UNIVERSITY OF LJUBLJANA
SCHOOL OF ECONOMICS AND BUSINESS

MASTER'S THESIS

TITLE

TO CLOUD OR NOT TO CLOUD: SECURITY ISSUES AND THREATS OF CLOUD COMPUTING

Ljubljana, April 2021 IVANA DIMITROVSKA

AUTHORSHIP STATEMENT

The undersigned Ivana Dimitrovska, a student at the University of Ljubljana, School of Economics and Business, (hereafter: SEB LU), author of this written final work of studies with the title "To cloud or not to cloud: Security Issues and Threats of Cloud Computing", prepared under supervision of Mojca Indihar Štemberger, PhD and co-supervision of ____

DECLARE

1. this written final work of studies to be based on the results of my own research;

2. the printed form of this written final work of studies to be identical to its electronic form;

3. the text of this written final work of studies to be language-edited and technically in adherence with the SEB LU's Technical Guidelines for Written Works, which means that I cited and / or quoted works and opinions of other authors in this written final work of studies in accordance with the SEB LU's Technical Guidelines for Written Works;

4. to be aware of the fact that plagiarism (in written or graphical form) is a criminal offence and can be prosecuted in accordance with the Criminal Code of the Republic of Slovenia;

5. to be aware of the consequences a proven plagiarism charge based on the this written final work could have for my status at the SEB LU in accordance with the relevant SEB LU Rules;

6. to have obtained all the necessary permits to use the data and works of other authors which are (in written or graphical form) referred to in this written final work of studies and to have clearly marked them;

7. to have acted in accordance with ethical principles during the preparation of this written final work of studies and to have, where necessary, obtained permission of the Ethics Committee;

8. my consent to use the electronic form of this written final work of studies for the detection of content similarity with other written works, using similarity detection software that is connected with the SEB LU Study Information System;

9. to transfer to the University of Ljubljana free of charge, non-exclusively, geographically and time-wise unlimited the right of saving this written final work of studies in the electronic form, the right of its reproduction, as well as the right of making this written final work of studies available to the public on the World Wide Web via the Repository of the University of Ljubljana;

10. my consent to publication of my personal data that are included in this written final work of studies and in this declaration, when this written final work of studies is published.

Ljubljana, May 15th, 2021 Author's signature: Ivana Dimitrovska

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF APPENDICES

LIST OF ABBREVIATIONS

sl. – Slovene

CC – (sl. Računalništvo v oblaku); Cloud Computing

CIA triad – (sl. CIA triada); Confidentiality, Integrity and Availability triad

I.D.C. – (sl. Mednarodna Podatkovna Korporacija); International Data Corporation

NIST – (sl. Nacionalni Inštitut za Standarde in Tehnologijo); National Institute of Standards and Technology

NAS – (sl. Omrežna shramba); Network Attached Storage hardware

ARPANet – (sl. Mreža Agencij za Napredne Raziskovalne Projekte); Advanced Research Projects Agency Network

IT – (sl. Informacijska Tehnologija); Information Technology

IaaS – (sl. Infrastruktura kot Storitev); Infrastructure as a Service

PaaS – (sl. Platforma kot Storitev); Platform as a Service

SaaS – (sl. Software kot Storitev); Software as a Service

ISACA – (sl. ISACA Slovenija); Information Systems Audit and Control Association

DoS – (sl. Zavrnitev Storitve); Denial of Service

CSA – (sl. Aliansa o Varnost v Računalniškega Oblaka); Cloud Security Alliance

OS – (sl. Operacijski Sistem); Operating System

API – (sl. Vmesnik za programiranje aplikacij); Application Programming Interface

UI – (sl. Uporabniški Vmesnik); User Interface

CRM – (sl. Upravljanje Odnosov s Strankami); Customer Relationship Management

PMI – (sl. Philip Morris International); Philip Morris International

FMCG – (sl. Blago za Hitro Porabo); Fast-Moving Consumer Goods

B2B – (sl. Poslovanje/trgovanje Med Podjetji); Business to Business

DOOEL – (sl. Družba z Omejeno Odgovornostjo); Company with limited liability

R&D – (sl. Raziskave in Razvoj); Research and Development

2FA – (sl. Dvofaktorski Avtentifikator); Two-Factor authenticator

INTRODUCTION

Cloud computing – CC, is a relatively new technology that is still developing and is rather indefinable and vague to individuals outside the IT industry. The best way to describe the model of Cloud computing is the process of instantiating clusters of on-demand, scalable and modifiable computing resources that can be accessed online by a client with little to no effort. (Bhuvaneshkumar, Anitha, Kalarani, & Gunasundari, 2014). Currently, the cloud computing's popularity is greater than ever before, however, concerns are being expressed about the security issues connected to its adoption (Mijuskovic & Ferati, 2019).

This thesis attempts to demystify and explore the unique security difficulties present in the cloud computing environment. Trust is vital for users to feel safe while storing their data on the cloud. Commonly, security is associated to the aspects of confidentiality, integrity and availability - CIA. Thus, they came to be the foundation for designing a secure system for potential users – the CIA triad (Srinivasan, 2013). Throughout the thesis, the focus falls on various types of security and privacy issues concerning cloud computing users according to the CIA triad.

The point of departure of this thesis is to identify the common security challenges for adopting cloud computing, and on the other hand the possible solutions adopted in order to see if users are aware of their existence. Based on the identified research gap that the existing CC researches all are focused on CC implementation in business, I am writing this thesis trying to include the individuals' point of view and experience with security threats. The overarching research question addressed in the present thesis is: Are cloud computing users (business users and individual users) aware of the security issues and threats and whether they take preventive methods/actions?

Motivated by the security problems cloud users are facing, the research aim is to:

- To identify existing cloud computing security challenges and their solutions from literature and practice
- To interview at least two companies (a cloud user and a cloud non-user), in order to get relevant data for a valid comparison
- To conduct a survey with individual users of cloud computing about their experience and opinion about the topic of the thesis
- List their opinions/solutions/guidelines/practices to the cloud computing challenges
- Give my own view of the topic an suggest solutions

Despite the growing popularity, clients are still uncertain about cloud computing. International Data Corporation – I.D.C., conducted a survey where 74.6 % of the respondents ranked security as the greatest challenge of cloud computing (I.D.C., 2019).

The hypothesis thus posits: Users of cloud computing are aware of the security issues and are prepared to take appropriate actions.

Throughout the thesis, I use methods of description and analysis. Each chapter is based on the method of compilation of given resources and the description of more prominent theoretical emphasis, in order to outline the subject area from a theoretical point of view.

The thesis is built upon primary and secondary data. The secondary data is the foundation of the thesis and helps with developing the theoretical framework. The resources used are different literatures and research papers from online depositories (Google Scholar, Emerald Insight and Dicul).

The first section of the paper guides the reader through the brief history of cloud computing as well as explaining the theoretical elements of the topic. The second section is tailored by the primary data collected through interviews with business users and non - users and an online survey with individual users. Continuing is the analysis of the information gained and synthesis of key findings. The conclusion draws together the findings and views on the topic as well as proposed solutions to the threats. The results from my thesis can be used by anyone with interest for this topic, wheter it is for improving their day to day business operation, as well as protecting their own sensitive data from the CC services used in their private lives.

1 CLOUD COMPUTING

We live in a data oriented world. We have to accept that this is our present and definitely our future. With the data that is accessible to us, we try to reach information that will help us with our desire for (self) improvement. Generating information from data is vitally important for private usage, as well as the use in the business environment. The increase in the amount of data sources also helps with the rise of data acquired. Hence, the storage and processing of data cannot just relay on only the classical methods used so far.

For years, organizations and individuals have been using computer hardware to store their data (for instance hard discs, DVDs, discs and floppy discs). However, with the introduction of Clouds, information management and controlling was boosted, while making it more effective at the same time (Krishnan, 2017).

Therefore, these days, it is very common to hear an infinite number of terms connected to one single word - Cloud (Cloud Drive, Cloud Server, Cloud Security or even Cloud Ecosystem). It all comes down to a single, new and aggregated computing technology that now is used everywhere. Cloud computing is now spread, and in a way commercialized, by the vast request from the Internet market (Shah & Anandane, 2013). But what in fact is Cloud Computing?

The cloud is named after the nature phenomenon due to its abstract boundaries, dynamic scale opportunities and its ambiguous location. It is a source that is used and shared by a vast number of users and its effectiveness is relied upon the ease of accessibility. In the background, the cloud represents a conglomeration and integration of advanced information technologies that expand beyond just software, hardware or services. This conglomerate of technologies is expanding by the day and as a result the size of the cloud expands as well (Ou, 2015).

The model of cloud computing in a nutshell is a set of easily accessible and convenient computing resources that can be provided to the end user at any point without substantial management efforts (Krishnan, 2017).

The Cloud Computing industry is likely to reach an outstanding revenue of $397 billion by 2022 (Mlitz , 2021). In Table 1, the statistics for 2019 display that the total global outflow reaches $210 billion. This is an increase of 23.8% from last year. The leader market is US, reaching $124.6 billion for cloud services, and following are (I.D.C., 2019):

Table 1: Top 5 leaders in cloud computing market

Country	**Cloud market in billion $**
USA	$ 124.6 billion
China	$ 10.5 billion
UK	$ 10 billion
Germany	$ 9.5 billion
Japan	$ 7.4 billion

Source: I.D.C. (2019).

Contrary to the popular opinion, cloud services are not only for business enterprises, but also for individual use in the everyday life. The data for 2018 shows a remarkable 3.6 bilion cloud users globally. This number keeps increasing constantly. To get a grip on how the numbers grew, we can compare it with the number of users in 2013 – $2.4 billion. This number refers to cloud solution services for business and individual users together (Lobert, n.d.).

Due to the large demand from the users and rapidly increasing popularity, moving data to the cloud has become a norm and therefore, the importance of data security and privacy has become a hot button issue (Aldossary & Allen, 2016).

1.1 Definition and history of cloud computing

Without a doubt, the attention surrounding cloud computing has spiked in the past years, with various media outlets covering the topic and renowned experts from the field providing insight. (Sadulov, 2016). This is all due to the opportunities the technology opens up and how those can help the users. There are various definitions clarifying cloud computing but one of the most known, quoted, and accepted one is according to National Institute of Standards and Technology - NIST:

“Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (for example, networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service-provider interaction” (Mell & Grance, 2011, p. 2).

Simply put, cloud computing delivers different services (storing and accessing data, servers, software and database and networking) over the Internet instead of the hard drive on your device. Nevertheless, we must not forget that cloud computing is not the hard drive. Hard drives keep you close to everything you need. It is a local storage representation. You can access your data quickly and easily (Zissis & Lekkas, 2012).

In addition, the cloud is neither a residential server nor a Network Attached Storage hardware - NAS. But, in order to complete the cloud computing process, an online connection is essential. Therefore, the Internet plays a vital part for the cloud (either to access your data or simply to synchronize it with other information on the Internet) (Griffith, 2016).

So, in conclusion, cloud computing is a combination of massive information technologies and their integration, not a set of hardware, software or services, enabled via Internet.

When someone hears about the term “cloud”, they can automatically think of some new and modern technology. When in fact, the basic concepts of cloud computing were starting to be developed in the middle of the 20th century (Dandekar, 2016).

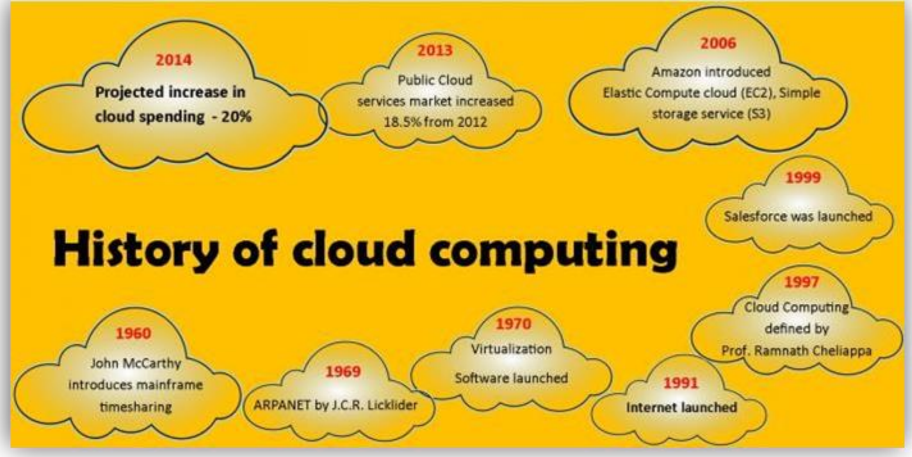
In Figure 8, the origin of cloud computing as we know it today is shown. The starting point can be traced back to:

- 1960 when John McCharty started to develop the concept of timesharing. This means that organizations can simultaneously use the same sources and at the same time. Considering the fact that a major promise of cloud computing is the efficiency of sharing the resoures amongst clients, we can see why timesharing had a big influence for its development (Kovačič, 2015).
- As I previously mentioned, the Internet plays a great role in the cloud computing process. And the precursor to the Internet was set in motion in 1969, when J. C. Licklider announced his project Advanced Research Projects Agency Network -

ARPANet. The mission was to make sure that people can have easy access to computers and effective communication method.

- In the 1970s, the focus was put on the term virtualization. Cloud computing in general offers on-demand Information Technology - IT services and products. Virtualization is the mechanism by which something can be made in a virtual version (e.g. storage devices, network resources, operating systems and hardware platforms). The way that cloud computing can provide a shared data and application platform as well as an infrastructure platform, is through the power of virtualization. (Krishnan, 2017).
- Moving forward to 1997, when for the first time Professor Ramnath Chellapa defined the concept of cloud computing. In his definition, he stressed that the boundaries of the progress and growth of cloud computing are more effected by economics than technology. In that same time (1999), businesses understood the benefits of cloud services, and Salesforce was already a well-established name on the market and an example of successful use of cloud computing (Foote, 2017).
- The next following years, many companies followed the example and recognized the potential of cloud computing. For example, Amazon launched Amazon Web Service in 2006, offering their users access to their computer through the cloud as well as storing their data in the cloud. The same year, the company launched the Google Docs service. Years later, in 2011, Apple launched iCloud, which focused more on storing personal information (Kotnik, 2017).

Figure 1: Historic milestones of cloud computing


2014
Projected increase in cloud spending - 20%
2013
Public Cloud services market increased 18.5% from 2012
2006
Amazon introduced Elastic Compute cloud (EC2), Simple storage service (S3)
1999
Salesforce was launched
History of cloud computing
1997
Cloud Computing defined by Prof. Ramnath Cheliappa
1960
John McCarthy introduces mainframe timesharing
1969
ARPANET by J.C.R. Licklider
1970
Virtualization Software launched
1991
Internet launched

Source: Dandekar, 2016.

1.2 Characteristics of cloud computing

In order to understand the extreme popularity of cloud computing and its massive business and private usage, we have to discuss its features. There are five different characteristics, which differentiate cloud computing from other computing models (Gong, Liu, Zhang, Chen, & Gong, 2010):

- On-demand self-service: This feature enables end-users to unilaterally provision computing capabilities when needed - such as server settings and network storage (Ko & Choo, 2015). This can be done without any contact from the service provider. In other words, a user can request and receive a computing service, without the need of interaction with the support staff for completing the request. Everything is automated for the customer and the provider (Rountree & Castrillo, 2014).
- Broad network access: All computing services are accessible over the network and at any time. Standard mechanisms can be also used (mobile phones, laptops and personal computers). This means that to access a cloud service, the user does not have to be at a specific location or time (Bauer & Adams, 2012).
- Multi-tenancy and resource pooling: Multi-tenancy permits numerous customers to share the same cloud computing resources while retaining privacy and without worrying about data spilling. Just like people living in an apartment building. They are all sharing the common infrastructure, but have their own apartments and privacy as well within the building. Resource pooling means that the service providers pool together their selected resources (servers, devices, storage, etc.) and they are shared across many users. The pool must be very large and flexible in order to service clients and provide economy of scale (El-Gazzar, Hustad, & Olsen, 2016).
- Rapid elasticity: Cloud capabilities can quickly scale out and scale in, depending to business demands. That is why rapid elasticity is a key feature of cloud computing. It enables users to quickly provision resources at any time, and then to remove them when they do not need them with no additional contract or penalties (Ikhar, Meghal, & Satpute, 2014).
- Measured service: The way the cloud computing systems control the use of the provided resources is by implementing a service level metering solution. These types of solutions can automatically optimize the usage of services like storage, bandwith etc. (Bhuvaneshkumar, Anitha, Kalarani, & Gunasundari, 2014). The user pays depending only on what they have used (Ambrose, Dagland, & Athley, 2010).

1.3 Cloud computing service models

Cloud computing delivery models includes three levels: Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), and Software (application)-as-a- Service (SaaS).

1.3.1 IaaS

IaaS is a model of cloud computing that provides the user with the infrastructure components that would otherwise be present on-premises, virtually through the internet (Anitha, 2016). It also serves other complimentary services to accompany those infrastructure components. A company can utilize the service to deploy databases and enterprise applications and further monitor the performance, manage issues and generate backups and recovery points. The performance varies based on the cloud service provider and their hardware capabilities, since the hardware is shared by multiple users (Chaudhary & Mishra, 2016).

Characteristics:

- The service is used by multiple clients simultaneously;
- Computing, storage, network and content delivery resources available as a service;
- Pay-as-you-go pricing for dynamic scalability

IaaS Examples: Amazon Web Services, Cisco Metapod, Microsoft Azure and Google Compute Engine.

1.3.2 PaaS

The PaaS cloud type provides the potential customers with a platform where they can deploy their created applications or software they had acquired. The requirement is that the applications have to be created using the programing language and supporting tools that the cloud computing provider provisions (Beimborn, Miletzki & Wenzel, 2011). The customer is authorized to manage the development of the application which is then hosted and operated within the system. All necessary hardware and software resources are managed and hosted by the CC provider, as well as the infrastructure, networks, servers, storage, middleware and services. Some PaaS systems have these components hidden behind an API (Application Programming Interface) but sometimes the CC provider makes them openly explicit. The customers can make use of visual environments and user interfaces, for developing their applications, web service delivery platforms and database management tools. This cloud implementation type is most suitable for organizations that want to grow their business models but be cost efficient at the same time and for companies that have different development teams or external parties working on the same project simultaneously (Žulič, 2017).

Characteristics:

- Multiple users sharing the same platform and development tools.
- The subscription fees and billings operated using cloud computing tools.
- Scalable resources used on demand by the PaaS virtualization technology.
- Variable services for developing, testing and deploying applications within a cohesive development platform.

PaaS Examples: Heroku18, Cloud Foundry19, OpenShift and Apprenda.

1.3.3 SaaS

The SaaS model gives the user the capability to use the applications, hosted on a cloud infrastructure, that belong to the cloud computing provider. These applications are available via a web browser and there is no need for a local installation of proprietary software (Anitha, 2016). Users have no control or ability to manage anything in regards to the application or the cloud infrastructure setup in general. The only settings the user is allowed to manage are pre-determined within the individual applications. By buying access to an already developed and hosted application, the user has no need for large investments pre or during the use of the service. In addition to this, the cloud computing provider is responsible for the maintenance and consistently updating and patching the software (Bohara, Mulay, & Jain, 2015). This ensures that the user will receive a secure product with no compatibility issues between multiple workstations. In the instance that the user needs to integrate a third party application, all of the development is done through API's given by the CC provider (Chaudhary & Mishra, 2016). Organizations that utilize this cloud service usually do because of the cost efficiency and ease of access. Examples are organizations working on short-term projects or need an application for a periodical use through the year, small businesses that lack the resources but have e-commerce business models or big companies that need web and mobile applications to manage their customer relationships.

Characteristics:

- Software solutions, easily accessible via the Internet, that are hosted on a remote server.
- Hardware and software (updates and patches) managed by the cloud computing provider.
- Difficult software customization

SaaS Examples: Google Apps, Salesforce, Workday, Concur, Citrix GoToMeeting, Cisco WebEx.

1.4 Cloud computing deployment models

Based on both the distribution of resources and the way they are used in accessing cloud services, we can discern between four deployment models. The choice of the model is also determined by the needs and objectives of the organization. Each of the models have their own unique characteristics.

1.4.1 Public cloud

Public cloud is a cloud hosting system that enables customers / users easier access to systems and services. Most common examples include: IBM, Google, Amazon, Microsoft, and many other companies. It is open for use for the general public as well. This kind of cloud computing is a true example of cloud hosting where service providers attend different customers who have very little in common. Technically speaking, there is the slightest difference in structural design between private and public clouds. Depending on service providers and the form of cloud clients used, only the level of security depends. The public cloud is far more business-friendly for load reduction making this particular type of cloud a lot more economic than others (Karmen, 2011).

The advantages of the public cloud are:

- Low Cost: The type of service provided by the public cloud enables the pay-as-you-go structure. Since the infrastructure is scalable based on the necessity of the organization, the virtual machines can be optimally used for their memory storage and computational power and thus the potential for a lower cost. Compared to the Private clouds' type of infrastructure, which may need to be designed to adapt to the potential growth of the organization, is inherently more expensive. The sacrifice an organization makes when choosing to utilize a Public cloud instead of a Private one, is ultimately repaid back with the flexibility of the cost (Krishnan, 2017).
- Increased Efficiency: The responsibility of the hosting, maintenance and management of the clouds infrastructure falls on the service provider. They employ dedicated teams that take care of the necessities that include infrastructure maintenance, implementing security measures and compliance with the latest software updates. This allows for the organization to utilize their time on improving the operating aspects of their business model (Hurwitz, Kaufman, Halper, & Kirsch, 2012).
- Scalability: The capability to meet the rising / diminishing demand for resources is the distinguishing factor that pushes organizations towards the Public cloud. Based on the type of business model, the computing power the cloud provides may need to scale up rapidly and subsequently scale down (Kajiyama, 2012).

The disadvantages of a public cloud include:

- No credible providers: While the perceived disadvantages are often over exaggerated, choosing a less credible i.e. smaller cloud service provider may prove to be costly. Outdated hardware, bad customer service and lesser execution speed are a few of the possible problems (Krishnan, 2017).
- Security: With a cloud infrastructure, the organization is only able to modify the operating level security factors. The physical level is the responsibility of the service provider which can become a potential security issue. In addition to this, the public cloud servers are exposed to the higher levels of threats due to their visibility on the internet. This makes the potentially vulnerable to attacks and breaches. However, choosing a credible cloud service provider with high level security decreases this vulnerability (Krishnan, 2017).

- Flexibility: A cloud service provider, although being flexible in terms of computing power and resources, can potentially have restrictive measures for their clients. They can restrict the type of Operating System – OS or type of storage the client can use as well as dictate certain software migrations (Krishnan, 2017).
- Data management compliance: Cloud service providers can operate from multiple locations and countries on the globe which from the perspective of data privacy compliance is a very serious disadvantage. Organizations that use the cloud for processing and storing data are faced with a potential breach of data privacy compliance laws. Based on the specific country or industry, the cloud service provider need to be able to confirm the physically location of the data, else compliance would be impossible (Krishnan, 2017).

1.4.2 Private cloud

The private cloud is a cloud computing infrastructure designed for the exclusive use of a single organization, within the security and set boundaries of that organization (Chaudhary & Mishra, 2016). It provides an easily accessible and internally managed computing power that scales on demand, with the benefit of a higher grade security based on the internal company policies. Opting for a private cloud solution means trading the cost efficiency of the Public cloud for the increased security, the control of the data management and the flexibility of the infrastructure (Inam ul Haq, 2013). Organizations with a business model that requires security and stability when it comes to data management, or the accessibility of scalable computing resources, mainly for IaaS and PaaS projects, are most suitable for the services of a private cloud.

Advantages of a private cloud:

- Flexibility and control: Since the structure is designed for a single entity, the possibility for a higher control comes naturally. Any required changes are done within the organization and therefore are faster and more effective (Martinez, 2013).
- Performance: The performance of any applications or services hosted on the Private cloud is innately better due to its closed nature.
- Security: Many aspects of the private clouds security are better than the ones of the public like the organizations freedom to control the parameters for both the software and hardware security measures. However, many misinterpreted this and claim that the private cloud is more secure. Based on the specific deployment type or internal security policy, the level of secureness can vary. Private clouds face the same amount potential threats as the public clouds and are susceptible to the same security risks. (Hurwitz, Kaufman, Halper, & Kirsch, 2012).

Disadvantages of the private cloud:

- Cost: The additional security and control features come with a higher price. Since it's internally controlled and maintained, the costs include hardware and software updates as well (Karmen, 2011).
- Maintenance: Public cloud applications provide their users with regular software updates and patches. This is not the case with private clouds that are not maintained by the software vendors.
- Scalability: The issue with scalability is connected with the cost of the service. The internally set boundaries and parameters limit the use of resources.

1.4.3 Community cloud

A community cloud is a type of private cloud model that utilizes the benefits of the public cloud solution. The computing resources in the community cloud are shared between two or more organizations with similar privacy and security standards. There are usually companies within specific business communities that are under strict regulations and compliance demands, or companies working on collaborative projects and community type software solutions (Anitha, 2016). The community cloud enables the separate entities to own their private clouds and at the same time share custom designed software tools within the community. The private cloud is designed to meet the compliance needs of the company and the community. A cloud service provider can build a custom set of clouds that suits a certain community and provide the businesses a way to utilize their own computing resources most efficiently within the community. This way the under-utilized resources can be effectively used between companies in the community (Chaudhary & Mishra, 2016).

Advantages of the community cloud:

- Costs: The cost for the deployment of a private cloud is higher compared to the community cloud because all the cost is divided between the members of the community (Karmen, 2011).
- Management: Since the community cloud is a closed off version of the public cloud, the same management structure can be utilized. The cloud service provider can potentially act as a third party manager.
- Tools: The possibility to create custom made tools and software solutions that tackle specific tasks relevant to the members of the community. This type of customization would be costly in the private cloud and impossible in the public.

Disadvantages of the community cloud:

- The concept of the community cloud is still a fairly new concept and because of that the implementation is costly.

- Sharing the same cloud has the disadvantage of capped bandwidth and data storage capabilities between the members.
- The cost of the security measures a company needs to establish is also very high.

1.4.4 Hybrid cloud

The hybrid cloud is an operating model where a company chooses to implement both a private and a public cloud infrastructure (Žulič, 2017). Companies decide to utilize the security benefits of the private cloud for the part of the operations that carries sensitive data and push the other part of their workload to the public cloud to benefit from the scalability and efficiency. Protecting the sensitive data within the private cloud where high security standards are constantly maintained, while executing the big data operations and projects that need fast implementation on the public. Hybrid cloud implementations are very specific and are unique to each organization. Based on their requirements, the organization needs to take in consideration the need for additional security measures. This type of implementation is susceptible to attacks from the public cloud (Chaudhary & Mishra, 2016).

Advantages of the hybrid cloud:

- Scalability: Utilizing the scalability of the public cloud.
- Cost efficiency: Pay-as-you-go resource allocation capabilities of the public cloud for temporary, big data projects. Optimization of costs during the different stages of the applications lifecycle.
- Better data security: On-premise private cloud infrastructure accompanied with company managed security standards (Chaudhary & Mishra, 2016).
- Flexibility: Gives the organization the possibility to improve their agility and flexibility with their business model by having the public cloud as a tool for fast implementation. This eventually leading to more revenue opportunities (Hurwitz, Kaufman, Halper, & Kirsch, 2012).

Disadvantages of the hybrid cloud:

- Increased security threats: The use of the public cloud opens up the organization to the internet and to potential security breaches. The data flow between the two clouds is also a vulnerability that can potentially be exposed. There are concerns connected with that kind of movement due to the variety of implemented controls and security standards between the public and private cloud. Encrypting the data is also affected because of the difference between the two environments (Kotnik, 2017).
- Management issues: In order to manage the complexity of the Hybrid cloud, companies usually use a management tool which can be either provided by the cloud service provided or by a third-party. Either way the security concerns over the use of

such tools are reasonably high due to the different cloud structures and requirements. These tools should be able to enforce the same security standards consistently between the Public and Private clouds (Žulič, 2017).

1.5 Advantages and disadvantages of cloud computing

It is evident that cloud computing provides numerous opportunities for individuals and organizations that are trying to improve their workflow or business. However, all the benefits that come from implementing cloud computing come with a caveat. That caveat is that like every technology, cloud computing has its own pitfalls and disadvantages.

1.5.1 Advantages of cloud computing

After reviewing several articles and thesis, the most common advantages connected to cloud computing are:

- Economical: One of cloud computing's major advantages is that it is relatively inexpensive. Due to zero server storage and server requirements, a company could save massive capital expenses because it does not need to provide powerful machines to start up the programs integrated in the cloud. It also eliminates the need for additional proffesional staff that would be responsible for the operation and maintenance of the hardware. There is also the fact that the customers have to only compensate for what they used and there are no upfront costs (Truong, 2010).
- Reliability: When it comes to the factor of reliability, the data in the cloud platform is protected without the possibility of being tempered with. Several copies are made making sure that if the database crashes, it can be recovered from the copies. Also there is the possibility of unlimited storage space, if the user is ready to pay for the service (Mišigoj, 2013).
- Manageability: Another benefit that comes with cloud computing is the ease of use. The management requirements with cloud computing are taken down to a minimum. Any device capabale to connect to the internet, like a computer or a laptop, and a reliable internet connection are the only things that the user has to provide. If anything happens to the database or any other part of the cloud, the customer has to only contact the host of the cloud. He manages each and everything and that is very beneficial to the customer (Bisong & Rahman, 2011).
- Data centralization: A big upside is also the fact that all the data is stored in one location and it can be accessed from various remote locations. This makes the collaboration between coworkers a lot easier considering the fact that files can be shared or edited no matter where users are-universal access (Kuyoro, Ibikunle & Awodele, 2011).
- Proper security: Considering the fact that we live in a world where our privacy and security are constantly in question, the cloud computing providers promise the highest

level of security for their clients that choose to store or process their data using their service. We have to agree that there is a higher possibility that the data can be lost on a hard drive rather than on the cloud (Mišigoj, 2013).

1.5.2 Disadvantages of cloud computing

Following, we have the pitfalls of cloud computing:

- Internet connectivity: One of the characteristics of cloud computing is that it constantly needs an internet connectivity. In other words, there is no other way the users can access their data from the cloud (Nežič, 2016).
- Lower bandwidth: Bandwidth defines the maximum data transfer rate of a network or Internet connection. In other words, it shows the quantity of data that can be transferred over a specific connection in a specific amount of time. When there is lower bandwidth, naturally this decreases the welfares of the clouds. The bad connection can end up with results of quality disruption (Žulič, 2017).
- Effect of speed: In order to get the maximum service from the cloud, the user has to be connected on a high-speed internet connection. The speed with which the Cloud delivers its service to the end user is directly affected by the amount of users that are accessing it simultaneously. For a client, the service can vary in quality based on amount of traffic the cloud is handling at that moment. (Turner, 2013).
- Security issues: Considering the fact that cloud computing services store the data on user's clouds, there are a lot of questions if the files are private and properly secured. It is always a good practice to consult with an IT company that deals cloud security. Ignoring and overlooking this fact can lead to a vulnerability of the business (Morsy, Grundy, & Müller, 2010).
- Agreements: Most cloud service providers offer non-negotiable agreements. This is one of the drawbacks for the users (Žulič, 2017).
- Lacks of support: Often, providers struggle to provide clients with adequate support. These companies try to minimize the cost of customer service and aim to force their customers to completely rely on FAQs (Markun, 2015).
- Variation is cost: Usually providers charge clients for extra features of cloud computing services (Bisong & Rahman, 2011).

2 SECURITY AND PRIVACY CHALLENGES IN THE CLOUD

So far, we established the fact that clouds can be cost-efficient and adjustable as well as the fact that the customer's information is stored on geographically isolated platforms under control of the cloud. However, the ease of use and convenience of cloud computing comes along with many security challenges due to its popularization. That is why, it is essential and obligatory to explain what actually cloud security is and analyse the main risks for the information kept on cloud platforms as well.

2.1 What is cloud security

Cloud computing security is a wide-ranging term that includes the set of policies, procedures and practises that work together to protect data and information inside a cloud architecture. These protection activities are designed to secure cloud content, to promote regulatory enforcement, to protect the privacy of clients, and to establish authentication standards for specific users and applications (Robu, 2010). In addition, cloud security detects incidents when they happen, includes the security process enhancements that toughen the system and notify about potential attacks. Because the security measures can be shaped to the exact requirements of the client, administration overheads reduce and IT teams can focus on other areas of the business (Arora, Wadhawan, & Ahuja, 2012).

2.2 Importance of security in cloud computing

After we covered the basis of cloud computing, we can now focus on explaining why security is important for all the users of cloud services. We can say with confidence that nowadays, our most valued asset, whether we talk about an individual or an organization, is our data.

Clients use cloud providers in order to store their sensitive and complex data. In that way as we already said, not only they have unlimited access to it, it is also very cost effective. Nevertheless, that is not the only thing that users are asking for in cloud solutions. Above all, they are interested in shielding their information from threats in the form of corruption, breaches, temporary or permanent loss of access or their data as well (Kumar, Kumar, Singh & Kumar, 2014). These are serious concerns that can badly effect the everyday lives of individual users and the normal operating of organizations.

With the popularization of CC, the amount of sensitive data being stored in clouds is increasing, so the security issue becomes the most important element that the cloud storage providers focus on. The ISACA/CSA study (2015) in their cloud vision series white paper “Cloud Computing Market Maturity” shows that one of the most challenging tasks is in fact securing the users data in a cloud. They are investing many resources to keep their security on a high level, so clients feel their data is safe, but they also must comply with the legal regulations for the handling of data.

Usually the businesses are more aware of the concept of cloud computing and all the underlying processes that are connected to it. On the other hand, employees are not as familiar with the details and base their opinions on popular misconceptions that are connected to the term. For example, they believe that hackers are the biggest threat to their data security, when in reality, they themselves pose an equal threat, if not bigger, because an accidental mistake can open the whole company to potential security threat. That is why implementing a cloud solution creates many challenges for an organization, but a smooth transition is possible if it is done right (Maddineni & Ragi, 2012).

2.3 Cloud security concerns

While cloud storage is an advanced and modern computer infrastructure, some of the main elements of privacy and safety could be illustrated from real world practice. Below, we discuss the different areas of cloud data security as defined in the NIST.

According to the authors, Timothy Grance and Wayne Jansen there are 9 different areas in the cloud services where security risks usually emerge (Jansen & Grance, 2011).

- Governance: A management model that provides a given company with an efficient strategic framework for meeting their objectives in the cloud environment while simultaneously navigating and complying with the security parameters and regulations. Simply put, cloud governance is a framework, applying a set of policies and standards to the use of cloud computing services. This helps with cost optimization and organization but, in reality, the control in this area is poor and without governance, organizations can lose themselves in the rapid growth in the cloud environment. It is crucial for both users and providers to be aware about their responsibilities so potential problems can be they avoided (Asma, Chaurasia, & Mokhtar, 2012).
- Compliance: Helps organizations and providers to comply with the laws and regulations while using the cloud. The law itself does not stop the process of cloud adoption. The problem occurs because there are a lot of different regulations and laws concerning cloud adoption in different countries. That there are a lot of regulations about data storage, they are constantly not only changing and updating making maintain compliance an impossible task for the users and providers in the same time (Cloud Security Alliance, 2013).
- Trust: The most important element in this area is the initial contract between the cloud provider and the customers. The decision for an organization for adaption the cloud services is difficult itself. But, with uploading and storing data to the cloud, users open themselves to risks not only from inside their own company, but from the cloud provider and their customers as well. The terms of data ownership should also be a part of the contract (Žulič, 2017).
- Architecture and infrastructure: Simply put, cloud architecture defines how various technologies and components are integrated to create clouds. The architecture defines the components of the cloud and relationship between them. In other words, the architecture gives all the characteristics that define the cloud services. The cloud infrastructure is the process of incorporation of the materials, while the architecture is

the blueprint. In practice, issues usually arise when clients are not aware of the technologies the cloud service provider uses for security (Takabi, Joshi, & Ahn, 2010).

- Identity and access management: We can argue that this element also plays a significant role in the security issue in the cloud. As a pair, their focus is on identifying and authenticating access in the cloud. But, it is crucial to understand that they are two different concepts. Each user, administrator or even a system requires an identity. Verifying that you are who you say you are is what makes the whole process of authentication. Access management makes sure that entities have the ability to perform tasks that are only theirs to perform. This is called the process of authorization (knowing who someone is). They both tremendously influence the overall issue of data sensitivity and privacy (Takabi, Joshi, & Ahn, 2010).
- Software isolation: Because clouds are accessed and used by a lot of people simultaneously, it is vital each user to act independently from the others. Therefore, isolated work can also bring threats of software infection of a user. The key is to make sure that these infections do not spread to other users of the cloud services (Cloud Security Alliance, 2017).
- Data protection: Because of the openness and the multitenancy characteristic of the cloud, the data security and privacy has its particularities (Chen & Zhao, 2012). The focus of data protection is adequately isolation and security of data that is kept on the cloud. This is also another important aspect of cloud security because of the massive amount of data and confidential businesses that is kept on clouds nowadays. Thus, it is important that the data is only accessed, controlled and managed only by the right people (Kotnik, 2017).
- Accessibility: Intentionally preventing access to the cloud data and gear failures are issues that threaten accessibility to a cloud environment. In these cases, the cloud kept data is in vulnerable because it can be lost and its quality is put at risk. They can only jeopardize the quality of the data, as data loss can also occur. It is important that cloud service users are aware of how to handle such situations (Cloud Security Alliance, 2013).
- Responsiveness to hazards: A great issue is when an attack is happening but the users are not informed about what their actions should be. Providers play a great role in this area because they not only have to correct the hazard, they should also educate their clients on how to handle certain situations (Žulič, 2017).

The list of potential issues span from untrustworthy service providers to the lack of awareness on the users' side about their data on the Cloud.

2.4 Types of issues and threats

Considering the fact that the use of cloud services is growing every day, new security vulnerabilities are consistently being discovered and traditional security vulnerabilities are still present in cloud environments.

There will always be concerns from corporations and individual users about maintaining the security and integrity in this environment. But there are also situations where users jump the broom and change to cloud computing while being unaware of what that means to them (Popović & Hocenski, n.d.).

As an answer to the ever-growing threat possibilities, the Cloud Security Alliance - CSA created standards for cloud security. Their well-known report, “The Treacherous 12 – Top Threats to cloud computing + Industry Insights” (Cloud Security Alliance, 2017), helps users and providers with knowledge and guidance their cloud security strategies. Based on their research, they point out these twelve risks:

- Data breaches: The leakage of confidential protected and sensitive data, which can be either used, stolen, viewed by a party that is not authorized is defined as a data breach. As a result of malicious data breach attacks, serious legal repercussions may fall upon the cloud service provider (Chaudhary & Mishra, 2016).
- Insufficient identity, credential, and access management: Substantial risks for cloud information security represent the practice of centralized passwords and faulty systems for identity verification. These conveniences present a potential threat to the cloud environment because they tend to be easily exploited by attackers (Sabahi, 2011).
- Insecure User Interfaces - UIs and Application Programming Interfaces - APIs: UIs and APIs represent a doorway in to the system and therefore are a potential security vulnerability. External parties may abuse these interfaces and breach the system (Kumar & Bhatt, 2015).
- System vulnerabilities: These vulnerabilities stem from the source code that is used to build the cloud environment. System bugs that are potentially exploitable by third parties to forcefully gain access to the protected data in the cloud or even take control (Kumar & Bhatt, 2015).
- Account hijacking: An attacker gains access to an account in the system through hijacking. This attack can lead to the leakage of sensitive information and manipulation of data and transactions in the system (Qaisar, 2012).
- Malicious insiders: a user within the cloud environment that is purposefully abusing and exploiting their authorized access to the information resources and systems (Kumar & Bhatt, 2015).
- Advanced persistent threats: Attacks that are specific and deliberate, carried out over a long period of time with the goal to infiltrate and exploit the system. These attacks utilize multiple stages and different attack techniques.
- Data loss: Losing data from the system due to accidents or deliberate attacks (Chaudhary & Mishra, 2016).
- Insufficient due diligence: Not performing adequate due diligence prior to implementing a cloud computing solution may result in legal, financial and compliance risks.

- Abuse of cloud services: Some cloud service providers’ offer appealing terms for potential clients with the intent to exploit their data.
- Denial of Service – DoS: DoS attacks are meant to indefinitely obstruct the user’s access to network resources and data (Sabahi, 2011).
- Shared technology vulnerabilities: The sharing of applications, infrastructures and platforms within a cloud environment present a potential vulnerability. The systems reliant on these shared technologies could be all affected at once as a result to an external attack or an internal system issue (Kumar & Bhatt, 2015).

2.5 CIA Triad

At this point, the use of information technologies is a very common occurence in our everyday lives - hence the increased security risks the users are potentially facing. That is why the use of security measures to address those risks is essential. In simple terms, risk is a vulnerable situation that involves the chance of something harmful happening and resulting in a loss. In the market, there are various researches available that discuss the problem of security while using clouds. The Garther Company released their report that increases the distress about the risks and threats in data security (storage), data recovery, privacy and integrity (Gartner, Inc., 2008). Data security is definitely the leading concern in this field, following the concerns for data integrity and availability (Kumar, Kumar, Singh, & Kumar, 2010).

The CIA triad is a well-known model for security policy development. It shows the vital components that have to be a part of the information security measures in an organization. The respected model for the development of security policies is used for not only detecting problems, but also finding required solutions.

The model contains three concepts:

- Confidentiality: This concept is connected to the cloud characteristic - multitenancy, or in other words resource sharing memory, programs, networks and data (Zissis & Lekkas, 2012). It is understandable why in today’s world, is important for cloud users to demand protection for their sensitive, private data kept on the cloud. The confidentiality concept is the set of measures that protect information from unauthorized access. Usually, this is implemented by passwords; access control lists, usernames and encryption. The limitation of access plays an important part because there is a constant need of confidentiality and protection from the risk of loss of privacy, unauthorized access to data as well as the problem of identity theft. There are even cases when confidentiality is more important than the other concepts in the CIA triad. Monitoring and controlling communication channels is necessary, so confidentiality can be guaranteed under the CIA triad (Maddineni & Ragi, 2012).

- Integrity: This component is vital due to its design to ensure data protection and maintaining the accuracy and consistency of said data. One of the security measures that integrity component is responsible for is the access of the protected data, which as a best practice is only allowed to authorized parties (Backe & Lindén, 2015). Due to the possibility of force majeure, events or external attacks there have to be backup procedures in place to provide data recoverability. Data integrity is maintained not only in regards to the access and modifying but also in the process of data transmission. Proper and secure data transmission protocols need to be respected in order to maintain the integrity (Manisha & Rani, 2014).
- Availability: Has the objective to ensure that authorized parties can access the information resources at any point they need to. This requires having in place appropriate systems to maintain the hardware and software and optimize the network solutions. There also have to be business continuity plans to mitigate the potential downtime and unreachability of data due to external attacks. These measures need to guarantee the availability of the data when the worst-case scenario occurs (Ashktorab & Taghizadeh, 2012).

Information security shields valuable information from unauthorized access, alteration and distribution. Understanding the CIA triad is vital because being informed helps with implementing security policies and measures the right way and dealing with the issues and consequences that come along with using the cloud every day (Maddineni & Ragi, 2012).

2.6 Types of attackers and attacks

The potential threats a user may face could come from an attacker within or outside the organization. There are two groups of attackers:

- External attacks: All organizations and individual users that are digitally present and store their sensitive data on the cloud are exposed to the most frightening and feared attack – the external attack. These attacks are not connected to employees and people within the organization (provider or user). These attackers do not have authorized access; they focus on finding and manipulating network vulnerabilities (Osman & Mustafa, 2015).
- Internal attacks: A usual mistake is completely forgetting about the insider threat. This is an attack that is initiated from the organization (service provider or user) itself. The attacker already has access to the cloud services, the sensitive information or the privileged accounts existing in the cloud environment. It is only influenced by the role they have in the organization, and how he misuses that access (Osman & Mustafa, 2015). According to Osman and Mustafa, the Table 2 explains the most common threats the cloud users and providers face, categorized based on the CIA triad components (Osman & Mustafa, 2015).

Table 2: Cloud threats

Threats	Explanation
Confidentiality	
Insider user threats: - Malicious cloud provider - Malicious cloud customer - Malicious third party user (supporting either the cloud provider or customer)	As the cloud delivery models are being widely used, the number of potential users within a certain cloud environment increases. This enhances the possibility of internal attackers who wish to exploit the system from within.
External attacker threats: - Remote software attack of cloud infrastructure / applications - Remote hardware attack against the cloud - Remote software and hardware attack against cloud user organizations' endpoint software and hardware	One type of cloud delivery model is not targeted more than any other, meaning that the external attacks focus on vulnerabilities in the source code or user facing applications like APIs and UI. These attacks focus on the software as well as on the hardware infrastructure of a cloud environment.
Data Leakage: - Failure of security access rights across multiple domains - Failure of electronic and physical transport systems for cloud data and backups	The leaking of data could be the result of a purposeful malicious attack, or a human error / faulty hardware. This could lead to exposing sensitive and personal information to the public and competitors.
Integrity	
Data segregation: - Incorrectly defined security perimeters - Incorrect configuration of virtual machines and hypervisors	The importance of proper data segregation in cloud environments that are designed to share computing resources, is greater due to the large amount of users on the platform. In order to maintain the integrity of the data the security measures need to take in account these potential threats.
User access: - Poor identity and access management procedures Data quality: - Introduction of faulty application or infrastructure components	The integrity of the data is potentially at risk if the user access procedures that are implemented do not meet the industry standards. Authentication schemes like SSO (Single Sign-On) have the benefit of scalability and promote security.
Availability	
Change management: - Customer penetration testing impacting other cloud customers - Infrastructure changes upon cloud provider, customer and third party systems impacting cloud customers.	The availability of the data to the users can be potentially compromised when changes are implemented in the cloud infrastructure. The responsibility of the change management fall upon the cloud provider and if not done properly, may result in system failures.
Denial of Service threat: - Network bandwidth distributed denial of service - Network DNS denial of service - Application and data denial of service	Internal or external parties can cause the discontinuation of processes within the cloud that could affect different components and deny the users access to their data, application and cloud services.

(Table continues)

(Continued)

Threats	Explanation
Availability	
Physical disruption: - Disruption of cloud provider IT services through physical access - Disruption of cloud customer IT services through physical access - Disruption to third party WAN providers services	Disruption of data availability can be caused by damage done to the physical infrastructure of the cloud providers' facilities. That is why cloud providers should invest in better security or use large data centers designed specifically just for that purpose.

Adapted from Osman & Mustafa (2015).

In a recent report executed by Oracle and KPMG, 750 cybersecurity and IT professionals from Europe, North America and Asia-Pacific, were asked whether they feel their organization has been expanding the use of cloud computing faster than development of their security platform and therefore creating an implementation readiness gap. In other words, has the companies been migrating systems to the cloud at a pace that the security measures covering those systems cannot keep up. A surprising (44%) of the interviewed professionals admitted that they have a substantial public cloud security readiness gap, and (48%) said that the gap is only moderate. Only (44%) were assured that they are well prepared to handle security threats. The possible reason stated in the report, that contributes to this rapid expansion and subsequent readiness gap that companies are experiencing, is the lack of collaboration between the cybersecurity team and all the other business units within the company. As new cloud technologies and solutions are introduced almost on a daily basis, the speed with which a team can implement that technology and immediately benefit from it becomes very important (KPMG & Oracle, 2020).

3 THE CLOUD AND BUSINESS USERS

As a central place on the internet that stores data, the cloud makes sure that the data is accessible anywhere and anytime from any device connected to the Internet. These days, businesses all over the world (large and small), have already incorporated the cloud and its variations because of the benefits I already discussed and mentioned before. Flexibility as a trait provides immense value to the business along with virtualization, automated security patching, scaling up and down to handle bigger workloads and rapid data collection, analysis and transfer (Reese, 2009).

The COVID-19 pandemic forced us into working remotely and constantly relying on video conferencing. Cloud services are currently the digital technology that drives this transformation engine that helped companies maintain continuity during the pandemic. The stay–at–home orders have also significantly increased the use of collaboration tools that are cloud based. According to results from the Canalys reports, during this quarter a growth of 33% was seen in the cloud market which amounted to $36.5 billion worldwide. The market leader AWS generates 32% of the markets revenue, followed by the 19% that belong the Azure. The remaining players are Google with 7% and Alibaba Cloud with 6% while the rest 37% of the market revenue is split between various smaller clouds. (Canalys, 2020).

Be that as it may, there are still businesses that are not comfortable with adapting the cloud and its variations in their everyday operations.

3.1 Research methodology

As previously stated, this study set out to determine whether users are aware of the security issues and whether they are prepared and taking appropriate actions regarding the threats. The hypothesis that is tested stands that users are aware of the security issues and are taking appropriate actions.

Having all of this in mind, two groups of subjects were interviewed, namely CC users and CC non-users, to see if the security issues and risks are the main reason why companies fear cloud computing as well as their actions and protocols for the same issues currently. The aim was to have companies from different sizes and business areas that cloud computing would be a great addition. The occupations I was interested were sales, accounting, logistics, technology, public/government services and marketing. After contacting 10 different companies four accepted to be a part of the research. The final participants are shown in Table 3:

Table 3: General information

	CC USERS		CC Non-Users	
	Philip Morris International	Zeppelin Lab GmbH	Ekom – D DOOEL	Expanda DOOEL
Employees	75.000	10.000	2	160
Country	Serbia	Germany	North Macedonia	North Macedonia
Business area	Tobacco sales /manufacturing	Sales and renting of construction	Accounting and finance	Logistics

Source: Own work.

Regarding the interview process, it has to be stated that the interviews were done online. I divided the interviewees in two groups:

- Companies that are cloud users
- Companies that are non-cloud users

The questions were formulated respectively to the purpose of the thesis. There are 14 questions for companies that use cloud computing on a daily basis and 9 for the companies that are not using cloud computing. The questions were separated in four main groups:

- General information about the company – These first set of questions were designed to get to know the companies better, industry, size of the company, their daily business operations, and position of the interviewee.
- Relevant software information questions – results can show which CC service and deployment model is mostly used by companies, as well as the programs used by CC non-users.
- Business implications questions – results can show us the main reasons why the decision to implement / not to implement CC was made.
- Questions about risks associated with the cloud – Information gained from users and non-users of how they are prepared for the risks and threats from their daily work.

All of the interviews were performed online, through a Skype meeting. For the whole interviews, please refer to the transcript attached to the appendices.

Following are the results of the interviews, divided in two groups: results from interviews with companies that use cloud and the ones that do not. The questions connected with the cloud are analyized in detail.

3.2 Companies that use cloud computing

When deciding whom to interview for the purpose of this subject, it was logical to me that I would need to incorporate big / international companies that would definitely use cloud services in their everyday operation. The interviewees are employees of "Philip Morris International" and "Zeppelin Lab GmbH".

"Philip Morris International" is a company that operates in the Tobacco / FMCG industry. The nature of the industry is quite specific because of the high amount of regulations and laws that apply to it. These regulations vary from one country to another and therefore the business environment for each affiliate is different. Philip Morris International is a large international corporation with over 75,000 employees. The affiliate, PMI Serbia, is the central hub for the South-Eastern Europe cluster within the company. Ms. Ilić works as a Digital Trade Content Executive. Her responsibilities are mainly related to maintaining the B2B mobile application and managing all of the CRM campaigns in the back-end and front-end.

“Zeppelin Lab GmbH” is a company focused on worldwide sales and renting of construction equipment, plant constructions as well as power systems. Globally, they have 10.000 employees. Mr. Stojanovski is a DevOps Engineer and his responsibilities within the company consist of migrating the old monolith infrastructure to a new, improved, as well as faster, scalable and cost-efficient cloud infrastructure in combination with the digitalization processes, as part of migrating the old infrastructure, which will help in bringing the company closer to the goal of having fast deployments and changes whenever there is a need of one.

3.2.1 “Philip Morris International” – Interview Findings

Philip Morris is a light user of cloud computing. As an international and large company, they opted for a Private Cloud and have an agreement with Salesforce.com for the use of their SaaS and PaaS services. As anticipated, this decision was made because of the size of the company as well as the cost and effectiveness. They are currently using the Salesforce cloud platform, which helped to standardize their current business model without complications. The company itself had done their own research and was aware about all the benefits and pitfalls of cloud computing and constructed a whole team responsible for managing any potential risks.

The company has already experienced a lot of standard difficulties while using the cloud but the most common was data leakage. When asked to elaborate about the security issues the company faced (Data breaches, Data Leakages, Insecure API’s, Hijacking…), Ms. Ilić answered: “Yes of course, almost all of the difficulties that you mentioned. There are groups of teams dedicated to fixing bugs and issues, so that whenever one of those difficulties occur, they are reported and handled by each respective team. One of the issues we had was when the Salesforce database was made available to all of the users globally, which caused the possibility for a potential data leakage and abuse of confidential data. Luckily, the protocols we had in place proved efficient and the above mentioned teams fixed the issue quickly by troubleshooting and escalating it in a timely manner.”

They also have protocols, which are updated each year according to the continuity plan, and employees are required to follow them. This way they prevent the abuse of confidential data or other potential risks. So far, their solutions for addressing the security issues have shown to be effective and most of all preventive.

When it comes to educating the staff, “Philip Morris International” organizes mandatory educational courses that each employee has to complete every year. With this, they are sure that employees are up to date with their knowledge and minimize the fear of changes and technology employment. When it comes to security standards, PMI has developed strict policies regarding security and are complying with external privacy laws. Overall, the company is very satisfied with the implementation of cloud computing besides the possible risks that come with it, they are continuing with their practice and even plan on expanding the sectors that use cloud services daily. When it comes to their protection from the risks and issues, they believe that it all comes down to having good risk policy organization, prepared team and education.

3.2.2 "Zeppelin Lab GmbH" – Interview Findings

"Zeppelin Lab GmbH" are experienced users of cloud services. They are using all service models, from Adobe Experience Cloud for SaaS, to Amazon Web Services for PaaS and IaaS solutions. Mr. Stojanovski is responsible for the product that is hosted on Amazon Web Services, which is a public cloud model. The company decided to use cloud services for its scalable and creative solutions that lead to not needing to take care of the hardware. This is a huge cost reduction to them and which ultimately affects their revenues and increases for R&D. The cloud solutions so far helped them by providing faster delivery of new features and implementing new products, since the company is not limited to hardware anymore. Their thoughts about cloud threats and risks are that they are not preventable. They are common and present whether companies use traditional systems or cloud systems. When it comes to issues they already faced, Mr. Stojanovski pointed out that naked IP address and open ports on some of their servers have resulted in a white hat attacks. They quickly reorganized and established a private network, reissued new security keys for every person who had access to those instances. Occasionally, they face DDOS attacks but have a stable protocol for that as well.

When asked about the already established company protocol for the potential security risks, Ms. Stojanovski answered: "We are doing routine checkups for flaws in the system, as well as one of the perks of using cloud computing, is having the ability to run daily tasks for anomalies and out of context patterns. For example, using machine learning on access logs, we are able to track anomalies in the beginning of some kind of DDOS attack and block all kinds of bad requests that are hitting our infrastructure. When it does happen, some security flaw, which was not foreseen before, our security experts and engineers will try to find a solution in the future on how to reduce this flaw and not happen again."

When it comes to educating the staff, twice a year every employee can choose which conference and seminar they would like to attend, in order to improve their cloud computing knowledge. In order to be compliant with the security standards, "Zeppelin Lab GmbH" are using AWS provided security standards, like TLSv1.2 with different cyphers included as part of the package of security policy by AWS, which are being updated from year to year. Additional security measures are the different types of firewalls and WAF rules that are used, which helps them to monitor and block the requests that are hitting the Cloud front.

The company is amazed from the benefits they have experienced. Their opinion regarding the security threats has not changed and they claim that the cloud helped them strengthen their position and that traditional systems are not an option for their company. The chance for issues and mistakes are bigger having in mind the human error factor. They are planning to expand the usage of cloud computing (AWS) in near future in all of their sectors.

3.3 Companies that do not use cloud computing

The participants are from two companies that decided not to use the cloud or any of its services at all. Both of the examples have tried to incorporate it, but failed and returned to their old programs that are not cloud based in any way. The first interview was with “Ekom – D DOOEL”, and the second one was with “Expanda DOOEL”.

“Ekom – D DOOEL” operates in the finance industry. They provide accounting and consultation services. This industry is specific because of the regulations and the national and international standards that shape the accounting process North Macedonia. “Ekom – D” is a small company with only two employees. Mr. Šterjov works as an accountant and in the same time is the sole owner of the company.

“Expanda DOOEL” is a logistics company that operates on the Macedonian market. They offer logistics, distribution as well as management services. Their main client is “Philip Morris International” but they also provide their services to “A1”, “Red Bull” and the Macedonian State Lottery. They operate on the Macedonian market and currently have around 160 employees. Mr. Dimovski is the Financial Director at the company and has been their employee for 28 years.

3.3.1 “Ekom – D DOOEL” – Interview Findings

During our talk, Mr. Šterjov explained that he in fact was aware of the benefits the cloud brings to a company having the wish to incorporate Pantheon cloud services in the company’s daily operation. The whole incorporation and switching process they have experienced was not what he expected and they terminated the whole process. Keeping in mind that the company has only two employees, they turned to a provider that can give them full service and guide them along the way.

They were not at all satisfied with the providers approach and their specialists. So they pointed out that that is the main reason that they switched back to their traditional system: “The specialist that was responsible for the training and helping us with the overall incorporation of the program was not up to the task. They did not have the experience with the program themselves, as well as the needed accounting background. So it is safe to say that they did not know how to adjust the program to our needs....”

Currently they use an accounting program that was specifically made for their needs. They are updating the program yearly and are using a local hardware storage as well (a disk) for back up just in case. According to the company, in 30 years they have not experienced any trouble with their data security. When asked about the difficulties concerning the cloud implementation, they focused on their lack of knowledge and how the whole implementation would take up a lot of their time to get used to. As a result of the fact that they were not satisfied with the provider in the first step, they were not convinced that the provider is capable of guarding their data after the implementation when they are faced with security issues. Their biggest issue is losing the data. So their protocol is not only keeping the data saved on their program, but saving it all again on their disk separately.

3.3.2 "Expanda DOOEL" – Interview Findings

Just as the previous company, Expanda DOOEL has tried to incorporate cloud services in their daily operations as well. The primary use of the cloud system was to track their vehicle fleet, and the application they used was cloud based. The physical devices were installed in the vehicles and the people that were responsible for the tacking could access the application from any personal device, PC or mobile phone. It brought not only convenience, but provided efficiency because it was very accessible and they did not need to have storage space for the data. All the bugs and issues were reported and solved by the service provider.

The main issue the company had, and why they decided to terminate the contract in the end, was that they could not integrate the data from the cloud GPS service with their core system. Their core system is a custom built desktop application, done by a local company and they used it since the beginning. It is constantly updated along the years, based on every additional need the company has had.

Time deficiency is the main reason why they are not considering implementing a cloud based solution again. Their custom solution is maintained and upgraded, and most importantly for them, the system is approved by their main client, "Philip Morris International". Also the company thinks that as a small organization, they do not think that the cloud implementation will bring a lot of benefits in comparison to a large company that operate on multiple markets. And that is the main reason they are not interested in transferring all their operations to the cloud.

Their data is stored locally, in a server room that is on-site. They also backup their data on secondary storage devices that are off-site. And according to Mr. Dimovski, when it comes to their security protocols: "We have disaster recovery plans in place, so we can deal with any situation that impacts the data. When it comes to cyber-attacks, we have a firewall and intrusion prevention systems that take care of those risks."

3.4 Comparing and discussing the findings

For the purpose of comparing and discussing the results, I am using the same grouping methodology as the one used for grouping the questions. The answers are separated in 4 different groups that make the comparison easy to follow.

- General information about the company – Name, industry and size of the organization. This part helps with getting to know the details for every company that took part in the interview. To make it easy to follow, the column *"Name of company"* is a part of every table in order to make it easier for the reader to follow and not get confused while reading the results.
- Relevant software information – Here, I summarized in few words the most common cloud computing services and/or programs or non-cloud programs the companies use in their daily operation.
- Business implications – The focus here falls on the main reasons why the decision to implement or not to implement cloud computing was made.
- Risks associated with the cloud – Presented here is the information gained from users and non-users about how they are prepared for the risks and threats from using or not using cloud computing in their daily work.

Following are the results and findings of the interviews.

Table 4: General information

Interview	General information		
	Name of interviewee	Position / Role	Name of company
1	Ana Ilic	Digital Trade Content executive	Philip Morris International
2	Nenad Stojanovski	DevOps Engineer	Zeppelin Lab GmbH
3	Dragi Šterjov	Accounting Manager / Owner	Ekom-D
4	Vladimir Dimovski	Financial Director	Expanda

Source: Own work.

Table 4, presents an overview of some general information about the companies interviewed. To understand whether the industry a company operates in is relevant to the implementation of cloud computing, it was important to include different types of companies for the research. Another factor that could be relevant to the implementation is the size of the company. Again, having this in mind, in this research there are representative companies accordingly. Lastly, all the participants had different roles in their companies, but they are all positions that would benefit from the cloud computing implementation.

Table 5: Relevant software information

Interview	Relevant software information					
		Information about the cloud service			Information about the software used by the company	
	Name of company	Name od cloud service provider	Type of service model	Type of deployment model	Name of application used	Where do you store your data
1	Philip Morris International	Salesforce.com	SaaS/PaaS	Private cloud	N/A	N/A
2	Zeppelin Lab GmbH	AWS / Adobe Experience Cloud	SaaS/PaaS/IaaS	Hybrid cloud	N/A	N/A
3	Ekom-D	N/A	N/A	N/A	MIL fmm	On the MIL fmm program and additional disk
4	Expanda	N/A	N/A	N/A	Expanda	On-site server room and secondary storage devices that are off-site

Source: Own work.

Looking at Table 5, it is apparent that the questions are connected to the software and/or programs the companies use currently in their day-to-day activities. Both cloud computing user companies are using a private cloud as a deployment model. When it comes to the provider, they have chosen one of the most common and known companies Salesforce, Amazon Web Services and Adobe Experience Cloud. As expected, businesses usually use the SaaS and PaaS service models.

The non-cloud computing user companies have chosen to use programs that are altered to their specific needs. “Ekom – D” are using a private program by the name of MIL fmm 20 (the numbers change with the yearly update) and Expanda are using their own application as well, named after the company itself. For storing their data, both of the companies are using additional storage disks (hardware), but “Expanda” has an on-site server rooms as well.

Table 6: Business implications

Interview	Business implications						
		CC Users		Non CC users			
	Name of company	Reason for business decision	How did the business model evolve	Have you ever heard of cloud computing?	Are you aware of the benefits?	Have you ever considered transferring your business processes to a cloud environment?	What is the company's biggest obstacle / difficulty regarding the implementation of cloud services?
1	Philip Morris International	Cost Efficiency, Time management, Scalability	Faster implementation	N/A	N/A	N/A	N/A
2	Zeppelin Lab GmbH	Cost Efficiency, Time management, Increased resources for R&D, Creative solutions	Reducing hardware costs, Increasing revenues and future implementation of the service to new affiliates across the company	N/A	N/A	N/A	N/A
3	Ekom-D	N/A	N/A	Yes	Yes	Yes	Time consuming, Not satisfied with provider, data security concerns
4	Expanda	N/A	N/A	Yes	Yes	Yes	GPS integration problems, Not enough benefits to justify the switch

Source: Own work

Table 6 covers the third group of questions, I was more focused on the answers from the non-CC users. The interesting element that stood out for both of the companies is that they were not satisfied with the provider of the cloud and how their program was not able to adjust their needs. Expanda also pointed out that they do not believe that the benefits of the cloud are going to be as impactful because of the company's size. The CC user companies gave the basic and standard answers about the benefits the cloud enables for them as companies, but also pointed out how it was beneficial from the process standardization point of view, being international companies.

Table 7: Risks associated with CC

Interview	**Risks associated with CC**								**Conclusion**
		CC Users					**Non CC Users**		
	Name of company	Risk awareness	Standards awareness	Standard compliance	Experienced difficulties	Established protocols	Security / availability issue regarding your data storage	Protocols when facing data security issues	Overall satisfaction
1	Philip Morris International	Yes	Yes	The company is compliant with all local and international regulative and standards.	Data vulnerability, data leakage, abuse of data	Business Continuity Plan, Various teams globally	N/A	N/A	4
2	Zeppelin Lab GmbH	Yes	Yes	The company is compliant with AWS standards	Data vulnerability, data leakage, DDOS	Routine check-ups, responsible teams	N/A	N/A	5
3	Ekom-D	N/A	N/A	N/A	N/A	N/A	Yes, but quickly restored because of the back up storage	No official protocols and policy. Just a back up disk that is updated every day	1
4	Expanda	N/A	N/A	N/A	N/A	N/A	No	Disaster recovery plans, Firewall and intrusion prevention systems	2

Source: Own work

The last group of questions shown in Table 7 are the most detailed and relevant to the thesis. The CC user companies have often experienced the standard security difficulties (data loss, data leakage, abuse of confidential data, DDOS attacks...). They are aware of the security threats and are taking measures. They are compliant with different standards and are frequently educating their employees about CC and the potential issues connected to the subject. Overall, the CC user companies are very satisfied with the cloud services and plan to expand to other sectors in the near future.

"Ekom – D" has experienced data loss on several occasions, but have recovered it quickly. Their actions connected to security issues are mainly related to data loss (taking into account that losing their data is their main fear). The only safety net is the hardware disk they use daily to store the data (daily update with new information). They are satisfied with their choice of program and are not planning to change it with CC because they are not sure if the cloud providers would be able to secure the data stored. "Expanda" has not experienced any kind of security issues with their program so far. They have disaster recovery plans in place of an emergency and firewall prevention systems as well. Their main reason for not using CC is not the security issues connected to it, but the fact that the GPS cloud service could not integrate with their core system and/or the problems with their cloud computing service provider. These findings are somewhat surprising given the fact that other researches show that security issues are far bigger reason for not implementing cloud computing.

One concern about the used interview method is that the results are difficult to compare because the interviewed companies fall on the two ends of the spectrum, two being relatively small companies and two being large international corporations. Although presented with the above-mentioned difficulty, I was able to get an insight regarding the decision-making within the companies. The key findings I managed to take away from the concluded interviews present two things:

First, the decision a company makes about implementing a cloud computing solution is solely based on whether their business needs outweigh the costs of implementation. This is evident from the answers given by the two relatively small companies implying that the costs of implementing cloud computing outweigh the benefits. On the other hand, the corporations opted for cloud computing because the investment in the cloud computing solution made sense and had a great impact on their overall business. It helped them standardize their work processes across their multiple affiliates, solve data sharing problems and improve time efficiency.

Second, all of the four companies have a basic awareness of the security and privacy risks connected to cloud computing. The companies that decided to implement CC established an infrastructure in order to prevent and detect any possible issues prior to the implementation. Using their CC solutions they have built upon that basic infrastructure by either having dedicated teams or a machine learning software. Their security protocols are constantly improving in order to keep pace with the new technologies and possible threats. Because they have the sufficient funds they can also invest in the education of their employees. With that they address one of the biggest potential risk in CC - human error (Maraž, 2016).

4 THE CLOUD AND INDIVIDUAL USERS

Even though the most common cloud users are usually companies and organizations, the wide spread implementation of the cloud technologies has indirectly made us all private cloud users.

For the purpose of this part of the thesis, the focus falls on SaaS considering the fact that IaaS and PaaS are mostly suitable for organizations. For personal use, SaaS provides the services and solutions via the Internet rather than a product that has to be installed on a computer. Usual examples of SaaS for companies include CRM applications like Salesforce and data applications by Coghead. Nevertheless, people use cloud based services every day and they are not always aware of it. Whether it is for entertainment (ex. Netflix, Spotify, Facebook), education (Google Docs, Zoom, Amazon Web Services), data storage (Dropbox, Gmail, iCloud), all of the services and applications, are mostly cloud based (Wyld, 2009, p. 3.). SaaS for personal use can be separated in two dimensions: cloud services and cloud storage (Ambrose & Chiravuri, 2010).

4.1 Research methodology

Having all of this in mind, I decided to do an online questionnaire were I would inquire about the individual’s personal use of cloud computing (services / storage) and their fears regarding the security. Considering the fact that we live in a digital era, there are very few examples of people that do not use any type of cloud-based service. Many of the most common applications used for communication (ex. Viber, Skype and WhatsApp) are technically cloud based, because they backup the user’s data on the cloud. In 2020, almost everybody uses communication applications and therefore it would be very hard to collect data from actual non – cloud users.

As previously stated, the research goal of the thesis is to see if users are aware of the security issues and whether they are prepared and taking appropriate actions regarding the threats. The hypothesis is that users are aware of the security issues and are taking appropriate actions.

The questionnaire I used had 14 questions. The design of the questionnaire was tailored specifically by myself in order to capture the knowledge and opinion of private cloud computing users regarding the risks associated with the technology. Surpisingly, there were not as many researches connected to the private use of cloud computing services as

I expected. Therefore, the services I listed in the questionnaire are based on the most popular reasons why and how individuals use cloud computing services in their everyday life: data storage, productivity, entertainment and communication. My questions were also inspired by the survey used in the research article “Better Safe than Sorry: A Study of Investigating Individuals’ Protection of Privacy in the Use of Storage as a Cloud Computing Service” (Visinescu, Azogu, Ryan, Wu, & Kim, 2016).

The selection of cloud services was made based on my personal opinion and combination of various researches (Athow, 2021; Shakeabubakor, 2015).

The questions are organized along four thematic blocks:

- Demographic: These are standard demographic questions with which I wish to gain a better understanding whether the age, gender and education level affect the use of CC.
- General CC knowledge: With these questions, I want to determine the level of understanding of the surveyees regarding the CC. The results from these questions I plan to compare with the demographic results, and determine the correlation, if one exists.
- The use of CC: This block of questions will determine which are the most used applications / services of the population sample. It will also provide me with a better understanding about the reasons the respondents chose to use CC.
- Risks associated with CC: Questions from the fourth block cover several aspects of the risks, awareness, attitude, knowledge, experience.

The questionnaire combined multiple-choice questions with predefined answers offering respondents the possibility to choose and rank among several options and questions that provided the possibility to grade a certain statement on a “very low” to “very high” scale. Several questions are semi open-ended providing the surveyees the option to specify their answer.

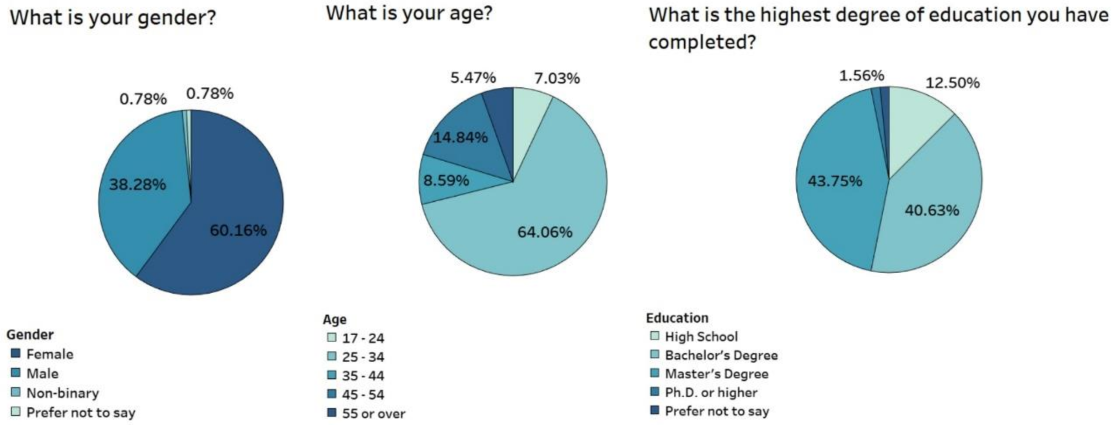
The targeted population is all private (individual) users and non-cloud computing users. Because my questionnaire will be published on my social media account for completing, the accessible population is 1720. My margin of error is 7% and confidence level is 90%. The total sample size is 128 surveyees.

Following, the results of the survey are presented and discussed.

4.2 Conducted survey results

The visualization of the results is done with the help of the application Tableau.

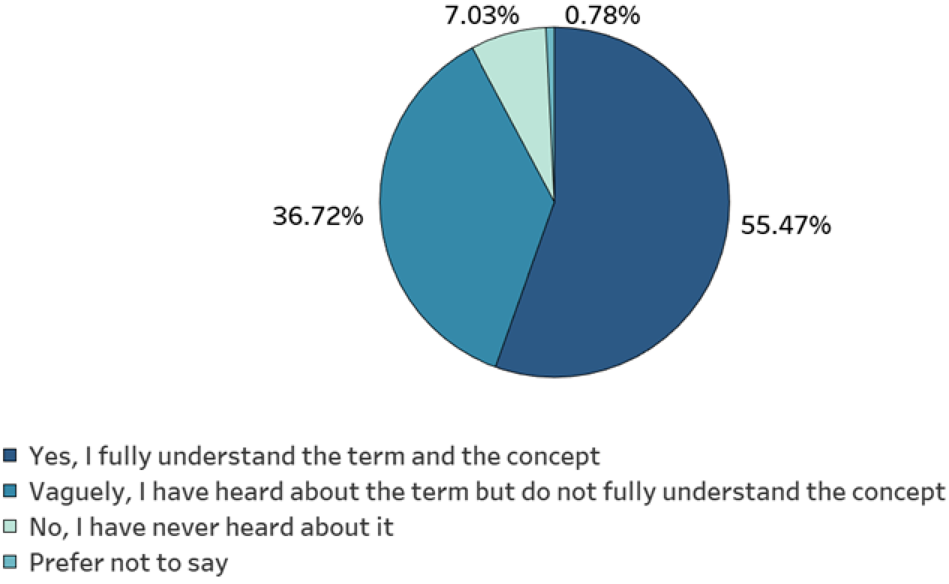
Figure 2: Demographic questions



Source: Own work.

The Demographic thematic block of the questionnaire, consisting of questions regarding the gender, age and level of education, yielded the results shown in Figure 2. Out of 128 questionnaire respondents the gender proportion was 60.2 % female, 38.3% male and 1.5% other. The majority of respondents belong to the 25-34 age group 64.1%, while the second largest represented age group is the 45-54 with 14.8%. When it comes to the level of education, Bachelor’s Degree and Master’s Degree combine for 85.4% while a High School level education is represented by 12.5%.

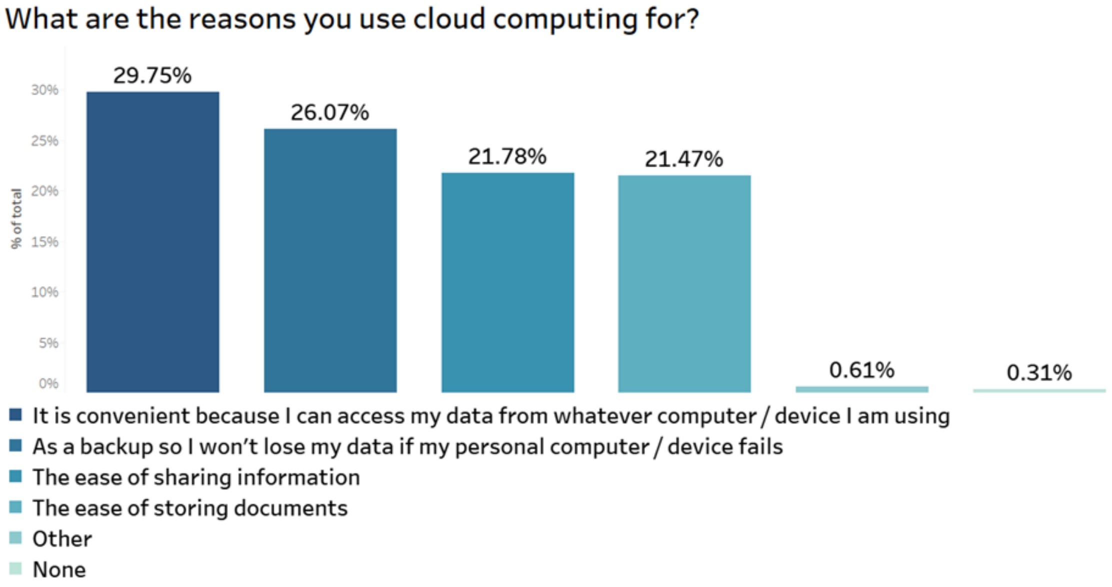
Figure 3: General CC knowledge



Source: Own work.

In the general cloud computing knowledge block, with the forth question it was important to determine the respondents’ understanding of the concept of cloud computing prior to discussing the risks associated with the use. The results presented in Figure 3, show that only a small minority of the respondents had never heard of the concept while the overwhelming majority fully understand it (55.5%), or have a vague understanding of the concept (36.7%). These results establish that the knowledge level of the respondents, regarding cloud computing, is very high. This gives the answers to the following questions more weight and validity towards proving my hypothesis.

Figure 4: Reasons for using CC services

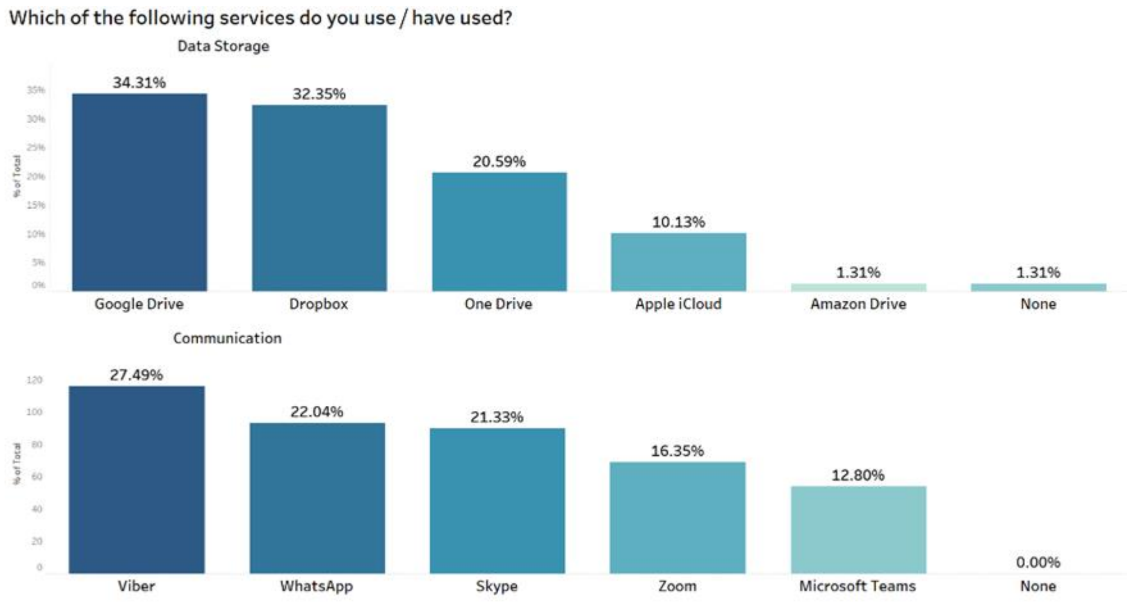


Source: Own work.

In the use of cloud computing block of the questionnaire, I wanted to focus on what the respondents used the cloud computing services for. As shown in Figure 4, the convenience of remotely accessing your data on the cloud (29.75%), along with using the cloud to back up your data (26.07%), were the reasons chosen the most by the participants. However, the ease of sharing (21.78%) and storing (21.4%) information were close behind. The results show that even though only (55.5%) of the participants fully understood the concept of cloud computing as a term, when shown some of the use cases and cloud computing services, they were able to clearly understand and choose from one of them.

What stands out in is the high rate of answers that show how many people actualy are aware of cloud computing services and their purpose. Surprisingly, only a minority of respondents have a vague or no representation of what cloud computing really is and what it represents. My expectations were not at all same with the results gotten. This can only confirm my hypothesis additionally.

Figure 5: The use of specific CC services



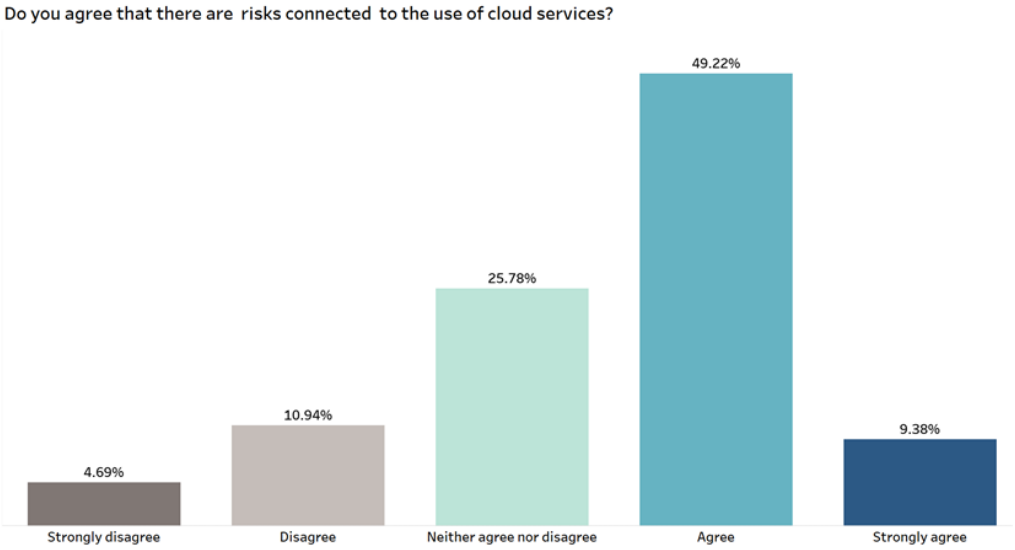
Source: Own work.

The second question in this block, delved into the use of specific cloud computing applications and services, shown in Figure 5. In the data storage portion of the question, Google Drive with (34.3%) and Dropbox with (32.4%) stood above the rest of the options. Following them, were One Drive with (20.6%) and Apple iCloud with (10.1%). The least popular answer was Amazon Drive with (1.3%).

In the Communication portion of the question on the other hand, the responses were less skewed. Viber with (27.5%) was chosen the most but the other options were not far behind, with WhatsApp (22.0%), Skype (21.3%), Zoom (16.4%) and Microsoft Teams (12.8%). According to a new report, as of 2020, Android is the operating system for 71.22 % of European mobile phones (StatCounter GlobalStats, 2021). This is well mirrored in the results from my survey as Google Drive and Dropbox are the leading choice. Based on the research from DataReportal (2021), the most popular global mobile communication apps as of January 2021 were WhatsApp, with 2000 million users followed by Facebook Messenger with 1300 million users. My survey results show that Viber was the most selected application for communication followed by WhatsApp. The divergence from the global trends were expected due to the popularity of Viber in the Balkan region, coupled with the fact that the majority of the respondents come from that region.

We have to take into consideration that the questionnaire was executed during the COVID-19 pandemic, and that factor may have had an effect on the results. Prior to the pandemic and the increase of working from home, the need for video communication and sharing data online and was not as prevalent.

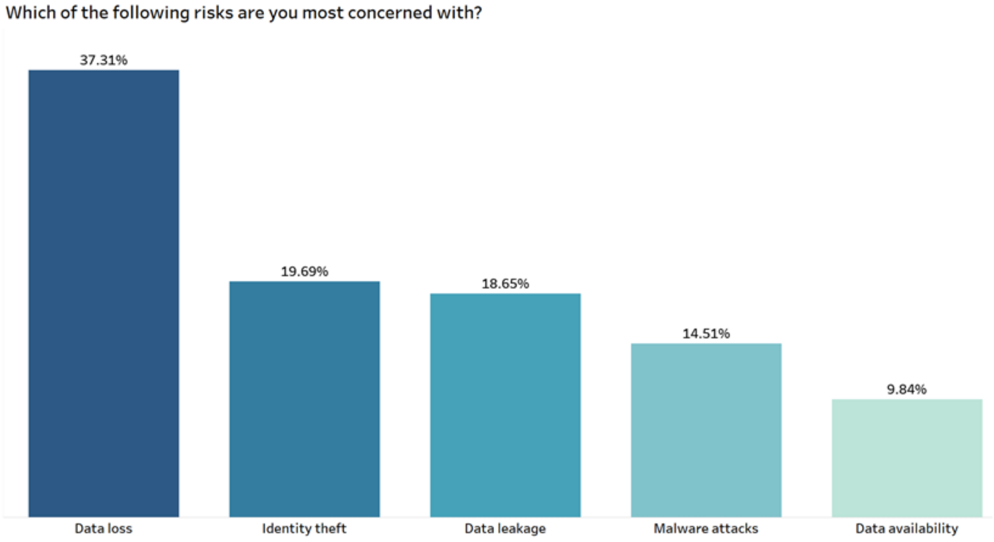
Figure 6: Likert scale – Risks connected to CC



Source: Own work.

The fourth block of the questionnaire was dedicated to the risks associated with the use of cloud computing services. The first question in the section asked the participant how strongly they agreed with the statement, that there are risks connected with the use of cloud services, as shown in Figure 6. The respondents overwhelmingly responded that they agree (49.2%) or strongly agree (9.4%). (25.8%) were in the middle and only a combined (15.6%) disagreed with the statement. This shows that the respondents are aware of the potential risks.

Figure 7: Risks connected to CC

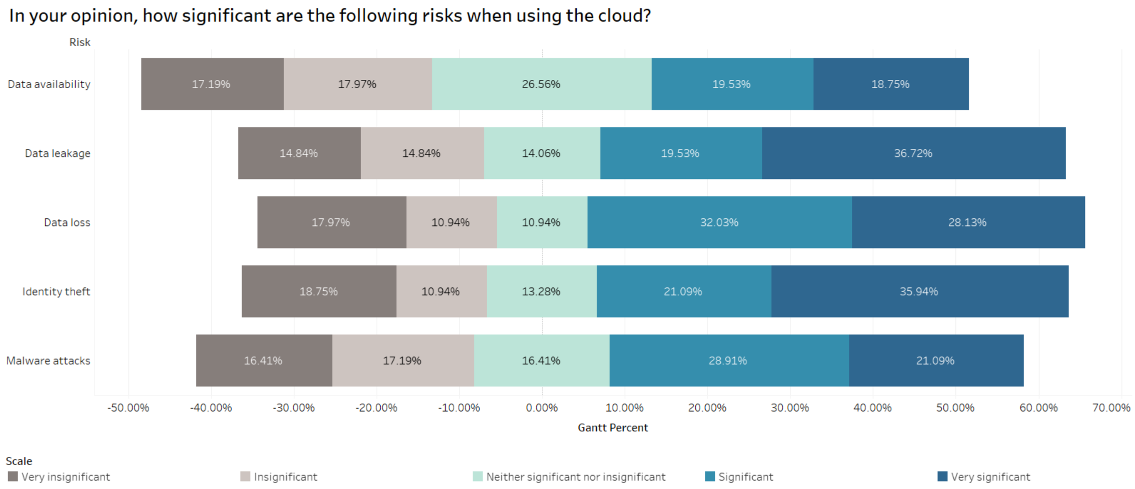


Source: Own work.

Figure 7 shows the results for the risks that the individual users chose to be most concerned with. The risks are divided into 5 major groups: Data loss, Identity theft, Data leakage, Malware attacks and Data availability.

A brief explanation and an example was given for each of the groups, in order to ensure that the participant fully understands the possible options. (37.31%) of the participants were mostly concerned with losing their data stored on the cloud. (19.69%) were concerned with identity theft and (18.65%) with having their data leaked. Only (14.51%) chose the risk of malware attacks and (9.84%) the risk of having their data be unavailable when needed.

Figure 8: Scale of significance of CC risks



Source: Own work.

After asking the participant what risk they are most concerned with, in this following question, I asked them to express their opinion on the significance of the risk associated with each risk group, as shown in Figure 8.

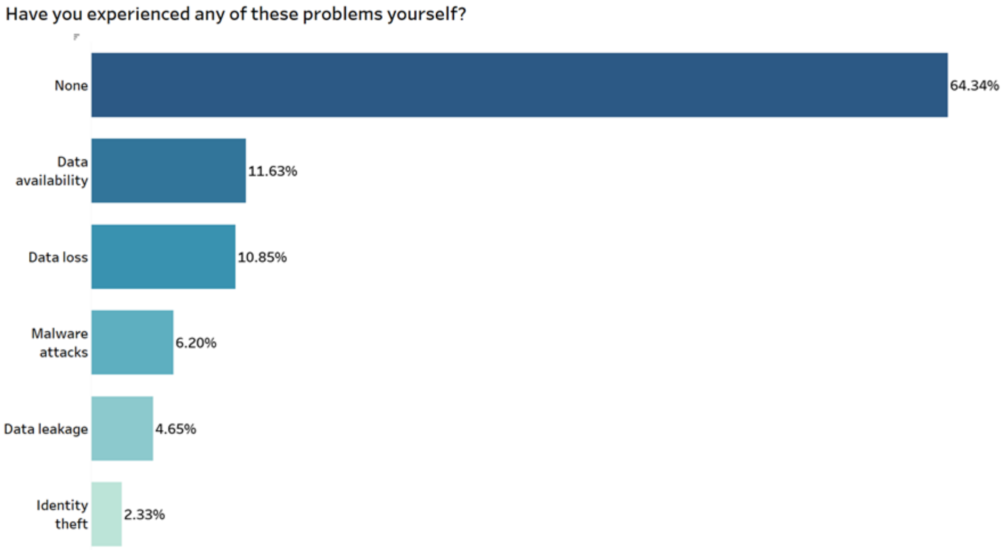
To best display the results from the Likert Scale, I used the multidimensional visualisation. The reason for using this method to display the data is because it clearly shows how the results skew to one or the other side of the axis. To determine the axis first, I divided the answers in 3 categories: Negative (Very Insignificant, Insignificant), Neutral (Neither significant nor insignificant) and Positive (Significant, Very Significant).

Second, I set the axis point (0.0%) to start in the middle of the Neutral category, so the Positive results can stack on the right side and the negative on the left, while the Neutral results are always in the center.

Finally, I chose grey tones to display the Negative results, which represent the participants that feel the risks are not significant, mint for the Neutral and blue tones for the Positive results that show the participants who feel that the risks are significant.

By displaying the results in this manner I was able to connect the results from the previous question and clearly see that the participants associate a higher risk significance to the risk group they are most concerned with. The answers for data loss, data leakage and identity theft are skewed more towards the positive side, that represents the opinion that the risks are significant. While the answers for malware attacks and data availability are more evenly distributed.

Figure 9: Experience with CC problems

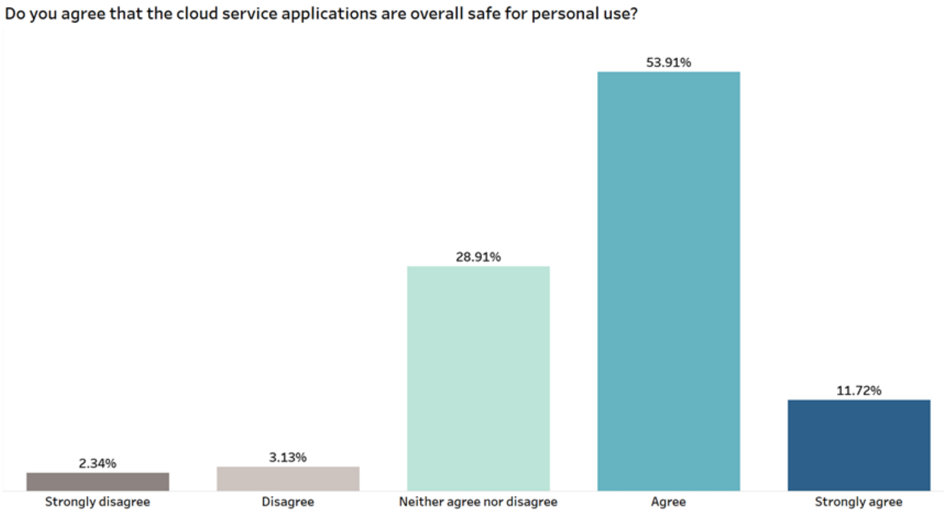


Source: Own work.

When asked if they had experienced any of the issues that arise from the risks in the previous questions, the overwhelming majority (64.1%) of the participants responded with none, as shown Figure 9. The remaining (35.9%) experienced data availability issues (11.7%), data loss (10.9%), malware attacks (6.3%) and data leakage issues (4.7%). The high percent of respondents that did not experience any of the problems may be connected to the amount of measures the respondents have taken to prevent these problems (Figure 11).

Considering the high possibility of security attacks and threats and the constant use of social media platforms and data storage services, it is surprising to see that a lot of the respondents have not experienced any issues. Even though, cloud service providers boast about their cumbersome security protocols, it has been proven in the past that they are vulnerable to attacks and breaches. Two prime examples are the Dropbox hack in 2012 that leaked 68 million of their users' passwords online, and the similar Google Drive hack in 2014 that leaked 5 million passwords (Hill, 2014). This prompted Dropbox to implement a 2FA (BBC News, 2016).

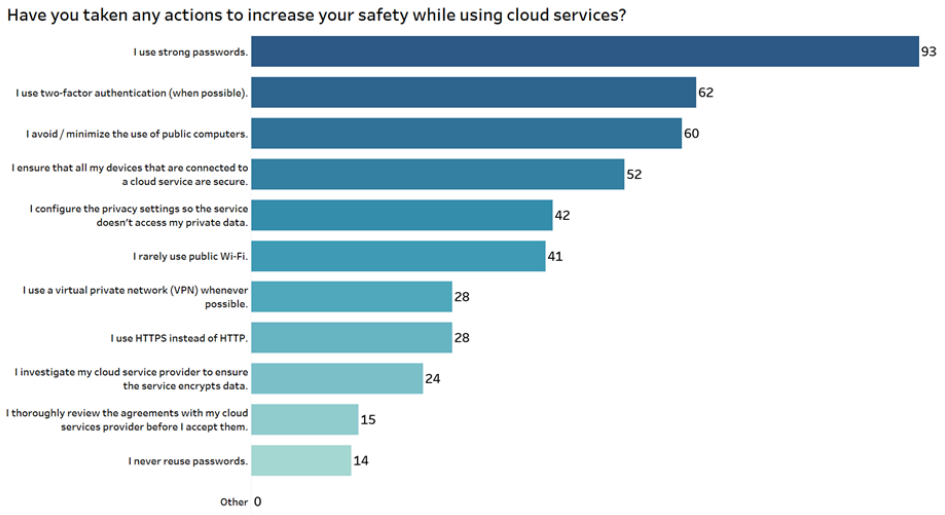
Figure 10: CC services risks



Source: Own work.

As shown in Figure 10, even though a majority of the participants (combined 58.6%) agreed that there are risks connected to the use of cloud services, (53.91%) Agree and (11.72%) Strongly agree that they are safe for personal use. (28.91%) are in the middle and a small minority of (combined 5.47%) feel that the cloud service applications are not safe for personal use. (Figure 10) These results coincide with the answers from the previous questions, where over (64%) of the respondents said that they had not experienced any problems while using the cloud computing services.

Figure 11: Actions taken for safety



Source: Own work.

Finally, the participants were asked what specific measures had they taken to increase their safety while using the cloud services, referring to Figure 11. Using strong passwords was the most common measure that (72.6%) of the participants in the survey selected. Next were the use of two-factor authentication with (48.4%) and minimizing the use of public networks with (46.8%). The least selected measures were reviewing agreements before accepting them with (11.7%) and never reusing passwords with (10.9%). These results prove that the respondents were aware of the potential risks and thus have taken actions to prevent any problems directly affecting them. Since more than (64%) had not experienced any issues in the past, the measures they had taken are proven to be effective. However, as the cloud technology is evolving and growing by the day, so are the new possible risks and threats.

The findings from questions 3-6 confirm the first part of my initial hypothesis that private cloud computing users are aware of the security issues and risks present with 90% of certainty. When it comes to the second element, whether users are taking appropriate actions regarding those risks (last question of the survey), this was also confirmed because on average a respondent chose 3, 5 of the possible listed measures.

5 SUGGESTIONS FOR IMPROVEMENT FROM MY EXPERIENCE

The most obvious finding to emerge from the analysis is that nowadays, it is difficult for businesses and/or individual users to go through a day without using the cloud. But, with the constant growth and development it goes without saying that our cloud stored data is constantly under threat.

To avoid the "another day, another data breach" possibility, users need to be not only aware of the threats, but also prepared for them (Martinez, 2013). When it comes to individual users, there are numerous tips and actions that help with keeping the data safe while on the cloud. No matter how simple and obvious they are, people often forget about them and/or consider them negligible:

- Password manager: Everybody is aware of the importance of a good and strong password. But, not everybody is obliged to the golden rule for online safety – use a different, random password for each account. Because a lot of users are not capable of remembering them, a good and useful tool is installing a password manager. Password managers can create distinctive, complex passwords for every site and store them. They can be used as a browser extensions or mobile apps that populate login pages with your username and password for you (with your approval).
- Use two-factor authenticator: 2FA, is an additional phase added to your logging-in process. Think of it as a code sent to your phone or a fingerprint scan, that helps you and makes the act of stealing your cloud kept data twice as hard to steal.

- Encrypt your valuable data: Encryption results with encoded data and keeps it hidden from or unreachable to unwanted and unauthorized users. It helps protect your private information and delicate data.
- Social media privacy: Social media services make it extremely easy for you to share your life online, but it’s easy to wind up sharing too much. With this you and your data become an easy target to all data security breaches.
- Clear your cache: One advice that individual users have to take away from this is to never underestimate your browser. Your browser's cache knows everything about you. The saved searches and cookies, the Web history could easily point to your sensitive data (home address or family information). Turning off the “Save Password” feature in browsers is also another tip that helps users with their cloud safety.

On the other hand, something that stood out in the interviews made with the companies is that they often forget about the possible human error. That is why, a lot of the suggestions mentioned are connected to the people using the CC services.

- Education and training: Preparing the employees is considered to be the base and starting point for all companies. Having a healthy and stable foundation means a lot, and it sure helps with the correct cloud computing employment.
- Use two-factor authenticator: Using 2FA, is important for keeping all business and sensitive data protected. Installing a 2FA app for all your employees is an additional measure that will definitely be an obstacle for data breaches.
- VPN usage: Making sure that the employees use a VPN can avoid web browsers and others from accessing your connection while keeping the information you send and receive anonymous and secure.
- Encrypt your valuable data: Cloud computing providers that collect, store and use personal data have to comply with the latest laws and regulations regarding the data privacy (ex. GDPR in Europe and CCPA in California USA). The most common method that companies use is data encryption. There are several popular encryption methods and algorithms and companies usually choose the one that is in line with their business logic.
- Legal compliance and risk management: The cloud computing providers are required to have consent from their customers in order to be able to collect, store and process their data. These conditions are incorporated in the legal contract that each customer is required to sign before they start using the services from the cloud computing provider.

All things considered, we have to keep in mind that there is never just one solution that will help up avoid the security risks while using cloud computing services. This list consists a lot of common measures. Even so, people often forget about the fact that even the simplest solutions, combined together can bring the necessary result. These world-wide known suggestions can in fact help you in the battle of keeping your sensitive data safe while kept on the cloud.

CONCLUSION

This study was not set out to prove whether cloud computing has a meaningful role in our everyday lives. Even though the term and technology are somewhat new, it is clear that cloud computing services are here to stay. The purpose of the study was to gain a better understanding of the impact that they have on the users.

Even with the countless benefits provided (quick deployment, cost efficiency, large storage space and easy access to the system anytime and anywhere), users of cloud computing also encounter a vast number of data security challenges simultaneously.

Returning to the question posed at the beginning of this study, it is now possible to state that according to the research findings, users are aware of the security risks that cloud computing services bring and are somewhat prepared for them.

The study has some potential limitations. The first is the sample size. The results of the thesis cannot be generalized given the small sample size of 4 companies for the interviews and 128 surveyees. Although the companies in question represent different industries and different sizes, the cloud computing experience from one representative cannot be generalized for the whole group of companies from the same type. This also refers to the results from the survey. Considering the widespread use of CC services in our everyday life, 128 answers cannot give us a full picture of the current situation. The second limitation concerns the selection of the sample. Because of the pandemic, there was also the limit of communication and option to select a true random sample. The survey was posted on Facebook and the people who responded may not truly be an example of a random sample. However, the results point that the obvious solution for a better CC implementation and adoption depends hugely on the awareness and preparedness of the users.

During the process, it was clear that a lot of the existing studies focus only on the business users of cloud computing. What is now needed is a cross-national study involving individual users of CC as well.

In conclusion, the security risks and issues are not something that can be completely avoided when it comes to the use of cloud computing. There is also not a single perfect solution for easy adaptation and implementation. It is a mix of knowledge and preventive actions that are changing and updating, while following the fast movement trends of new technologies. Users need to develop deeper understanding and what can CC actually provide them with i.e. the benefits and pitfalls of implementing it. With this, they will not only prepare for the risks, they will also eliminate the fear of changes and the unknown, and solely focus on enjoying the benefits provided.

REFERENCE LIST

1. Aldossary, S., & Allen, W. (2016). Data Security, Privacy, Availability and Integrity in Cloud Computing: Issues and Current Solutions. *International Journal of Advanced Computer Science and Applications (IJACSA), 7*(4). 485-496.
2. Ambrose, P., & Chiravuri, A. (2010). An Empirical Investigation of Cloud Computing for Personal Use. *Association for Information Systems*, *3*. Retrieved February 20, 2020 from https://aisel.aisnet.org/cgi/viewcontent.cgi?article=1023&context=mwais2010
3. Ambrose, W., Dagland, N., & Athley, S. (2010). *Cloud Computing: Security Risks, SLA and Trust*. Retrieved September 14, 2019 from https://www.diva-portal.org/smash/get/diva2:323596/FULLTEXT02.pdf
4. Anitha, Y. R. (2016). Security Issues in Cloud Computing. *International Journal of Thesis Projects and Dissertations (IJTPD)*. Retrieved October 10, 2020 from https://www.researchpublish.com
5. Arora, P., Wadhawan, R.C., & Ahuja, E.S.P. (2012). Computing Security Issues in Infrastructure as a Service. *International Journal of Advanced Research in Computer Science and Software Engineering. 2*(1), 1-7.
6. Ashktorab, V., Taghizadeh, S.R., & Mokhtar, H. (2012). Security Threats and Countermeasures in Cloud Computing. *International Journal of Application or Innovation in Engineering & Management (IJAIEM). 1*(2), 254-260.
7. Asma, A., Chaurasia, M.A., & Mokhtar, H. (2012). Cloud Computing Security Issues. *International Journal of Application or Innovation in Engineering & Management (IJAIEM). 1*(2), 144-146.
8. Athow, D. (2021). *Best cloud storage services of 2021*. Retrieved April 13, 2020 from https://www.techradar.com/news/the-best-cloud-storage
9. Backe, A., & Lindén, H. (2015). *Cloud Computing Security: A Systematic Literature Review (Degree project)*. Retrieved August 17, 2020 from https://www.diva-portal.org/smash/get/diva2:825307/FULLTEXT01.pdf
10. Bauer, E., & Adams, R. (2012). *Reliability and Availability of Cloud Computing* (1st edition). New Jersey: Wiley.
11. BBC News. (2016). *Dropbox hack "affected 68 million users."* Retrieved August 31, 2020 from https://www.bbc.com/news/technology-37232635
12. Beimborn, D., Miletzki, T., & Wenzel, S. (2011). Platform as a service (PaaS). *Business & Information Systems Engineering, 3*(6), 1-384.
13. Bhuvaneshkumar, M., Anitha, G., Kalarani, X. A., & Gunasundari, R. (2014). Cloud Computing Security from Single to Multi-Clouds. *International Journal of Emerging Technologies in Computational and Applied Sciences (IJETCAS)*. Retrieved April 20, 2020 from http://iasir.net/IJETCASpapers/NCRICA.pdf

14. Bisong, A., & M. Rahman, S. S. (2011). An Overview of the Security Concerns in Enterprise Cloud Computing. *International Journal of Network Security & Its Applications, 3*(1), 30–45.
15. Bohara, B., Mulay, S., & Jain, S. (2015). Cloud Computing: Security inside the Cloud. *International Journal of Computer Science and Information Security, 15*(8), 1–4.
16. Canalys. (2020, November). *Global cloud infrastructure market Q3 2020*. Retrieved March 5, 2021 from https://www.canalys.com/newsroom/worldwide-cloud-market-q320
17. Chaudhary, J., & Mishra, A. (2016). Literature Review: Cloud Computing-Security Issues and Data Encryption Schemes. *MIT International Journal of Computer Science and Information Technology, 6*(1), 1–3.
18. Chen, D., Zhao, H., & Ahuja, E.S.P. (2012). Data Security and Privacy Protection Issues in Cloud Computing. *International Conference on Computer Science and Electronics Engineering. 2*(1), 647-651.
19. Cloud Security Alliance. (2013). *The Notorious Nine Cloud Computing Top Threats in 2013*. Retrieved March 15, 2020 from http://www.cloudsecurityalliance.org/topthreats
20. Cloud Security Alliance. (2017). *The Treacherous 12 – Top Threats to cloud computing + Industry Insights*. Retrieved March 15, 2020 from https://downloads.cloudsecurityalliance.org/assets/research/top-threats/treacherous-12-top-threats.pdf
21. Dandekar, P. (2016). *What is the right hybrid cloud mix for you?*. Retrieved May 17, 2020 from https://www.kelltontech.com/kellton-tech-blog/what-right-hybrid-cloud-mix-you
22. DataReportal. (2021). *Digital 2021 April Global Statshot Report*. Retrieved May 2, 2021 from https://www.statista.com/statistics/258749/most-popular-global-mobile-messenger-apps/
23. El-Gazzar, R., Hustad, E., & Olsen, D.H. (2016). Understanding cloud computing adoption issues: A Delphi study approach. *Journal of Systems and Software, 3*(2), 64–84.
24. Foote, K. D. (2017). *A Brief History of Cloud Computing.* Retrieved 18 January, 2020 from http://www.dataversity.net/brief-history-cloud-computing/
25. Gartner, Inc. (2008, June). *Assessing the Security Risks of Cloud Computing*. Retrieved January 17, 2020 from https://www.gartner.com/en/documents/685308/assessing-the-security-risks-of-cloud-computing
26. Gong, C., Liu, J., Zhang, Q., Chen, H., & Gong, Z. (2010). *The Characteristics of Cloud Computing*. 39th Intl. Conf. on Parallel Processing Workshops, 275–279.
27. Griffith, E. (2016). *What is Cloud Computing?*. Retrieved June 29, 2020 from https://www.pcmag.com/article/256563/what-is-cloud-computing

28. Hill, K. (2014, September 11). *Google Says Not To Worry About 5 Million "Gmail Passwords" Leaked*. Retrieved May 2, 2021 from https://www.forbes.com/sites/kashmirhill/2014/09/11/google-says-not-to-worry-about-5-million-gmail-passwords-leaked/?sh=5e0829b27a8d
29. Hurwitz, J. S., Kaufman, M., Halper, F., & Kirsch, D. (2012). *Hybrid Cloud for Dummies* (2nd ed.). Hoboken, New Jersey: John Wiley & Sons.
30. I.D.C. (2019). *Worldwide Public Cloud Services Spending Forecast to Reach $210 Billion This Year, According to IDC*. Retrieved 25 December, 2019 from web adress https://www.idc.com/
31. Ikhar, N. M. I., Meghal, S. S., & Satpute, K. S. (2014). Cloud Based Security. *International Journal on Recent and Innovation Trends in Computing and Communication, 2*(3), 513–518.
32. Inam ul Haq, M. I. H. (2013). *The major security challenges to cloud computing* (Master thesis). Borås: University of Boras, Sweden. Retrieved August 17, 2020 from https://www.diva-portal.org/smash/get/diva2:1309139/FULLTEXT01.pdf
33. ISACA. (2015). *Cloud Computing Market Maturity*. Retrieved January 10, 2021 from https://downloads.cloudsecurityalliance.org/assets/research/collaborative/Cloud-Computing-Market-Maturity_whp_eng_0715.pdf
34. Jansen, W., & Grance, T. (2011). *Guidelines on Security and Privacy in Public Cloud Computing*. Retrieved January 17, 2020 from https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-144.pdf
35. Kajiyama, T. (2012). *Cloud Computing Security: How Risks and Threats Are Affecting Cloud Adoption Decisions* (Master thesis). Retrieved July 13, 2020 from https://www.researchgate.net/publication/320206981
36. Ko, R., & Choo, R. (2015). *The Cloud Security Ecosystem* (1st ed.). Syngress. Retrieved May 26, 2020 from https://books.google.si/books?hl=en&lr=&id=meycBAAAQBAJ&oi=fnd&pg=PP1&dq=Ko,+R.,+%26+Choo,+R.+(2015).+The+Cloud+Security+Ecosystem+(1st+ed.).+Syngress.&ots=E86mG68EOu&sig=rQGuT45yrdumF3b6KABEBG-l7_E&redir_esc=y#v=onepage&q&f=false
37. Kotnik, M. (2017). *Primerjalna analiza varnosti oblačnih storitev* (Bachelor thesis). Maribor: Univerza v Mariboru, Ekonomsko – Poslovna Fakulteta. Retrieved August 17, 2020 from https://dk.um.si/IzpisGradiva.php?id=67706
38. Kovačič, M. (2015). *Cloud Computing and Data Protection* (Bachelor thesis). Maribor: Ekonomsko - Poslovna Fakulteta.
39. KPMG & Oracle. (2020). Addressing Security Configurations Amidst a State of Constant Change. Retrieved May 23, 2021 from https://www.oracle.com/a/ocom/docs/cloud/oracle-cloud-threat-report-2020.pdf?fbclid=IwAR12HT41qNFCS5SseekAafdLJiTchVRWIhc60yiYRoWpZfainGsJWDKvR3o

40. Krishnan, R. (2017). *Security and Privacy in Cloud Computing* (Master thesis). Kalamazoo: Western Michigan University. Retrieved May 2, 2020 from https://scholarworks.wmich.edu/masters_theses/919/.
41. Kumar, A., Kumar, V., Singh, P., & Kumar, A. (2012). A Novel approach: Security measures and Concerns of Cloud Computing. *International Journal of Computer Technology and Applications*. Retrieved October 26, 2020 from https://scholar.google.si/scholar?q=kumar+A+Novel+approach:+Security+measures+and+Concerns+of+Cloud+Computing&hl=en&as_sdt=0&as_vis=1&oi=scholart
42. Kumar, P., & Bhatt, A. (2015). Literature Review: Cloud Computing Security Issues and Techniques. *International Journal of Computer Science and Information Security, 15*(8), 1–4.
43. Kuyoro, S.O, Ibikunle, F., & Awodele, O. (2011). Cloud Computing Security Issues and Challenges. *International Journal of Computer Networks .3*(5), 252-253.
44. Lobert, C. (no date). *7 Important Cloud Computing Statistics And Why They Matter*. Retrieved 25 December, 2019 from web address https://www.vcsolutions.com/7-important-cloud-computing-statistics-and-why-they-matter/
45. Maddineni, V.S.K., & Shivashanker, R. (2012). *Security Techniques for Protecting Data in Cloud Computing* (Master thesis). Karlskrona: School of Computing Blekinge Institute of Technology.
46. Manisha, T., & Rani, S. (2014). A Literature Review on Implementing Security in Cloud Environment. *International Journal for Research in Applied Science & Engineering, 5(6),* 2510–2513.
47. Maraž, N. (2016). *Človeški vidik varnosti računalništva v oblaku* (Master thesis). Kranj: Univerza v Mariboru.
48. Markun, T. (2015). *Varnost oblačnih sistemov za shranevanje podatkov* (Master thesis). Ljubljana: Fakulteta za elektrotehniko.
49. Martinez, D.J. (2013). *Privacy and Confidentiality Issues in Cloud Computing Architectures*. Barcelona: Polytechnic University of Catalonia.
50. Mell, P., & Grance, T. (2011). *Definition of Cloud Computing, Recommendations of the National Institute of Standards and Technology*. The National Institute of Standards and Technology. Retrieved October 5, 2019 from https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf
51. Mijuskovic, A., & Ferati, M. (2019, January). *User Awareness of Existing Privacy and Security Risks when Storing Data in the Cloud*. Retrieved November 17, 2020 form https://doi.org/10.4018/978-1-5225-8897-9.ch044
52. Mišigoj, N. (2013). *Zagotvljanje varnosti pri uporabi računalništva v oblaku* (Bachelor thesis). Maribor: Fakulteta za varnostne vede. Retrieved January 15, 2020 from https://dk.um.si/IzpisGradiva.php?id=42644

53. Mlitz, K. (2021). *Public cloud services market size 2017–2022*. Retrieved June 11, 2021 from https://www.google.com/search?q=Public+cloud+services+market+size+2017-2022+Published+by+Kimberly+Mlitz&rlz=1C1CHBF_enMK761MK761&oq=Public+cloud+services+market+size+2017-2022+Published+by+Kimberly+Mlitz&aqs=chrome..69i57.2345j0j7&sourceid=chrome&ie=UTF-8
54. Morsy, M.A., Grundy, J., & Müller, I. (2010). An Analysis of the Cloud Computing Security Problem. *APSEC 2010 Cloud Workshop*. Retrieved July 28, 2020 from https://www.cs.auckland.ac.nz/~john-g/papers/cloud2010_1.pdf
55. Nežič, B. (2016). *Zaupanje Slovenskih Podjetij v Računalništvo v Oblaku* (Bachelor thesis). Maribor: Fakulteta za organizacijske vede.
56. Osman, T. T. E. A., & Mustafa, A. B. A. N. (2015). Internal & External Attacks in cloud computing Environment from confidentiality, integrity and availability points of view. *Journal of Computer Engineering, 17*(2), 1–4.
57. Ou, Y. (2015). *The concept of cloud computing and the main security issues in it* (Bachelor thesis). Turku: University of Applied Sciences.
58. Popović, K., & Hocenski, Ž. (n.d.). *Cloud computing security issues and Challenges* (Working paper). Osiljek, Croatia: Institute of Automation and Process Computing Faculty of Electrical Engineering.
59. Qaisar, S., Taghizadeh, S.R., & Mokhtar, H. (2012). Cloud Computing: Network/Security Threats and Countermeasures. *Interdisciplinary Journal of Contemporary Research In Business. 3*(9), 27-29.
60. Reese, G. (2009). *Cloud Application Architectures: Building Applications and Infrastructure in the Cloud*. Retrieved November 17, 2020 from https://bibliotech2803.files.wordpress.com/2018/04/cloud-application-architectures-oreilly-media.pdf
61. Robu, M. (2010). Understanding the Risks of Cloud Computing Security Problem. *Journal of computing, 2*(11), 72-75.
62. Rountree, D., & Castrillo, C. (2013). *The Basics of Cloud Computing - Understanding the Fundamentals of Cloud Computing in Theory and Practice* (1st ed.). Syngress.
63. Sabahi, F. (2011). Cloud computing security threats and responses. *2011 IEEE 3rd International Conference on Communication Software and Networks*. Published. Retrieved August 25, 2020 from https://doi.org/10.1109/iccsn.2011.6014715
64. Sadulov, E. (2016, January). *Analysis of the IBM Bluemix Platform in a Cloud* (Master thesis). Ljubljana: University of Ljubljana, Faculty of Economics. Retrieved April 26, 2020 from http://www.cek.ef.uni-lj.si/magister/sadulov2040-B.pdf

65. Shah, H., Shrikanth, S.S.A., & Mokhtar, H. (2013). Security Issues on Cloud Computing. *International Journal of Computer Science and Information Security. 11*(8), 37-38.
66. Shakeabubakor, A. (2015). Cloud Computing Services and Applications to Improve Productivity of University Researchers. *International Journal of Information and Electronics Engineering, 5*(2), 33–36.
67. Srinivasan, S. (2013). Is Security Realistic In Cloud Computing?. *Journal of International Technology and Information Management. 22* (4), 47-54.
68. StatCounter GlobalStats. (2021, April). *Mobile Operating System Market Share in Europe - April 2021*. Retrieved April 1, 2021 from https://www.statista.com/statistics/639928/market-share-mobile-operating-systems-eu/
69. Takabi, H., Joshi, J. B. D., & Ahn, G.-J. (2010). Security and Privacy Challenges in Cloud Computing Environments. *IEEE Security & Privacy Magazine, 8*(6), 24–31.
70. Truong, D. (2010). How cloud computing enhances competitive advantages: A research model for small businesses. *The Business Review, Cambridge, 15*(1), 59-65.
71. Turner, S. (2013). Benefits and risks of cloud computing. *Journal of Technology Research, 4*, 1-7.
72. Visinescu, L. L., Azogu, O., Ryan, S. D., Wu, Y. A., & Kim, D. J. (2016). Better Safe than Sorry: A Study of Investigating Individuals' Protection of Privacy in the Use of Storage as a Cloud Computing Service. *International Journal of Human–Computer Interaction, 32*(11), 885–900.
73. Wyld, D. (2009). The Utility of Cloud Computing As a New Pricing–And Consumption-Model for Information Technology January 2009. *International Journal of Database Management Systems (IJDMS), 1*(1), 3.
74. Zissis, D., & Lekkas, D. (2012). Addressing Cloud Computing Security Issues. *Future Generation Computer Systems, 28*(3). 583–592.
75. Žulič, M. (2017). *Varnost informacijskih rešitev v oblaku v Evropi* (Zaključna strokovna naloga visoke poslovne šole). Retrieved January 20, 2020 from https://repozitorij.uni-lj.si/IzpisGradiva.php?id=101017
76. Zver, K. (2011). *Varnost računalništva v oblaku* (Bachelor thesis). Maribor: Ekonomsko-Poslovna fakulteta. Retrieved April 23, 2020 from https://dk.um.si/IzpisGradiva.php?id=20439

APPENDICES

Appendix 1: Povzetek (Summary in Slovene language)

Računalništvo v oblaku je razmeroma nov koncept, ki se še razvija in je za posameznike zunaj informatike precej nedoločljiv in nejasen. Računalništvo v oblaku omogoča uporaben omrežni dostop na zahtevo do skupnega nabora nastavljivih računalniških virov (npr. omrežij, strežnikov, pomnilnika, aplikacij in storitev), ki jih je mogoče sprostiti z minimalnimi napori upravljanja ali interakcijo s ponudnikom storitev.

Namen te naloge je opredeliti skupne varnostne izzive in možne rešitve pri sprejemanju računalništva v oblaku ter ugotovili, ali uporabniki vedo za njihov obstoj. Na podlagi ugotovljenih raziskovalnih vrzeli je glavno raziskovalno vprašanje, obravnavano v tej nalogi: Ali se uporabniki računalništva v oblaku zavedajo varnostnih težav in groženj ter ali izvajajo preventivne metode / ukrepe? Domneva hipoteza je: Uporabniki računalništva v oblaku se zavedajo varnostnih težav in so pripravljeni na ustrezne ukrepe.

Obstajajo različne opredelitve, ki pojasnjujejo računalništvo v oblaku, toda ena najbolj znanih, citiranih in sprejetih je po navedbah Nacionalnega inštituta za standarde in tehnologijo - NIST: "Računalništvo v oblaku je model, ki omogoča priročen dostop do omrežja na zahtevo do skupnega nabora nastavljivih računalniških virov (na primer omrežij, strežnikov, pomnilnika, aplikacij in storitev), ki jih je mogoče hitro zagotoviti in sprostiti z minimalnimi napori upravljanja ali interakcija med ponudnikom storitev" (v Mell & Grance, 2011).

Osnove računalništva v oblaku so lahko zajete s tremi elementi: njihovimi značilnostmi, modeli dostave in modeli uvajanja. Računalništvo v oblaku ima pet značilnosti: samopostrežba na zahtevo, dostop do širokega omrežja, združevanje večnajemniških virov, hitra elastičnost in merjenje storitev. Njeni modeli dostave vključujejo tri ravni: infrastruktura kot storitev (Infrastructure-as-a-service - IaaS), platforma kot storitev (Platform-as-a-Service - PaaS) in programska oprema kot storitev (Softwares-a-Service - SaaS). Prav tako lahko ločimo štiri modele uvajanja: zasebni, javni, skupnostni in hibridni. Izbira modela je odvisna tudi od potreb in ciljev organizacije. Vsak od modelov ima svoje edinstvene značilnosti, prednosti in slabosti (Gong, Liu, Zhang, Chen in Gong, 2010)

Pomemben dejavnik računalništvu v oblaku je varnostn. Varnost računalništva v oblaku je obsežen koncept, ki vključuje nabor politik, postopkov in praks, ki jih uporabljamo pri zaščiti podatkov in informacij znotraj arhitekture oblaka. S popularizacijo računalništva v oblaku se količina občutljivih podatkov, shranjenih v oblakih, povečuje, zato varnostna težava postane najpomembnejši element, na katerega se osredotočajo ponudniki teh storitev. Po besedah avtorjev Timothyja Grancea in Wayna Jansena obstaja 9 različnih področij v oblačnih storitvah, kjer se običajno pojavijo varnostna tveganja: upravljanje, skladnost, zaupanje, arhitektura in infrastruktura, upravljanje identitete in dostopa, izolacija programske opreme, zaščita podatkov, dostopnost in odzivnost na nevarnosti (Jansen in Grance, 2011).

Kot odgovor na vedno večje možnosti groženj je združenje Cloud Security Alliance - CSA ustvarilo standarde za varnost v oblaku. Njihovo dobro znano poročilo "The Treacherous 12 - Top Threats to cloud computing + Industry Insights" (2017) uporabnikom in ponudnikom z znanjem in smernicami pomaga pri njihovih varnostnih strategijah računalništva v oblaku. Na podlagi svojih raziskav opozarjajo na dvanajst tveganj: kršitve podatkov, nezadostna identiteta, poverilnice in upravljanje dostopa, negotovi uporabniški vmesniki - uporabniški vmesniki in vmesniki za programiranje aplikacij, sistemske ranljivosti, ugrabitev računa, zlonamerne informacije, napredne trajne grožnje, podatki izguba, nezadostna skrbnost, zloraba storitev v oblaku, zavrnitev storitve - DoS ranljivosti v skupni tehnologiji.

Triada CIA je dobro znan model za razvoj varnostne politike. Prikazuje vitalne komponente, ki morajo biti del ukrepov informacijske varnosti v organizaciji. Spoštovani model za razvoj varnostnih politik se uporablja ne samo za odkrivanje težav, temveč tudi za iskanje potrebnih rešitev. Model vsebuje tri koncepte: zaupnost, integriteta in razpoložljivost (Zissis & Lekkas, 2012).

Razumevanje triade CIA je ključnega pomena, ker informiranje pomaga pri izvajanju varnostnih politik in ukrepih na pravi način ter obvladovanju težav in posledic, ki se pojavljajo pri vsakodnevni uporabi oblaka (Maddineni & Ragi, 2012).

V tej študiji sem želela ugotoviti, ali se uporabniki zavedajo varnostnih težav in ali so pripravljeni ter ustrezno ukrepajo glede groženj. Hipoteza, ki sem jo preizkušala, je, da se uporabniki zavedajo varnostnih težav in sprejemajo ustrezne ukrepe. Raziskava je bila kvalitativna in kvantitativna, sestavljena je bila iz intervjujev s predstavniki podjetij in spletne ankete o zasebni uporabi računalništva v oblaku.

Opravila sem razgovore z dvema skupinama zaposlenih in sicer uporabniki in neuporabniki računalništva v oblaku, da bi ugotovila, ali so varnostna vprašanja in tveganja glavni razlog, da se podjetja bojijo računalništva v oblaku. Ugotavljala sem tudi, kakšni ukrepi in protokoli so v uporabi na tem področju. Ključni sta dve ugotovitvi intervjujev.

Prvič, odločitev podjetja o uvedbi računalništva v oblaku temelji izključno na tem, ali njihove poslovne potrebe odtehtajo stroške izvedbe. To je razvidno iz odgovorov obeh podjetij, ki niso uporabniki računalništva v oblaku, kar pomeni, da so stroški izvajanja računalništva v oblaku večji od koristi. Po drugi strani pa so se korporacije odločile za računalništvo v oblaku, ker je bila naložba v rešitev za računalništvo v oblaku smiselna in je močno vplivala na njihovo poslovanje. Pomagalo jim je standardizirati delovne procese v več podružnicah, rešiti težave pri izmenjavi podatkov in izboljšati časovno učinkovitost.

Drugič, vključena podjetja se v osnovi zavedajo tveganj varnosti in zasebnosti, povezanih z računalništvom v oblaku. Podjetja, ki so se odločila za izvajanje računalništva v oblaku, so vzpostavila infrastrukturo, da bi preprečila in odkrila morebitne težave pred uvedbo. Z uporabo svojih rešitev so na tej osnovni infrastrukturi zgradili bodisi posebne ekipe bodisi programsko opremo za strojno učenje. Njihovi varnostni protokoli se nenehno izboljšujejo, da bi sledili novim tehnologijam in možnim grožnjam. Ker imajo dovolj sredstev, jih lahko vložijo tudi v izobraževanje svojih zaposlenih. S tem obravnavajo eno največjih potencialnih tveganj računalništva v oblaku, to so človeške napake.

Čeprav so najpogostejši uporabniki oblaka običajno podjetja in druge organizacije, je računalništvo v oblaku vse bolj zanimivo tudi za zasebne uporabnike. Za namen tega dela naloge sem se osredotočila na programsko opremo kot storitev, da sta infrastruktura kot storitev in platforma kot storitev večinoma primernejša za organizacije. Za osebno uporabo programske opreme v oblak je ta na voljo preko interneta kot storitev in ne kot izdelek, ki ga je treba namestiti na računalniku. Glede na vse to sem se odločila za spletni vprašalnik, s pomočjo katerega se, preverjala posameznikovo osebno uporabo računalništva v oblaku in njegove strahove glede varnosti. Rezultati kažejo, da se tudi zasebni uporabniki dobro zavedajo koncepta računalništva v oblaku ter tudi upoštevajo varnostna tveganja, ki so jim izpostavljeni vsak dan. Glede na veliko možnost varnostnih napadov in groženj ter nenehno uporabo platform za družbene medije in storitev za shranjevanje podatkov je presenetljivo videti rezultate, ki kažejo, da veliko uporabnikov ni imelo nobenih težav.

Če se vrnemo k vprašanju, zastavljenemu na začetku te raziskave, lahko zdaj trdimo, da se uporabniki po ugotovitvah raziskave zavedajo varnostnih tveganj, ki jih prinašajo storitve računalništva v oblaku, in so nanje nekoliko pripravljeni.

Raziskava ima nekaj omejitev. Prva je velikost vzorca. Rezultatov magistrske naloge ni mogoče posploševati glede na majhno velikost vzorcev 4 podjetij za kvalitativno raziskavo in 128 respondentov, ki so sodelovali v kvantitativni raziskavi. Čeprav obravnavana podjetja predstavljajo različne panoge in so različnih velikosti, izkušenj računalništva v oblaku enega predstavnika ni mogoče posplošiti za celotno populacijo podjetij iste vrste. To se nanaša tudi na rezultate kvantitativne raziskave. Glede na široko uporabo storitev računalništva v oblaku v našem vsakdanjem življenju nam 128 odgovorov ne more dati popolne slike trenutnega stanja. Druga omejitev zadeva izbiro vzorca. Zaradi pandemije je bila komunikacija težja, prav tako možnost izbire resničnega naključnega vzorca. Raziskava je bila objavljena na Facebooku in ljudje, ki so se odzvali, verjetno niso primer naključnega vzorca. Rezultati pa kažejo, da je očitna rešitev za boljše izvajanje in sprejetje računalništva v oblaku zelo odvisna od zavesti in pripravljenosti uporabnikov. Med raziskavo je bilo jasno, da se veliko obstoječih študij osredotoča le na poslovne uporabnike računalništva v oblaku. Zdaj bi bila potrebna nadnacionalna študija, ki vključuje tudi zasebne uporabnike računalništva v oblaku.

Skratka, varnostna tveganja in težave niso nekaj, čemur bi se lahko popolnoma izognili pri uporabi računalništva v oblaku. Prav tako ni niti ene popolne rešitve za enostavno prilagajanje in izvedbo. Gre za kombinacijo znanja in preventivnih ukrepov, ki se spreminjajo in posodabljajo, hkrati pa sledijo trendom hitrega razvoja novih tehnologij. Uporabniki morajo razviti globlje razumevanje, kaj jim prinaša računalništvo v oblaku, po eni strani koristi, po drugi pasti. S tem se ne bodo samo pripravili na tveganja, zmanjšali bodo tudi strah pred spremembami in neznanim ter se osredotočili izključno na uživanje zagotovljenih prednosti.

Appendix 2: Interviews with companies

Interview - Philip Morris International

Please describe the nature of the business and industry your company operates in.
Answer: The Company I currently work for, Philip Morris International, operates in the Tobacco / FMCG industry. The nature of the industry is quite specific because of the high amount of regulations and laws that apply to it. These regulations vary from one country to another and therefore the business environment for each affiliate is different.

Please describe your role in the company.
Answer: My official title is "Digital Trade Content Executive". My responsibilities are mainly related to maintaining the B2B mobile application and managing all of the CRM campaigns in the back-end and front-end.

What is the size of your company or organization?
Answer: Philip Morris International is a large international corporation with over 75,000 employees. The affiliate, PMI Serbia, is the central hub for the South-Eastern Europe cluster within the company.

What type of service models is your company currently using? (SaaS, IaaS, PaaS)
Answer: Philip Morris has an agreement with Salesforce.com for the use of their SaaS and PaaS services.

What type of deployment model is your company currently using? (Public, Private, Hybrid, Community model)
Answer: We are currently using a Private Cloud deployment model.

Why was the business decision made by your company to use cloud computing software?
Answer: Having in mind the size of the company and the monetary and logistical implications, an internally developed solution would be very costly and time consuming. The company also decided to transform its current business practices to a more efficient and scalable model. That is why the decision was made to use a cloud computing service.

What is the cloud service or platform that you currently use for your daily operation?
Answer: That would be Salesforce.com

How did your business model evolve with the introduction of cloud computing?
Answer: Using the Salesforce.com eco-system and their already developed environment, we succeeded in deploying our now business model to all affiliates with relative ease and very low costs.

Were you and your company aware of the risks and threats prior the implementation of the cloud services?
Answer: Yes, there is entire team that is responsible for managing any potential risks and developing business continuity plans.

Have you already experienced some difficulties while using cloud services? (Data breaches, Data Leakages, Insecure API's, Hijacking…)? If you have, can you please elaborate the problem and the measures taken to address it?
Answer: Yes of course, almost all of the difficulties that you mentioned. There are groups of teams dedicated to fixing bugs and issues, so that whenever one of those difficulties occur, they are reported and handled by each respective team. One of the issues we had was when the Salesforce database was made available to all of the users globally, which caused the possibility for a potential data leakage and abuse of confidential data. Luckily, the protocols we had in place proved efficient and the above mentioned teams fixed the issue quickly by troubleshooting and escalating it in a timely manner.

Do you have an already established protocol in your company for the potential security risks?
Answer: Yes, each affiliate has a business continuity plan set up for their respective market. These plans are reviewed and updated each year, in order to address new potential risks.

Do you have any educational seminars for your employees about cloud services and security?
Answer: Yes, on a regular basis. There are mandatory educational courses each employee needs to complete every year.

Are you aware of any Cloud Security standards and if you are, is your company in compliance with any of them?
Answer: Yes, indeed. One of the most important aspects of my job is to be aware of the potential compliance issues and roadblocks that can occur on a daily basis. The company takes great pride in having very strict policies regarding security standards and complying with external privacy laws.

Are you satisfied with the benefits of the cloud services and are you planning to implement the cloud in other business processes / sectors in your company?
Answer: Yes, there is high rate of satisfaction within the company since the implementation of the cloud service. The cloud has already been implemented in some other sectors as a great business innovation and transformation tool that has all the data in one place.

Interview - Zeppelin Lab Gmbh

Please describe the nature of the business and industry your company operates in.
Answer: Worldwide sales and renting of construction equipment, Plant Constructions as well as Power Systems**.**

Please describe your role in the company.
Answer: Migrating the old monolith infrastructure to a new, improved, as well as faster, scalable and cost-efficient cloud infrastructure. Also, automating the digitalization processes, as part of migrating the old infrastructure, which will help in bringing closer to the goal of having fast deployments and changes whenever there is a need of one.

What is the size of your company or organization?
Answer: Globally around 10 000. My department around 50.

What type of service models is your company currently using? (SaaS, IaaS, PaaS)
Answer: We are using all services models, from Adobe Experience Cloud as a SaaS, to Amazon Web Services for PaaS and IaaS solutions.

What type of deployment model is your company currently using? (Public, Private, Hybrid, Community model)
Answer: My department is using Public cloud, but I believe we have Private cloud as well in the company, cannot say with certainty, since I am responsible for the product which is hosted on Amazon Web Services as part of the public model.

Why was the business decision made by your company to use cloud computing software?
Answer: Faster, scalable and more creative solutions, which ends up in not needing to take care of the hardware. Reducing the hardware costs and resources for taking care of the hardware, increased the resources for R&D on new features and products based on cloud which will affect in increasing the revenues.

What is the cloud service or platform that you currently use for your daily operation?
Answer: Amazon Web Services
How did your business model evolve with the introduction of cloud computing?
Answer: Faster delivery of new features and implementing new products, since we do not have to limit ourselves on hardware anymore.

Were you and your company aware of the risks and threats prior the implementation of the cloud services?
Answer: Risks and threats are always there, whether you are using traditional systems or cloud systems. It is up to the people responsible for particular tasks to make sure their

infrastructure is secure, whether it is on cloud or traditional hard systems. In this case, I think the traditional systems in one company can be more vulnerable, because of all the dots that are needed to be connected before everything can be functional and running. Human errors are usually one the main causes of data breaches and security flaws.

Have you already experienced some difficulties while using cloud services? (Data breaches, Data Leakages, Insecure API's, Hijacking…)? If you have, can you please elaborate the problem and the measures taken to address it?
Answer: Naked IP address and open port on some instances (servers) resulted in white hat attack where it was pointed on this issue, so we needed to reorganize everything, put behind private network and reissue new security keys for every person who needed access to those instances. In the future we reduced this by cutting all access to every instance in our infrastructure. Occasional DDOS attacks, which resulted in tracking access logs and using machine learning to track and act on them before they cause any damage.

Do you have an already established protocol in your company for the potential security risks?
Answer: We are doing routine checkups for flaws in the system, as well as one of the perks of using cloud computing, is having the ability to run daily tasks for anomalies and out of context patterns. For example, using machine learning on access logs, we are able to track anomalies in the beginning of some kind of DDOS attack and block all kinds of bad requests that are hitting our infrastructure. When it does happen, some security flaw, which was not foreseen before, our security experts and engineers will try to find a solution in the future on how to reduce this flaw and not happen again.

Do you have any educational seminars for your employees about cloud services and security?
Answer: Twice a year every employee can choose on which conference and seminar he would like to go, in order to improve his knowledge on certain topics that are helpful for him and the company.

Are you aware of any Cloud Security standards and if you are, is your company in compliance with any of them?
Answer: Well, we are using AWS provided security standards, like TLSv1.2 with different cyphers included as part of the package of security policy by AWS, which are being update from year to year. Different types of firewalls and WAF rules, which help us in monitoring and blocking the request that are hitting Cloudfront as part of one additional security layer.

Are you satisfied with the benefits of the cloud services and are you planning to implement the cloud in other business processes / sectors in your company?

Answer: Yes, the guaranties from the cloud computing companies, such as Amazon Web Services about their stability and security, 99,99% is the case that I will implement more and more products into the cloud.

Interview – Ekom-D Dooel

Please describe the nature of the business and industry your company operates in.
Answer: We are a small accounting firm.

Please describe your role in the company.
Answer: I am the owner and the accounting director as well.

What is the size of your company or organization?
Answer: The firm is small with only two employees, DOOEL (LTD Company)

Have you ever heard about the concept of cloud computing? Do you think a cloud is suitable for your company?
Answer: To be honest, this is the first time I am hearing about this term. I had to google it just to see what it was about. After reading a bit, I have to say that I know what it is and how it works, but did not know it was called cloud computing. I come from an older generation.

Are you aware of the cloud computing benefits/pitfalls for an organization?
Answer: I was already familiar to the advantages yes. We even started incorporating Pantheon in our company. And for the disadvantages, definitely not. I have not thought about the consequences before our conversation.

Have you ever considered transferring your business processes to a cloud environment?
Answer: As I already said, yes. There were a few months last year were we wanted to switch to using Pantheon as our accounting program for a client. I have to say, it was a waste of time. The specialist that was responsible for the training and helping us with the overall incorporation of the program was not up to the task. They did not have the experience with the program themselves, as well as the needed accounting background. So it is safe to say that they did not know how to adjust the program to our needs. So we paid for it for a whole year but used it for just a couple of months. We did not have a good experience with it. We even tried to switch to other specialist that has a bit more experience, but the provider said that their more experienced employees did not have time for that. So maybe we had difficulties with the provider rather than the program itself.

Where do you store your data? Have you ever experienced a security / availability issue regarding your data storage?

Answer: We have an accounting program that was made just for the needs of our company 30 years ago. So far we are extremely satisfied with it because it can be updated with elements that we need, upgraded yearly, and we only paid for it in the beginning. We are still using local hardware storage for our data (a disk) for backing up data just in case. In 30 years we have not experienced any difficulties with it, no data loss, leakage or intrusion just because it is not cloud based.

What is the company's biggest obstacle / difficulty regarding the implementation of cloud services?

Answer: We are a small company and to be honest we do not have the time to work and do all the required training for new programs. We tried and thought that it will be better for us to keep up with the technology, but as it turns out we are not ready for it. After some time we just gave up and continued with our so far great program that has every feature that we need for our day to day business. Or maybe it's the years, I am a bit older you know…my mind is not where it was 30 years ago.

What are your protocols when facing data security issues?

Answer: Our biggest issue is losing the data. So, even though the data is already saved on the program, as a backup, we save everything again on our disk. We do this at the end of our day, every single day. It is an extra step and sometimes takes time, but it is for us, and it is not a hurdle we cannot overcome. I can honestly say that cloud computing is not the right path for my company.

Interview – Expanda Dooel

Please describe the nature of the business and industry your company operates in.

Answer: "EXPANDA DOOEL" is a logistics company that operates on the Macedonian market. We offer logistics, distribution as well as management services. Our main client is "Philip Morris International" but we also provide our services to "A1", "Red Bull" and the Macedonian State Lottery.

Please describe your role in the company.

Answer: I have been with the company for 28 years and my current role is the financial director of the company.

What is the size of your company or organization?

Answer: We operate on the Macedonian market and we currently number around 160 employees.

Have you ever heard about the concept of cloud computing? Do you think a cloud is suitable for your company?

Answer: I have heard about the cloud, and that you can store your data on there, but I have never heard the term cloud computing.

Me: It means that not only you can store your data there, but you can also run applications and perform your work there. If an application is on the cloud it does not need to be installed on your computer, you just need to use the internet to access it.
Answer: Well then yes, I am familiar with this concept, as a matter of fact we have used a similar type of service once for our company.

Are you aware of the cloud computing benefits/pitfalls for an organization?
Answer: Having the experience of using a cloud computing service I can say with confidence that it can brings a lot of benefits to an organization. We used a GPS tracking system for our vehicle fleet that was cloud based. The physical devices were installed in the vehicles and the people that were responsible for the tacking could access the application from any personal device, PC or mobile phone. It proved very convenient and efficient because it was very accessible and we did not need to have storage space for the data. All the bugs and issues were reported and solved by the service provider. The issue we had, and why we decided to terminate the contract in the end, was that we could not integrate the data from the cloud GPS service with our core system. Our core system is a custom built desktop application, done by a local company and we have used it since the beginning. It has been updated along the years, based every additional need we have had.

Have you ever considered transferring your business processes to a cloud environment?
Answer: To be honest, we had. But after considering the effort it would take to implement a new system and to completely change our current way of working we decided it would not be worth it. Our custom built solution is maintained and upgraded based on our needs and what is most important to us, it was approved by our main client, Philip Morris International. The have request changes so their systems could be integrated with ours and it has worked perfectly. Also the benefits a cloud computing solution would potentially bring are more suitable for large companies that operate on multiple markets. For us, our current system is more than sufficient, we even managed to upgrade it with a GPS tracking module.

Where do you store your data? Have you ever experienced a security / availability issue regarding your data storage?
Answer: We store all of our data locally, in a server room that is on-site. We also backup our data on secondary storage devices that are off-site.

What is the company's biggest obstacle / difficulty regarding the implementation of cloud services?
Answer: As I have mentioned before, we currently do not have a strong business reason and need to change to a cloud service. Our current systems work perfectly well.

What are your protocols when facing data security issues?

Answer: We have disaster recovery plans in place, so we can deal with any situation that impacts the data. When it comes to cyber-attacks, we have a firewall and intrusion prevention systems that take care of those risks.

Appendix 3: Survey Questions

Private Use of Cloud Computing

Hey, glad to see you around here! First of all, let me thank you for taking my 5-minute survey. You are a great help! ☺ I as a student, am on a daring quest to collect the right data regarding my thesis. Don't worry, the data will be used just for research purposes at my University, so you will remain completely anonymous.

* Required

1. What is your gender? *

– Female
– Male
– Prefer not to say
– Other: ________________________

2. What is your age? *

– 16 or under
– 17 - 24
– 25 - 34
– 35 - 44
– 45 - 54
– 55 or over
– Prefer not to say

3. What is the highest degree or level of education you have completed? *

– Some High School
– High School
– Bachelor's Degree
– Master's Degree
– Ph.D. or higher
– Prefer not to say

4. Do you understand the concept of Cloud Computing? *

– Yes, I fully understand the term and the concept
– Vaguely, I have heard about the term but do not fully understand the concept
– No, I have never heard about it
– Prefer not to say

5. Have you ever used at least one of the following services? (communication) *

Viber Facebook Instagram

Skype WhatsApp

- Yes
- No

6. Have you ever used at least one of the following services? (storage) *

OneDrive Google Drive Google Docs

Dropbox Amazon Drive iCloud Drive

- Yes
- No

7. What are the reasons you use cloud services for? Select all that apply. *

- It is convenient because I can access my data from whatever computer / device I am using
- The ease of storing documents
- As a backup so I won’t lose my data if my personal computer / device fails The ease of sharing information
- Other:

8. Which of the following services do you use / have used? Select all that apply. *

	Amazon Driv	Google Driv	Dropbox	One Driv	Apple iCloud Driv	None
Data storage	□	□	□	□	□	□

	Skype	Vibe	WhatsApp	Microsoft Teams	Zoom	None
Communication	□	□	□	□	□	□

9. Do you agree that there are risks connected to the use of cloud services? *

– Strongly disagree

– Disagree

– Neither agree nor disagree

– Agree

– Strongly agree

10. Which of the following risks are you most concerned with? Select all that apply. *

– Data loss (ex. your data is lost due to a phishing attack; the cloud service was attacked or it happened as an unintentional accident)

– Identity theft (ex. your personal information / pictures and videos are stolen and used by someone else)

– Malware attacks (ex. your device gets infected by a malware (virus) attack that is also attacking the cloud service you use)

– Data leakage (ex. your credit card information is stolen and used for unauthorized purchases)

– Data availability (ex. the cloud service you use is hit with a Denial of Service attack and you are not able to access your data)

11. In your opinion, how significant are the following risks when using cloud? (Grade from Very insignificant to Very significant) *

Mark only one oval per row.

	Very insignificant	Insignificant	Neither significant nor insignificant	Significant	Very significant
Data loss (ex. your data is lost due to a phishing attack: the cloud service was attacked or it happened as an unintentional accident)	○	○	○	○	○
Identity theft (ex. your personal information / pictures and videos are stolen and used by someone else)	○	○	○	○	○
Malware attacks (ex. your device gets infected by a malware (virus) attack that is also attacking the cloud service you use)	○	○	○	○	○
Data leakage (ex. your credit card information is stolen and used for unauthorized purchases)	○	○	○	○	○
Data availability (ex. the cloud service you use is hit with a Denial of Service attack and you are not able to access your data)	○	○	○	○	○

12. Have you ever experienced any of these problems yourself? Select all that apply.

- Data loss
- Identity theft
- Malware attacks
- Data leakage
- Data availability
- None
- Other

13. Do you agree that the cloud service applications are overall safe for personal use? *

- Strongly disagree
- Disagree
- Neither agree nor disagree
- Agree
- Strongly agree

14. Have you taken any actions to increase your safety while using cloud services? Select all that apply. *

- I thoroughly review the agreements with my cloud services provider before I accept them.
- I investigate my cloud service provider to ensure the service encrypts data.
- I configure the privacy settings so the service doesn't access my private data.
- I ensure that all my devices that are connected to a cloud service are secure.
- I use strong passwords.
- I never reuse passwords.
- I use two-factor authentication (when possible).
- I avoid / minimize the use of public computers.
- I rarely use public Wi-Fi.
- I use HTTPS instead of HTTP.
- I use a virtual private network (VPN) whenever possible.
- Other: