloud-based or on-premise approach several aspects/metrics are necessary for the decision making, below are some of the most important aspects to take into consideration during the decision process.

5.1 Resilience and Elasticity

When it comes to resilience, cloud computing takes the upper hand, since backups and performance are consistent, sufficient, and automatically managed. The information hosted in the cloud is evenly distributed

across their servers, meaning that if one server fails, all the information can be retrieved without downtime. To maintain consistent performance, these systems use what is known as cloud elasticity, which is the provision of resources based on the needs of a machine. This means that they automatically deliver or remove resources to provide the right amount needed, ensuring the concept ”You only pay for what you need”.

Traditional computing is not so resilient and is limited to a certain maximum server performance, which is conducive to server downtime. What these systems lack the most is automation, like the elasticity provided by the clouds.

5.2 Flexibility and Scalability

Modern applications are continually evolving due to ever-increasing demand and user requirements. Infrastructure has to be flexible and scalable so that the user experience does not suffer.

5.2.1 Storage

Aside from the costs, it is worth mentioning some differences in how storage and their management differ from cloud and on-premise. On-premise storage resources are procured, owned, secured, and managed by the enterprise, this way storage resources remain dedicated to the company. The cloud storage resources are owned and managed by a third party, they may be purchased on a pre-paid or pay-as-you-go basis, they may also be shared in a multi-tenant environment, the software is kept up-to-date as part of an active subscription, and the IT team does not have to install software updates and patches on databases' software.

Cloud computing not only provides unlimited storage capacity and server resources but also allows to scale these resources according to the business needs, allowing for a more flexible and scalable model in comparison to traditional data centers. These server resources include bandwidth and internet usage. For cost-saving purposes, Cloud servers are scaled down or shut down when usage is low. This flexibility is possible due to the servers' virtual location and resources, which are increased or decreased conveniently. Cloud resources are administered through an admin panel or API.

In terms of OS dependency, cloud-based applications are fully independent, as they are not a constraint on a system with a specific OS, which is the case of the less flexible traditional applications.

5.2.2 Network

Traditional IT systems do not require an internet connection to access any data, but this is more a disadvantage than an advantage, as users can not access this data anywhere. Cloud hosting breaks this limitation by providing a fast and reliable internet connection, so it can be scalable to a wider range of people.

On-premise offers little flexibility in this respect because physical servers are in use. If the operations are ran on-site, resource scaling requires buying and deploying new servers. There are just a few cases where scaling is possible. A few involve controlling the number of active processors per server, increasing memory, and increasing bandwidth.

However, it is worth mentioning that network options depend hugely on what are the organizations' intentions. Sometimes they just need it for local usage and therefore, it is better to have the data center close to the facilities to decrease the latency.

5.2.3 Computing Power

Cloud computing allows better and easier management of the computing resources such as CPU and RAM. They grant the ability to easily scale vertically and horizontally the computer resources any time and on-premise solutions to do this require handling the physical aspect of this and integration in the software if necessary.

In general, cloud computing offers superior scalability options and is a good option for small and medium businesses that need little computing resources to start with and hope to scale their infrastructure in time.

5.3 Technical Involvement

Another critical factor that affects an organization's decision is the amount of technical involvement required.

On-premise involves on-location physical resources, as well as on-location staff that is responsible for that infrastructure. It requires full technical involvement in configuring and maintaining servers by a team of experts. Employing people devoted to ensuring the infrastructure is secure and efficient is very costly.

Cloud solutions are usually fully managed by the provider. They require minimum technical expertise from the client. However, service providers allow a certain amount of flexibility in this regard. Outsourcing maintenance allows to focus on other business aspects. Still, not all companies are willing to hand over their infrastructure and data.

Cloud offers a convenient solution for organizations. Especially if an organization doesn't have the staff or expertise to manage its infrastructure. However, organizations often opt for an on-premise solution because they need full control due to security requirements, continuity, and geographic requirements.

5.4 Security

Compliance and security are the most critical aspects of both on-premise and cloud computing. It is the most significant barrier to the adoption of these services. Current providers have made many innovations in securing their platforms across both on-premise and Cloud. For example, the introduction of the Private Cloud was a significant step towards achieving greater security in the Cloud.

Owners of in-house infrastructure manage all the security by themselves. They are responsible for the policies they adopt and the type of security they implement. Therefore, the level of security depends on the knowledge of the staff that manages the servers. Furthermore, there is less chance of losing data.

Cloud platforms are highly targeted by hackers because they store large amounts of sensitive information. However, it might be better to trust the data security needs to a reputable cloud provider, rather than dealing with the security ourselves.

Security becomes more critical with Cloud computing workloads. Client applications and data can spread across many servers or even data centers. The provider ensures Cloud security, including physical security. Providers should provide security measures like biometric access control, strict visiting policies, screening clients, and CCTV monitoring. These add another layer of protection in case of a physical attack. However, there is an increase in cost when opting for more security layers from the providers.

Certain countries and industries require data storage within a particular geographic region. Others require a dedicated server that is owned by the client and not shared with other organizations. In such cases, it becomes easier to manage with on-premise.

In summary, on-premise has the upper hand. Even though, there are also benefits to Cloud computing. The provider takes care of the security of both hardware and software. They also possess security certifications that are difficult for individual organizations to obtain.

5.5 Cost

The core difference between on-premise vs. cloud computing is also the very reason for their contrasting pricing models.

"Cost" can have different meanings. For example, there's the cost of purchasing on-premise resources versus using cloud resources. For on-premise, it is wise to identify underutilized storage resources before deciding how much capacity is needed. Under buying or overbuying assets is a common lament.

5.5.1 On-premise

With on-premise, the client uses in-house dedicated servers. Therefore, obtaining them requires a considerable upfront investment that includes buying servers, licensing software, and hiring a maintenance team. As said previously, on-premise is not as flexible when it comes to scaling resources, and not using the full potential or having a necessity for an upgrade might result in unwanted operating costs.

Clusters include any computing system. The total cost of a local compute cluster can be broken down into fixed and variable cost components. Fixed cost represents capital expenditure that does not change with usage time, whereas variable cost describes operational costs that depend on the duration for which the cluster is in use.

$$C_c = C_f * C_v \tag{1}$$

C_c: Cluster Cost
C_f: Fixed Cost
C_v: Variable Cost

The fixed cost term covers the cost of hardware equipment (computers, storage servers, cluster networking equipment) and facilities cost (cooling equipment, building alterations):

$$C_f = N * C_n + C_s + C_ne + C_fa \tag{2}$$

C_f: Fixed Cost
N: Number of Nodes
C_n: Node Cost
C_s: Storage Cost
C_{ne}: Network Cost
C_{fa}: Facilities Cost

Some of these variables may be very small or even ignored if they are not properly justified, for example, if the number of clusters is relatively small, it might not be necessary to add the cost of cooling them, or if the facilities are already available and working.

The variable cost includes operational costs, such as electricity, parts replacement, depreciation, software license and technical staff costs. These are easy to forget but evidence shows that up to two third of the overall cost is attributable to variable cost. Assuming a uniform monthly operational cost (the same average computing load, staff working hours and replacements each month), the following linear model describes the variable cost for the entire lifetime of the system:

$$C_v = m * (C_e + C_r + C_s t + C_d) + C_s o \tag{3}$$

C_v: Variable Cost
m: Cluster Lifetime (months)
C_e: Eletricity Cost
C_r: Replacement Cost
C_{st}: Staff Cost
C_d: Deprecation Cost
C_{so}: Software Cost

Electricity cost includes the cost of running the computers, storage units, cooling system, and networking equipment. In the simplest case, if the cluster operates in a 24/7 mode and computers are not under an energy-saving operating scheme, the monthly cost of electricity is calculated from the average power consumption of the hardware devices.

$$C_e = \frac{24 * 365}{12 * 1000} * (N * P_n + P_s + P_n e + P_c) + c_e \tag{4}$$

C_e: Eletricity Cost
N: Number of Nodes
P_n: Nodes Power Consumption (Watts)
P_n: Storage Power Consumption (Watts)
P_n: Network Power Consumption (Watts)
P_n: Cooling Power Consumption (Watts)
c_e: Electricity Cost Unit (USD/kWhPower)

Replacement cost is the average monthly cost of hardware parts replaced or repaired to keep the cluster operational. A first-order estimate of the cost of repair per year can be given as a percentage of the total cluster hardware cost. Staff cost covers all the personnel costs associated with operating the cluster. Cost components (hardware, salary, and electricity costs) should be adjusted to the local rates and hardware energy consumption characteristics when the model is used for actual calculations.

5.5.2 Cloud Computing

Cloud computing has fewer upfront costs. The infrastructure belongs to the provider, while the client only pays for using the devices on a monthly or annual basis. This is known as the pay-as-you-go model where the

user only pays for the units it consume and only for the time used. Cloud computing also doesn't require the cost of investing in a technical team. If not agreed upon otherwise, the provider takes care of maintenance.

Resources accounted for in the cloud model are the main cloud infrastructure elements; i.e. compute, storage, and networking services. There is a rich set of services offered on top of these infrastructure components, e.g. MapReduce/Spark data processing, containers, various database solutions, serverless Function/Lambda execution, and so on, but all of these can be incorporated into the proposed cloud model as trivial adjustments.

Tables 1, 2 and 3 list the unit price of the resources of the major cloud providers. Table 1 includes the hourly cost of virtual machine (VM) instances (compute nodes). Since vendors offer a wide selection of general, compute, memory, or storage optimized hardware configurations (AWS: over 160, Azure: over 240, GCP: over 60), only a representative set is included in Table 1. For more information and updates, it is necessary to visit the provider's websites and fetch the latest details.

Table 1: Cloud compute instance costs at the major service providers

Compute Instance Type	**Price C_{VM} (USD/h)**		
	AWS	Azure	GCP
vCPUs: 2, RAM: 8 GB	0.096	0.1	0.067
vCPUs: 4, RAM: 16 GB	0.192	0.21	0.134
vCPUs: 8, RAM: 32 GB	0.384	0.437	0.268
vCPUs: 16, RAM: 64 GB	0.768	-	0.536

Table 2: Cost of storage at the major cloud providers

Storage Type	**Price C_{st} (USD/GB/month)**		
	AWS	Azure	GCP
Standard Object Storage	0.023	0.0184	0.02
Nearline Storage (Once A Month)	0.0126	0.01	0.01
Coldline Storage (Once A Quarter)	0.004	-	0.004
Archive Storage (Once A Year)	0.00099	0.00099	0.0012

Table 3: Cost of networking at the major cloud providers

Network Resource	**Price $C_{network}$**		
	AWS	Azure	GCP
Ingress Traffic (USD/GB)	Free	Free	Free
Egress Traffic (USD/GB)	0.09	0.087	0.02
External IP Address (USD/h)	Free	Free	0.004

Cloud storage can be considerably cheaper than on-premise at lower data levels. But as the total amount of storage increases, so does the total cost, which may end up being more expensive in long term to use only the storage from the cloud provider.

In general, cloud computing has the upper edge. Not only does it have a pay-as-you-go model with no upfront investment, but it is easy to predict costs over time. Pay-as-you-go may seem attractive cost-wise until unused resources (such as virtual machines) are left running unmonitored for hours, days, weeks, or even months. Similarly, prepaid public cloud capacity can seem attractive because it tends to be less expensive

than pay-as-you-go. However, pre-paying for unused resources involves unnecessary costs. Comparing to on-premise computing, we can avoid the licensing costs and the investments inexpensive equipment to operate and maintain the servers. Besides, as off-premise computing can be locally manipulated, the infrastructure costs also decrease.

It is also important to recall that cloud providers handle redundancies. If one VM, server, or data center goes down or is destroyed, it does not affect the end user's cost. However, when on-premise equipment fails, there is an additional cost of replacement. The staff as mentioned previously, also is something important, in general, more IT personnel are required to manage on-premise storage than public cloud storage due to the physical layers that require specific maintenance and installation.

On a summarizing note, using the cloud short-term is an economically justifiable alternative to running a local cluster system. If a team does not want to commit long-term to a local infrastructure, the cloud option should be preferred. High-end clusters are always more expensive than the cloud. Budget and normal cluster systems are only cost-efficient if operate under a very high compute load and store large amounts of data.

6 Use Cases Analysis

6.1 Informations System 1

6.1.1 Context

A company wants to develop a product that can be used to share data/files among themselves. The company demands it to be very secure, so the product is trustworthy for all types of users to share data without worrying about leaks. Since the main focus is to share the data securely, the time it takes during the sharing process is not a priority and can take longer to upload and download data from the product. An example of this product would be *Dropbox*.

6.1.2 Requirements

To be able to build a product that can fit the context given above, the most important specification is **Security** and **Storage**. Note that Bandwidth, Throughput, and Computing Power are still necessary but with as much importance.

6.1.3 Analysis

With the given scenario, security is key. Therefore, it is known that owning your own data center is a lot safer than the public cloud. However, it comes at a cost, a company has to invest in infrastructures, staff that is trustworthy and reliable for handling them, make sure it follows all legal protocols, and, that is secure. For start-up companies that intend to build this product, doing investment for an on-premise approach would be very costly, unless it already has the infrastructure and resources to do so. However, given these requirements, if security is of extreme importance, it might be the best way to go for on-premise and invest in it early on since in the long-term it would compensate the investment.

Highly regulated companies tend to split their storage between on-premise and cloud. Sensitive data are stored on-premise while non-sensitive data is stored in a public cloud. This hybrid approach can be extremely beneficial for this use case.

One example of this hybrid approach is Dropbox, a popular provider of cloud-based document storage and

collaboration services, which developed a fast-growing business by relying on Amazon S3 (Simple Storage Service) to house data while keeping metadata on-premise. That hybrid architecture worked well for a time. Dropbox executives weighed the options and decided that moving data storage in-house was the best choice, despite daunting challenges that included improving on the S3 storage architecture, moving vast quantities of data in a short amount of time, and running large numbers of data storage devices economically and reliably.

Dropbox completed one of the largest reverse cloud migrations ever undertaken, moving around 600 petabytes of data from Amazon's cloud to its own data centers. It was a moonshot-caliber undertaking that's paying dividends for Dropbox in faster performance and lower costs. But it's not an either-or proposition: The company is going back to Amazon to provide major new cloud services in Europe. When it comes to hybrid cloud strategy, Dropbox has learned that striking the right balance is key. Another lesson, and which applies to many IT leaders as they weigh on-premises versus cloud deployments, is that each solution might be right, depending on the data that's being stored and the needs of the users who access the data. Although that statement applies to Dropbox, it is important to remain mindful that when it comes to hybrid cloud, balance is key.

If the company is considering building a private cloud, it must make sure it's strategically critical to its corporate objectives. If it decides to have some on-premise data centers, it is recommended to use the same software as a public cloud service because if a migration is necessary it makes it a lot easier to move the data. Even after building its' infrastructure, keep in mind that a public cloud service might offer advantages down the road. Embrace standards that will enable to move of applications and data to the cloud should the need arise.

6.2 Informations System 2

6.2.1 Context

A company needs to develop a product that must support multiple concurrent users accessing it and exchanging loads of data/files. Their end-users must be able to share data on the fly without much effort and time to wait. In contrast to the previously analyzed use case, this product doesn't require a high level of security because the main goal is to share data quickly.

6.2.2 Requirements

For this type of product, it is key to prioritize **Bandwidth**, **Throughput** and **Storage** for the system. Also, it doesn't require as much Security, even though it is still always necessary a decent level of security.

6.2.3 Analysis

This use case is similar to the first one, except one if its' priorities are not security, but rather focuses more on bandwidth and throughput to handle multiple requests to download or upload data.

Moving data between cloud servers and end-user devices takes time. The company must be able to host data in regions that are geographically proximate to the end-users helps to reduce delays.

Having a good bandwidth is also of extreme importance. Sometimes cloud providers do not offer enough bandwidth, especially when it comes to uploading larger amounts of data, but for this specific use case, this isn't a problem and cloud providers have come up with creative ways of improving that. On-premise servers are only limited by the internal network's infrastructure, and it is possible to access it at any given time, but they also might cause other issues as already discussed above.

Cloud providers have improved their performances and networks over time and now offer far better services than a few years ago. Nowadays, going for a cloud approach is usually a good option not only for startups but also for large companies as they offer ways of easily increasing throughput and bandwidth performances. Given these three requirements, a cloud provider would be able to provide them at ease and with all the flexibility and scalability advantages. Similar to the previous use case, the company should still evaluate its approach constantly taking into account not only costs but other aspects as well.

6.3 Gaming Software

6.3.1 Context

A gaming company needs to build a game in the form of an app. This product must be able to withstand multiple online users at the same time and handle the information of all the users playing the game. It must also be smooth and with rapid feedback to the user so he can have a better in-game experience.

6.3.2 Requirements

This type of product prioritizes fast operations, for that to be possible it must prioritize **Computing Power** (CPU and RAM), and to handle concurrent users, **Bandwidth** and **Throughput**.

6.3.3 Analysis

A gaming company would generally need to have several data centers scattered around the world if they want to have it available for everyone, so users can have similar low latency and be able to play with each other with a good experience.

For this scenario, if the company is just starting up, in the early stages of digital transformation, then the cloud will almost always be the best option to make a first release of the game around the world due to the lower cost of doing so. After that, they should evaluate the requirements and adapt to their needs and with their available resources.

Evaluating the requirements frequently is important because, for example, if their game doesn't demand low latency for users around the world, then an on-premise approach could be a good investment in the long run.

Some of the biggest gaming companies have their own data centers, however, almost all of them are starting to migrate to the cloud their servers that connect the players. This allows to pay and scale for the resources on demand. This is very useful for this scenario because the popularity of a game is very uncertain and there are a lot of periods where there are peaks of concurrent users and it the company can easily upgrade resources.

Modern games require flawless technical execution, constant innovation, and seamless online experiences. Cloud computing offloads the task for running the game so that game makers can concentrate on making a great experience. An example of this is, one of the biggest gaming companies, Riot Games, overcame their technical debt by taking their most popular game, League of Legends, platform into the AWS Cloud. AWS services gave Riot Games the infrastructure agility they were lacking within their data centers and empowered them to focus more on new player features and less on legacy infrastructure. They can use the infrastructure of AWS to innovate at every stage of development — from production to live streaming via Twitch. AWS can support scalable multiplayer infrastructure management, live service operations, Twitch integrations, innovations with Alexa voice-enabled gameplay, and massive-scale machine learning.

In conclusion, a gaming company at any development phase should consider the cloud services rather than building their infrastructures when there is a need for low latency around the world, mainly because of the flexibility and cost-effectiveness the cloud offers, however, if latency is not as relevant, on-premise could be worth in long term.

7 Conclusion

For this assignment, a lot of research was required to obtain essential information. Starting with the definition of cloud computing and on-premise solutions, and then comparing both approaches in different aspects that are relevant when deciding on the type of infrastructure to utilize, such as scalability, cost, security... After this, three scenarios of use cases with different requirements were analyzed and then recommend an approach based on that analysis.

In conclusion, cloud computing and on-premise solutions are very different from each other, and even though cloud services are getting better and increasing in usage every year around the world, on-premise approaches will most likely always be present because they are essential for certain scenarios.

It is important to remember that for many organizations, particularly larger ones, a hybrid model that employs both cloud and on-premises systems and operations may make the most sense. It may also be necessary to run a hybrid model during a transition period, for example, when there is a significant investment in legacy systems and/or custom applications. This will extend the analysis beyond a cloud versus on-premises comparison.

Every company has unique operations and needs— and the factors that determine the appropriateness of internal or cloud-based infrastructure and applications will be unique to the company, as well. For financial investors, costs and impact on EBITDA will be key factors in this equation. Many financial buyers dislike the idea of adding operating expenses, but often these costs, when invested the right way, make more sense than on-premises capital expenditure, both in the short and long term. Spending time to understand the costs and financial implications of each scenario is time well spent and potentially a source of greater value down the road.

8 References

[1] *Cloud Computing vs. Traditional IT Infrastructure*. LeadingEdge IT Services & Solutions. https://www.leadingedgetech.co.uk/it-services/it-consultancy-services/cloud-computing/how-is-cloud-computing-different-from-traditional-it-infrastructure/

[2] *Traditional IT security vs. Cloud security: Which approach is right for your business? (2019, July 24)*. Security Infowatch. https://www.securityinfowatch.com/cybersecurity/information-security/article/21089929/traditional-it-security-vs-cloud-security-which-approach-is-right-for-your-business

[3] *Meinardi, M. (2020, October 28). Is Public Cloud Cheaper Than Running Your Own Data Center?* Marco Meinardi.

https://blogs.gartner.com/marco-meinardi/2018/11/30/public-cloud-cheaper-than-running-your-data-center/

[4] *Network Throughput vs Bandwith*. Auvik
https://www.auvik.com/franklyit/blog/network-throughput-vs-bandwidth/

[5] *Morgan, L. (2021, February 23). On Premise vs Cloud: Key Differences, Cost, Pros & Cons. Enterprise Storage Forum.*
https://www.enterprisestorageforum.com/cloud/on-premise-vs-cloud-storage/

[6] *Blog: On Premise vs. Cloud: Key Differences, Benefits and Risks. (n.d.). Cleo. Retrieved July 7, 2021.*
https://www.cleo.com/blog/knowledge-base-on-premise-vs-cloud

[7] *Juhasz, Z. Quantitative cost comparison of on-premise and cloud infrastructure based EEG data processing. Cluster Comput 24, 625–641 (2021).*