universität wien

MASTERARBEIT / MASTER'S THESIS

Titel der Masterarbeit / Title of the Master's Thesis

Factors influencing the corporate Austria towards the transformation into cloud computing solutions

verfasst von / submitted by

Zsolt Keller

angestrebter akademischer Grad / in partial fulfilment of the requirements for the degree of

Master of Science (MSc)

Wien,2018 / Vienna 2018

Studienkennzahl lt. Studienblatt / degree programme code as it appears on the student record sheet:	A >066 914<
Studienrichtung lt. Studienblatt / degree programme as it appears on the student record sheet:	Masterstudium Internationale Betriebswirtschaft
Betreut von / Supervisor:	Univ.-Prof. Dr. Oliver Fabel, M.A.

Eidesstattliche Erklärung

Ich erkläre hiermit an Eides Statt, dass ich die vorliegende Arbeit selbständig und ohne Benutzung anderer als der angegebenen Hilfsmittel angefertigt habe. Die aus fremden Quellen direkt oder indirekt übernommenen Gedanken sind als solche kenntlich gemacht. Die Arbeit wurde bisher in gleicher oder ähnlicher Form keiner anderen Prüfungsbehörde vorgelegt und auch noch nicht veröffentlicht.

Wien, den 28.09.2018

Table of Contents

Abstract

Cloud solutions have the potential to revolutionize the way we do business by optimizing corporations' business processes. But the attitude toward the transformation to cloud in Austria is still conservative and is still behind other European countries. The change from on-premise to cloud based solutions is facing economic, technical and psychological barriers. This thesis seeks to explore and introduce the influencing factors of cloud computing adoption in Austria by asking cloud experts from Microsoft Austria and existing cloud customers. The results from these two groups suggested that cloud providers and their customers have some significant differences in their opinions regarding cloud adoption factors. Therefore, this thesis provides insights into the Austrian cloud market that can be used by cloud providers to identify and tackle the main issues holding current and potential future customers to adopt cloud computing solutions.

Abstrakt

Cloud-Lösungen haben das Potenzial, unsere Wirtschaftsleben durch die Optimierung der Geschäftsprozesse von Unternehmen zu revolutionieren. Aber die Attitude zur Cloud-Transformation in Österreich ist immer noch konservativ und liegt immer noch hinter anderen europäischen Ländern. Der Wechsel von On-Premise- zu Cloud-basierten Lösungen steht vor wirtschaftlichen, technischen und psychologischen Barrieren. In dieser Arbeit werden die Einflussfaktoren der Cloud-Computing-Einführung in Österreich untersucht und vorgestellt, indem Cloud-Experten von Microsoft Österreich und bestehende Cloud-Kunden befragt werden. Die Ergebnisse dieser beiden Gruppen deuten darauf hin, dass Cloud-Anbieter und ihre Kunden erhebliche Meinungsunterschiede hinsichtlich der Cloud-Akzeptanzfaktoren haben. Daher bietet diese Arbeit Einblicke in den österreichischen Cloud-Markt, die Cloud-Anbieter nutzen können, um die Hauptprobleme zu identifizieren und anzugehen, die aktuelle und potentielle zukünftige Kunden dazu bewegen, Cloud-Computing-Lösungen zu übernehmen.

Introduction

The introduction of this paper presents recent statistics on cloud computing services in the industry and compares the cloud adoption rates within Europe. A bird's eye view of the concept and market of cloud computing will be provided. Throughout the literature review, I will examine more sides of cloud computing and I identified a broad range of factors that influence the rate of cloud adoption.

Cloud computing has the power to transform lives, societies, how organizations function and definitely it can shape our future. Hospitals, schools, business units, and researchers depend on mobile and cloud technologies without knowing it. Cloud computing makes it possible to collect, store, and analyze a huge amount of data to provide insights and intelligence. Thanks to cloud technologies, a university in Greece, leveraging cloud data, is helping firefighters to predict and prevent massive wildfires. These technologies collect various data, which are useful for the Greek firefighters. So, they are now provided by remote sensors with intelligence on the rate of the fire`s spread, intensity, and movement so they can catch early, saving lives and property. Cloud computing has emerged as one of the most influential technologies in the economic. It creates many new opportunities for organizations across the world. Nowadays, cloud services are available at affordable prices and accessible for companies in any size or in any industry. Many companies are already embracing the enormous benefits of cloud computing. The recent technological emergence has helped to improve the cloud computing capabilities. It offers unique possibilities to take advantage of service-based IT solutions at a low cost, globalize their processes rapidly and perform business operations easier. By moving IT functions such as storage, business applications, and services to the cloud, organizations can potentially reduce the overall cost of IT. Furthermore, cloud computing deploys computational tools rapidly, reduces upfront capital expenditures and makes it possible to respond more quickly to changing market conditions (Nadella, 2017, p.42-43).

According to Gartner - one of the world's leading research and advisory company – global public cloud services market is projected to grow 21.4 percent in 2018 to total $186.4 billion, up from $153.5 billion in 2017 (Table 1). The research company's forecast shows that by 2020 the market doubles its size from 2016. The growth rates clearly sign that as cloud services gain maturity and mainstream status the companies will spend more on cloud IT solutions.

	2017	2018	2019	2020	2021
Cloud Business Process Services (BPaaS)	42.6	46.4	50.1	54.1	58.4
Cloud Application Infrastructure Services (PaaS)	11.9	15.0	18.6	22.7	27.3
Cloud Application Services (SaaS)	60.2	73.6	87.2	101.9	117.1
Cloud Management and Security Services	8.7	10.5	12.3	14.1	16.1
Cloud System Infrastructure Services (IaaS)	30.0	40.8	52.9	67.4	83.5
Total Market	**153.5**	**186.4**	**221.1**	**260.2**	**302.5**

BPaaS = business process as a service; IaaS = infrastructure as a service; PaaS = platform as a service; SaaS = software as a service
Note: Totals may not add up due to rounding.
Source: Gartner (April 2018)

Table 1: Worldwide Public Cloud Service Revenue Forecast (Billions of U.S. Dollars). Source: Moore, S., van der Meulen, R. (2018)

When it comes to major cloud providers, there are three top contenders - Microsoft, Amazon, and IBM. Taking into consideration all three layers (IaaS, PaaS, SaaS) of cloud computing than Microsoft posted for the trailing 12 months ending March 2018 a commercial cloud revenue of $20.8 billion while Amazon's total for the same 12-month period was $19.24 billion and IBM's was $17.7 billion (Evans 2018b). We have to bear in mind that we are only in the very early days of the competition of the biggest cloud players and that the cloud movement is not in complete motion yet. The growth rates are also significantly high, which is a clear indicator for further increasing cloud market. Microsoft had a growth rate of 58% in the first quarter of 2018 and Amazon finished Q1 with a 49% growth rate (Evans 2018a). As business customers start to realize that embracing the cloud could the best approach toward digital transformation the competition – particularly among the most powerful cloud service providers – will intensify.

In general, we can say that cloud adaption is slower in the European Union as in the USA. But even among the member states in Europe, we can see big variances. The European Union conducted a research (Eurostat, 2018) on cloud service usage in the EU countries. Table 2 demonstrates the stake of companies that used cloud services in Europe from 2014-2016 (Eurostat, 2017). Based on the research in 2016, practically all businesses in the EU (97 %) had access to the internet. Among them, 22 % used cloud computing services in 2016 compared to the 19% usage in 2014. Large businesses (45 %) used significantly more the cloud services than SMEs (21 %). Some European countries are far behind the cloud performance of some others. The Scandinavian countries are Europe's role models regarding the transformation into the cloud, especially Finland. With 57% of cloud usage, Finland leads the digital transformation by a long shot. It is a country with a long tradition of outsourcing IT services, which strongly aligns with the spirit of the cloud. In other member states like Sweden 49% and Denmark (42%), the purchase

of cloud services by business was also very common. The top companies, as well as the consumers in these countries, are not afraid of the cloud and the changing business models anymore. On the contrary, Austria is far behind the average cloud transformation rate. Austria's rate was about 14% in 2014 and 17% in 2016, which allows us to safely say that Austria is years behind the top performers in the industry. Even the average 21% rate of the EU-28 in 2016 is 4% away for Austria. This raises several questions about the reasons for Austria`s slow transformation in comparison to other countries such as Finland.

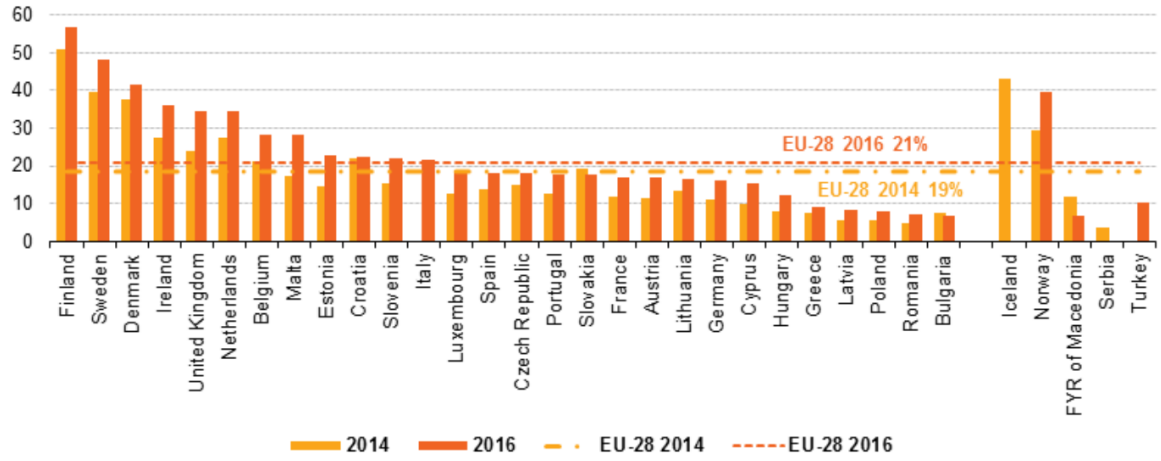

Table 2: Use of cloud computing services in Enterprises, 2014 and 2016 (% of enterprises). Source: Eurostat (2016)

Despite the proclaimed advantages of this new technology and the astonishing growth rate of the cloud market, we can see that not all companies are hurrying to adopt cloud-based solutions. The growth doesn't meet the expectations, there are notable factors that have hindered the growth over the years. There are various factors that have affected the adoption rate of cloud computing to be slower than the expectations.

Accordingly, the thesis tries to answer the following research question:

"What are the most important determinants for enterprises when adopting cloud computing services and what is their effect?

Research aim and methodology

For finding answers and solutions for the research question above the factors that influence cloud adoption will be identified throughout the literature review and hypotheses will be designed to examine the effect of these factors on cloud adoption.

The thesis wants to provide an experiment, which gives a good basic to examine the factors of the cloud computing adoption and its influence on the slow adoption rate in Austria. Since the research question and the topic described above are targeting an important topic in todays' corporate world I think it gave a good basic to create a relevant experiment.

The topic of cloud computing adoption is gaining significance day to day and its influencing factors are in focus of many studies and research papers. Consequently, after presenting the chosen research design, an extensive theoretical part is introduced which involves the profound introduction of the background of cloud computing: cloud history, technical terms and processes, economics of cloud, security concerns of cloud, cloud adoption in the European Union, Austrian cloud computing environment and last, but not least the offerings of Microsoft. The cloud portfolio of Microsoft will further demonstrate the cloud computing technologies and emphasize its importance in todays' business.

The literature part helps to gain a common understanding of cloud computing and its adoption. Throughout the literature, the most important influencing factors of cloud adoption are identified and used to create the questionnaire that will help to test the developed hypotheses. I used two groups of respondents to test my hypotheses, on the one hand, a group of cloud experts and on the other hand a group of current cloud computing customers. This will give a good basic to examine the similarities and differences between the two point of views and identify how cloud adoption could be enhanced by the cloud providers. The detailed research methodology and the hypotheses will be introduced after the literature review.

Defining Cloud Computing

We can differentiate three types of IT solutions: cloud -, on-premise – and hosted offering solutions. The main decision to be made by organizations is to either stay with on-premise solutions, use hosted offerings or cloud solutions. On-premise offerings mean the traditional IT deployment. It means that the organization acquires the necessary IT infrastructure, among others the physical assets, servers, operating systems. Thereby, the organizations' IT department is responsible for all the components and for the maintenance. The hosted services are hosted by a company specialized in this field within their datacenters or other facilities. These offerings are usually regulated contractually between the provider and the user (Murugesan, Bojanova 2016, p. 433).

A universally accepted definition of cloud computing has been developed at the National Institute of Standards and Technology (NIST) and was published in 2011. According to the official NIST definition, "cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction." (Mell, Grance, 2011). When choosing a cloud service provider, users are basically renting a small portion of an enormous infrastructure of datacenters, computers, storage, and networking capacity. Many of these datacenters are multi-million-dollar investments by the companies that run them (Sosinsky, 2011, p.13).

In the business perspective cloud services provide many advantages. The IT Infrastructure is operated and maintained by the service provider, so the customers can use all benefits without having to worry about administration, up-front commitments or IT workforce. Cloud computing services delivered by service providers have the following mandatory characteristics: on-demand self-service, the elasticity of provision, payable services (pay-per-user, pay-per-use or pre-paid). This gives even the small businesses flexibility and scales up or scale down possibilities depending on business demand (Armbrust et al. 2010 pp. 50-52). Large and small enterprises are also adapting their (IT) strategies to introduce cloud computing resources. Their strategic priorities lie increasingly on flexibility, innovation potential, economic advantage, therefore they tend to take cloud computing into consideration as it has huge potential to fulfill these strategic ambitions. Cloud computing makes it possible to transform business processes, lower IT spending, offer access to pervasive storage capacities, unlimited computational power and so achieving business efficiencies. Cloud computing thus offers monetary benefits that businesses can no longer ignore (Oliveira, Thomas & Espadanal, 2014).

With the latest technological developments in computing resources, processing, and storage capabilities, computing resources have become cheaper and more accessible. This new computing model makes it possible for the users to lease and release resources through the internet in an on-demand fashion. As the organizations become more experienced in cloud computing they start to utilize its potential and tend to shift their core businesses onto cloud-based platforms (Avram, 2014).

We can differentiate some key stakeholders that are subject to cloud computing. The main stakeholders are the consumers, providers, enablers, and regulators. The group of consumers needs to understand the cloud computing's potential to use it effectively. The users use, own, maintain and upgrade the systems while the providers own and operate the cloud computing systems to deliver to the users. They are also responsible for maintaining and upgrading the systems. As often the providers are focused on developing the best possible solutions they are relying on the so-called "enablers" that will sell products and services. They can, for example, build the cloud infrastructure for the users. A regulator can be a national governing body or an international entity that has to regulate the business of cloud. Inflexible regulation can be a relevant blocker for cloud adoption (Marston et al., 2011, pp. 182-183).

The cloud history

It is not possible to understand the present or the future of cloud computing without looking back on its history. In the past 10 years, cloud computing changed the IT environment and the expectations from IT by increasing the capabilities of it. It became an important part of today's IT and an essential catalyst for innovation across the companies, therefore they should focus on

even bigger investments (Panetta, 2017). And we can say that the evolution of cloud computing over the past few years is potentially one of the biggest advances in the history of computing (Marston et al., 2011, pp. 182-183).

The emergence of cloud computing had a simple, logical reason. After the worldwide PC revolution in the 1980's most of the homes and offices had computers. The need for sharing data over the networks have so dramatically increased that the servers couldn't keep up with the pace. So, the need for shifting the economics of cloud, standardize and pool computing resources and automated maintenance tasks led to developing cloud computing. If thousands of people would be trying to reach to one server than it would break it. Therefore, there is the need came about to distribute evenly the queries evenly among the servers. This elasticity is a key attribute of cloud computing (Nadella, 2017, p.45-49).

Cloud computing is not a totally new concept. It can be originated from the early large-scale distributed computing technology emerged from the fusion of traditional computing technology and network technology like grid computing, distributed computing parallel computing, etc. It aimed to construct a perfect system with powerful computing capability and using the advanced business models like SaaS, PaaS, IaaS to finally serve the powerful computing capacity to end users' hands (Yang, Chen 2010, p. 1). Even though the idea of cloud computing is not a new one, the term started to gain popularity only after it was used by Google's CEO Eric Schmidt used it in 2006. Cloud computing started as a disruptive technology for delivering Internet services, but now it is more mainstream, and it became an enhancer for innovation for the IT sector as a whole (Botta et al. 2016). Already the predecessors of the internet – ARPANET by 1977 and CSNET by 1981 used the cloud symbol for representing networks of computing equipment (Computer History Museum, n.d.).

The vision of computing facilities providing computing utility to the general public originates from John McCarthy, dating back to the 1960s. Cloud computing is strictly seen is a new operating model which connect more already existing technologies to operate in a more effective way. It leverages these technologies in order to maximize their utility and meet today's business demands on technologies. Such related technologies are like grid computing (coordinates network resources), utility computing (provide resources on-demand, packaging resources), autonomic computing (self-managed systems) and virtualization. Virtualization is a crucial part of cloud computing. Virtual Machines (virtualized servers) provide pooled resources from server clusters in order to balance resources to applications on-demand. In short cloud computing has evolved through a number of phases that include these technologies and by leveraging their advantages and reviving them in a somewhat modified form in order to provide on-demand resources in the best possible way under the banner of cloud computing. Hence the cloud developed with the goal of allow users to take benefit from all of these technologies, without the need for deep knowledge

about or expertise with each one of them (Zhang, Cheng & Boutaba 2010) We will see in the following sections which unique characteristics differentiate cloud computing from these related technologies and from traditional service computing.

Virtualization (mentioned above) was a major enabler of the IT transformation. It has been around for many years, but it has been recently rediscovered by the IT professionals. It was introduced by IBM in the 1960s under the name "Time sharing". Generally speaking, virtualization consolidates the computing resources by reusing hardware. As an example, we can imagine a company with 10 hardware servers, each running its own operating system and an application, which need low CPU power. The virtualization would make it possible to replace these servers with 2 servers without any change in a software environment. Virtualization makes it possible of installing operating systems or applications on a hardware, which does not exist at all. A key piece for that is the so-called hypervisor, which emulates the hardware environment so that each operating system and application "thinks" that they are running on their own hardware and not on one hardware together with other ones. This data can then be divided or shared through Virtual Machines (VMs). These VMs can exist within a single computing environment (Host) and they act as a separate computer running applications etc. Thanks to the virtualized environment the companies need fewer servers to purchase and maintain. That translated into savings in Capital Expenditure (CapEx) and Operational Expenditure (OpEx). That leads to significant cost reductions, taking into account that two-thirds of a typical IT budget is devoted to maintenance. Also, virtual servers are better than physical ones in availability, flexibility and disaster recovery. From the infrastructure perspective, cloud introduced a platform that is multi-tenant (many users on the same physical infrastructure), equipped with a programmable interface (Application Programmer's Interface - API), automated and low-cost solution. A cloud API is a backbone solution in cloud computing that interacts with the cloud infrastructure to allocate cloud resources for requested cloud demand (Mishra et. al., 2013, pp. 36-39) (Faynberg, Lu & Skuler, 2016, pp. 9-10).

The first large adopters of this technology (like Amazon, Microsoft, and IBM) started to deliver services over the Internet, gaining both economic and technical benefits. Amazon created its subsidiary Amazon Web Services in 2006 and introduced its Elastic Compute Cloud (EC2) (aws.com, 2006). In 2008, Google released Google App Engine (McDonald 2008) and Microsoft also released Microsoft Azure but made first in 2010 general available (Hauger 2010). IBM (IBM SmartCloud) and Oracle (Oracle Cloud) also announced their own cloud solution in 2011 and 2012, respectively.

The cloud computing architecture

This section presents a general overview of cloud computing, including its deployment models, architecture models, and main characteristics. It is important to have a general overview of the cloud model, therefore the service models and the essential characteristics of cloud computing will be discussed as well.

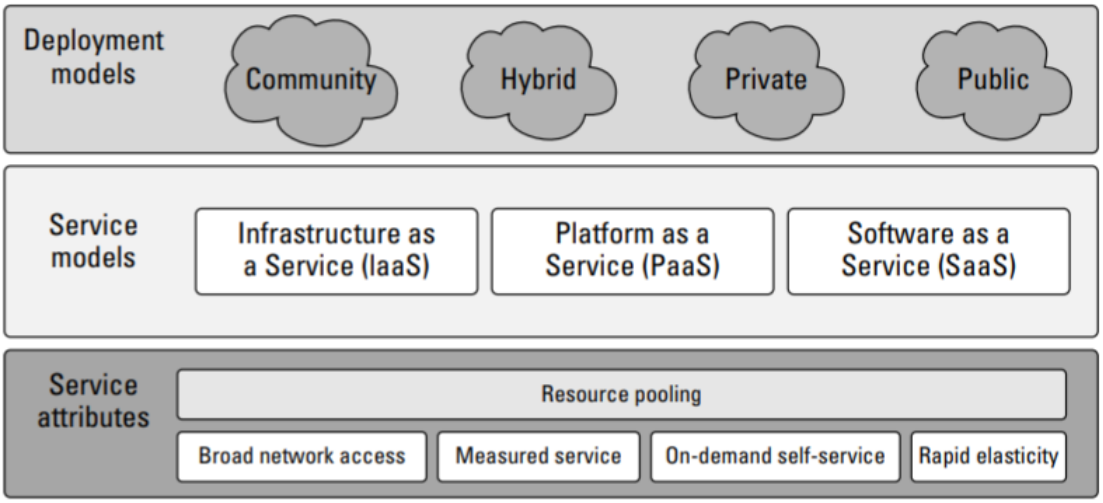

Figure 1: The NIST cloud computing definitions. Source: Sosinsky, 2011, p.6.

Cloud deployment models

One of the key elements of cloud computing is the deployment model. A deployment model refers to the purpose of the cloud and the nature of how and where the cloud is located. We can differentiate several different deployment models, but the most important ones are public cloud, private cloud, community cloud, and hybrid cloud. In cloud viewpoint, deployment means where the service is made available, who can access the data and who is the owner of the storing device. Every deployment model has its own advantages and disadvantages, so if an enterprise makes the decision which model to choose it should consider different aspects, i.e. what are the main business goals, security concerns, availability, costs etc. (Zhang, Cheng & Boutaba 2010, pp. 9-10).

Public cloud

Public cloud is the most common and well-known cloud model. In general, the biggest public cloud solutions are provided the big cloud providers like Amazon, Microsoft, Oracle, Google or IBM. But it also may be owned, managed, and operated by a business, or government organization, but of course on a smaller scale. The access happens via the internet and the mega scalable infrastructure is owned, operated and maintained by the professional cloud supplier. Due to reaching the economies of scale public cloud providers can offer their cloud services below the costs of a medium-sized private cloud provider. The biggest concern regarding public cloud

solutions is that the consumer has generally no control or knowledge over the exact location of the resources, which raises some concerns among cloud users. The resources are offered for open use by the general public on a pay per use model. For higher resiliency cloud providers use multiple data centers and storage is redundant. It is considered as a way to scale IT resource in demand without having to maintain the infrastructure and bear the (Faynberg, Lu & Skuler, 2016, pp. 4-5).

Private Cloud

Private cloud refers to internal data centers of a business, government or another type of organization. It is also called as internal cloud and they are designed for the exclusive use by a single organization. Therefore, it is not made available to the general public. From a technical point of view, there are hardly any differences regarding the structure between public and private clouds. Private cloud solution has some disadvantages compared to public cloud. An upfront investment in infrastructure is unavoidable, it doesn't make the user able to access infinite computing resources, short time access to resources is not possible and economies of scale is usually not reached. Despite some clear disadvantages, private cloud operators can get benefits through hybrid cloud computing and they have a greater control over their data, reliability, and security as well as more transparency compared to the other cloud models (Armbrust et al. 2010 pp. 50-52).

Hybrid Cloud

A third type can be the hybrid cloud that is a typical composition of public and private cloud or even community cloud. It enables the organizations to overcome the limitations of each approach. The different cloud models remain unique entities, but they will bound together by a proprietary technology that enables data and application portability (e.g. cloud bursting). Cloud bursting means if an application runs on private cloud, but the local resources are not sufficient, and it needs higher computing capacity then it "bursts" into public cloud to meet this peak application demand. (Guo et al. 2014, p. 1) (Yang, Chen 2010, p. 2)

In a hybrid setup part of the workload runs on private cloud while the remaining part runs in public clouds. So that way it can offer more flexibility than both private and public cloud. One important component of using hybrid cloud is to decide the best possible split between private and public cloud usage. It enables the user to use the public cloud for intensive computing resources when peak workload occurs, then returns to private cloud if the extra workload is no longer needed. Another use case for hybrid cloud could be if an organization stores its sensitive, critical client data or highly regulated data in house, in private cloud and aggregate or integrate a public cloud service for extending either its capacity or capability, so the analytical inquiries will not take internal resources (Zhang, Cheng & Boutaba 2010, pp. 9-10).

Community Cloud

This type of cloud model is created for exclusive use by a group of consumers from organizations. The access to the community cloud is restricted for the participants that work on the same projects, research etc. that demand a common cloud computing basis. They share common concerns e.g. mission, legal issues, efficiency demands, security requirements, policy. The cloud infrastructure could be hosted in this closed network itself (by one or more companies) or by a third party or combined. The costs are spread among the companies, so it has less cost advantage as public cloud, but more than private cloud. Generally speaking, it is a closed private cloud for a group of users and as such it makes possible to keep the benefits of economy of scales with the private cloud approach. Therefore, community cloud is known as a cost saving alternative of cloud infrastructure (Mell, Grance, 2011) (Yang, Chen 2010, p. 2).

The layer model of cloud computing

The architecture of cloud computing is based on a layer model. The cloud environment can be divided into 4 different layers which together build up the cloud architecture: hardware -, infrastructure -, platform – and application layer. These layers do not need to be related, for example, a program can be run on IaaS, but accessed directly without using SaaS. Figure 2 shows which layer manage which resources with examples of cloud service providers.

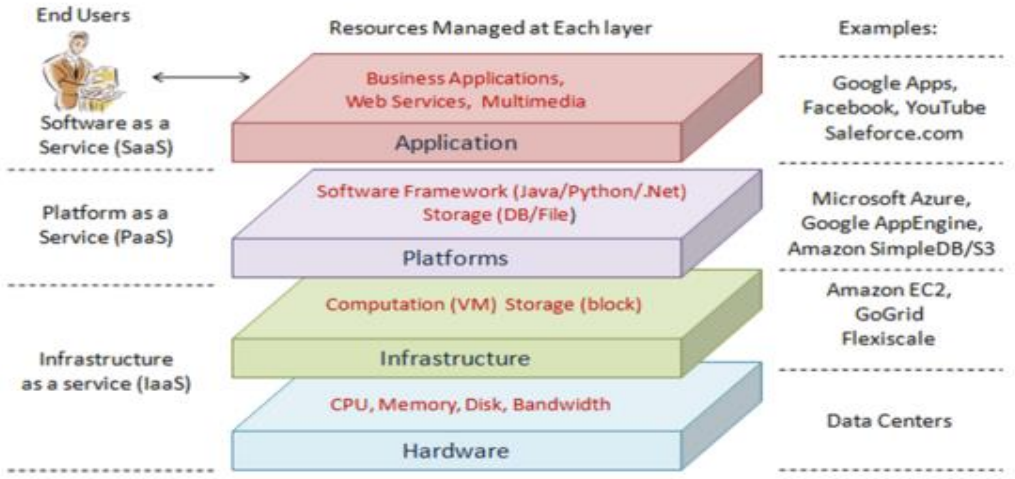

Figure 2: Cloud computing architecture (Zhang, Cheng & Boutaba, 2010, p. 9)

1. *Hardware layer*: this layer is practically implemented in data centers, it is the physical foundation for the whole cloud architecture. The physical resources like servers, switches, routers, and cooling systems run on it and are managed by the operator. A cloud data center consists of thousands of servers that are interconnected with routers, cooling systems, and switches to easily scale up and down the resources. The data centers are managed by network engineers and architects. That is the backbone of cloud computing. The main challenges at

this layer are the continuous operating without off-time, traffic management and cost management for power and cooling (Zhang, Cheng & Boutaba 2010, p. 9).

2. After comprising all the needed hardware for cloud computing the next layer is the *infrastructure layer*. This layer is responsible for virtualization technologies (i.e. VMware), which makes able to use the hardware layer, so it is also a key component of the cloud technology. Virtualization provides the agility required to increase infrastructure utilization by enabling dynamic resource assignment (Zhang, Cheng & Boutaba 2010, p. 9).
3. The infrastructure layer makes it possible to have a *platform layer*. It consists of application frameworks as well as operating systems and is used mainly by web developers, coders, and programmers to create applications, programs and web tools. It is basically used to build the highest-level layer, the application layer. This way this layer helps to reduce the number of issues when deploying applications into virtual machine containers (Zhang, Cheng & Boutaba 2010, p. 9).
4. The highest-level *application layer* hosts the actual cloud solutions and makes them available over the internet. The cloud applications provide better performance, availability, lower operating costs thanks to their automatic scaling feature (Zhang, Cheng & Boutaba 2010, p. 9).

The characteristics of cloud computing

The National Institute of Standards and Technology (NIST) defines 5 key characteristics of cloud computing (Mell, Grance, 2011).

1. *On*-demand *self-service:* A consumer is able to manage its required computer resources itself by deciding on capacity of parameters like server time and network storage. The user is therefore able to skip the human interaction with each service provider and manage its capacity settings itself.
2. *Broad* network *access:* Capabilities are available over the network and can be accessed by all different types of devices e.g. mobile phones, tablets, laptops, and workstations.
3. *Resource pooling:* A service provider pools its resources to make the capabilities available for multiple consumers (multi-tenant model). Physical and virtual resources can be dynamically assigned and reassigned according to user demand. Thereby, the consumer has generally no control or knowledge over the exact location of the resources, but sometimes can specify the country, state or datacenter of the provided capabilities.
4. *Rapid elasticity:* resources can be provisioned and released elastically based on the fluctuating demand. Cloud platforms are therefore considered to be highly elastic and capable of providing resources in almost any quantity at any time.
5. *Measured service:* data traffic is controlled and monitored by the cloud system automatically. Both the *provider* and the consumer of the service can monitor, control and

report resource usage. These functions increase the transparency for all parties involved in the process (Mell, Grance, 2011).

Service Models

The National Institute of Standards and Technology (NIST) identifies three service models of cloud computing offered to the consumer. The models are listed below in compliance with the increasing concretization of each form of service at the 4 different layer level (Mell, Grance, 2011).

Cloud computing is a service driven business model. This means that every layer of its architecture described previously can be and practically is offered as a service. As the layers are built on each other so are the services. Therefore, a customer of a layer is perceived as a customer of the layer below. Basically, we can differentiate 3 types of services: software as a service (SaaS), platform as a service (PaaS), and infrastructure as a service (IaaS) (Zhang, Cheng & Boutaba 2010, p. 10). There are many different service models described in different literatures, but the three universally accepted are IaaS, PaaS and SaaS (Sosinsky, 2011, p.10).

Infrastructure as a Service (IaaS)

IT infrastructure in cloud context refers to the collection of hardware and software that enables cloud computing. The cloud infrastructure includes both a physical layer and an abstraction layer. The physical layer typically includes server, storage, bandwidth, CPU and network components and as outlines in the "layer model of cloud computing" chapter it refers also to the physical data centers. The abstraction layer is the software, which is used among the physical layers, i.e. virtual machines, storage. With the help of IaaS, the customers do not have to purchase servers, data center space, network equipment etc., but instead buy those resources as fully outsourced service without having to manage or control the underlying infrastructure. With IaaS the customers can use different computing resources, i.e. storage, network, processing etc. and can run different software, like operating systems or applications (Mell, Grance, 2011). The biggest IaaS provider is doubtless Amazon. Other big IaaS providers are Rackspace Cloud Servers, Joyent and Terremark (Marston et al., 2011, p. 178).

Platform as a Service (PaaS)

PaaS is the integration layer between the infrastructure and software layer. PaaS providers offer a platform for software developers an environment, so they can create applications, web apps, websites etc., which will run smoothly in the given cloud environments. PaaS works by developers deploying the cloud infrastructure of the cloud services provider, which then can be used as the platform to build software, application etc. The purchased infrastructure comes mostly with pre-installed developer tools, operating system, web server, database, programming

languages, software development frameworks, services and tools preferred by the cloud service provider. These targeted tools aim to reduce the complexity of software offerings and this way offering a better quality of service. As it was pointed out previously at this layer of cloud computing the users do not have to care about the managing the underlying infrastructure, but they have the possibility to control the deployed application and the configuration settings for the application-hosting environment. This cloud service created the possibility to practically every developer to use the needed equipment and necessary infrastructure to develop their own program and deliver it to users through internet (Mell, Grance, 2011) (Boniface et al. 2010). Some outstanding examples of PaaS include Microsoft's Azure Services Platform, Salesforce's Force.com, Google App Engine, Amazon's Relational Database Services and Rackspace Cloud Sites (Marston et al., 2011, p. 178).

Software as a Service (SaaS)

SaaS is the top most layer of cloud built on top of both IaaS and PaaS. It refers to software which is rented for a given period of time rather than purchased once and for all. It is based on a "pay as you go" model. The upgrades happen automatically during the subscription. As defined by NIST it is the capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The service is provisioned over the internet hence it is available from various client devices, such as computer, mobile phones, web browser or a program interface. And again, the customer is not involved in the control or management of the underlying cloud infrastructure (Mell, Grance, 2011) (Sosinsky, 2011). A few solutions that are offered as SaaS are Google Cloud Connect, Microsoft SharePoint and so on (Murugesan, Bojanova 2016, pp. 22-23).

The three different service models taken together are generally known as the SPI model of cloud computing. SPI model encompasses all the other possibilities. As mentioned earlier there are many other service models, which have the form of XaaS ("something as a Service). Some examples: StaaS, Storage as a Service; IdaaS, Identity as a Service; CmaaS, Compliance as a Service; and so forth (Sosinsky, 2011, pp. 65-66).

The economics of Cloud Computing

As cloud computing is moving towards mainstream adoption there are of course some concerns and criticism. Many people are confused about cloud computing's real benefits and key risks. In this chapter cloud computing will be examined from the economy's point of view. The benefits and the limitations will be outlined and the most important factors that influence the cloud adoption rate will be introduced. As the thesis seeks to examine the corporate Austria the cloud adoption in the European Union will be examined as well to give a big picture about the environment in which Austria and the other member states have to increase the use of cloud

computing. This includes the EU's measurements to enhance cloud adoption and exploit the benefits of cloud, the GDPR which is in effect since this year May. Finally the Austrian market's specific attributes will be outlined as well.

Benefits and limitations of cloud systems

Cloud computing offers many important benefits to its individual and enterprise users. But it also has limitations and poses some risks, the effects of which depend on the application type and liabilities involved. The huge pressure on organizations placed by global competition to reduce costs and increase profitability in order to survive in todays' challenging environment is a key factor for the IT industry to further improve technologies. And this also encourages IT managers to adopt the most up-to-date technologies like cloud computing that enable them to be more competitive (Harfoushi et al. 2016, pp.88-89). This paragraph will help to understand, acknowledge in order to being able to address these disadvantages and issues.

Benefits of cloud computing

It was already noted in the previous chapters that cloud computing has a wide range of benefits. As outlined previously NIST assigns five main characteristics that a cloud service provider must offer: on-demand self-service, broad network access, resource pooling, rapid elasticity, measured service. As these benefits are a "must offer" category for anybody in the cloud business the following advantages should also be considered (Sosinsky, 2011, pp. 17-18):

- Lower costs: higher operation efficiency and better utilization with cloud. Reduced capital and operational costs. No upfront licensee fees for software as well as no for hardware and software maintenance and upgrade by the user.
- Ease of utilization: it depends always on the business needs. Sometimes users do not need any hardware or software investment. Easier and quicker application deployment, ease of use and availability of vast resources.
- Quality of Service (QoS) and reliability: reliable service with relatively short downtimes and failovers. On-demand scalability solution to meet the actual demand.
- Outsourced IT management, simplified maintenance and upgrades: no need to control or manage IT infrastructure. There is also no need to worry about patches and upgrades, they happen centrally.
- Low barrier to entry: practically no upfront investment is needed. Cloud resources are available from anywhere in the world at any time.

The practically immediate access to hardware resources with no upfront capital investment helps businesses market and scale up their ideas faster. The traditional IT is very capital intensive and its model is called "Cap-ex" (capital expenditure), while cloud solutions treat IT as an operational

expense “Op-ex” (Avram, 2014, p.531). The cloud benefits are particularly attractive to small- and medium-size enterprises, as well as promising startups and application developers as they can use cloud solutions to try their ideas without investing in their own infrastructure (Marston et al., 2011, p. 178) (Murugesan, Bojanova 2016, p. 52). Cloud computing also represents a huge opportunity to many third-world countries that are behind of IT developments. It makes enterprises able to easily scale their services based on client demand and allows users to take advantage of the unlimited processing power to analyze huge amount of data in relatively short periods of time. Compute intensive business analytics that need high amount of computing power for a short period of time were traditionally available only to the largest corporations, but not available to the smaller firms. As cloud makes it possible to dynamically have access to resources and lowered the entry costs, hence smaller firms now can benefit from this type of business. Another key feature of cloud computing is that it enhances innovation, as can be witnessed many promising startups, but also from established corporations, like Facebook or YouTube (Avram, 2014, pp. 531-533).

A very good example of scaling up as the user base or the client demand grow is Instagram. Before Facebook bought Instagram for one billion dollars it had 11 employees managing 30 million customers. They had no physical infrastructure, no physical servers. Hence there was no need for big upfront investment, no technicians to maintain the infrastructure and so on. Therefore, they could focus on the business relevant activities, like customer acquisition retention (Faynberg, Lu & Skuler, 2016, p. 11).

Energy efficiency and carbon emission reduction has recently received considerable attention. The challenge here for the service providers to have a good trade-off between energy savings and service quality. The biggest corporations are on a good way for data center operational efficiency. As an example, Microsoft Azure is already carbon neutral since 2012. According to a new Microsoft study, running applications on their cloud is a more sustainable way, then running them in traditional on-premise data centers. It found that Microsoft cloud services are up to 93 percent more energy efficient and up to 98 percent more carbon efficient than traditional data centers. There are four key investments that reduce their ecological footprint: renewable electricity, operational efficiency, infrastructural efficiency and equipment efficiency (Branscombe, 2018).

Limitations of cloud computing

We have already discussed many significant cloud benefits above and it is easy to fall in love with the simplicity and power that cloud offers, but cloud has its downside too and some of these challenges are very real.

Basically, the most significant concern regarding cloud computing are the *security risks*. As critical company data are now replicated in the Cloud it is crucial who has the controlling and accessing rights of the data as it is a subject to regulatory and legal constraints (Yang, Chen 2010,

p. 2) (Faynberg, Lu & Skuler, 2016, p. 13). As it is an important issue, the topic security will be addressed more detailed in a following chapter.

Another problem is reliability. The users are dependent on the cloud solution provider's service model, as their servers also can have downtimes and slowdowns, which then can not be influenced by the user, thus there is a big business risk. As cloud computing is a dynamic operating environment, the capabilities of providing resources on-demand, achieving high agility and responding to rapid demand fluctuations are key ones. As already discussed virtualization is an important element of balancing load across the data center and to avoid hotspots, but this is also not that straightforward. Currently, detecting the need of balancing the resources lacks the agility to respond to it quickly and effectively (Zhang, Cheng & Boutaba 2010, pp. 14-17).

As introduced previously, hybrid cloud solution uses the advantages of private and public cloud solutions. For doing so the service providers have to ensure the interoperability and portability of information between private clouds and public clouds. If this hurdle is not tackled good enough, then it could be a strong blocker for broad adoption of cloud computing (Avram, 2014, pp. 532-533).

Another important area of challenges for cloud service providers are the legal and compliance issues. There are numerous regulations that pertain where the physical data resides, where it is processed, and from where it is accessed. Service providers have to comply appropriately with these privacy rules and regulations. This is a part of cloud adoption, which sometimes can not be influenced by the cloud service providers as politics becomes here an element of the adoption process. The development of the cloud should be not pulled back by these regulations, because it can have a significant negative impact on it. Europe is a great example for the challenges this regards. Each European country has its own regulations and data protection laws, but a new EU law, the General Data Protection Regulation (GDPR) came into force in May 2018 may have positively influenced the effects of the diversity in Europe (Avram, 2014, pp. 533-534) (Why Is Europe Slower to Embrace the Cloud?, 2017) (Yang, Chen 2010, pp. 2-3).

Economic considerations of cloud computing

In the previous paragraphs we discussed as well the most important non-functional as the economic advantages and disadvantages why organizations should introduce cloud. In recent years, cloud computing and its services became popular in the IT market, and it is one of the most promising technologies of the decade. "Everything as a service" is the concept that helps small and large organizations migrate from on-premises and hosted applications to off-premises cloud services (Murugesan, Bojanova 2016, p. 150).

From economic point of view adopting a new technology should start by evaluating its impact on the economical processes of the organization. As IT is an integrated part of a business that support and improve the economical processes, therefore it needs a thorough consideration which advantages could cloud bring to their businesses. Particularly, smaller enterprises are moving towards cloud for their computing, storage, networking, and application needs, as they have less complex business processes than the larger organizations (Avram, 2014, p. 534). Organizations should consider the cut-off between the loss of control and the reduction of costs. The important question they have to ask is: does the organization gain more advantage by using public cloud offerings or should host its own private cloud? Cloud solution providers should enhance the users to realize the most important economic considerations. We already identified many economic advantages, that can be realized with cloud solutions: cost reduction, pay per use, reduce time to market, ROI, turning Cap-ex into Op-ex and being more "green" by reducing energy consumption (Jeffery, Neidecker-Lutz., 2010, p. 12-15).

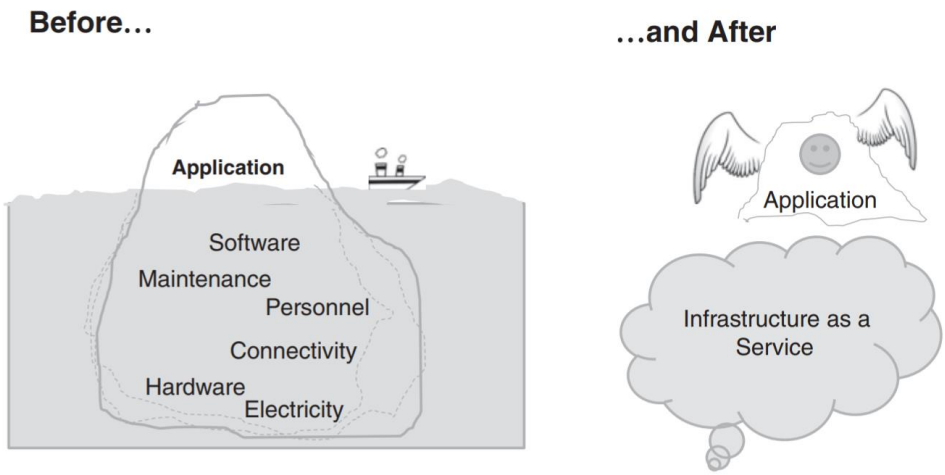

Figure 3:Investment in application development – before and after cloud era. (Faynberg, Lu & Skuler, 2016, p. 11)

One of the main benefits of cloud infrastructure that it enables the software developers to solely focus on the application development itself. The metaphor in Figure 3 illustrates this in an easy and very understandable way. Before the cloud solutions an application used by users was just the tip of an iceberg. Every application development needed a cost intensive, for the users mostly invisible phase, in which organizations have to invest in the infrastructure up-front. And nowadays in the cloud era all of infrastructure related tasks, like acquiring, installing and maintaining the database software, load balancing etc. are provided by the cloud solutions providers and software developers have more time to focus on the development (Faynberg, Lu & Skuler, 2016, pp. 11-12).

As introduced the biggest players in cloud computing in the chapter of "Defining Cloud Computing", which described the different business models of cloud computing we have seen the many companies that have taken the opportunity and adopted a cloud environment in order to

ensure that both the users and the companies benefits from this. These companies, like Microsoft, Amazon, IBM, Google and so on now provide a wide range of tools and services to their customers. They are running huge data centers that function highly effective usually with very small operational teams. With the help of a new, advanced business model that uses among others automation, self-service and standardized commodity levels provides a new level of infrastructure efficiency and business agility (Faynberg, Lu & Skuler, 2016, p. 11).

Economics of cloud also include aspects such as pricing and markets, hence quantifying economic benefits is crucial for cloud adopting decisions. Decision makers often struggle with identifying and predicting the related costs and so they can not easily identify the benefits of going to the cloud. The solution for this issue is of course looking at the costs related to staying with the on-premise solutions. As we have already discussed previously these costs range from server, software, cooling, real estate to human resources costs. We can take a really representative example in the research-intensive pharmacy industry, where the organizations need to make computing-intensive processes. In one example a drug have been developed 8 months faster and with an average savings of $130 million. Another example indicate that a molecular modeling problem was solved in approximately 8 hours at a fee of just $1279/hour using 30 472 instances, which was equivalent to 95 078 hours of manual computer work. But of course, in addition to cost considerations there are other factors that influence cloud adoption, such as security and privacy, regulations, operational factors etc. (Murugesan, Bojanova 2016, pp. 476-477).

As for now it became clear that cloud computing is here to stay in our life. From a business aspect it can be stated that if the supply -in this case computing resources offered by cloud solution providers – can be consolidated than the demand – users general-purpose computing need – can be satisfied with a large economy of scale (Marston et al., 2011, p. 188).

Challenges of adopting cloud computing

Presently cloud computing created countless opportunities to the organizations with high level of accessibility and at affordable prices. And as the organizations are embracing more experience with the cloud solution they start to shift more of their core processes in the cloud. This wider acceptance offers on one hand many benefits, but on the other hand it made the cloud adoption a more complex process as one would suppose. The technological improvements are enhancing the adoption of cloud, but as it was pointed out in the introduction chapter, not all organization or country meet the expected growth rate as in the beginning of the cloud era. The complexity derives mainly from data management, system integration and from the management of multiple cloud providers. Due to the high interest of cloud some organizations still see greater obstacles to the adoption of cloud (Raza et al., 2015, p. 1114) (Avram, 2014, p. 529).

Cloud computing requires to give up to some extent the control of the computing resources, hence the organizations depend on third party providers to get fixed any upcoming problem with a hardware. As IT workforce is in general not ready to give up the control it had been in the past and is still a major hindrance to the adoption of cloud computing. Also, the lack of regulatory agencies had an impact of the adoption rate. Agencies such as NIST or Cloud Security Alliance started to educate the public about the cloud computing and started to set rules that must be followed by cloud users and providers (Raza et al., 2015, pp. 1115-1116)

An organization that wants to adopt cloud should develop a cloud computing strategy to accelerate and advance the adoption. The strategy should be applied for the whole organization, use a structured engineering approach, support the key goals and mission of the organization and present the advantages of implementing cloud solutions in the core processes. The success or failure of the strategy can only be measured if rational, specific, measurable and timely goals are set along the way to the cloud. The goals need to be part of an organization wide approach including the major steps and phases that lead to successful adoption. Obviously adapting any new challenges goes hand in hand with many upcoming challenges, so it is with cloud adaption. Some of the key challenges to keep in mind: technical and management risks, security, cloud provider bankruptcy, performance, sensitive data, interoperability, and application migration. In summary for adopting cloud preparation is key. Organizations should develop a sound strategy that help them to introduce cloud in the processes in way they can embrace and realize its benefits and certainly they need to deviate and adapt the strategy for as technologies evolve and priorities change (Murugesan, Bojanova 2016, pp. 396-405).

As we have seen many of the adaption challenges are substantive and organization specific. However, we can identify some cognitive biases in people and organizations that are obstacles for cloud adoption and worth mentioning. Humans are a mixed of bounded rationality, predictable irrationality; cognitive, emotional, and financial decision-making anomalies; and other various biases. In some cases, these anomalies are enhancers for cloud, sometimes they are obstacles. Organizations and people that are decision makers in cloud adopting should be aware of these biases and should take into consideration when making decisions. Not only them, but the service providers also should keep in mind that there are more to cloud adoption than cost and efficiency factors. If we expand these behavioral factors to cloud adoption than there are 10 behaviors that impact it.

- *People are risk and loss averse.* Exteriorized this recognition to cloud adoption means that the fear of cloud adoption concerns are greater than the potential benefits of it.
- One of the key features of cloud services is the pay-per-use model they implement. This could enable great economic benefits, but people still often prefer flat-rates. The *flat-rate*

bias may not be that irrational: in an example when an employee left the company and let software running in the cloud and so let the bills wind up.

- The *need for control and autonomy* is a fundamental directive for people. Without at least the illusion of control we do not function well. The cloud providers should strive after visibility and transparency. Cloud providers offer higher degree of control than IT departments as resources can be easily scaled up or down. They also offer high degree of transparency with real time stats on availability and performance.
- *People fear change*. In general, every change goes along with uncertainty. This phenomenon is also true for cloud adaption.
- *The Endowment effect* states that people value more what they own rather than what they are given. That is why often IT professionals and organizations rather prefer to stay with their already existing IT resources rather than use the benefits of cloud computing.
- *People prefer to invest in the status quo*. The related behavioral bias is the *escalation of commitment*, which means the willingness to dig oneself into their choice even deeper and try to prove they made a right one. The *sunk-cost fallacy* can also be related to cloud adoption decisions. It involves the consideration of prior investments and the need of attempting to gain some returns from it and not considering other options.
- Instant gratification is preferred to any delay. These biases are in favor of cloud adoption. After all, both public and private cloud are an on-demand service, so the instant gratification factor is greater than in traditional IT.

(Weinman, 2012, pp. 303-314); (Sosinsky, 2011, pp.30-33).

Cloud adoption in Europe

The member states of the European Union are facing economically challenging times. Therefore, it is more important than ever to recognize and seize on opportunities like cloud computing to drive growth and innovation. The significant advantages of cloud computing - as already outlined in the previous sections - can benefit also the European citizens, businesses and governments. The EU made efforts to ensure that this potential is captured by the member states.

According to the latest studies on cloud adopting in the EU it is estimated that in 2013, the adoption of cloud computing contributed EUR 27.9 billion (0.2% of total) to EU GDP and it was estimated that in the years from 2016 to 2020 cloud computing will add a cumulative total revenue of EUR 449 billion to EU GDP. Cloud computing not only benefits the GDP and macro-economic performance, but it benefits the society as a whole as well. In the period from 2012-2015 estimates for job creation vary widely, but they all show definitely a positive impact on new job creation. Cloud computing also influences the business creation thanks to its features, such as reducing market entry barriers (mainly SMEs) (Wauters et al., 2016, pp. 51-54). The EU identified cloud

computing as a disruptive technology with the potential of generating economic growth, productivity and employment and enhancing market entry. As such, cloud technology is a crucial part of the EU's Digital Single Market strategy. This strategy aims to open up digital opportunities for EU citizens and companies (European Commission, Digital Single Market). The EU identifies in the framework of the strategy the main issues and develops actions in order to support the development of a cloud adoption supporting economic environment in the EU (Wauters et al., 2016, pp. 4-5). In 2012, the European Commission announced the adoption of the Cloud Computing Strategy for the European Union and the establishment of a European Cloud Partnership that has included private industry and public sector users (Cheung, Weber, 2015, p. 10).

Why is Europe embracing the cloud slower?

Despite the clear benefits of cloud computing many member states are still lagging behind in terms of cloud computing. As it was discussed in the introduction chapter only 21% of the European enterprises use cloud solution according to the latest EU statistics. Statistics about the cloud adoption in the US point to a much higher cloud adoption rate (Why Is Europe Slower to Embrace the Cloud?, 2017).

One of the key challenges for cloud service providers in Europe is that they have to navigate among different laws and directives regarding data privacy and security. Every European country has its own legislation in these regards and in such a complex environment it is challenging for the cloud solution providers to manage services across borders. Based on the EU country of origin principle, every personal data must be stored and processed within the borders of the country where it is hosted. Microsoft, AWS and Google all have already launched data centers in Europe, but in order to wider adoption a higher rate of presence across the continent is inevitable (Why Is Europe Slower to Embrace the Cloud?, 2017).

Despite the strong security features of cloud computing, it still widely considered less secure than on-premise solutions. The EU also considers security issues as an overarching one and aims to tackle it by correct, supporting legislation. In order to ensure a high common level of network and information security (NIS) across the EU, the Network and Information Security Derivative – as part of Digital Agenda – have been adopted in July 2016.

As pointed out above these issues still limit the pace of cloud adopting therefore the EU commission has put in place different measurements and identified three key actions to fully realize the benefits of cloud computing EU-wide:

- Key Action 1: Cutting through the Jungle of Standards;
- Key Action 2: Safe and Fair Contract Terms and Conditions;

- Key Action 3: European Cloud Partnership to drive innovation and growth from the Public Sector (Wauters et al., 2016, p. 5).

We can see that EU is working on a improving the cloud adoption rate in the member states by putting in place different measures to address the barriers that limit the adoption rate. The tasks of any cloud service providers, such as Microsoft is to be aware of these regulations and adapt their sales strategy to benefit from the opening opportunities.

Biggest cloud service provider in Europe

It is inevitable to be aware of the market condition and the key player, in which Microsoft wants to increase its sales. Cloud adoption rate is still not reaching its predicted heights therefore there is a lot of work to do by the cloud providers to increase the growth rate. The European cloud market has a big potential to grow. 17 from the 25 biggest cloud solution providers in Europe is US-based and only 8 are headquartered in Europe. These 17 US cloud providers are responsible for 83% of the total revenue, while the EU based top 8 provider generate only 14% of the total revenue.

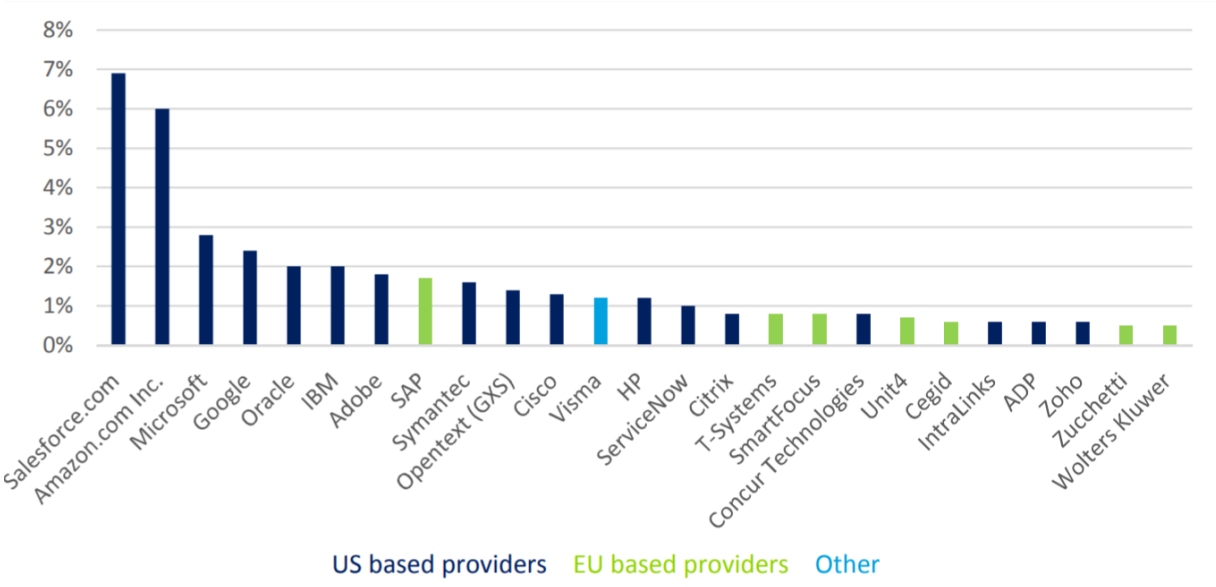

Figure 4: Top 25 Cloud Solution Providers' EU market share Source: (Wauters et al., 2016, p. 70).

Figure 4 shows the estimated market share of the top 25 cloud providers in the EU. Salesforce is clearly the biggest cloud provider, followed by Amazon and Microsoft. Amongst all the vendors the European ones are the largest group, they are responsible for about 50% of the overall revenue.

GDPR

The General Data Protection Regulation (GDPR) law came into force in May 2018. Generally speaking GDPR provides to every individual the right to protect his or her personal data and it requires every business to meet a minimum data protection threshold. The enforcement of this law shows clearly the EU's legislative efforts around data privacy. As a European regulation,

GDPR applies to all companies that collect, store or process personal data related to any EU person. Todays' business world is of course mostly global and crosses country boarders, therefore all of the businesses that somehow work (maintain records and personal data of European users) with businesses that reside within the EU have to comply with the GDPR regulations. If they do not comply with GDPR than they will face significant penalties, with a maximum in the millions of euros per breach, per customer. Organizations can be fined up to 4% of the worldwide annual revenue, or up to EUR 20 million, whichever is higher. GDPR effects both the cloud service providers and their customers within the EU. Data privacy and security questions are challenging as well for the cloud service providers as for the enterprises. As enterprises must comply with these legislations they face double challenges, hence they have to make sure that they choose cloud providers that are compliant to GDPR and they also have to make sure that their operations are also compliant, such as data access and deletion rules, risk assessment procedures, secured back-ups or data breach notification processes (Bernhard 2018).

For cloud providers GDPR offers the possibility to comply with data protection requirements by harmonizing the individual data protection laws of the member states into a single set of EU-wide rules. The major players like AWS, Microsoft and Google have moved rapidly to make their cloud services GDPR compliant. They welcomed the regulation as it raised the standards for data protection, security and compliance and it also created an opportunity to build a broad range of tools and services to enable their customers to build a GDPR compliant cloud infrastructure based on its services. The cloud service providers that started in time to work on their GDPR compliancy and emphasized it to its users get a higher level of visibility in the European Market. For example, there have been developed different associations by some stakeholders, such as the cloud Selection Industry Group on Code of Conduct (C-SIG CC, established by the Commission). Another example is the Cloud Infrastructure Services Providers of Europe (CISPE), which is an association of cloud infrastructure services providers operating in the EU, aiming to "defend firstly the interests of European industry". For cloud solutions providers participating in these associations provided visibility for the companies and therefore a good visibility for existing and potential new customers (Loshin, 2017) (Tolsma, 2018).

Microsoft didn't hesitate to take advantage of the GDPR challenges. Back in 2017, Brendon Lynch, Microsoft's Chief Privacy Officer called GDPR "the most significant change to European Union (EU) privacy law in two decades," in a blog post. He also highlighted that complying with the regulation will not be easy and Microsoft is ready to support its customers path to compliance, but he emphasized the GDPR compliancy is a shared responsibility. Microsoft is also known for its commitment to provide education and compliance resources for its customers (Lynch, 2017).

In cloud computing context GDPR continues to support the use of standard contractual clauses, company policies and the regulations of the member states to establish lawful collection and

transfers of personal data in third countries. It facilitates for cloud services providers to approve these mechanisms at EU level. GDPR should contribute to eliminate or ease some of the barriers to the free flow of data, hence it should impact the uptake of cloud computing in the EU. It will still take some time to examine the exact effects of this new regulation, but the concept is clearly a challenge, but at the same time also an enhancer for adopting the cloud computing resources as cloud computing plays a key role in helping cloud services providers and their customer to become and remain GDPR compliant (Loshin, 2017).

There are some main GDPR specific challenges for cloud users and vendors: under GDPR *personal data may not be stored longer than predefined*. It is a challenging requirement as data can be stored at multiple locations and backup processes should also be taken into consideration for deletion of data. *Breaching response and coordination* should be included in the agreements between cloud user and vendor. An agreement must define what a breach is and how the cloud vendor must response to it and let the organization know about the threats immediately. Due to the fact that data can be *stored outside the European Economic Area (EEA) the processing of this data* needs appropriate safeguards by defining multi-country cloud strategy and by compliancy to all regulations and data localization laws. Cloud providers must be able to provide the technical capability to cloud users to make their *data portable*. Also, a contract should include that the *cloud user maintains control and ownership* of their own data. Cloud vendors should provide proper *risk management* for their users in the agreement the right to audit the cloud vendor must be incorporated. For a proper audit an audit plan and a control framework are also inevitable. As cloud users have their own IT security requirements cloud vendors must offer that an appropriate IT control is in place. Cloud vendors can demonstrate the compliance and security measures by using ISO certifications (Tolsma, 2018).

Cloud Computing in Austria

As already pointed out in the introduction part cloud adoption is clearly slower than the top performers in the European Union. Based on statistics from 2016 only 17% of the Austrian companies are using cloud computing services, which is well below from the EU average cloud usage of 21%. Austria has the 18. place in the cloud usage ranking of Eurostat (derstandard.at, 2017).

When examining the usage of cloud services mainly bigger companies (over 250 employees) are using them (24%) (trend.at, 2014) These bigger companies are mostly more aware of the cloud computing solutions, they have more resources and knowledge to implement them. Based on a recent study (Weiss, 2018) conducted by an Austrian IT company (Anexia), 45% of the organizations with more than 49 employees think that they will use more of the technologies in the future. Furthermore, the study showed the two third of the organizations that currently don’t

use any kind of cloud computing solutions would like to invest in the near future more intense. When organizations were asked about the location of their data 21% of the IT decision makers did not know where their data is stored. Yet despite the previous results it is remarkable that 80% of the interviewed IT professionals think that the data stored in Austria is very trustable. Followed by the EU cloud providers (49%) and by vendors from the USA (11%). Based on that concern A1 Digital in Austria promise to its customers that their data will be stored exclusively in Austria located servers (industriemagazin.at, 2017).

The Anexia study also proved the wrong concept of thinking that having on-premise IT solutions is more reliable and secure than using cloud services. Therefore, it is crucial for cloud providers to provide communication and enlightenment on the topic and so build trust in the long run in cloud services. Downtime and data security, trust and flexibility were among the most important factors when choosing among cloud providers organizations. The fact that 20% of the questioned IT professionals from bigger organizations think that they will not use more from cloud services in the future is remarkable and it points into a conservative attitude of the Austrian market.

Security, privacy and trust

Transitioning to cloud from on-premise solutions inherent challenges as it involves the transfer of responsibility and control of data, which were previously under the organizations` direct control to the cloud service providers. This transition means that organizations give up a high degree of their control over data to get more flexibility, availability and to save costs in the cloud environment. Yet, this increases the chance for being attacked by hackers, as remote, shared resources are always a bigger target for cybercriminals (Cheung, Weber, 2015, p. 18). With cloud adoption becoming a common strategy for enterprises, IT decision makers are facing challenges and concerns in terms of security and privacy of the cloud. Cloud computing, like other areas of IT, suffers from a number of security issues, which need to be addressed. Because it has a given set of technologies, processes, people, services and regulations. These risks relate to policy and organization risks, technical risks, legal and other risks. Many research papers examined the role of security in cloud computing and its adoption and in most of the cases it has been outlined that trust in the security of cloud computing plays an important role. International Data Corporation (IDC) in 2011 showed that 74.6% of IT decision makers ranked security as a major challenge (Ramachandra, Iftikhar & Khan, 2017, p. 465) and the uncertainty around how security can be achieved at all levels has led IT decision makers to state that security in cloud computing is their number one concern (Avram, 2014, p. 529). Another research paper said also that security is the main issue behind the slower adoption of cloud computing as security breaching in cloud can be more damaging than on-premise security breaches (Raza et al. 2015).

Like any other technology, cloud also has its security vulnerabilities. It is clear that security is an issue in cloud, no question. Therefore, the question regarding security and cloud computing is if cloud solution enhances or weaken the security. As any other technology cloud will continue to have security issues and in this view cloud security should not be compared against perfection but against a next best alternative. To demonstrate cloud security, we can say that data are as important assets as is money. In this analogy money can be kept under our mattress, like in IT on-premise solutions or we can keep our money in a bank, like a cloud solution. If we consider which one has more security a bank can afford stronger security. Just like a bank, the cloud solution providers have also similar advantages. Therefore, it seems that although there will be security issues with cloud, but if done properly that it has clear advantages compared to on-premise IT solutions (Weinman, 2012, pp. 59-60). Now the question remains what cloud service providers can do to better communicate on that issue to increase the level of trust in their security solutions.

As cloud services happen in a shared environment where many customers data is gathered and countless customer application is running therefore it is subjected to risk. Security is a key risk when considering the conversion into the cloud, so it plays a central role in building trust in cloud vendors. Many customers are reasoning that they are due to the security risks more cautious before entering an agreement with a cloud service provider (Khan, Malluhi 2010, p.21).

Trust and control in cloud computing

Generally speaking trust in any IT environment -and in the cloud computing context- trust is based on several factors, such as control over data, ownership, reputation, reliance and predictability. It means that customers can rely on the cloud service providers ability to provide their services as expected. Control as an important component of trust influences the decision of cloud adopting significantly. Control means that the customers -that give their valuable data to cloud providers- can decide any time what could happen with their data in the cloud environment. It is an important component as almost any customer might feel comfortable consigning control of their data (Khan, Malluhi, 2013, p. 94).

Cloud providers could increase the adoption rate of their services by focusing on giving more control of sensitive data. We can differentiate five broad areas of control in cloud computing: control over stored data, data during processes, software, regulatory compliance and billing. Cloud providers could improve in granting more control to the customers in each of these areas. By providing remote monitoring and control of data access and data ports better data visibility and more transparency could be granted and so more control for the customers over their data. One workaround for protecting sensitive data during processing could be to let clients control which data should be seen by servers and in what form. Control over Software and protecting it is often an overlooked issue. Customers can develop and run their own software in cloud and so this process includes valuable knowledge, business practices and information that the clients do

not want to share with the cloud providers. For cloud provider to run a software on its servers the customers must reveal what computations the software is performing. To build trust in this regard making able for customers to protect the internals of software function (with garbled circuits) and using technologies for oblivious computation could help. As it will be pointed out later regulatory compliance is an important trust builder between cloud providers and customers. Currently checking the cloud providers compliances for customers is overwhelmingly difficult. Making this process at least semi-automatic could help cultivating more trust in cloud computing. Regarding the control of billings in cloud computing customers have to be able to monitor how much resources they have used in a given timeframe. In cases of hacker attacks often the customers do not realize that their metered cloud resources are used by a criminal, but they are responsible for this usage and they have to pay for the services they didn't consume. A solution here would be to adopt a solution in which the customer could review real-time data for its subscription and to make it possible to detect any fraudulent resource consumption. In summary it can be said that giving more control to the customers could increase the confidence in using cloud computing and so increase the rate of cloud adoption (Khan, Malluhi, 2013, pp. 95-96).

Security challenges in cloud computing

As stated above cloud computing entails security issues, which should be solved by cloud providers, legislators and policy makers. As security challenges are still one of the major concerns that society cites as a reason for a cautious attitude toward cloud computing adoption. By putting our personal data on remote servers bring unprecedented challenges, because we may lose control over our data and it may be that we do not even know how, where and by whom our data is being handled in cloud computing processes. Many references highlighted the relevance of security concerns. For example personal data protection issues have been identified as one of the most important issues for cloud adoption by OWASP (Open Web Application Security Project), a commonly referenced worldwide organization, which focuses on improving the security of application software. Other major survey also named security considerations as a critical hurdle for cloud computing. Another proof for mistrust in cloud security is that the US government does not store classified data in the public cloud due to national security reasons (Cheung, Weber, 2015, p. 10).

General security threats

There have been identified nine major threats in cloud computing by the Cloud Security Alliance in 2013:

- Data breaches: intentional or unintentional release of secure information to an untrusted environment.
- Data loss: deletion of data by malicious hackers or by careless cloud providers.

- Account or service traffic hijacking: for example, if attackers gain access to credentials
- Insecure APIs (Application Programming Interface)
- Denial of Service (DoS): when hackers use up the virtual machines` processing time and make applications unable to provide their services
- Malicious insiders
- Abuse of cloud by outsiders: for example, a hacker can use cloud servers to make virus attacks
- Inadequate knowledge about cloud: when an organization moves to the cloud without having proper knowledge about cloud security
- Technology vulnerabilities when a cloud provider use software that is not designed to offer proper isolation properties in a multi-tenant environment like the cloud (Cheung, Weber, 2015, pp. 17-18).

Of course, there exist other security issues identified by other references, so we can see that there is not a general approach to security issues in cloud computing. There are instead different scenarios, approaches and aspects to the problems. Most of the references although had overlapping and to highlight the most important security considerations the list above should be complemented with the following important security challenges (Murugesan, Bojanova 2016, pp. 209-210):

- Protection of data at rest: providing confidentiality, integrity, and availability of data
- Fine-grained access: enabling fine-grained retrieval and query execution on critical data
- Selective access: owner-regulated access control and authorization enforcement
- User privacy: providing privacy of users accessing data and using cloud resources
- Query privacy: providing privacy for users when using cloud resources
- Collaborative query execution with multiple providers: enabling controlled data sharing for collaborative queries and computations when a customer use multiple cloud providers
- SLA and Auditing: specifying security requirements in SLA
- Multi-tenancy and virtualization

Accessing the organizations' sensitive and critical data include high security risk and therefore Identity and Access Management ensures that access to these is controlled and secured. Identity management is therefore critical, it focuses on the creation, management and removal of access rights (CSA, 2012, pp. 11-12).

Security issues that are specific to cloud infrastructure are related to virtualization environment. The issues in this paragraph should be covered mainly by the cloud service providers. The *insecurity of Application Programming Interface (API)* which is used by the users to connect to the cloud services include vulnerabilities like unauthorized access, content transmission etc. *Quality of Service* (QoS) is another issue which should be a focal point for cloud vendors. It could

be resolved by not purely focusing on providing fast and cheap services but also on security considerations. The issue of *fate sharing incidents* means to identify in time and avoid error transfers from an infected mobile VM to other servers. The *suppliers should also be reliable* by checking the background of their staff that access and control data and processes. *Security misconfiguration* of the servers, platform, application etc. could lead to intruders having access to the system. *Multitenancy* is an important attribute of cloud computing, but it imposes risks, so it needs to be considered in terms of security by cloud providers just like the terms of *server location and offline back up* (Khalil, Khreishah & Azeem 2014, pp. 6-8).

Solutions to security threats

The following paragraph gives an overview of the instruments used to cater appropriate security measurements. The security threats are well known for cloud vendors and cloud consumers; therefore, they have to make countermeasures and controls to mitigate the risks. One technique to maintain security is to have "golden" system image references that users can return if needed. A "golden" system image is a screenshot that creates a copy of the users' whole environment that includes application, data, firewalls, machine images. With the help of it, users can go back to the environment when everything did not contain any security problem (Sosinsky, 2011, pp. 250-251).

Further general solutions are configuration control, vulnerability testing, security audits and providing greater consistency by cloud vendors. In addition, cloud providers also should provide better resilience and disaster recovery strategies for tackling quick and big deviations of services demand. Furthermore, to provide better off-site repository for a user's data by provisioning better backup and restore processes (Cheung, Weber, 2015, pp. 21-22).

Of course, as mentioned earlier security is a shared responsibility of the vendors and users. CSA (Cloud Security Alliance) accurately states that "the lowest common denominator of security will be shared by all tenants in the multi-tenant virtual environment unless a new security architecture can be achieved that does not „wire in" any network dependency for protection(Mishra et. al., 2013, pp. 36-39)

Cloud Governance

Cloud governance is a basic requirement for organizations being able maintain control over their complex services, systems and environments. It is a set of policies, processes and technologies that describe how cloud environment is governed and controlled by the organization. In order to have an effective cloud governance model must include the following components: workforce education, Identity and Access Management (IAM), Risk and Event Management and Monitoring and Audit. Cloud solution providers must build on the fact that a proper cloud governance framework is essential for using cloud in a secure way (Murugesan, Bojanova 2016, pp. 220-221).

Service Level Agreements

Service Level Agreements (SLA) have become significantly more important in compliance with the further development of the cloud. It refers to the binding agreement between cloud provider and customer. An SLA documents the assurance of the cloud vendor that it will deliver the promised services and it will protect the customers' critical data and applications in the cloud and it specify the conditions under which the services must be delivered. Users usually negotiate with cloud vendors specific terms about security requirements and the security services delivered. In the past SLAs mainly focused on quality aspects of the delivered services, but today the security considerations are as crucial part of an SLA as quality. Today SLAs may include the specification of the security guarantees. For instance, it can be specified the data is stored, its possession, its handling etc. After the parties agree on the terms than they commit to the SLA and the cloud service provider will start to deliver the services. SLAs also make it possible for users that they can monitor the service if it implemented as agreed. An SLA can be renegotiated in cases if the user wants to change the terms of the agreement or if any violations of the SLA have been detected (Cheung, Weber, 2015, pp. 21-22) (Murugesan, Bojanova 2016, p. 218).

Multitenancy and virtualization

Multitenancy is an important feature of cloud computing. It basically means that multiple tenants (multiple applications inside and outside the enterprise) can share resources by using a common cloud infrastructure at the same time. Each tenant (user) shares network, memory, computation and storage resources, thus utilize the many advantages of cloud computing such as cost reduction, utilized resources, scalability, reliability etc. Basically, each tenant creates its own, secure virtual environment. There exist different levels of multitenancy due to the various needs of the tenants. The concept is applied in all the layers of cloud: in IaaS, PaaS, SaaS. Of course, IaaS and PaaS mean the lowest levels of multitenancy, where it is limited to infrastructure and platform. On the highest level of multitenancy all levels of cloud are developed to be multitenant. However, the capability of sharing resources is a crucial in cloud computing, but it is also a main security concern due to uncontrolled sharing of resources and coexistence of different tenants (Mishra et. al., 2013, pp. 36-39) (Murugesan, Bojanova 2016, p. 218).

Virtualization is the basic mechanism which enables multitenancy in the cloud. It is also a crucial instrument in cloud security. Virtualization is not a new technology, it has been already introducing as "time-sharing" in the 1960's by IBM. It creates a virtual version of, for instance, an operating system, storage device, network resources, and all that within a single physical system. It is a way of making a physical computer function by installing an operating system on a hardware that does not really exist. The virtualized resources can be shared through multiple environments which are called virtual machines (VMs). VMs are basically virtualized representations of physical machines in operated and maintained by the so-called hypervisor, which goal is to create and run the virtual machines. This is a very useful feature because multiple

virtual machines can exist on a single physical host. Although, VMs offer many advantages, but it also introduces security concerns. The security depends highly on the used operating system, therefore a VM should be handled as it was a physical machine. From the security point of view there should not be made any differences between VMs and physical server. VMs are potential attacking points for hackers and there are two main ways to access a VM. One is through the network connections and the other is through the hypervisor. Not only the VMs are vulnerable, but also against the host servers can happen hacker attacks, like a DoS (Denial of Service) attack. In cloud environment these security concerns are even higher because hackers can use cloud services, as a customer, and start to attack with the help of a malicious VM the other VMs over the network and so the traditional security controls are not able to follow these processes as VMs communicate through the hypervisor and not through a physical server (Mishra et. al., 2013, pp. 36-39) (Murugesan, Bojanova 2016, p. 218). In conclusion virtualization and multitenancy are coming with its own security issues. There introduce new possibilities and surfaces to be attacked and this requires a new form of network security controls. This means that cloud providers have to introduce new robust security controls to assure proper security and to be compliant with the ever-changing laws and regulations. If tackled properly than the security challenges can mean opportunities for cloud vendors to increase the trust in the users and provide an improvement if they move to the cloud.

Further security technologies

There are many other measurements, using which can help organizations to create and keep their organizations secure safe by protecting themselves against security threats and attacks in the cloud environment. As mentioned previously Identity Access Management is an important security risk, which can be avoided with proper measurements.

Single Sign-On: in todays` cloud environment user log in to multiple applications and tools. Single Sing-On is an important tool in access management, where the log-in credentials of a user are trusted and that enables user access multiple applications, data and services in the cloud. Access to sensitive data should have strong authentication requirements. Single Sign-On helps organizations to have strong authentication mechanisms that guarantee valid credentials and determines the authentication rights at user level (Tripathi & Mishra 2011).

Services of Identity Management: it plays an important role in cloud security with its main components. It controls *provisioning and deprovisioning*, hence creating or deleting user accounts and control access to resources in cloud. The so-called *Centralized Directory Service*s are considered as a main security component. The concept for cloud environment means that identity and access information for security purposes is stored and identified by a unique identifier and at location. *Audit and Monitoring* is also an essential part of cloud security. It helps to create access control mechanism based on the given role, distribute and isolate tasks, evaluate risk levels and

prevent access violations. Instead of first-generation firewalls *virtual firewall* appliances should be used in order to be able to monitor all levels of traffic, such as peer to peer traffic or web browser traffic. Finally, another important measurement is the *security of virtual machines* as they are just as vulnerable as a physical one. To prevent them both from internal and external threats the networks should be inspected, and they should be isolated from other network segments. Against internal threats the organizations can protect themselves with the help of using intrusion prevention systems and against external threats by using secure remote access technologies (CSA, 2012, pp. 13-14) (Tripathi & Mishra 2011).

Security in the different deployment and services models

Security and trust in cloud computing depends on the selected deployment and services model: different types of deployment and services models offer different levels of security services. In traditional IT the governance of the data and applications was in the hand of the owner, but in cloud computing it is outsourced and delegated out to cloud service providers. This, of course imposes a broad range of threats, as security relies on trusting the cloud vendors capabilities to provide IT security. Therefore, it is crucial to differentiate the different models from a security point of view. The users get the lowest level of security services with IaaS and they get the most with SaaS (Zissis, Lekkas, 2012, p. 585).

As pointed out previously, cloud computing has different deployment and service models. Each of these different models have unique security considerations. The three standard deployment models: private-, public- and hybrid cloud. In private cloud models the main security concern is caused by high costs of implementation and management, skills requirements and vulnerability of the system. In this model the organizations have high level of influence on the cloud architecture, processes and tools, hence positive security implications are high. In public cloud models the cloud services providers have already realized the importance of security therefore they have a comprehensive and layered security model with high level of investment into security solutions which can provide a high degree of security to the customers. Furthermore, thanks to its scale of business the customers get their security for a relatively low price. But on the other hand, security challenges are raised, as the resources are not committed to one customer but are leveraged among many and of course due to its scale it is more attractive target to hackers. In hybrid models it is possible to target the business processes or data with purpose-built, focused security solutions to address potential vulnerabilities, threats and risks. This makes the security question in this model cost-effective and targeted. On the other hand, due to its complexity with heterogenous environment and automation tools which goes along with higher risk exposure (Ramachandra, Iftikhar & Khan, 2017, p. 468).

The three most common service models: IaaS, PaaS and SaaS. As mentioned in the previous paragraph each of these have unique security implications as well. IaaS service model has a shared

risk model, in which the cloud vendor and the consumer equally shares the security responsibility. In PaaS model the cloud provider brings more than just the infrastructure to the customers therefore it has more responsibility in security relation than in the case of an IaaS model. Like IaaS model it is still a shared risk model, however, as mentioned before cloud vendors bear more responsibility than the customers. In the case of SaaS service model, the cloud services providers carry the most risk and security responsibility. The customers only must take care about risks and security from their clients' side (Ramachandra, Iftikhar & Khan, 2017, p. 468).

As mentioned previously depending on the service model used, cloud security is a shared responsibility between cloud service providers and users. Generally speaking cloud service providers are responsible for network-based security while the users are responsible for host-based security. But in the cloud environment the responsibility of cloud solution provider is more often emphasized while the responsibility of the users is often overlooked. For instance, web browsers used by the users, different applications running simultaneously, or the mobile devices used to access cloud services increase all the vulnerabilities. Further risk is added up by plug-ins, software extensions, malware of operating systems, backdoor Trojan keystroke embedded in the apps running on cloud etc. (Cheung, Weber, 2015, pp. 20-21).

The different cloud service delivery models create the security boundary between vendor and the user. The security boundaries can be defined as following:

- IaaS: it is the model with the least built-in security. Everything that comprise application is the user's responsibility.
- PaaS: in this model the vendor is responsible for the software framework and middleware layer, while the user is responsible for the security of the applications and the user interface.
- SaaS: in this model the vendor is responsible for the security of the entire stack by providing compliance and governance of security. It is mostly stipulated as part of the Service Level Agreements (Sosinsky, 2011, pp. 253-254).

Legal landscape of cloud computing - International regulations and certifications

The legal and regulatory landscape around cloud computing is not static. There are new laws being proposed that could change the responsibilities of cloud vendors and cloud customers as well. The main challenges are to understand how laws apply to a wide variety of information management scenarios, to the different parties under various scenarios. There are in almost every case an applicable national, international and industry specific regulation that should be considered as legally compliant. Being in legal compliance is a shared responsibility between vendor and customer and different enterprises often are under different regulations depending on their activities, in which market they operate etc. (Winkler, 2012).

In the era of cloud international regulations and certifications are inevitable. These standards can help the cloud customers to choose a cloud services provider and it provides the cloud computing providers the possibility to prove that their services are reliable and secure. As security concerns are very important to the cloud customers they prefer to deploy cloud services providers that implement safety procedures and fulfill certifications showing their compliancy. From a customer point of view keeping data safe and private is not an easy task today. As mentioned already laws and regulations differ country to country. As it was discussed in the previous sections the EU is working on creating a more cloud welcoming environment in its member states and the GDPR - came into regulation on May 25, 2018 – has the potential to provide better privacy and security (Vlajin, 2018).

An important international standard is the ISO 27018, which is a standard for protecting personally identifiable information (PII) in the cloud, which was adopted by the International Standards Organization (ISO) in July 2014. Due to its importance both cloud vendors and cloud vendors should be familiar with the standard. Microsoft was among the first major cloud vendors that certified its Azure cloud service, Dynamics CRM, Office 365 and ERP cloud-based applications. The cloud vendors that want to adhere to this code of practice for cloud privacy must be a subject to an annual audit by an accredited third-party certification body, providing independent validation that the company operates with applicable security controls. This international standard is based on two, already existing security standards, the ISO 27001 and the ISO 27002, which are defining general security policies and as such it is belonging to the ISO 27000 family. The ISO 27000 family of standards addresses privacy, confidentiality and technical security issues. The standards define hundreds of potential controls and control mechanisms. As an evolutionary addition, the ISO 27018 standard deals exclusively with regulating how personal data in the cloud is processed by formulating data protection requirements for cloud services, hence it provides a useful framework for data protection (Gibson, 2015) (Dinnes, 2014). What includes the ISO 27018 standard:

- ISO/IEC 27018 requires certified CSPs to inform customers of the countries in which their data may be stored, so the customers where their data is stored and have the visibility they need to comply with any applicable information security rules.
- Compliant cloud services providers will not use customer data for advertising or marketing, without the customer's explicit consent.
- ISO/IEC 27018 requires a policy that establishes clear and transparent parameters for the return, transfer, and secure disposal of personal information within a reasonable period of time, hence customers know what is happening to their PII.

- Compliant cloud vendors will comply only with legally binding requests for disclosure of customer data, but first they will always notify the customer unless it is prohibited by law from doing so:
- The standard requires cloud vendors to disclose the identities of any sub-processor they engage to help with data processing before customers enter into a contract and if cloud vendors change the sub-processors than they are required to inform customers promptly to give them the opportunity to object or to terminate their agreement (Microsoft.com, n.d.) (Gibson, 2015).

Cloud incidents

As we have seen cloud computing is linked with a wide range of potential security threats. There have been some bigger data breaches which influenced many users and caused serious damage and distrust against cloud service providers. Data breaches and other kind of security incidents mean as well for the users and for the cloud vendors serious damages, such as negative media attention, emerging lawsuits, worse company valuation and other potentially long-term consequences. It is important to learn from these incidents as it could happen to any provider and to any user if they are not paying enough attention to proper cloud using.

The biggest data breach of history

The biggest data breach happened in 2013-2014 and the victim was *Yahoo*. The web titan Yahoo is using cloud infrastructure as well. In a series of attacks real names, email addresses, dates of birth, security questions with answers and telephone numbers have been compromised. The company finally revealed in 2017 that 3 billion user accounts were subjects of the data breaches. This incident is considered as the biggest data breaches of all time (Armerding, 2018).

Dropbox

The cloud-based file sharing giant *Dropbox* had experienced a major incident of its services in 2012 hackers gained access to data of more than 68 million users. The stolen credentials made their way to dark web marketplaces where they have been sold. After this incident Dropbox had to regain the trust of its customers so they requested from their user base a site-wide password reset (Bradford, 2018).

Uber

Another data breach worth mentioning is the case of Uber in 2016, which affected 57 million Uber users and 600,000 Uber drivers. The attackers gained access to Uber's GitHub account, used a developer's AWS credentials, where they find the personal data of users and drivers (Armerding, 2018) (Moyle, 2018)

LinkedIn

LinkedIn was also a subject of data breaches. The first happened in 2012 when 6.5 million encrypted passwords have been stolen and posted to a Russian crime forum. The bad luck continued in 2016 when hackers stole and posted 167 million of login credentials. As a resolution LinkedIn requested its users to change their passwords and additionally it introduced optional two-way authentication for users for being more secure (Hackett, 2016)

Microsoft

In this section I will introduce the company Microsoft, one of the leading cloud service providers in the world. I think it is important to get a short background about the company itself and its offerings. First of all I asked the cloud experts of Microsoft via my questionnaire about the cloud adoption factors, secondly the evolution of Microsoft is a great example that cloud technology will largely define the future of the IT industry and will play a more and more important part in it.

Microsoft stated that its mission is "Empowering every person and every organization on the planet to achieve more". Their business strategy is based on a "mobile-first, cloud first" world with the goal of build best-in-class platforms and productivity services for an intelligent cloud, for every area of our lives. This mobile-first, cloud-first world means a continuous change in the times of digital transformation, when the way how individuals and organizations utilize and interact is changing. The users use multidevice and the way they interact will become more and more multisensory based, like gestures, voice or gaze. This new technology paradigm with an intelligence cloud will be led by Microsoft. Microsoft was founded in 1975 and it operates now worldwide in over 190 countries. Microsoft develops, licenses, and supports a wide range of software products, services, and devices for as well small and medium-sized business as large organizations. The marketing and distribution of the products and services happen through the following channels: OEMs (Acer, Asus, Samsung etc.), direct, and distributors and resellers (Microsoft Annual Report, 2017).

Microsoft's mobile-first, cloud-first strategy was introduced when the current CEO, Satya Nadella take over from the previous CEO Steve Ballmer. It was a clear paradigm shift from the previous "connected devices and continuous service" strategy to a cloud and mobility focused strategy. Microsoft is now at the leading edge of today`s cloud-based solutions. But this was not the case, just a few years ago. For about ten years ago Microsoft was financially struggling as the PC shipments dramatically decreased. While other big players like Apple and Google were becoming stronger as the smartphone and tablet business was on the rise. Additionally, Amazon was the first company that started to cash in with cloud computing as they had quietly launched Amazon Web Services (AWS), establishing itself as a leader cloud service provider. They realized early on that the same computing infrastructure they use for selling their retail items can be rented

for other companies at a lower price than it would cost to build for each company their own cloud infrastructure. By 2008, when Amazon already had 180,000 developers working on their cloud platform, Microsoft did not yet have one (Nadella, 2017, pp. 45-46).

Microsoft's distribution channels

As explained above Microsoft markets and distributes its products and services through different channels. The sales force of Microsoft primarily works directly with enterprises and public-sector organizations worldwide to identify and meet their technology requirements; manages OEM relationships and other partners who engage directly with our customers to perform sales, consulting, or fulfill other functions for Microsoft products and services.

Original Equipment Manufacturers (OEMs)

A large part of the software offerings, such as the Windows operating system or the Office 365 productivity software are sold through OEMs. These manufacturers sell their products (PCs, mobile phones, tablets, servers etc.) preinstalled with Microsoft products.

Direct

Many organizations that license Microsoft's products and services transact directly with Microsoft through the so-called Enterprise Agreements and Enterprise Services contracts. In this case these organizations get their sales support from system integrators, independent software vendors, web agencies, and partners that advise organizations on licensing these products and services.

Distributors and Resellers

Customers can license the products and services indirectly, primarily through licensing solution partners ("LSP"), distributors, value-added resellers ("VAR"), OEMs, and retailers. Although each type of reselling partner may reach organizations of all sizes, LSPs are primarily engaged with large organizations, distributors resell primarily to VARs, and VARs typically reach small and medium organizations (Microsoft Annual Report, 2017).

Microsoft's cloud offering

Microsoft evaluate helping customers to digitally transform and move to the cloud as one of their biggest business opportunities. The cloud offerings of Microsoft benefit from main economies of scale, such as their large datacenters and multi-tenancy locations. These enable low costs, coordinate diverse customers, improve utilization of computing, storage and network resources etc.

The Intelligent Cloud segment of Microsoft consists of public, private, and hybrid server products and cloud services. This comprises:

- Server products and cloud services, including Microsoft SQL Server, Windows Server, Visual Studio, System Center, and related CALs, and Azure.
- Enterprise Services, including Premier Support Services and Microsoft Consulting Services (Microsoft Annual Report, 2017).

Azure

"Azure is a scalable cloud platform with computing, networking, storage, database, and management, along with advanced services such as analytics, and comprehensive solutions such as Enterprise Mobility Suite. Azure includes a flexible platform that helps developers build, deploy, and manage enterprise, mobile, web, and IoT applications, for any platform or device without having to worry about the underlying infrastructure. Azure enables customers to devote more resources to development and use of applications that benefit their organizations, rather than managing on-premises hardware and software" (Microsoft Annual Report, 2017).

The core strength of Microsoft Azure lies on the heritage of the company. The possibility to integrate Azure with other Microsoft products and services makes it very attractive to the customers that are strategically committed to Microsoft technology. Of course, there are some challenges when using Microsoft Azure. A Gartner report highlight that sometimes, adopting Azure is challenging due to the expertise and knowledge needed for implementing it and to the complexity Azure offers without clear guidance when and which solution should be used. Also, the reliability needs to be improved, as it is an important factor for cloud adoption, but sometimes reliability issues affects individual users (Smith, Leong & Bala, 2018).

Microsoft Office 365

Microsoft Office365 is the web-based version of Microsoft's traditional Office suite for enhanced productivity. It is a cloud-based subscription service that brings together many tools. It combines many well-known applications like Word, Excel, Power Point or Skype with cloud services like OneDrive (storage) or Microsoft Teams (collaboration). This helps everyone create and share at any time on any device (Microsoft Office, 2018).

Microsoft Dynamics 365

The last cloud offering I would like to highlight is the Dynamics 365.

Dynamics 365 offers a set of cloud-based business solutions across financial management, enterprise resource planning (ERP), customer relationship management (CRM), supply chain management and analytics application. These unified set of intelligent business applications will

be used more and more in the future, the 78% year on year revenue growth shows this clearly (Microsoft Annual Report, 2017).

Experimental Research Model and Hypotheses

Cloud computing is still in emerging phase and there is still a lack of evidence which factors are the most important for its adoption. The main objective of this paper is to find out, which factors influence the diffusion and acceptance of cloud technologies within organizations. Through a review of the literature the paper provided a background for cloud computing and it introduced the different elements of its adoption. We got a big picture about the technological terms and advantages of cloud computing, the benefits, and limitations of its solutions and the different security, privacy and trust considerations. In the paragraphs which examined the unique cloud adoption factors and the environment in Europe showed insights about the biggest cloud solution providers in Europe, about the willingness of the European Union to make cloud computing more adopted and exploit its advantages and the different regulations that are in effect currently. During the literature review the question

"What are the most important factors for enterprises when adopting cloud computing services and what is their effect?

was examined and the following hypotheses were developed:

- **H1: Security- and legislation-related issues negatively influence the tendency for cloud computing adoption.**
- **H2: Organizational factors positively influence the tendency for cloud computing adoption.**

I will test both hypotheses from Microsoft experts' point of view and from cloud customer's point of view. This will give us important insights about the similarities and differences how cloud suppliers and customers perceive the different cloud adoption factors.

Data

For data collection, I used quantitative primary research in form of a survey. In the attempt to find answers to the problem statement and to test the hypotheses from above an online and a paper-based questionnaire were conducted. Two types of questionnaires were used in order to be able to directly reach out to Microsoft experts by using paper-based questionnaires and to reach out as many cloud users as possible by using the online type of questionnaires. (Kwiksurveys.com). The questions asked from Microsoft experts and cloud users were created based on the cloud adoption factors identified throughout the literature review. I identified for both the security-related and for the organizational-related hypothesis different influencing factors:

- Security-related influencing factors (H1):
    - Control over resources (Q1)
    - Moving data in the cloud (Q2)
    - Cloud vs. on-premise security (Q3)
    - Ownership of the data (Q4)
    - Transparency of data location (Q5)
    - Data protection regulation (Q6)
    - Cloud computing certifications and standards (Q7)
    - Effect of GDPR regulation (Q8)
    - Laws and standards and its coverage (Q9, Q10)
    - Role of SLAs in security (Q11)
    - Data encryption policy (Q12)
    - Customers' unique security challenges (Q13)
    - Cloud incidents (Q14)
    - The EU's attempt to stimulate cloud adoption (Q15)
    - Legislation framework provided by the EU (Q16)
- Organizational factors influencing cloud adoption (H2):
    - Economic benefits of cloud computing in general (Q17)
    - Economic benefits for unique needs of different organizations (Q18)
    - Cloud computing flexibility for unique needs of different organizations (Q19)
    - Effects of transitioning to cloud (Q20)
    - Positive attitude toward changes on organizational level (Q21)
    - Fear of cloud adoption (Q22)
    - Technological readiness of workforce (Q23)
    - General knowledge about cloud computing (Q24)
    - Cloud vs. on-premise in economical aspect (Q25, Q26)
    - Predicting cloud computing related costs (Q27)
    - Cloud strategy (Q28)
    - Psychological barriers (Q29, Q30)

The factors from above are tested with the help of the data collected through the questionnaires. The two questionnaires contained questions examining the different cloud adoption factors. Both of the questionnaires actually ask the same questions, but one of them examine the cloud solution providers' point of view and the other one examines the aspect of cloud users. The questions for Microsoft cloud experts were designed to recognize their assumption about the cloud customers' attitude toward the different factors. This gave a better base for comparing the two groups. My goal was to test the two hypotheses by using this separation of cloud vendor and cloud user and to test the two hypotheses in both cases and finally compare the results of the collected data. In

sum, 30 questions were designed to examine the identified factors. Furthermore, two general questions were asked which asks the general assumption toward the independent variables of the hypotheses. These two questions (question "A" (H1) and question "B" (H2)) were used to make a correlation analysis. I used Pearson correlation test to examine if the participants' average answer on the questions regarding the factors identified for H1 and H2 correlate to the average answer given to the general questions ("A" and "B"). This will show if the identified factors are important to cloud adoption. The general questions "A" and "B" can be assumed as questions examining the groups of the factors (H1 factors and H2 factors).

Questionnaire participants

The two questionnaires can highlight the different approach to the problem of slow cloud adoption rate from Microsoft experts and cloud customers. The questionnaire filled in by Microsoft experts gives us answers about what they think what factors influence the cloud adoption. And the questionnaire filled in by cloud customers answer what the customers think are influencing the adoption of cloud.

As I am lucky to know many customers from Microsoft Austria and many other cloud users, therefore was able to reach out to them via email or using my LinkedIn account to send out and spread the questionnaire and reach out to a broad range of workforce that uses daily different cloud computing solutions. The survey was executed in English language and was open for 4 weeks. Given that the topic needs some knowledge about IT business in general and about cloud computing I filtered my respondents accordingly. To do so, the first two questions of the questionnaire sent to cloud customers were "Do you use cloud computing for your daily work? (yes/no)" and "How would you evaluate your knowledge about cloud computing solutions?" (on a scale of 1-7, where I expected to claim a knowledge of at least 4 or above). These questions helped me to get more accurate results.

Likert Scale

To measure the attitudes and opinions regarding the identified cloud adoption factors I used a 7-point Likert scale. It is a quite popular method because it is a reliable way to measure opinions, perceptions, and behaviors. It offers answers ranging from one extreme attitude to another and typically it includes a moderate or neutral midpoint. It helps to uncover and understand different opinions hence it helps to identify areas where there is room for improvement (SurveyMonkey, n.d.).

I created the Likert scale questions to my survey in order to find out what factors are influencing for cloud adoption. I think it is a good way to find out what people think about this specific topic. I tried to avoid too broad questions and asked more specific ones with a simple, direct language.

The questions about security- and about organizational cloud adoption factors were grouped in order to add up the responses and get a "score" on the hypotheses. These questions are the previously described question "A" and question "B".

Model Specification

From the research model point of view, we can say that Microsoft experts and the cloud users are 1-1 groups for testing the hypotheses.

The goal of the experiment was to find out how the independent variable affects the dependent variable. I designed the two questionnaires to implement these variables into an experiment. The participants had to answer the questions that are created to subjectively measure their anticipated tendency to adopt cloud computing.

Hypothesis 1:

- **H1: Security- and legislation-related issues negatively influence the tendency for cloud computing adoption.**

I designed my first hypothesis that the *independent variable* is the group of *security- and legislation-related issues,* which is defined by various factors, like control over resources, moving data in the cloud etc. The *dependent variable* is the tendency for cloud computing adoption.

There is always a corresponding null hypothesis H0 to each explicitly formulated hypothesis. The null hypothesis for H1 is the following:

- H0: Security- and legislation-related issues have no influence or a positive influence on the tendency for cloud computing adoption.

Hypothesis 2:

- **H2: Organizational factors positively influence the tendency for cloud computing adoption.**

Organizational factors	Independent Variable	Dependent Variable
• Economic benefits of cloud computing in general • Economic benefits for unique needs of different organizations • Cloud computing flexibility etc.	• Organizational factors	• Tendency for cloud computing adoption

The *independent variable* of the second hypothesis is the group of the *organizational factors*, which depends on elements like economic benefits of cloud computing in general, economic benefits for unique needs of different organizations, cloud computing flexibility etc.

The *dependent variable* is at both hypotheses the tendency for cloud computing adoption. At an experiment, we had more possibilities to measure this variable, but finally, I choose that the participants will fill out a questionnaire, where they faced different questions about the cloud adoption factors and how important they perceive them.

H2 has the following H0:

- H0: Organizational factors have no influence or negative influence on the tendency for cloud computing adoption.

From the research model point of view, we can say that Microsoft experts and the cloud users are 1-1 groups for testing the hypotheses. 2 different treatments in this sense have been conducted, hence the results can be divided in Microsoft's point of view and the customer's perspective.

Research results

I collected a total of 31 completed questionnaires from Microsoft experts and after spreading the questionnaires on social media a total of 87 cloud customers completed it. 44 of these did not use cloud computing daily or declared that his/her cloud knowledge is below 4 (on the scale of 1-7) therefore I excluded the answers of these respondents from the results and were not included in further examinations, therefore I have 43 useful completed questionnaire.

The frequency analyses shown in the following tables provide an overview of the responses. To avoid non-reliable responses the participants were also given the choice of not answering a question.

Frequency Analysis – Microsoft experts

	Valid	Missing

	1	2	3	4	5	6	7	no opinion
Q1	0	0	0	1	3	4	23	0
Q2	0	0	0	0	4	4	23	0
Q3	2	0	2	5	4	8	10	0
Q4	0	0	0	3	6	7	15	0
Q5	0	0	0	0	0	3	28	0
Q6	10	8	4	3	3	2	0	1
Q7	2	4	4	5	7	5	4	0
Q8	18	7	4	2	0	0	0	0
Q9	0	0	0	2	5	7	17	0
Q10	0	0	0	4	6	9	12	0
Q11	17	5	3	3	1	1	0	1
Q12	5	5	4	4	3	3	7	0
Q13	0	0	1	3	3	6	16	2
Q14	0	0	0	0	2	5	24	0
Q15	13	8	7	2	0	0	0	1
Q16	13	7	7	3	0	0	0	1
Q17	0	0	3	3	2	3	20	0
Q18	0	0	2	3	1	4	21	0
Q19	0	2	3	5	8	6	7	0
Q20	7	6	7	6	2	3	0	0
Q21	0	0	0	0	1	4	26	0
Q22	2	4	3	2	4	4	12	0
Q23	9	13	3	0	2	3	1	0
Q24	0	0	0	0	1	3	27	0
Q25	10	9	7	3	1	1	0	0
Q26	5	6	5	5	5	3	2	0
Q27	13	6	6	0	1	2	3	0
Q28	0	0	1	1	2	2	25	0
Q29	2	3	4	3	4	7	6	2
Q30	7	7	5	4	4	1	2	1
“A”	0	0	2	7	16	5	1	0
“B”	0	0	2	9	8	10	2	0

Table 3: Frequency Analysis - Microsoft Experts

Frequency Analysis – Customers’ point of view

	Valid							Missing
	1	2	3	4	5	6	7	no opinion
Q1	1	1	0	3	3	6	29	0
Q2	0	0	0	0	1	7	35	0
Q3	4	0	2	5	2	1	29	0
Q4	2	0	1	0	6	7	27	0
Q5	0	0	2	0	0	5	36	0
Q6	2	1	0	1	3	5	31	0
Q7	1	1	1	0	7	5	28	0
Q8	17	7	8	6	1	2	1	1
Q9	1	1	0	7	5	7	20	2
Q10	17	10	7	3	4	1	0	1

Q11	7	8	13	5	5	3	2	0
Q12	9	8	9	9	3	3	2	0
Q13	0	0	2	6	3	8	22	2
Q14	0	0	0	0	1	5	37	0
Q15	18	5	9	2	4	2	2	1
Q16	13	10	7	11	0	2	0	0
Q17	0	0	0	3	2	18	20	0
Q18	5	2	2	2	6	14	12	0
Q19	17	8	10	4	1	2	1	0
Q20	13	9	14	4	1	2	0	0
Q21	1	0	2	7	6	5	22	0
Q22	3	3	4	3	2	7	21	0
Q23	18	10	6	3	2	3	0	1
Q24	0	0	0	3	1	6	33	0
Q25	0	2	2	2	1	6	30	0
Q26	23	9	6	3	1	1	0	0
Q27	25	6	2	1	2	3	4	0
Q28	1	0	1	1	10	9	21	0
Q29	7	6	17	8	0	1	2	2
Q30	25	7	5	1	4	1	0	0
“A”	0	1	1	10	22	7	2	0
“B”	1	1	4	26	10	1	0	0

Table 4: Frequency Analysis – Customers’ point of view

The following tables summarize the means of the given answers:

Hypothesis	**Question #**	**Factor**	**Microsoft Experts Group**	**Cloud Customers Group**
			Mean	**Mean**
H1	1	Control over resources	6.6	6.
H1	2	Moving data in the cloud	6.6	6.
H1	3	Cloud vs. on-premise security	5.4	5.
H1	4	Ownership of the data	6.1	6.
H1	5	Transparency of data location	6.9	6.
H1	6	Lack of data protection regulation	2.6	6.
H1	7	Cloud computing certifications and standards	4.4	6.
H1	8	Negative effect of GDPR regulation	1.7	2.
H1	9	Difficulty of laws and standards and its coverage I	6.3	5.
H1	10	Difficulty of laws and standards and its coverage II	5.9	2.
H1	11	Trust in SLAs regarding security	2.0	3.
H1	12	Trust in data encryption policy	4.0	3.
H1	13	Customers’ unique security challenges	6.1	6.
H1	14	Cloud incidents	6.7	6.
H1	15	The EU’s attempt to stimulate cloud adoption	1.9	2.
H1	16	Legislation framework provided by the EU	2.0	2.
Average H1			**4.7**	**4.**

H1	"A"	General question regarding security issues	5.0	4.9

H2	17	Economic benefits of cloud computing in general I	6.1	6.3
H2	18	Economic benefits of cloud computing in general II	6.3	5.1
H2	19	Cloud computing flexibility for unique needs of different organizations	5.1	2.4
H2	20	Effects of transitioning to cloud	3.0	2.5
H2	21	Positive attitude toward changes on organizational level	6.8	5.8
H2	22	Fear of cloud adoption	5.0	5.4
H2	23	Technological readiness of workforce	2.5	2.3
H2	24	General knowledge about cloud computing	6.8	6.6
H2	25	Cloud vs. on-premise in economical aspect I	2.3	6.3
H2	26	Cloud vs. on-premise in economical aspect II	3.5	1.9
H2	27	Predicting cloud computing related costs	2.6	2.4
H2	28	Cloud strategy	6.6	6.0
H2	29	Psychological barriers I	4.7	3.0
H2	30	Psychological barriers II	3.1	2.0
Average H2			**4,6**	**4,1**
H2	"B"	General question regarding organizational factors	5.2	4.2

Table 5: Responses on the questions by groups

Examining the differences between the two groups

We can see that based on the average evaluation of the different factors the difference between the two groups is perceptible at some of the questions. In most of the cases, Microsoft experts and cloud customers agreed on the importance of the examined factors, but I found 11 questions where their opinion differed with more than 1 average point (6, 7, 10, 11, 18, 19, 21, 25, 26, 29, 30). In case of these questions, I assume that the groups would not agree on the significance of the underlying factors. We can say that in average the two group has the more or less the same scores for H1 (4,7 and 4,9) and the average results for H2 slightly differs (4,6 and 4,1).

Although on average there is almost no pertinent difference between the two groups, but as mentioned before at some of the questions there are relevant differences. It would be useful for cloud solution providers to check on these factors and think about what could cause these differentiating points of views. I would like to highlight some of these questions. A great example is that cloud experts think that the customers do not observe that the majority of cloud solution providers would lack strong, detailed data protection legislation (Q6, 2.6 vs. 6.3 perceived importance). So, in my opinion, this topic would worth an examination from the cloud suppliers why their customers consider this topic as not proper enough. Another interesting observation we can make is at the question 9 and 10. Both questions examine the perceived importance of laws

and standards in cloud computing regards. Question 9 asks if it is difficult to have an overview of all these laws and standards and question 10 asks if all aspects of cloud computing are covered by such laws and standards. The results show that while both groups think it is difficult to have an overview (Q9), but only the cloud experts group thinks that practically all aspects are covered by laws and standards (5.9), because the cloud customers group judge it as not all aspects are covered (2.3). In my viewpoint cloud providers lack appropriate education offering for cloud customers about current laws and standards and it could lead to such differences. The question 19 highlights for us that the cloud customers that participated in the research are not so certain about the economic benefits of cloud solutions as the cloud experts are if we are speaking about satisfying unique organizational needs (5.1 vs. 2.4). I would emphasize again the importance of educating the cloud customers. Cloud solution providers should play a big role in educating their current and potential clients. The last question I would like to highlight where I observed significant differences between the two groups is the question 25. I just mentioned the importance of educating the potential and current cloud customers. But this question would suggest to us that cloud customers think that their IT workforce would be able to tackle the technological challenges of cloud computing. However, on the other side cloud providers think that customers' IT workforce sometimes lack the needed knowledge for cloud computing. It is hard to judge for me which group thinks correctly about this question, but there is no doubt that cloud providers should give some thoughts about why they think that customers are not cloud ready enough and if it is true or not.

Examining the individual factors

Although based on the means I assume a significant correlation between the factors and the cloud adoption rate. But to unveil the relationship between the dependent and independent variables of the hypotheses several statistical analyses will be conducted in the next paragraph. Before that, I would like to take a look at the individual factors I identified as important for cloud adoption. On average I said that the factors are relevant for cloud adoption, but not all are at the same influential level. If we take a look at Table 5 then we can see that at 13 questions from 30 one or both groups evaluated the factor as less significant (3.0 or below). Here I have to conclude, that some of these factors are not supporting my hypotheses. For example, question 8 said that GDPR does not help gain trust. This is not supported based on the responses. The questions which are not supported and therefore do not support H1:

- Negative effect of GDPR regulation
- The EU's attempt to stimulate cloud adoption
- Legislation framework provided by the EU

It can not be concluded that these questions were not important, it is just how they and the hypothesis have been formulated make them not supporting each other. For example, if I would ask if "GDPR help gain trust in cloud computing data protection" than it probably would have supported the H1. And the questions that are examining the EU's attempt to make the member states easier to exploit cloud computing advantages seemed not to be important, but I think it could be caused by the lack of knowledge about the EU's regulations for both groups.

The questions that are not supporting H2:

Cloud computing flexibility

- Effects of transitioning to cloud
- Technological readiness of workforce

The technological readiness of the workforce seems to negatively influence cloud adoption, although the general knowledge about cloud computing was evaluated as important. I think it shows that the decision makers about cloud computing think it is important to have knowledge about cloud computing, but they do not trust their workforce that they would be able to tackle the cloud challenges and benefit from the technology.

Normality test

First, we had to test whether the answers are normally distributed or not. For that, I used Kolmogorov-Smirnov test with the help of SPSS Statistics Software.

- Normality test of the results from the cloud customer questionnaire (excluded the questions "A" and "B"):

Tests of Normality

	Kolmogorov-Smirnov[a]		
	Statistic	df	Sig.
q1	.377	43	.000
q2	.487	43	.000
q3	.402	43	.000
q4	.338	43	.000
q5	.471	43	.000
q6	.400	43	.000
q7	.364	43	.000
q8	.222	43	.000
q9	.241	43	.000
q10	.219	43	.000
q11	.206	43	.000
q12	.150	43	.017
q13	.269	43	.000
q14	.507	43	.000
q15	.238	43	.000
q16	.190	43	.000
q17	.266	43	.000
q18	.271	43	.000
q19	.210	43	.000
q20	.181	43	.001
q21	.298	43	.000
q22	.270	43	.000
q23	.233	43	.000
q24	.447	43	.000
q25	.396	43	.000
q26	.301	43	.000
q27	.325	43	.000
q28	.265	43	.000
q29	.202	43	.000
q30	.329	43	.000

a. Lilliefors Significance Correction

Table 6: Kolmogorov-Smirnov test - cloud customers' questionnaire

The K-S test (Table 6) for the cloud customers questionnaire tells us that it is statistically significant from a normal distribution as the significance value is less than 0.05 at every question, despite the small size of the sample.

- Normality test of the results from the Microsoft experts' questionnaire (excluded the questions "A" and "B"):

Tests of Normality

	Kolmogorov-Smirnov[a]		
	Statistic	df	Sig.
q1	.440	31	.000
q2	.448	31	.000
q3	.227	31	.000
q4	.290	31	.000
q5	.530	31	.000
q6	.219	31	.001
q7	.156	31	.052
q8	.344	31	.000
q9	.327	31	.000
q10	.229	31	.000
q11	.318	31	.000
q12	.143	31	.105
q13	.263	31	.000
q14	.463	31	.000
q15	.254	31	.000
q16	.255	31	.000
q17	.382	31	.000
q18	.395	31	.000
q19	.152	31	.066
q20	.149	31	.077
q21	.496	31	.000
q22	.215	31	.001
q23	.332	31	.000
q24	.510	31	.000
q25	.211	31	.001
q26	.150	31	.075
q27	.232	31	.000
q28	.470	31	.000
q29	.186	31	.008
q30	.181	31	.011

a. Lilliefors Significance Correction

Table 7: Kolmogorov-Smirnov test - Microsoft experts' questionnaire

It is quite surprising that we can see at 5 question a not normal distribution (significance level above .05) of the answers (Q7, Q12, Q19, Q20, Q26). This means that at these five questions the Microsoft experts gave relatively different answers. These questions are examining the following factors: cloud computing certifications and standards, data encryption policy, cloud computing flexibility, effects of transitioning to the cloud, cloud and on-premise comparison. The difference in the responses on these questions can have various reasons. One of the limitations of my research is that I did not group the cloud experts based on the segment they are working in. Because it is clear that an IT professional working with commercial enterprises are facing other cloud adoption issues than an IT professional working with public organizations. This would also apply to the

customers. In their opinion, the industry they are operating would also be an important influencing factor, although my data did not suggest it.

Pearson Correlation Test

To find out if the survey results are significant I used the Pearson r correlation test. It helps to figure out if the null hypothesis needs to be rejected or the alternative hypothesis accepted. The Pearson correlation measures the degree of the linear relationship between two variables. It can examine the positive, negative or neutral relationship between different factors. The correlation coefficient (r) put a value to the relationship. It can have a value between -1 and 1. "0" means there is no relationship between the variables at all, while -1 or 1 means that there is a perfect negative or positive correlation (Statistics How To, n.d.).

The answers to the questions regarding the factors presented in subsection "Data" were tested concerning correlations with the answers to the questions "A" (H1) and "B" (H2). In order to make the analysis I took the average of the answers by the respondents to the questions examining H1- (1-16) and H2- (17-30) factors and I tested concerning correlations with their answers to question A (examines H1) and to question B (examines H2). To conduct my analysis I used SPSS.

- Results for H1 (questions 1-16)
    - Microsoft experts' point of view

Correlations

		q_1_16	q_A
q_1_16	Pearson Correlation	1	.689**
	Sig. (2-tailed)		.000
	N	31	31
q_A	Pearson Correlation	.689**	1
	Sig. (2-tailed)	.000	
	N	31	31

Table 8: Results of the correlation analysis concerning the tendency for cloud computing adoption (Microsoft experts` point of view)

Hypothesis H1 claims that there is a negative correlation between security- and legislation-related issues and the tendency for cloud computing adoption. It means that the more relevant the respondents evaluate the factors of security and legislation elements the lower the tendency for cloud computing adoption. As we have seen in the analysis of the means above Microsoft experts evaluated security related issues (questions 1 to 16) as an important influencing factor of cloud computing adoption (4.7 average). They responded to the question "A" which have been used to examine the correlation with an average of 5.0. This question claims that security issues hinder cloud computing adoption. As Table 8 shows, the question aiming at the perceived importance of security and legislation related issues in cloud adoption show a significant statistical positive

correlation (.689) with the actual perception of the rate security issues hinder cloud adoption. Therefore, hypothesis H1 (the more important the security issues the lower the tendency for cloud adoption) is supported by the survey results asked Microsoft experts.

- Cloud customers' point of view

Correlations

		q_1_16	q_A
q_1_16	Pearson Correlation	1	.685**
	Sig. (2-tailed)		.000
	N	43	43
q_A	Pearson Correlation	.685**	1
	Sig. (2-tailed)	.000	
	N	43	43

Table 9: Results of the correlation analysis concerning the tendency for cloud computing adoption (cloud customers' point of view)

I tested the hypothesis H1 not only from the Microsoft expert's point of view, but also from the cloud customers' perspective. Cloud customers evaluated the security and legislation related issues (questions 1-16) as an important influencing factor of cloud computing adoption (4.9). They slightly rated it more important than Microsoft experts, but we can say that both groups agree on the importance of this component. Cloud customers answered on the question "A" with an average of 4.9, therefore it is no surprise that the Pearson correlation analysis shows that concerning the perceived importance of cloud security issues and factors showed a significant positive (.685) correlation on the hindrance effect of security issues on cloud adoption. Therefore, hypothesis H1 is also supported by the survey results asked cloud customers.

- Differences and similarities of the two groups

As shown above, both group results supported hypothesis H1. Even the correlation rates of the two groups are very similar (.685 and .689). Therefore, we can say that both groups are on the same page regarding security related factors. The questions for the Microsoft experts were designed to find out what the experts think about how the cloud customers perceive the different factors, hence we can say that the cloud experts know very well what the customers concern the most. This is a good sign for the future of cloud computing adoption as the only question remains is how to solve these problems and build trust in the customers.

- Results for H2
  - Microsoft experts' point of view

Correlations

		q_17_30	q_B
q_17_30	Pearson Correlation	1	.884**
	Sig. (2-tailed)		.000
	N	31	31
q_B	Pearson Correlation	.884**	1
	Sig. (2-tailed)	.000	
	N	31	31

Table 10: Results of the correlation analysis concerning the tendency for cloud computing adoption (Microsoft experts' point of view)

Hypothesis H2 claims that organizational factors positively influence the tendency for cloud computing adoption. It assumes that the more important the organizational factors are perceived the higher the tendency for cloud computing adoption. As showed previously Microsoft experts evaluated organizational factors (questions 17-30) with an average importance of 4.6. Their response to the question "B" was averaged at 5.16. These numbers slightly differ from each other, but the correlation analysis showed a significant positive correlation of .884, which means a strong positive correlation between organizational factors and cloud adoption willingness. Based on that hypothesis H2 (the more important the organizational factors perceived, the higher the tendency for cloud computing adoption) is supported by the collected data.

- Cloud customers' point of view

Correlations

		q_17_30	q_B
q_17_30	Pearson Correlation	1	.737**
	Sig. (2-tailed)		.000
	N	43	43
q_B	Pearson Correlation	.737**	1
	Sig. (2-tailed)	.000	
	N	43	43

Table 11: Results of the correlation analysis concerning the tendency for cloud computing adoption (cloud customers' point of view)

Similarly, as above the hypothesis H2 has been tested with the help of the data collected from the questionnaires. This time I examined the answers filled in by the cloud customers. We already identified that cloud customers evaluated the importance of organizational factors with an average of 4.1, while they evaluated the general importance of the organizational factors (question "B") with an average respond of 4.16. Examining the individual respondents' average evaluation and their response to question "B" the statistical analysis shows a correlation of .737, which clearly shows that the more important cloud customers assume the organizational factors the higher the

tendency for cloud computing adoption is. Consequently, the hypothesis H2 is also supported by the data collected through the questionnaires filled in by cloud customers.

- Differences and similarities of the two groups

As shown above, both group results supported hypothesis H2. Both groups have a high positive correlation rate (.884 and .737). The questions for the Microsoft experts were designed similarly as for H1 to find out what the experts think about how the cloud customers perceive the different factors. Here I found a 1-point difference between the average responds. Microsoft experts feel that the organizational factors are more important for cloud adoption (5.16) than cloud customers think (4.16). This have to be concluded and Microsoft experts (and any other cloud solution suppliers) should think about solutions how they could make their present and future customers more aware about the positive organizational factors of cloud computing in order to make it more adopted.

Evaluation	**Statement**
4.7 and 4.9	H1 is supported by data in both groups. Security- and legislation-related issues negatively influence the tendency for cloud computing adoption.
6.9, 6.7 and 6.6 respectively	In Microsoft experts' opinion the biggest blockers for cloud adoption are the intransparency of data location, cloud incidents and the fear of moving data in the cloud and losing control over resources.
1.7, 1.9 and 2.0 respectively	Microsoft experts think that GDPR has the least negative effect on cloud adoption, followed by the EU's attempt to stimulate cloud adoption and the EU's legislation framework.
6.8 and 6.7,6.7 respectively	For cloud customers the biggest cloud adoption blockers are the same as for Microsoft experts, only in other sequence: cloud incidents, fear of moving data to cloud and intransparency of data location.
2.3, 2.5 and 2.6 respectively	Cloud customers evaluate that not all aspects of cloud computing are covered by regarding laws and standards and this is the biggest influencer why security considerations negatively influence cloud adoption. This is followed by GDPR regulation and the EU's attempt to stimulate cloud adoption and the EU's legislation framework.

4.6 and 4.1	H2 is supported by data in both groups. Organizational factors positively influence the tendency for cloud computing adoption.
6.8, 6.8 and 6.6 respectively	Microsoft experts think that a positive attitude toward cloud adoption and general knowledge are head to head the most important factor for higher cloud adoption tendency. The third most important economic factor in their opinion is having a cloud strategy.
2.3, 2.5 and 2.6 respectively	For Microsoft experts if a customer does not know the main economical differences between cloud and on-premise solutions than it is a factor that does not support cloud adoption. Furthermore, they said that technological readiness and the capability to predict the cloud-related costs are also needed for higher cloud adoption rate.
6.6, 6.3 and 6.3 respectively	Also, for the cloud customers, the general knowledge about cloud computing is a very important influencing factor for cloud adoption. Followed by the familiarity with the economic benefits of cloud computing and with the economic differences between cloud and on-premise solutions.
1.9, 2.0 and 2.3 respectively	For cloud customers if they are not sure if cloud solution would be more cost effective than on-premise solution than it would not support cloud adoption. Furthermore, cloud customers still do not think that cloud computing is a necessary technology for their organization to expand and they are not sure about their workforce's knowledge for cloud technology.

Table 12: Key learnings of the research

Discussion

The following part is designed to reflect on the results of the executed questionnaires. The objective is to link the results back to the literature and compare the perspectives between Microsoft's point of view and the customer's perspective in order to develop reasonable implications and discuss similarities and differences.

This paper investigates factors influencing the cloud adoption rate in Austria. 27 factors were derived from scientific literature dealing with the adoption of cloud computing. Throughout the literature I introduced the most important basics of cloud computing. The history and the reasons why and how cloud computing evolved was shortly discussed. After that, I explained more specific the technical details of cloud computing including the different deployment models,

layers and service models. The economics of cloud computing were also presented, so we got some insights about the benefits and limitations of cloud computing. In this part of my thesis, I introduced some of the economic factors I examined later and also showed some examples of cloud computing benefits and some challenges of cloud adoption. Statistics show that Europe is taking up cloud technology slower than the USA. As I conducted my research in Austria I thought it is important to give a big picture about the environment in which Austria should adopt and exploit cloud computing technologies. In the section about Europe, I discussed the latest statistics about cloud adoption and touched on among other topics, such as the biggest cloud service providers and how the EU is working on creating a more cloud welcoming environment or the GDPR.

In the security, privacy and trust part I introduced the most important factors regarding cloud adoption. As my hypothesis H1 shows not proper security attributes of a cloud provider clearly deteriorates the tendency for cloud computing adoption. Therefore, this section tries to give a common understanding of cloud security and trust considerations. This part gives the reader a big picture about the most important definitions regarding cloud security, introduces the most common security threats and also shows general solutions to these. Finally, as organizations face more and more security challenges, security breaches happen also more often, therefore I examined some of the biggest cloud incidents happened until nowadays.

The paragraph about Microsoft shortly introduces the company's history, main activities, offerings, and its strategy. It gives us a sense how cloud providers function in general and it explains the paradigm shift at Microsoft and why its mobile-first, cloud-first strategy is very important in order to continue enhancing and accelerating cloud adoption.

The research part of my thesis introduced the two hypotheses that were developed based on the factors identified throughout the literature review:

- H1: Security- and legislation-related issues negatively influence the tendency for cloud computing adoption.
- H2: Organizational factors positively influence the tendency for cloud computing adoption.

A quantitate survey was conducted to reveal insights from a group of Microsoft co-workers and from a group of Austrian cloud customers. The factors have been used to investigate the two hypotheses I designed. The first 15 factors investigate Hypothesis H1 and 12 factors investigate Hypothesis H2.

Both hypotheses were tested from Microsoft experts' point of view and from the cloud customer's point of view. This gave us important insights about the similarities and differences how cloud suppliers and customers perceive the different cloud adoption factors. The main similarities and

differences were examined in the “Research results” paragraph and the key findings can be found summarized in Table 12 also in the previous section.

As the results suggest that not all factors are equally important for the two groups. But in general, we can say that both groups are on the same page and evaluated security issues as a negative influence on cloud adoption, while on the other hand there are less economic barriers for cloud adoption, but more positively influencing economic factors. It is evident for both groups that the cloud enables scalability, cost-reduction, and flexibility. However, the precise potential of cost-reductions and other economic benefits for existing and potential customers seem to be communicated insufficiently. Therefore, my implication would be to provide more transparency on the cloud providers’ side by communicating the potential benefits more efficiently and build interest on the customers’ side.

In my opinion, my thesis showed clearly that there is a significant number of challenges remaining in cloud computing adoption. The main factors have been discussed and most of them have been proven as important ones regarding the tendency to cloud computing. Based on the results, I believe that from the cloud providers’ point of view they would be more successful by thinking of their end customers and how their needs will be met, rather than just developing cloud applications that are useful in their opinion, but not necessarily serve the customers’ interest. Migration of the existing customer applications need organizational- specific knowledge, therefore cloud providers should strive to create technologies that enhance adopting cloud-based solutions for customer needs and promote interoperability among different applications and services. That would lead to a greater level of confidence in cloud adoption and a greater level of trust in its security as well.

I think Microsoft does a great work in differentiating the various sizes of the customer organizations. I recognized during conducting my research that focusing on the organization size could have helped to recognize size-specific influencing factors.

Regarding the security issues, which are big concerns not only for the potential cloud customers but also for the existing customer base I believe that building a broad customer base would help allay fears again cloud adoption and would help build even more experience in cloud solutions and improve their security practices for the providers. Therefore, I think it is important to not solely focus on large organizations but reaching out to small and medium-sized organizations could help diminish the cloud adoption challenges. I think the psychological reasons could play a big role in Austria’s slow cloud adoption rate. To some degree, I examined psychological reasons (questions 29 and 30) by asking about the influence of negative attitude toward cloud computing and about the approach toward cloud computing and its importance for the future, but it would be a potential research topic in cloud adoption topic. We can say that in Austria there is a relatively conservative attitude toward these types of changes, this is supported by the 4.7

average evaluation of question 29 from the cloud experts. In general, the stricter hierarchical approach in Austria's businesses is also not beneficial for introducing new technologies. Whereas the Scandinavian countries are well known for their open culture in business and prosperous start-up scene which leads to a much higher rate of cloud adoption. Another important step in the future is to manage the expectations for cloud technologies. SLAs, standards, compliance, and regulations could be useful with that.

The Austrian market will definitely experience a growth in cloud adoptions over time. In my opinion, as these technologies will be more and more broadly applied the Austrian organizations will have more confidence in introducing them. As the solutions will emerge to the discussed issues and as the discussed positive factors get more highlight for the customers the more courage the Austrian market will have. Therefore, I would like to emphasize the role of cloud solution providers like Microsoft as their duty is to make cloud solutions more reachable and accepted in the countries they are present. But not forgetting about the uniqueness of every country and every organization they are working with.

Limitations

Throughout writing my research I explored the complexity of the topic cloud computing and its adoption. We can differentiate a broad range of topics that can be researched, such as cloud computing economics, security issues, technology, and implementation or regulatory issues. Of course, these topics are not individual units, but all have overlapping when we examine cloud computing. I think that among all these research topics two are fundamental: the economics of cloud computing and security issues of cloud computing. Although I tried to include many factors that I considered important for my research, it was maybe to some degree too broad.

My research paper had two directions. One examined the point of view of Microsoft cloud experts, while the other one considered the opinions of existing cloud customers. First of all this separation led to a too broad focus again, secondly, in the customer base, the opinion of the potential future customers is missing, as I tried to avoid not proper responds from survey respondents that may not be enough experienced with cloud technologies.

Another limitation of my research is that I did not group the cloud experts based on the segment they are working in. Because it is clear that an IT professional working with commercial enterprises are facing other cloud adoption issues than an IT professional working with public organizations. This would also apply to the customers. In their opinion, the industry they are operating would also be an important influencing factor, although my data did not suggest it. Also, the size of the organization could be an important factor. As a customer in a large organization may consider cloud technologies not the same as a customer in a small organization. The same applies to customers in the public sector and customers in the enterprise segment.

As I did not specify which applications or cloud solutions I am referring to when conducting my research it led also to a too broad meaning of cloud computing. Therefore, narrowing the applications or services we examine would be also potential future research direction.

References

- Armbrust et al. (2010), *A view of Cloud Computing*, Communications of the ACM, Vol. 53 No. 4, pp. 50-58.
- Armerding, T. (2018), *The 17 biggest data breaches of the 21st century*, IDG Communications, viewed 21 July 2018 <https://www.csoonline.com/article/2130877/data-breach/the-biggest-data-breaches-of-the-21st-century.html>.
- Avram, M.G. (2014), *Advantages and Challenges of Adopting Cloud Computing from an Enterprise Perspective*, Procedia Technology, Procedia Technology, Volume 12, pp. 529-534
- aws.com (2006), *Announcing Amazon Elastic Compute Cloud (Amazon EC2) – beta*, viewed 4 May 2018, <https://aws.amazon.com/about-aws/whats-new/2006/08/24/announcing-amazon-elastic-compute-cloud-amazon-ec2---beta/>
- Bernhard, T. (2018), *One Month with GDPR. How Can the Channel Help?*, CloudCheckr, viewed 12 August 2018 < https://cloudcheckr.com/2018/06/channel-help-gdpr/>.
- Bradford, C. (2018), *7 Most Infamous Cloud Security Breaches*, viewed 3 August 2018 <https://blog.storagecraft.com/7-infamous-cloud-security-breaches/>.
- Branscombe, M. (2018), *How Microsoft is Keeping Its Cloud More Efficient Than Your Data Center*, Information USA, Inc., viewed 3 June 2018 < https://www.datacenterknowledge.com/microsoft/how-microsoft-keeping-its-cloud-more-efficient-your-data-center>.
- Boniface, M., Nasser, B., Papay, J., Phillips, S.C., Servin, A., Yang, X., Zlatev, Z., Gogouvitis, S., Katsaros, G., Konstanteli, K., Kousiouris, G., Menychtas, A., Kyrizais, D. (2010), *Platform-as-a-Service Architecture for Real-time Quality of Service Management in Clouds*, 2010 Fifth International Conference on Internet and Web Applications and Services.
- Botta, A., de Donato, W., Persico, V., Pescape, A. (2016), *Integration of Cloud computing and Internet of Things: A survey*, Future Generation Computer Systems, Volume 56, pp. 684-700.
- Cheung, A.S.Y., Weber, R.H. (2015), *Privacy and Legal Issues in Cloud Computing*, Edward Elgar Publishing Ltd., ISBN 9781783477067.

- Computer History Museum (n.d.), *Internet History of 1970s*, CHM, viewed 9 April 2018, <http://www.computerhistory.org/internethistory/1970s/>
- CSA, (2012), *SecaaS Category 1 Identity and Access Management Implementation Guidance,* Secaas Implementation Guidance, September Issue, pp.1–43
- derstandard.at (2017), *Österreichs Unternehmen bei Cloud Computing im unteren Drittel der EU*, viewed 15 May 2018 < https://derstandard.at/2000055127006/Oesterreichs-Unternehmen-bei-Cloud-Computing-im-unteren-Drittel-der-EU>.
- European Commission (n.d.), *Digital Single Market,* viewed 2 July 2018, < https://ec.europa.eu/digital-single-market/>.
- Eurostat (2016), *Cloud computing - statistics on the use by enterprises*, European Union, viewed 12 March 2018, < https://ec.europa.eu/eurostat/statistics-explained/index.php/Cloud_computing_-_statistics_on_the_use_by_enterprises>
- Evans, B (2018a), *Microsoft Tops Amazon In Q1 Cloud Revenue, $6.0 Billion To $5.44 Billion; IBM Third At $4.2 Billion*, Forbes Media LLC, viewed 13 March 2018, https://www.forbes.com/consent/?toURL=https://www.forbes.com/sites/bobevans1/2018/04/27/microsoft-tops-amazon-in-q1-cloud-revenue-6-0-billion-to-5-44-billion-ibm-third-at-4-2-billion/#40c9728c5d4b.
- Evans, B (2018b), *Top Cloud Vendors Will Crush $100 Billion In 2018 Revenue; Microsoft, Amazon, IBM Hit $75 Billion*?, Forbes Media LLC, viewed 20 February 2018, <https://www.forbes.com/sites/bobevans1/2018/05/21/top-cloud-vendors-will-crush-100-billion-in-2018-revenue-microsoft-amazon-ibm-hit-75-billion/#b4a37697548c>
- Faynberg, I., Lu, H.-L., Skuler, D. (2016), *Cloud Computing: Business Trends and Technologies*, Wiley, ISBN 9781118501214.
- Gibson, S. (2015), *ISO 27018 compliance: Here's what you need to know*, IDG Communications, viewed 21 July 2018 < https://www.infoworld.com/article/3000021/cloud-computing/iso-27018-compliance-heres-what-you-need-to-know.html>.
- Guo, T., Sharma, U., Shenoy, P., Wood, T., Sahu, S. (2014), C*ost-Aware Cloud Bursting for Enterprise* Applications, ACM Transactions on Internet Technology, Volume 13, No. 3, Article 10.
- Hackett, R. (2016), *LinkedIn Lost 167 Million Account Credentials in Data Breach*, Time Inc, viewed 8 August 2018 < http://fortune.com/2016/05/18/linkedin-data-breach-email-password/>.

- Harfoushi, O., Akhorsaideh, A., Aqqad, N., Janini, M.A., Obiedat, R. (2016), *Factors Affecting the Intention of Adopting Cloud Computing in Jordanian Hospitals*, Communications and Network, 2016, Volume 8., pp. 88-101.
- Hauger D. (2010), *Windows Azure General Availability*, viewed 4 May 2018 < https://*blogs*.technet.microsoft.com/microsoft_blog/2010/02/01/windows-azure-general-availability/>
- industriemagazin.at (2017), *Telekom Austria gründet neue Tochterfirma für Cloud-Dienste*, WEKA Industrie Medien GmbH, viewed 22 May 2018 < https://industriemagazin.at/a/telekom-austria-gruendet-neue-tochterfirma-fuer-cloud-dienste>.
- Jeffery, K., Neidecker-Lutz, B. (2010), *The Future of Cloud Computing: Opportunities for European Cloud Computing Beyond 2010*, European Commission.
- Khalil, I.M., Khreishah, A., Azeem, M. (2014), *Cloud Computing Security: A Survey*, Computers, Vol. 3, pp. 1-35
- Khan, K., Malluhi, Q. (2010), *Establishing Trust in Cloud Computing*, IEEE, IT Professional, Vol. 12 Issue 5., pp. 20-27.
- Khan, K., Malluhi, Q. (2013), *Trust in Cloud Services: Providing More Controls to Clients*, IEEE, IEEE Computer Society Vol. 46, Issue 7., pp. 94-96.
- Loshin, P. (2017), *AWS promises to be GDPR compliant by May 2018 deadline*, Techtarget, viewed 28 July 2018 <https://searchsecurity.techtarget.com/news/450417704/AWS-promises-to-be-GDPR-compliant-by-May-2018-deadline>.
- Lynch, B. (2017), *Get GDPR compliant with the Microsoft Cloud*, Microsoft, viewed 14 June 2018 <https://blogs.microsoft.com/on-the-issues/2017/02/15/get-gdpr-compliant-with-the-microsoft-cloud/>.
- Marston, S., Li, Z., Bandyopadhyay, S., Zhang, J., Ghalsasi, A. (2011), *Cloud computing - The business perspective*, Decision Support Systems, Volume 51, Issue 1, pp. 176-189.
- McDonald, P. (2008), *Introducing Google App Engine*, viewed 4 May 2018 < http://googleappengine.blogspot.com/2008/04/introducing-google-app-engine-our-new.html>
- Mell, P., Grance, T. (2011), *The NIST Definition of Cloud Computing Recommendations of the National Institute of Standards and Technology*, National Institute of Standards and Technology, NIST Special Publication 800-145.
- Microsoft (2017), *Annual Report 2017*, viewed 6 June 2018 https://www.microsoft.com/investor/reports/ar17/index.html.
- Microsoft Office (2018), viewed 10 June 2018 < https://products.office.com/en-us/microsoft-office-for-home-and-school-faq>.

- microsoft.com (n.d.), *Microsoft and ISO/IEC 27018*, viewed 20 July 2018 <https://www.microsoft.com/en-us/trustcenter/Compliance/ISO-IEC-27018>
- Mishra, A., Mathur, R., Jain, S., Rathore, J.S. (2013), *Cloud Computing Security*, International Journal on Recent and Innovation Trends in Computing and Communication, Volume 1, Issue 1, pp. 36-39.
- Moore, S., van der Meulen, R. (2018), *Gartner Forecasts Worldwide Public Cloud Revenue to Grow 21.4 Percent in 2018*, Gartner Inc., viewed 27 February 2018, <https://www.gartner.com/newsroom/id/3871416>
- Moyle, E. (2018), *Cloud security lessons to learn from the Uber data breach*, TechTarget, viewed 10 August 2018 <https://searchcloudsecurity.techtarget.com/tip/Cloud-security-lessons-to-learn-from-the-Uber-data-breach>
- Murugesan, S., Bojonova, I. (2016), *Encyclopedia of Cloud Computing*, John Wiley & Sons, Ltd, ISBN 9781118821954.
- Nadella, S. (2017), *Hit Refresh: The Quest to Rediscover Microsoft's Soul and Imagine a Better Future for Everyone*, Harper Business, ISBN 9780062652515.
- Oliveira, T., Thomas, M., Espadanal, M. (2014), *Assessing the determinants of cloud computing adoption: An analysis of the manufacturing and services sectors*, Information & Management Vol. 51, Issue 5, pp. 497-510.
- Ramachandra, G., Iftikhar, M., Khan, F.A. (2017), *A Comprehensive Survey on Security in Cloud Computing*, Elsevier B.V., Procedia Computer Science Vol. 110, pp. 465–472.
- Raza, M., Adenola, A.F., Nafarieh, A., Robertson, W. (2015*), The Slow Adoption of Cloud Computing and IT Workforce*, Elsevier B.V., Procedia Computer Science, Vol. 52, pp. 1114 – 1119
- Panetta, K. (2017), *Cloud Computing Enters its Second Decade*, Gartner Inc., viewed 29 March 2018 <https://www.gartner.com/smarterwithgartner/cloud-computing-enters-its-second-decade/>.
- Smith, D., Leong, L., Bala, R. (2018), *Magic Quadrant for Cloud Infrastructure as a Service, Worldwide*, Gartner Inc. , viewed 10 June 2018 <https://www.gartner.com/doc/reprints?id=1-50WJ5CK&ct=180525&st=sb>.
- Sosinsky B. (2011), *Cloud Computing Bible*, Wiley Publishing, Inc., ISBN 9780470903568
- Statistics How To (n.d), *Correlation in Statistics: Correlation Analysis Explained*, viewed 20 August 2018 <https://www.statisticshowto.datasciencecentral.com/probability-and-statistics/correlation-analysis/>.

- SurveyMonkey (n.d.), *What is a Likert scale?*, viewed 15 August 2018 <https://www.surveymonkey.com/mp/likert-scale/>.
- Tolsma, A., (2018), *GDPR and the impact on cloud computing: The effect on agreements between enterprises and cloud service providers*, Deloitte, viewed 4 August 2018 <https://www2.deloitte.com/nl/nl/pages/risk/articles/gdpr-update-the-impact-on-cloud-computing.html>.
- trend.at (2014), *So nutzen Österreichs Unternehmen Cloud Computing*, viewed 20 May 2018 https://www.trend.at/technik/oesterreich-unternehmen-cloud-computing-5165689.
- Tripathi, A., Mishra, A. (2011), *Cloud computing security considerations*, IEEE, IEEE International Conference on Signal Processing, Communications and Computing (ICSPCC).
- Vlajin, B. (2018), *What You Need To Know About Cloud Laws and Regulations*, Cloudwards.net, viewed 15 July 2018 < https://www.cloudwards.net/what-you-need-to-know-about-cloud-laws-regulations/>.
- Wauters, P., Van Der Peijl, S., Cilli, V., Bolchi, M., Janowski, P., Moeremans, M., Graux, H., Taylor, G., Cocoru, D. (2014), *Measuring the economic impact of cloud computing in Europe*, European Commission, ISBN 9789279635700
- Weinman, J. (2012), *Cloudonomics: The Business Value of Cloud Computing*, John Wiley & Sons, Inc., ISBN 9781118229965.
- Weiss, O. (2018), *Österreichs Unternehmer haben größtes Vertrauen in heimische Cloud-Anbieter*, Computerwelt.at, viewed 22 May 2018 < https://computerwelt.at/news/topmeldung/oesterreichs-unternehmer-haben-groesstes-vertrauen-in-heimische-cloud-anbieter/?cn-reloaded=1>.
- Why Is Europe Slower to Embrace the Cloud? Roadblocks to Wider Cloud Adoption (2017), CloudCheckr, viewed 10 June 2018 < https://cloudcheckr.com/2017/11/why-is-europe-slower-to-embrace-the-cloud-roadblocks-to-wider-cloud-adoption/>.
- Winkler, V. (2012), *Cloud Computing: Legal and Regulatory Issues*, viewed 14 July 2018 < https://technet.microsoft.com/en-us/library/hh994647.aspx>.
- Yang, J., Chen, Z. (2010), *Cloud Computing Research and Security Issues*, IEEE, 2010 International Conference on Computational Intelligence and Software Engineering.
- Zhang, Q., Cheng, L., Boutaba, R. 2010, *Cloud computing: state-of-the-art and research challenges*, Journal of Internet Services and Applications, Volume 1, Issue 1, pp. 7–18.
- Zissis, D., Lekkas, D. (2012), *Addressing cloud computing security issues*, Elsevier B.V., Future Generation Computer Systems, Vol. 28, Issue 3, pp. 583-592.

List of figures and tables

Taylor, G., Cocoru, D. (2014), *Measuring the economic impact of cloud computing in Europe,* European Commission, ISBN 9789279635700.

Appendix

Questionnaire

Cloud Computing Adoption – Microsoft`s point of view

Do you think that security- and legislation-related issues negatively influence the current and potential future customers' tendency for cloud computing adoption? (choose on the scale from 1 to 7, with 1 indicating not at all and 7 indicating completely true)

1 2 3 4 5 6 7

Do you think that organizational factors positively influence the current and potential future customers' willingness for cloud computing adoption? (choose on the scale from 1 to 7, with 1 indicating not at all and 7 indicating completely true)

1 2 3 4 5 6 7

1. Do you think that customers are concerned about losing control over resources (data, processes, human resources) when using cloud computing solutions and this negatively influence their tendency to adopt cloud solutions? (choose on the scale from 1 to 7, with 1 indicating not at all and 7 indicating completely true)

   1 2 3 4 5 6 7
2. Do you think that customers are hesitant when moving their sensitive data to cloud? (choose on the scale from 1 to 7, with 1 indicating not at all and 7 indicating completely true)

   1 2 3 4 5 6 7
3. Do you think that customers consider on-premise solutions more secure than cloud solutions, hence you would stay with your traditional IT solutions? (choose on the scale from 1 to 7, with 1 indicating not at all and 7 indicating completely true)
4. Do you think that customers are uncertain about who owns the data in the cloud and that makes them uncertain to move in the cloud? (choose on the scale from 1 to 7, with 1 indicating not at all and 7 indicating completely true)

   1 2 3 4 5 6 7

5. Do you think that customers feel uncertainty about the transparency of data location in cloud computing and this negatively influence their tendency for cloud computing? (choose on the scale from 1 to 7, with 1 indicating not at all and 7 indicating completely true)

   1 2 3 4 5 6 7

6. Do you think that majority of cloud solution providers lack strong, detailed data protection legislation? (choose on the scale from 1 to 7, with 1 indicating not at all and 7 indicating completely true)

   1 2 3 4 5 6 7

7. Do you think that cloud solution providers do not promote enough of existing relevant certifications and standards to gain trust in cloud computing? (choose on the scale from 1 to 7, with 1 indicating not at all and 7 indicating completely true)

   1 2 3 4 5 6 7

8. Do you think that GDPR regulation does not help gain trust in cloud computing data protection? (choose on the scale from 1 to 7, with 1 indicating not at all and 7 indicating completely true)

   1 2 3 4 5 6 7

9. Do you consider it difficult to have an overview of all cloud computing related laws and standards for cloud customers? (choose on the scale from 1 to 7, with 1 indicating not at all and 7 indicating completely true)

   1 2 3 4 5 6 7

10. Do you think that not all aspects of cloud computing are covered by laws and standards and this negatively influences cloud adoption? (choose on the scale from 1 to 7, with 1 indicating not at all and 7 indicating completely true)

    1 2 3 4 5 6 7

11. Do you think that service level agreements (SLA) do not provide enough trust in cloud computing security from the cloud customers' point of view? (choose on the scale from 1 to 7, with 1 indicating not at all and 7 indicating completely true)

    1 2 3 4 5 6 7

12. Do you think that customers are mistrustful about their cloud provider's data encryption policies and practices? (choose on the scale from 1 to 7, with 1 indicating not at all and 7 indicating completely true)

    1 2 3 4 5 6 7

13. Do you think that the security standards of the cloud solution providers are not always relevant in comparison with the security the customers are looking for?

(choose on the scale from 1 to 7, with 1 indicating not at all and 7 indicating completely true)

1 2 3 4 5 6 7

14. Do you think that the different cloud incidents are a big concern for cloud users when using cloud computing solutions?

    1 2 3 4 5 6 7

15. Do you think that the European Union's attempt to stimulate cloud adoption is proper enough?

    1 2 3 4 5 6 7

16. Do you think that the legislation framework for cloud computing security provided by the European Union is proper enough?

    1 2 3 4 5 6 7

17. Do you think that the majority of cloud customers are clear about the general economic benefits of cloud computing? (choose on the scale from 1 to 7, with 1 indicating not at all and 7 indicating completely true)

    1 2 3 4 5 6 7

18. Do you think that the customers are mostly aware that also their organization could benefit from adopting cloud computing solutions and this positively influence their cloud usage decision? (choose on the scale from 1 to 7, with 1 indicating not at all and 7 indicating completely true)

    1 2 3 4 5 6 7

19. Do you think that cloud customers would perceive that cloud computing offerings in general are flexible enough to different organizations' unique needs?

    1 2 3 4 5 6 7

20. Do you think that customers are confident that transitioning to cloud would not disturb their current IT and business operations? (choose on the scale from 1 to 7, with 1 indicating not at all and 7 indicating completely true)

    1 2 3 4 5 6 7

21. Do you think that positive attitude toward changes helps to exploit the benefits of new technologies like cloud computing? (choose on the scale from 1 to 7, with 1 indicating not at all and 7 indicating completely true)

    1 2 3 4 5 6 7

22. Do you think that the fear of cloud adoption concerns is greater than the potential benefits of it – from customers' point of view? (choose on the scale from 1 to 7, with 1 indicating not at all and 7 indicating completely true)

    1 2 3 4 5 6 7

23. Do you think that cloud using organizations are certain that their workforce possesses the required skills and knowledge to exploit the benefits of cloud computing and if yes than it positively influence cloud adoption tendency? (choose on the scale from 1 to 7, with 1 indicating not at all and 7 indicating completely true)

    1 2 3 4 5 6 7

24. Do you think that knowledge about cloud computing is positively associated with the tendency for cloud computing adoption? (choose on the scale from 1 to 7, with 1 indicating not at all and 7 indicating completely true)

    1 2 3 4 5 6 7

25. Are customers mostly aware of the difference between cloud and on-premise solutions from an economical point of view? (choose on the scale from 1 to 7, with 1 indicating not at all and 7 indicating completely true)

    1 2 3 4 5 6 7

26. Do the customers think that the costs of using cloud computing are always lower than that of on-premise? (choose on the scale from 1 to 7, with 1 indicating not at all and 7 indicating completely true)

    1 2 3 4 5 6 7

27. Do you think that customers can always easily identify and predict the cloud computing related costs? (choose on the scale from 1 to 7, with 1 indicating not at all and 7 indicating completely true)

    1 2 3 4 5 6 7

28. Do you think that having a cloud strategy positively influences the cloud adoption rate? (choose on the scale from 1 to 7, with 1 indicating not at all and 7 indicating completely true)

    1 2 3 4 5 6 7

29. Do you think that the majority of potential customers have a negative attitude on organizational level toward adoption of cloud computing solutions?

    1 2 3 4 5 6 7

30. Do you think that customers have the opinion about cloud computing that it is a necessary technology to expand their organization? If yes, then it would increase your tendency for adopting cloud solutions.

    1 2 3 4 5 6 7

Questionnaire

Cloud Computing Adoption – Customers' point of view (used with kwiksurveys.com)

Do you use cloud computing for your daily work? (yes/no)

How would you evaluate your knowledge about cloud computing solutions? (choose on the scale from 1 to 7, with 1 indicating not at all and 7 indicating completely true)

Do you think that security- and legislation-related issues negatively influence your willingness for cloud computing adoption? (choose on the scale from 1 to 7, with 1 indicating not at all and 7 indicating completely true)

Do you think that organizational factors positively influence your willingness for cloud computing adoption? (choose on the scale from 1 to 7, with 1 indicating not at all and 7 indicating completely true)

1. Are you concerned about losing control over resources (data, processes, human resources) when using cloud computing solutions? If not, it would positively influence your cloud adoption/usage decision. (choose on the scale from 1 to 7, with 1 indicating not at all and 7 indicating completely true)
2. Are you hesitant when moving your sensitive data to cloud? (choose on the scale from 1 to 7, with 1 indicating not at all and 7 indicating completely true)
3. Do you consider on-premise solutions more secure than cloud solutions? (choose on the scale from 1 to 7, with 1 indicating not at all and 7 indicating completely true)
4. Are you uncertain about who owns the data in the cloud? (choose on the scale from 1 to 7, with 1 indicating not at all and 7 indicating completely true)
5. Do you feel uncertainty about the transparency of data location in cloud computing? (choose on the scale from 1 to 7, with 1 indicating not at all and 7 indicating completely true)
6. Do you think that majority of cloud solution providers lack strong, detailed data protection legislation? (choose on the scale from 1 to 7, with 1 indicating not at all and 7 indicating completely true)
7. Do you think that cloud solution providers do not promote enough of existing relevant certifications and standards to gain trust in cloud computing? (choose on the scale from 1 to 7, with 1 indicating not at all and 7 indicating completely true)

8. Do you think that GDPR regulation does not help gain trust in cloud computing data protection? (choose on the scale from 1 to 7, with 1 indicating not at all and 7 indicating completely true)
9. Do you consider it difficult to have an overview of all cloud computing related laws and standards? (choose on the scale from 1 to 7, with 1 indicating not at all and 7 indicating completely true)
10. Do you think that not all aspects of cloud computing are covered by laws and standards and this negatively influences cloud adoption? (choose on the scale from 1 to 7, with 1 indicating not at all and 7 indicating completely true)
11. Do you think that service level agreements (SLA) provide enough security in cloud computing? If yes, than it would increase your tendency to adopt/use cloud solutions. (choose on the scale from 1 to 7, with 1 indicating not at all and 7 indicating completely true)
12. Are you mistrustful about your cloud provider's data encryption policies and practices? If no, then it would increase your tendency to adopt/use cloud solutions.
    (choose on the scale from 1 to 7, with 1 indicating not at all and 7 indicating completely true)
13. Do you think that the security standards of your cloud provider are not always relevant in comparison with the security you are looking for and this decreases your tendency to adopt cloud solutions? (choose on the scale from 1 to 7, with 1 indicating not at all and 7 indicating completely true)
14. Do the different cloud incidents concern you when using cloud computing solutions?
15. Do you think that the European Union's attempt to stimulate cloud adoption is proper enough?
16. Do you think that the legislation framework for cloud computing security provided by the European Union is proper enough?
17. Are you clear about the general economic benefits of cloud computing? (choose on the scale from 1 to 7, with 1 indicating not at all and 7 indicating completely true)
18. Do you think that also your organization could benefit from adopting cloud computing solutions? (choose on the scale from 1 to 7, with 1 indicating not at all and 7 indicating completely true)
19. Do you think that cloud computing offerings in general are flexible enough to your organization's unique needs?

20. Are you confident that transitioning to cloud would not disturb your current IT and business operations? (choose on the scale from 1 to 7, with 1 indicating not at all and 7 indicating completely true)
21. Do you think that positive attitude on organizational level toward changes could help to exploit the benefits of new technologies like cloud computing? (choose on the scale from 1 to 7, with 1 indicating not at all and 7 indicating completely true)
22. Do you think that the fear of cloud adoption concerns is greater than the potential benefits of it? (choose on the scale from 1 to 7, with 1 indicating not at all and 7 indicating completely true)
23. Are you certain that the workforce of your organization possesses the required skills and knowledge to exploit the benefits of cloud computing? If yes than it positively influences your tendency for cloud adoption. (choose on the scale from 1 to 7, with 1 indicating not at all and 7 indicating completely true)
24. Do you think that knowledge about cloud computing is positively associated with the tendency for cloud computing adoption? (choose on the scale from 1 to 7, with 1 indicating not at all and 7 indicating completely true)
25. Are you aware of the difference between cloud and on-premise solutions from an economical point of view? (choose on the scale from 1 to 7, with 1 indicating not at all and 7 indicating completely true)
26. Are you sure that the costs of using cloud computing are always lower than that of on-premise? If not than it would negatively influence your tendency for cloud adoption? (choose on the scale from 1 to 7, with 1 indicating not at all and 7 indicating completely true)
27. Can you always easily identify and predict the cloud computing related costs? (choose on the scale from 1 to 7, with 1 indicating not at all and 7 indicating completely true)
28. Do you think that an organization-wide cloud strategy would positively influence cloud adoption and usage? (choose on the scale from 1 to 7, with 1 indicating not at all and 7 indicating completely true)
29. Do you feel a negative attitude in your organization toward adoption cloud computing solutions?
30. Do you think that cloud computing is a necessary technology to expand your organization? If yes, then it would increase your tendency for adopting cloud solutions.

Abstrakt

Cloud-Lösungen haben das Potenzial, unsere Wirtschaftsleben durch die Optimierung der Geschäftsprozesse von Unternehmen zu revolutionieren. Aber die Attitude zur Cloud-Transformation in Österreich ist immer noch konservativ und liegt immer noch hinter anderen europäischen Ländern. Der Wechsel von On-Premise- zu Cloud-basierten Lösungen steht vor wirtschaftlichen, technischen und psychologischen Barrieren. In dieser Arbeit werden die Einflussfaktoren der Cloud-Computing-Einführung in Österreich untersucht und vorgestellt, indem Cloud-Experten von Microsoft Österreich und bestehende Cloud-Kunden befragt werden. Die Ergebnisse dieser beiden Gruppen deuten darauf hin, dass Cloud-Anbieter und ihre Kunden erhebliche Meinungsunterschiede hinsichtlich der Cloud-Akzeptanzfaktoren haben. Daher bietet diese Arbeit Einblicke in den österreichischen Cloud-Markt, die Cloud-Anbieter nutzen können, um die Hauptprobleme zu identifizieren und anzugehen, die aktuelle und potentielle zukünftige Kunden dazu bewegen, Cloud-Computing-Lösungen zu übernehmen.