SECURITY ASPECTS OF CLOUD COMPUTING

PERSPECTIVES WITHIN ORGANIZATIONS

Bachelor`s thesis in Informatics (15 credits)

Julia Gustafsson
Mariam Said

Fall 2015: 2015KANI08

..

UNIVERSITY
OF BORÅS

Title: Security Aspects of Cloud Computing – Perspectives within Organizations
Year: 2015

Author/s: Julia Gustafsson, Mariam Said
Supervisor: Patrik Hedberg

Abstract

Cloud computing has become a significant and well-known term within a short period of time. Some parts of it might even be considered as unclear, including its vague definition. Cloud computing has rapidly and successfully come to perform an essential role within information technology and therefore in how organizations are managing their IT departments today. Its many advantages allure organizations to deploy a cloud solution. Despite the flourishing growth of cloud computing it still has its draw backs. One of its problems has come to be acknowledged as security issues, which has resulted in many companies deciding not to deploy a cloud solution and instead retain their traditional system. This qualitative study will come to investigate the perspective of organizations regarding security within cloud computing. The aim is to outline the security aspects conferred by Swedish organizations as there already is existing information concerning security issues. The empirical study is based on the gathered information from conducted semi-structured interviews. This study resulted in the findings of seven security aspects outlined by organizations, with the main reason concerning the uncertainty and towards the services of cloud computing. These security aspects are essential as they are set by organizations that have the potentiality to become cloud users, but for certain reasons decide not to. From the outlined security aspects, a close relationship can be identified to the already known security problems. These problems have strengthened the meaning of the security aspects, and that they are based on real concerns that can be connected to real problems.

Keywords: cloud computing, security, security problems, security aspects, cloud solution

Acknowledgements

This Bachelor Thesis presents the results of the study “Security Issues of Cloud Computing - Perspectives within Organizations” that was conducted during Fall 2015.

Special thanks to Patrik Hedberg for the critical guidance during the process of writing this research study, as well as for the support and time invested. Great thanks to the organizations that agreed on participating in this research for interviews, the research could not have been conducted without their contribution.

Thanks to family and friends for the support throughout the writing of this research.

Borås, 2015

Julia Gustafsson Mariam Said

Table of Contents

List of Figures:

List of Figures:

1 Introduction

1.1 Background

Information Technology (IT) is a well-known term among individuals today, particularly within organizations (Chowdhury 2014). As the technology is continuously under development by the IT industries, it has resulted in new trends unceasingly being followed and applied by companies (ibid). One of the most popular technologies today is the internet, that by the elegance of IT has deserved its revolutionary position. This has resulted in resources being globally shared and managed from anywhere and at any time (ibid). The main component of the explained standard is cloud computing, which provides these resources as a service rather than a product (ibid). Chowdhury (2014) mean that it has been shown that Small and Medium Business (SMB) companies are becoming more aware of the beneficial aspects that are provided in a cloud environment. Despite the fast growth of cloud computing, Barnatt (2010) indicates that traditional computing is still commonly used by organizations today. Unlike cloud computing, the data in traditional computing is not accessible from anywhere and anytime, instead the systems and databases are locally implemented within the organization (ibid). The definition of cloud computing may vary depending on who the descriptor is (ibid). Therefore, it becomes problematic to provide a generally accepted and completely accurate definition of cloud computing (ibid). Balasubramanian and Aramudhan (2012) explain that there are many definitions of cloud computing that emphasize on its characteristics. With its involvement in software application, processing power and data storage over the Internet (ibid). Barnatt (2010) defines cloud computing from a general perspective as scalable, device-independent and task-centric where the computing assets are accessible online. Additionally, it includes a 'pay as you use' system, which benefits the users as it saves financial costs (ibid).

The National Institute of Standards and Technology (NIST) (2010) definition of cloud computing has become the most commonly used definition; it is defined as a model that provides access to an on-demand network. This network, which can be explained as a shared pool of different types of configurable computing resources, that rapidly can be provisioned and service provider interaction or with little management effort can be released (ibid). NIST (2010) exemplifies that these computing resources often include applications, network, storage, servers or services. Kumar, Kumar, Singh and Saxena (2013), along with Balasubramanian and Aramudhan (2012) agree on that the definition of cloud computing by NIST is the most widely used one. A shorter and also commonly used explanation of cloud computing is that computing resources are delivered on-demand over the Internet (Potdar, Patil, Bagla & Pandey 2015). Many of its important purposes are illustrated, such as testing and development, big data analytics, reduction of cost, Customer Relationship Management (CRM) and universal access (ibid). The popular approach of cloud computing has been rapidly developing the IT industry with its further definition and description by specialists as one of the most important changes within the IT sector that benefits companies and end users (Ogigau-Neamtiu 2012). One of the few reasons due to the popularity of cloud computing is its shared pool of resources, convenience, and on-demand network access along with more characteristic features, such as scalability, elasticity, measured service, and self-provisioning of resources (Sinjilawi, Al- Nabhan & Abu- Shanab 2014). Chowdhury (2014) demonstrates that cloud computing is offered as a service for individuals, companies and even governments. Cloud computing includes three fundamental delivery models, Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS) that are offered as services

from the cloud (ibid). Private, public, community and hybrid clouds are the four deployment models that also are basic layers of cloud computing (ibid).

It is acknowledged that cloud computing is a new emerging term in the IT industry (Zissis & Lekkas 2010). However, the term has been identified since the 1960s with the purpose of attempting to disengage users from the need of hardware (ibid). Cloud computing has a distinctive similarity to virtualization technology that dates back to 1967 and was only available for mainframe systems, but today, this is considered as basic for cloud computing (ibid). At the beginning of the 1990s, a new idea came to the surface and was known as grid computing (ibid). It was created through fast data communication links and had an aim of supporting complex calculations, but it was for data-intensive scientific applications (ibid). Zissis and Lekkas (2010) explains that grid computing, utility computing and SaaS together formed what today is known in the IT industry as cloud computing. Despite the benefits provided when adopting a cloud solution, Potdar et al (2015) mean that there still have its drawbacks as any new technology. One of its definite challenges it faces is data thefts, which particularly is associated with insider attacks and Distributed Denial of Service (DDoS) (ibid). Potdar et al (2015) continues to explain that other major threats include data breaches, loss of data, malicious insiders, abuse of cloud services and issues concerning shared technology. Zissis and Lekkas (2010) explain that it is important to identify and recognize the challenges and threats in order to understand the Information System (IS). Another essential factor is to handle the security accurately within the organizations (ibid). Despite the benefits with cloud computing, companies are unwilling to deploy it into their business, mainly because of the security issues (ibid).

1.2 Research Overview

The revolutionary cloud computing and its services provided to the IT world is resulting in larger organizations implementing this type of solution (Lourida, Mouhtaropoulos & Vakaloudis 2013). Lourida, Mouhtaropoulos and Vakaloudis (2013) explain that individuals and companies are benefiting from the accessibility of its data storage, applications, servers and resources online (ibid). Barnatt (2010) explains it as organizations no longer need to invest in hardware and software as they are available for renting and can be used directly through the Internet. It becomes more cost efficient as the expenses of hardware and software are reduced, while the user is only consuming the functions and services that are either bought or rented (Barnatt 2010). Lourida, Mouhtaropoulos and Vakaloudis (2013) mention in their article that sometimes the benefits of cloud computing compensate all the security issues concerning security depending on the situation.

Several studies outline that some of the main problems and challenges concerns the security problems within a cloud solution (Zissis & Lekkas 2010; Ogigau-Neamtiu 2012; Younis, Kifayat & Merabti 2014). Barnatt (2010) and Kumar et al (2013) agree that the main concerns with cloud computing are security, trust, and privacy issues. Meanwhile, Srinivasan (2012) describes that organizations are mainly threatened of attacks by hackers that can result in loss of confidentiality, integrity or availability of data. The great concerns with cloud computing are according to Barnatt (2010) related to reliability and availability. There is a need for the services provided by the cloud to be secure enough for usage, or else it is not fully reliable from a consumer perspective, and therefore the adoption of it is rather seen as an obstacle (Chowdhury 2014). On the other hand, reliability is being improved through the implementation of cloud computing as it is suitable for a business and its disaster recovery

(Zissis & Lekkas 2010). Individuals and organizations fear that they will not be able to access their data and applications on the cloud when needed, which can create a concern (Barnatt 2010). The trust towards the vendor to ensure that the data is safe is therefore essential, means Barnatt (2010). The importance of security within cloud computing is reflected by Chowdhury (2014) along with its beneficial aspects. Chowdhury (2014) explains that it is essential to know that cloud computing is not mainly insecure; it only needs to be accessed and managed securely. A further discussion is made by Ogigau-Neamtiu (2012), which highlights the importance of identifying the major security issues for both decision makers and users. An organization needs to be informed and aware of both the issues and beneficial aspects of cloud computing before adopting it (ibid). Lourida, Mouhtaropoulos and Vakaloudis (2013) explain further that traditional IT systems are more controllable and easy to manage compared to cloud computing. Policies and controls are easier applicable within traditional computing as all resources are known (ibid). Lourida, Mouhtaropoulos and Vakaloudis (2013) mean that the risks can easily be recognized that can lead to the adoption of more manageable methods to increase the risks. The limitations of traditional computing are restricted to larger companies that are able to invest on security departments (ibid).

Karnwal, Sivakumar and Aghila (2011) illustrate what service models that can be provided from a cloud environment, such as Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS). The services are provided in different ways depending on the resource the user want to adapt for their business (ibid). There is also a choice between different kind of clouds provided for the users, which depends on the choice of service model and deployment model. Balasubramanian and Aramudhan (2012) illustrate that the choice between public, private or hybrid cloud solutions reflects on the possible issues that might come with these services. Public and private clouds are differentiated by each of their unique roles, methods and applicable techniques (Karnwal, Sivakumar & Aghila 2011). Therefore, each service has its own security problems (Jangwal & Singh 2012). Subashini and Kavitha (2011) state that despite that more IT companies are adopting cloud services, its security challenges are still reducing the growth of cloud computing. This results in greater insecurity among potential users regarding the safety and privacy of their data (ibid). The suggestion presented by Subashini and Kavitha (2011) is to analyze every level in both micro and macro before implementing any type of security framework. They also explain that there is a need of finding a solution for this problem in order to attract potential users to adopt cloud solutions (Subashini & Kavitha 2011). For that reason, Ficco, Palmieri and Castiglione (2015) describe the importance of a new security paradigm as crucial to solve because of the problems in a cloud environment that can lead to attract more users.

Srinivasan (2012) discusses that each cloud provider has different procedures regarding security and that companies are in need of this security measure. Today there are several models available, but they need to be customized explicitly for each organization as it is complicated when comparing organizations (ibid). The service-level agreement (SLA) is described by Karnwal, Sivakumar and Aghila (2011) as an agreement between cloud provider and cloud user where suggested rules are highlighted by the provider. Despite many solved problems with the adoption of cloud solutions, Sinjilawi, Al-Nabhan and Abu-Shanab (2014) explain that there are still many left unsolved. According to Lourida, Mouhtaropoulos and Vakaloudis (2013) the process of cloud computing is still evolving and the security issues are still being acknowledged, explored and tackled. Previous research not only indicates, as explained, on the beneficial aspects of cloud computing. Many papers prove that the security issues are viewed as a large problem when deciding to adopt a cloud solution or not.

1.3 Problem discussion

The security issues within cloud computing are seen as a barrier and are therefore one of the main reasons why today's companies are prevented from adopting a cloud solution and instead continue using the traditional system (Ogigau-Neamtiu 2012). In order to attract more companies to start using cloud computing, a solution is needed to keep the data secure and confidential (Karnwal, Sivakumar & Aghila 2011). Ogigau-Neamtiu (2012) explains that keeping the data confidential and secure, are problems related to what are seen as the major concerns regarding security when moving to a cloud. It is further explained by Ogigau-Neamtiu (2012) that there are additional problems that arise regarding the data; these problems are all composed in the data security life cycle, which relates to controlling the data. The problems include the creation, storage, modification, backup and removal of data. The cycle can be found in both a cloud environment and in a non-cloud environment, but the stages in the cloud environment tend to be more complex with higher security risks and therefore a more attentive management is essential (ibid). According to Ogigau-Neamtiu (2012) the threats can be reduced by the cloud user adopting security measures that during the lifecycle helps the data to stay secure and private. The problem relates to the fact that companies are still unwilling to enter the cloud, despite the benefits that can be provided from a cloud service (Chowdhury 2014). Chowdhury (2014) explains that the reduce of growth in adopting cloud computing, is mainly related to the security problems. Zissis and Lekkas (2010) explain that in order to identify unique challenges and threats it is important to understand the Information System (IS). According to Zissis and Lekkas (2010), two terms are needed when handling the security in a right way; security identification of threats and trust. The identification concerns the confidentiality, privacy, integrity and availability. Through these factors the perception and understanding of a cloud's security is easier to attain (ibid).

In 2009 a survey was conducted by IDCI where 74 percent of the participants stated that security is seen as a main challenge that prevents organizations from deploying cloud solutions mentioned by Subashini and Kavitha (2011). The participants in whom this survey was conducted on were IT executives and CIO's (Chief Information Officer) (ibid). Balasubramanian and Aramudhan (2012) discuss another survey that was made in 2011, a global information security that was conducted by Ernst and Young, with almost 1700 organizations in 52 countries whom participated. The results revealed that during the next 12 months 16 percent of the participants had no plans to implement cloud services (ibid). This indicates that there is a potential for the rest of the 84 percent that might consider implementing it, but there are reasons that are preventing them from that (ibid).

The importance of the adoption of the cloud and its beneficial features has raised attentiveness among companies. This is explained thoroughly by Subashini and Kavitha (2011) that companies today, mainly Small and Medium Business (SMB) are becoming more aware of the beneficial services that are provided. The benefits provide fast access to some of the best applications and services that will drastically change their infrastructure, by adopting cloud computing to their business, to a negligible cost (ibid). Subashini and Kavitha (2011) discuss that it is estimated by analysts that within the five upcoming years, 12 percent of the worldwide software market will be moving to the cloud and within this period of time and the growth of cloud computing's global market will reach up to $95 billion. More companies are becoming tempted by the cloud's virtualization techniques with the target of providing companies with improved utilization of resources and decrease the workload for the company

(ibid). The role of the cloud in the IT world and its importance for the companies is essential as it is continuously growing.

As shown in previous parts in this chapter the existing research and studies outline that the major problems why companies decide not to implement cloud computing relies within the lack of safety, trust and privacy. What is indicated by Subashini and Kavitha (2011) is the uncertainty regarding the security in the cloud, which is the reason why potential users are scared to adopt cloud solutions. Ogigau-Neamtiu (2012) complements that security issues are one of the largest concerns from a customer's perspective, which is seen as a motive for not adopting a cloud solution. What can be withdrawn from the background and research overview relates to the issues and challenges of the cloud. The problems are mainly emphasized along with what types of security frameworks there are to apply as a user. However, there is no indication of information or research related to the security aspects required by potential cloud users that can be found. If there are identified security aspects required by organizations, they might be related to the underlying reasons for them not to adopt cloud solutions. These underlying reasons are essential as they are resulting in organizations choosing not to enter the cloud environment. They are prevented from becoming cloud users and are therefore referred to as potential cloud users. This refers to the main reason behind their action that involves what these potential cloud users essentially require in order to implement a cloud solution within their organization.

1.4 Research question

Based on the problems presented in the problem discussion, it was found that security problems are one of the main reasons why organizations choose not to adopt cloud computing into their business. Studies and research illustrate the benefits by moving to the cloud environment. But even if companies may be aware of these benefits, many companies are still in use of the traditional system. The concern is seen as a large problem among scientists, but also among the users. Today there is no existing research regarding the security aspects that companies today have towards the cloud environment. It is important to grasp the organizations point of view regarding these issues. The definition of an aspect in this research is explained as something that an organization think and feel regarding a subject. The research will explore what Swedish organizations perceive regarding this area, among those companies that has at least once considered moving to the cloud.

The research question that was answered in this research is: *What security aspects are identified by potential Swedish users focusing on data storage when implementing a cloud solution?*

1.5 Research purpose

The purpose of this research is to develop and increase a deeper knowledge about what security aspects organizations have towards different cloud solutions. Including to provide knowledge about familiar security issues that might be related to the security aspects. In the research overview it was displayed that numerous of previous research, specifies that the security issues are viewed as a large problem and explained as one of the main factors why companies decide not to move to the cloud. Cloud computing has a big role within the IT industry today, and the beneficial services may be a central reason for its fast growth. In order

to improve the industry, the problems need to be identified and solved. By identifying the security aspects outlined by the companies themselves, it can be described as one step closer towards the long term process of finding and providing appropriate solutions. The research will focus on companies that have considered deploying a cloud solution into their entire business, but for some reason declined the idea. This is viewed as important, mainly because the security aspects might be the reason why they did not accomplish the adoption of cloud computing. The organizations were perceived as potential users, because if they have considered the idea they may move to the cloud when these problems are solved. The main purpose in this research is therefore to highlight what organizations consider as security aspects, but also to contribute with knowledge for the improvement of cloud computing.

1.6 Target audience

The main target audience for this research is the cloud providers. By gathering information about the security aspects exposed by the companies, there are possibilities to continuously develop cloud computing towards an accurate and successful direction. When receiving diverse opinions of the problems, different viewpoints can be found. It is not guaranteed that cloud providers have similar opinions regarding the security problems, compared to the companies. By making the users aware of what security aspects that are highlighted within other organizations will provide further knowledge among users. Students and researchers within the field of informatics that have an interest for cloud computing and its further research are also included in the targeted audience.

1.7 Delimitations

Cloud computing is a broad and popular research area, therefore the appropriate need of limitations. The need of limitations is necessary to be able to answer the research question of this research. As the research question indicates, the focus is not on all the aspects, it focuses on the security aspects. Another limitation that has been drawn is that no organization outside the boundaries of Sweden will participate in this research. The focus of this research will be companies that have considered adopting a cloud solution for their entire business, but for some reason decided not to. The term cloud solution will in this research mainly be referred to as data storage, as it is mainly associated to cloud computing and its functions. Applications and other minor services such as email will not be the primary focus in this research. The importance relies within the larger decisions within an organization regarding the entire data storage.

2 Theoretical Framework

2.1 Traditional computing

Traditional computing refers to the organization's self-owned software, hardware, operating systems and servers located within the organization (Molnar & Schechter 2010). During the last decades IT has dramatically changed, from mainframe computers to a computer held in the hands of the people (Hedman & Kalling 2002). In 1954, the first business computer was installed, and from there IT seized its start (ibid). This has contributed to what organizations today have managed and used computers for over a half century (ibid). IT consists of hardware, such as computers, and software that instruct the hardware for the computer to function (ibid). Hedman and Kalling (2002) explain that different programs in the software control the activities such as the sequence of operations, and also feed the hardware with data that is being processed.

The argumentation whether self-hosted infrastructure is inherently more secured than cloud-hosted infrastructure is being frequently discussed (Molnar & Schechter 2010). Potential buyers for cloud-hosting often have higher requirements about the security than those who use traditional web hosting (ibid). Molnar and Schechter (2010) states that by using traditional computing will result in better control over the constructions as operations and the infrastructure are available. It is found that traditional approaches are uncooperative and expensive explains Olekar and Sreekumar (2013), and not as elastic as cloud computing. The traditional desktop software is seen as a high cost for a company, including additional costs for license fees to provide the software for people within the organization (ibid). A difference from cloud computing is that traditional computing is not managed by the provider, but totally within the company (ibid).

2.2 Cloud computing

Cloud computing is seen as one of this decade's major developments in the IT industry means Rajaraman (2014). Cloud computing provides a wide range of services for both companies and private users, and has during the last years increased which is reflected in the high number of organizations implementing it (ibid). Cloud computing is a model used to combine software and hardware where the data is accessible from a web browser (ibid). A further definition of cloud computing is outlined by Barnatt (2010) that states its occurrence when programs, data storage and processing power can be reached through the Internet from a computer unit. Cloud computing started to be used as an umbrella term, as during 2008 many variations of new services were developed that came to permit computing resources to be accessed through the Internet (ibid). 'The cloud' is a label for online computing resources rather than the entire Internet explains Barnatt (2010). The term cloud computing is beneficial in the sense that it distinguishes the activities completed online through the recent decades from a completely new era of processing power and online software (ibid). Computing utility is a preferred description of cloud computing by Rajarman (2014), as he states that the reflection of the new term describes the 'pay as you use' model in a cloud.

Cloud computing services are frequently consumed by many users without any notification of awareness (ibid). This includes publicly provided services such as emailing via Gmail, Outlook or Yahoo, which is the reason for its famousness (ibid). These types of services are

labeled as 'free' cloud services, mainly because they can be accessed by customers for free (ibid). Rajaraman (2014) explain that cloud computing has come to change the era; the users has gone from owning their own computers to an epoch where they do not anymore. It could instead be described as attaining software and hardware maintained by the cloud provider (ibid). Scientists explain that the need of cloud computing is becoming utilized just as electrical power (ibid). Users can through a browser access computing facilities by running on a 'cloud device' and a 'pay as you use' model (ibid). There are several types of clouds that are provided for the user (ibid). These clouds are provided for users in different forms based on how they are deployed and accessed (ibid).

Rajaraman (2014) presents five major characteristics with the cloud model:

- Computing resources can be beneficial for the customer, such as storage, space and application programs.
- The resources provided through the cloud can be accessed from anywhere, at anytime, as long as the web is accessible.
- A provider is pooled to give the contracted services through the computing resources. The pooled resources can be distributed across many data centers as well as graphically distributed that can be shared by several customers.
- Computing resources are in certain cases availed elastically. This provides the customer a possibility to develop more resources when there is a need of it, and less when the demand of resources is not requested.
- The systems by cloud computing are adaptive, the balance and optimization of the use are automatically balanced. This permits the user to control and monitor.

In figure 3.1 presented below, the associations in a cloud are presented. The four deployment models are displayed: public, private, hybrid and community cloud that will come to be further explained. These deployment models are described by Vairagade and Vairagade (2012) as cloud storage models, which permit users to maintain control over their data. Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS) are also shown in the picture as the service models towards a cloud. The last part presented in the picture is its essential characteristic including broad network access, rapidly elasticity, measured service, on-demand self-service and resource pooling.

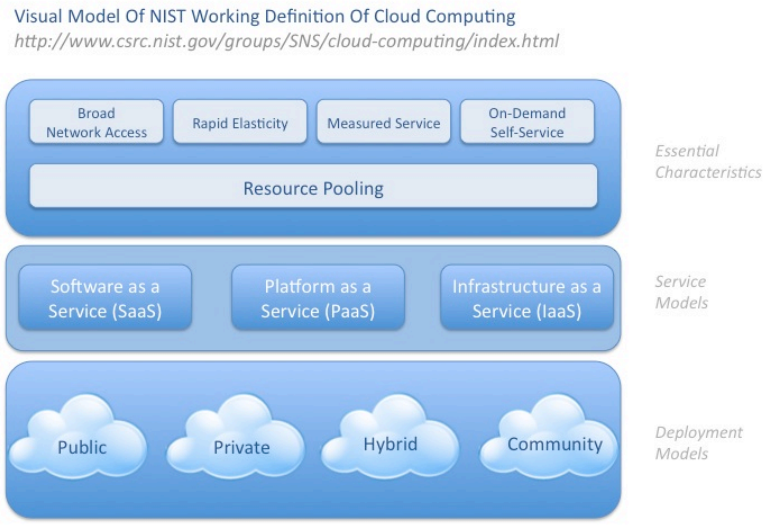

Figure 1: Cloud security Alliance (2009)

2.2.1 Public cloud

A public cloud is visible for the general public but also to large industry groups, and the infrastructure is owned by the cloud provider (Zissis & Lekkas 2010). This type of cloud is provided to everyone, and the infrastructure is shared by several customers (Rajaraman 2014). The location of a public cloud is generally the provider's premises in which he has full control (ibid). There are both paid and free public clouds provided (ibid).

2.2.2 Private cloud

Rajaraman (2014) explains that a private cloud is provided for an exclusive single organizations use. It can be interconnected computing systems that are physically distributed and belong to an organization universally accessible for every member of the organization (ibid). The infrastructure of the cloud can be owned and maintained by the organization itself, outsourced to a third party, or a combination of these two (ibid).

2.2.3 Community cloud

A community cloud is provided and available for a specific community that has exclusive use with the same interests in common explains Rajaraman (2014). An illustrated example might be a group of students creating a community cloud for shared infrastructure (ibid). Through this type of cloud, all the members have access to the cloud (ibid). It can be owned or operated by every member, both in-house and outsourced. This cloud is mostly based on grid computing (ibid).

2.2.4 Hybrid cloud

A hybrid cloud is described as a combination of two or more clouds, and often two or more distinct entities from public, private and community clouds (Rajaraman 2014). They are still distinct but the purpose is to bring them together with the help from standardized protocols that allows data and portability for applications (ibid).

2.3 Services available in cloud computing

Different services are available by the cloud; the three major ones will be further explained. Figure 3.2 below explains the relationship between these services and how they are interrelated to one another.

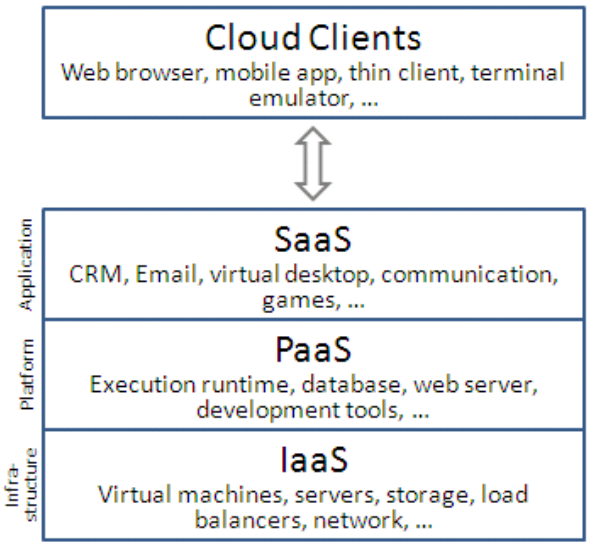

Figure 2: Ogigau- Neamtiu (2012)

2.3.1 Infrastructure as a Service (IaaS)

Ogigau-Neamtiu (2012) explain Infrastructure as a Service (IaaS) as a service provided through the cloud. The user is able to manage the process, storage, networks and other computing resources (ibid). All the functions mentioned makes it possible for the users to run and deploy determine applications and software systems (ibid). The user of the cloud does not control or manage the infrastructure, but partly controls the storage, operation systems and the deployed applications (ibid). Operating systems and application software are the company's responsibility to maintain (ibid). This type of platform can provide possibilities for businesses, where equipment can be used in different ways and forms, such as servers, hardware, and storage space like a pay-per-use service (ibid).

2.3.2 Platform as a Service (PaaS)

Platform as a Service (PaaS) is another type of service provided to the cloud user which is explained by Ogigau-Neamtiu (2012). This service provides the user with a cloud to deploy in the infrastructure of the cloud, which are applications created by the consumer (ibid). There are different programming tools that are being used, such as programming language and tools supported to the provider (ibid). This inspires the user to create and run its own created software solutions (ibid). Ogigau-Neamtiu (2012) explains that these solutions are made on a cloud platform and without any cost or complexity of buying and handling other hardware or software layers. Platform as a service is not handling the infrastructure, only the applications and its related parts (ibid). This service is built on the IaaS, and provides the customer with software infrastructure (Rajaraman 2014).

2.3.3 Software as a Service (SaaS)

Ogigau-Neamtiu (2012) explains Software as a Service (SaaS) as a service that provides the user with accessibility to the application created by the provider. This application is running on a cloud infrastructure (ibid). SaaS is accessible from different locations and clients and is provided through a thin-client interface which be explained as the web browser (ibid). The user is not in control more than what this service has to offer, which excludes the control over the infrastructure, operating systems and servers (ibid). The only controlled part means Ogigau-Neamtiu (2012) is the configuration settings that are limited for certain user-specific applications. The software applied on the infrastructure is installed by the IaaS provider or application provider through the Internet (Rajaraman 2014). These types of services Rajaraman (2014) explains can be used by several consumers that have access to it from an appropriate access device.

2.4 Security in cloud computing

The general idea of cloud computing is described by Ryan (2013) as a storage of programs and data that are centrally positioned in a cloud that permits the opportunity to be reached at any time, from anywhere. Although the cloud provides many benefits, such as flexibility of access, data ubiquity and release, it however enhances security as a cloud provider may afford a better up-to-date solution than a data owner (ibid). There will be arising security issues, as the data is out of control from the owner (ibid). Ryan (2013) explains cloud computing security as:

> *"Cloud computing security concerns all the aspects of making cloud computing secure. Many of these aspects are not unique to the cloud setting: data is vulnerable to attack irrespective of where it is stored. "*
>
> (Ryan 2013, p. 2263).

The mainly reason why cloud computing covers computing security within all of its topics, such as minimization of attack surface, protecting the cloud from malwares, the design of the clouds security architectures, enforcement of the cloud to controlling access (Ryan 2013). Aspects will persist from a specific domain derived from the security of cloud computing (ibid).

2.4.1 Cloud Security Alliance

Cloud Security Alliance (CSA) (2009) is a non-profit organization that generates guidance for security in cloud computing. The document *Security Guidance for Critical Areas of Focus in Cloud Computing* has the purpose to enlighten organizations to adopt these recommendations (Cloud Security Alliance 2009). In the document five essential characteristics are mentioned, that demonstrate and differ from the traditional computing approaches, on-demand self-service, broad network access, resource pooling, rapid elasticity and measured service (ibid).

One of the main reasons for information security is to protect the data which powers the systems and applications in an organization (Cloud Security Alliance 2009). Security controls in cloud computing is usually the same as in all IT environments (ibid). When people

nowadays are transforming their organizations into a cloud computing approach, the methods used in traditional computing for securing data creates a challenge to implement them into a cloud-based architecture (ibid). This therefore comes to require new security strategies (ibid).

Cloud Security Alliance (2009) explains that there are key challenges in a data security lifecycle inside a cloud such as:

- Location of data, which can be explained as the storage of essentially assurance data is located where only permitted by the contact, Service Level Agreement (SLA) or/and regulation.
- Data remanence or persistence, where data has to be completely and effectively removed to ensure that it is deemed destroyed.
- Commingling data with other cloud customers, sensitive data cannot commingle with other customer's data.
- Data backup and recovery schemes for recovery and restoration.
- Data discovery
- Data aggregation and interface
- Data security

Data security is explained as one of the main challenges for when strategies must be changed from the traditional computing (Cloud Security Alliance 2009). There are primarily seven parts included, confidentiality, integrity, availability, authenticity, authorization, authentication, and non-repudiation (ibid). Cloud Security Alliance (2009) has provided information in a process of guidelines for assisting companies to prevent attacks and other forms of threat regarding the security.

2.5 Security issues in cloud computing

2.5.1 Confidentiality

Zissis and Lekkas (2010) description of confidentiality is being compared to users that are authorized or that can accesses protected files when needed. There is a threat against the data that companies have made, this is because the increasing number of partners and access (ibid). The systems should be able to transport the ability, despite if authorities misbehave, in order to continue with its operations (ibid).

Ogigau-Neamtiu (2012) further indicates that confidentiality is a security issue. Two of the mainly concerns when a company decides to move to the cloud are confidentiality and data security (ibid). Ogigau-Neamtiu (2012) presents a few of the arising problems that are:

- Who is permitted and able to create data
- Where is the data stored
- Who can manage and modify data
- What happens when deleting data
- Backup of data

This is also referred to as the data security lifecycle (Ogigau-Neamtiu 2012). In Figure 3.3 the steps in the data security lifecycle is demonstrated. The relationship between create, store, use, share, archive and destroy are presented by the Cloud Security Alliance (2009).

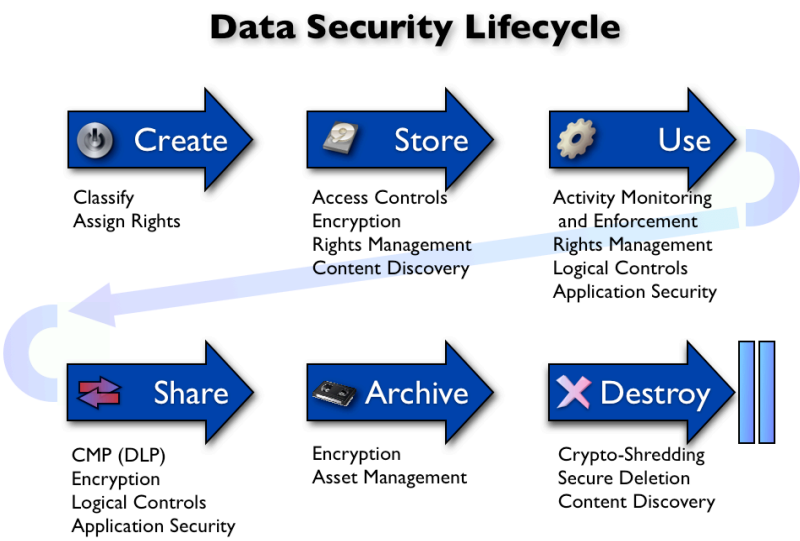

Figure 3: Cloud Security Alliance (2009)

2.5.2 Integrity

Integrity is one of the key aspects in information security (Zissis & Lekkas 2010). It means that only the authorized is able to modify the assets such as hardware and software (ibid). To protect data from unauthorized modification, deletion or fabrication is the implementation of data integrity (ibid). Another type of integrity that Zissis and Lekkas (2010) presenting is software integrity, which protects the software from the same threats, deletion, modification, fabrication and theft.

2.5.3 Privacy

Privacy is an issue that affects the employees at a company, essentially to control and protect the personal information within an organization (Zissis & Lekkas 2010). Companies that handle personal data are required to obtain appropriate privacy and confidentiality protection (ibid). A number of legal challenges are illustrated regarding the cloud, which describes issues about storing data in several locations in the cloud, and automatically increasing the risks of confidentially and privacy (ibid).

2.5.4 Availability

Zissis and Lekkas (2010) describe that operating systems have must be functioning upon demand and accessible by all authorized entities within an organization. The availability is by Ogigau-Neamtiu (2012) defined as another aspect of the security issue. It is important with the availability of the provided services in order to avoid operations being mismanaged within the cloud (Ogigau-Neamtiu 2012).

2.5.5 Reliability

Zissis and Lekkas (2010) explain that the cloud needs to be reliable for the user. Cloud providers have set high standards that are rarely achieved in an internal environment (Zissis & Lekkas 2010). Subashini and Kavitha (2010) illustrate a factor, which is related to IaaS and reliability where the data is stored within the hardware of the provider.

2.5.6 Hackers

Srinivasan (2012) explains that one of the main threats for an organization using cloud computing are hackers, which creates attacks that can lead to loss of integrity, confidentiality or availability of data.

3 Research methods

3.1 Research perspective

This research has taken on a hermeneutic perspective. Kvale and Brinkmann (2009) explain hermeneutics as the study of the interpretation of texts. The meaning of a text from a hermeneutics perspective is meant to attain a valid and mutual understanding (ibid). The purpose of choosing this perspective is to help the researcher to obtain a deeper understanding of the research area by interpreting theory and empiricism. Bryman and Bell (2015) describe it as a conducted form of interpretivism that creates an understanding of human action and its social world rather than defining it, which for the purpose of the research is an essential part. By questioning companies about the security, a deeper understanding is required in order to gain appropriate answers from them.

The hermeneutical perspective has been fundamentally important for this research, both for the interpretation of the empirical part, and for the collection of the literature. It was especially important because there is currently no research regarding security aspects from an organizations point of view, therefore there was a large need of interpretation. When analyzing these parts, the study benefited from what Kvale (1996) explains as a hermeneutical circle, which is explained as a process of the interpretation. Kvale (1996) means it is the way the interpretation of meaning is characterized. The process of understanding the texts takes place from a process where the purpose is to determine the global meaning of the separate parts conducted (ibid). The closer determination of these parts may change the anticipated way of meaning, which will be helpful during this research (ibid).

Kvale (1996) describes it as an infinite process, even if it will end in practice when a sensible meaning has been accomplished. Throughout this research, the hermeneutical circle has been assisting to not only collect the data, but also to further grasp an understanding of its meaning. When there were obstacles, the circle helped tackling these problem that concerned understanding and categorizing data. The circle mainly functioned during the analysis, where it had its largest impact and where the interpretation assisted to generate a result. The result found from the analyzing step would probably be different without the help of the hermeneutic perspective. As a result, from the hermeneutical circle, generated in the first outcome in the process explained by Kvale (1996) as the hermeneutical canon, which is a back and forth process between all the parts within the circle.

According to Kvale (1996) the next canon and step is that the interpretation continues, but was not finished until ‘Good Gestalt’ was reached. ‘Good Gestalt’ is explained by Kvale (1996) as when texts are free from logical constrictions within an inner unity. The third canon focuses on the testing that will be outdrawn towards the global meaning and place the text against and in a comparable position with other authors (ibid), which were made within an early stage of the analyzing part. The purpose of the fourth canon is to focus on the autonomy of texts, where it should be understood on the reference basis given with an explanation of what theme the text has (ibid). Obtaining knowledge about the theme is explained as the fifth canon, where explanations of texts are prepared (ibid). This is the part where the aspects started to appear that led to finding the results. Interpretation of texts for the sixth canon involves focusing on that the text is not presuppositionless (ibid). This was an important element, which Kvale (1996) explain as the researcher shall not cross the line in relation to the traditions concerning the interpretation of data. The last canon, clarifies that for every

interpretation there is an improved understanding that involves innovation and creativity (ibid).

The choice of research perspective gave the opportunity for finding an answer to the research question applied for this research, but also for achieving the aim. Companies may be aware of these security problems that can occur in a cloud environment, as discussed by Ogigau-Neamtiu (2012) it is important to find what the problems are. By applying this hermeneutical perspective companies are not in need of describing all the detailed security problems within the organization, but more in general. Robson (2011) describes that the hermeneutic approach focuses on how the understanding is achieved rather than what is understood, which is related to the purpose of this research.

3.2 Research strategy

Social theory has many aspects due to its vagueness, therefore the reason for its division into five major aspects (Neuman 2006). One of the aspects is the direction of theorizing that will be particularly used in this research that in turn can be either deductive or inductive (ibid). Neuman (2006) explains deductive approach as when a theory is developed or confirmed with a starting point that includes theoretical concepts and relationships working toward empirical evidence that are more concrete. A hypothesis is often applied with a purpose to test the hypothesis that emerges from existing theories and data (Bryman & Bell 2015). This research has an inductive approach, mainly because there is no current research to conduct a hypothesis on. Furthermore, because there is no intention of applying a hypothesis as it has no relation to the purpose of the research that requires a different strategy. The importance in this research is to understand what companies consider regarding the security aspects and the best way to accomplish that is to take on the empirical world in order to find the answers. Therefore, it is not convenient to select a theory, as this research require more information about companies' opinions and thoughts of security aspects, which currently are non-existing. By deciding upon an inductive approach, it provided a greater opportunity for the usage of the hermeneutical perspective that also was chosen for this research. These two combined together interpret and find the data in the empirical world appropriate for this research. According to Bryman and Bell (2015) inductivity proceeds from existing observations or discoveries that lead to theory. In this research the concluded theory has been created from existing data and the discoveries made. Bryman and Bell (2015) further explain that a research with inductive approach aims to explore different phenomena that might include existing data taken from different perspectives (ibid), which is important when understanding the viewpoints of organizations on a more detailed level regarding the security in cloud computing. For the aim of this research to be achieved, there is an appropriate solution that includes the gathering of data that then withdraws relevant patterns that will lead to creating a theory (Oates 2006).

3.2.1 The role of theory

The role of theory in this research has served as a support for implementing the empirical data, and has also made it possible to analyze and reflect upon the data that has come to be collected. The questions in the interview guide were emerged from the theory. Despite the theory's smallness it has a consistent role that gained the findings in the empirical study,

which in turn answered the research question of this research. The theory consists of information about traditional computing, cloud computing and its services, the advantages and drawbacks of cloud computing followed by the already identified security problems.

3.2.2 The role of empirical data

The role of empiricism in this research has been to illustrate and present what security aspects organizations actually have. The purpose was to find the answer to the research question, and related to the choice of inductive approach, it was to be found from the empiricism. Therefore, the empiricism has been of great importance for the research, mainly because there is no research about it, as well as it essentially steers the focus towards it. The empiricism has therefore been supportive for preserving a created and developed theory. The role of empiricism has been an important part for the analysis of this research, which gave the opportunity to answer the research question.

3.3 Research approach

Within research methods, Bryman (2012) explains that the steering of the research may be divided into two different approaches, qualitative and quantitative. These can either be used separately or combined together (ibid). Bryman (2012) explain that a research with a qualitative approach often emphasizes on words and texts, rather than quantifications when collecting and analyzing data. The purpose of this research was to develop a deeper understanding of what security aspects companies have today. One option would be to choose the quantitative approach in order to generate what a large group of companies consider as security aspects, but it will not be deeply understood. The purpose of this research is to find out the reflections of organizations on a more in-depth level in order to perceive and grasp the organizations opinions and thoughts. Therefore, a qualitative approach was a more convenient choice for this research, because it focuses on the words of the participants and the produced texts. Bryman (2012) explains that inductivism, constructionism and interpretivism are the three research strategies that are frequently used in qualitative research. With the choice of hermeneutical perspective and inductive approach, it will become easier to interpret texts and words rather than quantifications. Features in this research match the typical features of a qualitative research (Robson 2011; Payne & Payne 2015). One typical feature is the usage of inductive logic when collecting data that theoretical ideas and concepts will emerge from (ibid). The focus in this research will be on the participant's description of security aspects regarding cloud computing, it will therefore emphasize on a more subjective point of view that will lead to understanding the meaning of human action (Payne & Payne 2015). The adoption of a qualitative approach facilitates when answering the research question as it includes analysis of words, texts and their meaning. For this research the understanding of the participant's thoughts and reasoning behind their behavior is crucial where quantifications will not benefit the findings.

According to Bryman and Bell (2015) a qualitative approach encourages flexibility for the participants and allows open-questions in the choice of method that result in more freely answers. This was essentially considered in order to create an appropriate research, and with this tool allowed the flexibility that aided when discovering the security aspects. Bryman and Bell (2015) states that the qualitative research approach is closely related to the hermeneutic approach that simplifies the interpretation of the gathered texts. Combining qualitative research and the hermeneutic approach will result in a deep analysis with a broader

understanding of the research. Patton (1990) further indicates that qualitative methods are used by hermeneutics researchers as the establishment of context and meaning of human behavior is in focus. These combined approaches and perspectives gave the opportunity to prepare and develop a solid and well-connected base.

3.4 Research design

Based on the previously mentioned decisions about approaches and perspectives, a case study design has been applied for this research. Kumar (2014) explains that a case study design is often used within a qualitative research, but its establishment is not completely excluded in quantitative research. Bryman and Bell (2015) describe it as an intensive and detailed analysis form of normally one single case, or in some studies extended to two or three. As mentioned before, the purpose for this research where to go deep inside a company to get a further understanding of what they consider as a security aspect with cloud computing and a case study design will help with that. With the opportunity to do intensive and detailed analysis and focus on a small group of companies, will provide the research with great tools.

According to Kumar (2014) the case study design enables the exploring of the aspect to become detailed as the case is studied intensively on an in-depth level. This was an important step to get closer to the results. This is also considered as one of its advantages, along with its usefulness when there is little known in the exploring field (ibid). The relevance of this research design is needed for answering the research question as security aspects required by companies are not included in any existing literature. A detailed level is emphasized for lifting up the required security aspects, which generates the findings of this research. Recker (2012) describes case study as one of the most popular types of qualitative methods, as well as one of the most published and well-established methods, when conducting a research in IS. Recker (2012) defines case study as a method that containing intensive research on a specific phenomenon (case) in its natural setting, in a special period of time.

Recker (2012) also mentions strengths, which was considered when the choice of this design was made. The chosen design allowed the study to have different types of phenomenon from the natural settings of the study related to the information. By applying a case study design the ability of understanding the nature was more likely to occur. These benefits that are provided clarified that this type of design was the most appropriate one for this research. It not only allowed the study of natural settings, but also to learn the state of art and from that create the theory, which is closely connected to the choice of inductive approach. To obtain a deep-level of knowledge from the organizations, it is important to use methods that permit it, which can be conducted from here. It has a closely connection to the qualitative approach and the connection is mainly the context regarding both of them.

There are not only beneficial aspects of a case study, Recker (2012) illustrates that there are limitations with the use of a case study. In this research there is no problem as the choice of an inductive approach has been applied, but it could create problems in other researches, resulting in lack of adequate and support for the evidence. The last limitation outlined by Recker (2012) is that problems can occur from controlled mechanisms, to clarify rival explanations or in some cases a potentially confusing factor (ibid). All these strengths and limitations was fundamental during the entire research, specifically during the empirical part.

According to Kumar (2014) a case can be an individual, a group, a community, a subgroup of a population, an event, an instance, an episode or a city. Therefore, in this research there was a strong focus on two organizations that from now on will be considered as cases. The choice of research design relied mostly on what it can provide to this study. What may distinguish this research design from other designs is that restricted situations or systems are in focus. The possibility of attaining in-depth information is more possible when adopting a case study design rather than including a large sample (Kumar 2014). Therefore, by focusing on two units of cases resulted in a more detailed and beneficial outcome rather than involving a larger sample. A case study often emphasizes on only one single case, but it is still allowed to use two, as it did in this research. The purpose of choosing two cases to include in the intensive analysis, was based on perceiving a more general picture of what companies think and feel and not only focusing on one organization. If instead choosing only one organization to focus on, the view would not have been as wide as when including two organizations. This was evaluated as a good choice, when the both cases operate in different industries and not the same business, which generated in a wider knowledge. The choice of research design is also supported by the choice of hermeneutical perspective as mentioned in the research perspective with the purpose of interpreting texts.

3.5 Data collection

Khan (2014) refers to the methodology as a helpful process when answering the research question and identifying relevant objectives, it furthermore simplifies the conduction of data from different resources. For this research, interviews have acted as a tool for collecting the data. The interviews allowed more focus on that one respondent that participated in the interview and with the help from other adopted approaches and perspectives, attained a deeper knowledge. Bryman and Bell (2015) explain that interviews with a qualitative approach are less structured than the ones within quantitative research, which allows more flexibility in the research. This method is therefore closely related to the previously mentioned approaches and perspectives, because it allows the flexibility within a research. The flexibility of the interviews is beneficial as it is important to understand the security aspects the participants set and their primary reasons in relation to their thoughts. Oates (2006) describes semi-structured interviews as the interviewer introduces a topic which gives the interviewee a chance to talk freely, share ideas, and to comfortably become more expressible. Despite its open-mindedness this method is less manageable from the researcher's perspective compared to other interview methods (ibid). Semi-structured interviews lead to a more conversational type of interview that made it more efficient to conduct.

Semi-structured interviews generally start with a general topic or question asked to the respondent, which commonly are formulated ahead (Recker 2012). The subjects related to the questions and topics was the foundation for the questions asked towards the respondent, as they later on came to be formed into a detailed level. Recker (2012) describes that this interview form provides the possibility to probe for details, because of its flexibility. As explained by Bryman and Bell (2015) the interview topic controls the interview, which it did when the interviews were conducted for this research.

Recker (2012) means that one major advantage with interviews are outlined such as of being targeted and its insightfulness. To find the security aspects within the two chosen cases, it is an important part using a data collection method that leads to insightfulness, to be able to identify the aspects. Recker (2012) presents three benefits with using semi-structured

interviews, which was basis for the decision of applying this type of method in this research. When the semi-structured interviews were conducted it was less intrusive for the respondents as it is according to Recker (2012) seen as a two-way communication. The interviewed participants mentioned parts that are already known, as well as new information that generated the reasons for their answers. The benefits aided the research, for instance by allowing a two-way communication that made the interviews more freely and conversational. This generated with that sensitive topics such as security was easier to discuss with the participants, because it provided a more personal and conversational approach. Security is a sensitive subject for most organizations, and by conducting interviews it became more freely as it was easier to discuss this topic than it would have been if another method was applied. The choice of a semi-structured interview in this research is due to its flexibility that results in the interviewee feeling comfortable enough to share important opinions and ideas. Its advantage underlies in the flexibility of the interview and when to ask which question when needed that leads to a deeper understanding of the thoughts and feelings of the participant. Robson (2011) mentions that there are several types of interviews which are differentiated by their level of structure. It is further indicated that an interview guide must be made by the interviewee that functions as a checklist while the questions can be asked freely in any order including the option to add questions during the interview (ibid).

The choice of method is partly related to the chosen case study design that is presented by Robson (2011). Case study is chosen as the design of this research, and it was necessary to choose a method that will benefit this research. As Bryman and Bell (2015) direct, the interviews were made at a single point of time at one occasion as the case study design that included two different organizations. The organizations participating in the interviews wanted to be anonymous and will therefore be referred to as Case 1 and Case 2 in this research. The interviews were held as a meeting, but with an interview guide as a starting point. The interview guide was formed as the semi-structured interview suggests, with general topics and more general questions that allowed the respondents to speak more freely. The questions were created and formed from the theoretical framework with the purpose to generate answers relevant to the security aspects and therefore the aim of the research. The reason for choosing these exact questions was based on the purpose of the research and its research question. The interview questions aimed to steer the participant's answers towards the findings of this research. The interview guide introduces a few general questions about the organizations that are followed by more specific questions regarding cloud computing and security aspects. The interview guide (Appendix 1) provided a framework for the interview, but several questions and comments were however not based on the guide, they were formed after the respondents' answers.

As explained semi-structured interviews are not as structured as other interviews and allows open-ended questions, which made the interview pleasant for both parts. The duration of the interviews was approximately one hour each and was located within each company. Both interviews were introduced by asking general questions about the organization itself, followed by questions about their current IT situation and cloud computing. The interview guide was used as a tool during the conducted interviews. The interviews were audio-recorded via an iPhone and notes were taken during the interviews as a back-up. The recorded files were then relocated to different hardware to mitigate the risk of data loss. Both interviews were transcribed carefully to ensure that all parts were included, which is suggested by Bryman and Bell (2015).

The purpose of the theoretical framework was to build a stable ground to support the empirical study in this research. The data collection for the theoretical framework was supported from the literature along with the purpose to contribute with knowledge to form the interview guide. Books found at the library of University of Borås were used, in which most of them were recommended in earlier research studies. Scientific articles also contributed to this research, as most of them were primarily found on the database summon on the webpage of University of Borås.

3.5.1 Sampling

Bryman and Bell (2015) explain that when deciding what sampling method to apply there are several decisions that have to be made. The research question partly impacts the decision, mainly because the question provides guidelines on what category of people that will be interesting for the research and therefore focus on (ibid). The decision about which sampling method to use was an essential part for what to include in this research, as it involved companies, respondents and literature. There are different methods and techniques within sampling, which are used as guidance tools (ibid). The sampling methods that have been applied for this research will be presented below.

3.5.1.1 Sampling for empirical data

The choices of organizations and respondents have been essential in order to obtain relevant data from the interviews that are necessary when answering the research question. The sampling for this research was based on a set of criteria which is stated below. These criteria were conducted and organized to include appropriate participants for the research. The criteria were set for both the organization and respondent within it, as their participation was important for gathering accurate and relevant data for this research. To be able to trust the data from both sources, it is important that the chosen participants have knowledge regarding the topic area of the interview. It relies upon the respondents and the answers generated from the interview questions. The criteria are based upon and steered by the research question. Therefore, the sampling in this research was based on the criteria outlined below.

Criteria for the participation of organizations

- Small or medium sized organization
- Daily usage of IT in the organization
- Highly dependent on their current system
- Are currently using traditional computing
- Are currently not using any cloud solution (excluding public cloud services)
- Have been considering adopting any type of cloud computing solution

Criteria for the participation of respondents within the organization

- Have an important decision making position within the organization
- Have knowledge about cloud computing
- Have knowledge about the organization and its working procedures
- Have knowledge about how the data is stored within the organization
- Have been working within the organization for at least two years

In the problem discussion (section 1.3) it is emphasized by Lourida et al (2013) that mostly larger companies are using traditional computing as they are able to afford it. This is the reason why larger companies were excluded to participate in the empirical study. The definition of a small and medium sized company is defined by the European Commission (2009) as an enterprise with less than 250 employees. The criterion that the company must have daily usage of IT and be highly dependent on it, resulted in companies that would not function with the security problems that today can occur. It was also important that the chosen companies were using traditional computing right now, mainly because it is set as a boundary for this research but also because it was an important factor. It was important to choose a company that has been considering adopting a cloud solution for their whole organization, but for some reason decided not to.

The criteria regarding the respondent's knowledge and role within the organization are essential, which was reflected in the decision of including IT managers as participants as their role as decision makers was essential. It was important that the respondent was well aware of all parts and risks that can occur within the organization, to be able to respond. Another factor that was important in this case was that the respondent had been working within the organization for at least two years, so that the information the respondent provided was based on knowledge within the organization.

3.5.1.2 Sampling for literature

The literature has been sampled based on articles and books from databases. When searching through the university database the search was restricted to peer-reviewed publications for scientific articles. Books relevant to the subject were searched and found in the same database. The literature was chosen as a basis and to highlight the research question. Bryman and Bell (2015) describe the importance of source criticism when managing the collection of relevant and accurate information. This research has therefore been restricted to reliable sources as references. The selection of articles was made based on the level of interest for the research and its relevance for answering the research question. Many of them were found through lists of references from previous conducted studies with similar research area. The literature included in this research is relatively new partly because there are many studies and articles conducted about cloud computing as it is a well-known term.

3.6 Data analysis method

Oates (2006) describes two available methods for analyzing qualitative data; textual data analysis and non-textual analysis. Non-textual analysis is implemented when the research method is provided with audio-tapes, sound clips, and videos, photographs and multimedia (ibid). Textual analysis studies the content and meaning of the collected text, and has a

relation to the hermeneutic approach discussed in the research perspective (section 2.1), and will therefore be applied for the analyzing part of this research. For a research with a combination of qualitative approach, hermeneutic approach and semi-structured interviews, the most suitable analysis method according to Oates (2006) is textual data analysis.

The data that was used in the analysis was collected from conducting semi-structured interviews, based on what was mentioned above, the most appropriate choice is to use textual analysis. After conducting the interviews, the transcriptions were transcribed carefully as suggested by Oates (2006). The main idea when transcribing the interviews is to avoid leaving out any data, as all of it has to be included (ibid). The importance of collecting relevant data in an accurate way is crucial according to Oates (2006). Notes were taken during both case studies that served as a helpful role when filling in some of the key words that was difficult to understand from the recordings. Based on the transcriptions, the analyzing part was created. Oates (2006) describes that it is important to have a general impression of the collected data before starting to analyze it further, by glancing at the transcripts again this was completed.

According to Oates (2006) there are commonly three themes, which will create three groups of according to the relevance of the research.

- Segment not relevant for the research,
- Segment relevant for explanation to readers and;
- Segment relevant for research question

The first segment is the data that has no overall relation to this study (Oates 2006). The second segment includes descriptive information that might be needed in describing the context of the research for the readers (ibid). Lastly, the third segment concerns the relevance of the data for the research (ibid). For this research the relevant data was related to the security aspects. This was an essential step where the relevant data connected to the security aspects could be highlighted and therefore focused on, while the rest was filtered away.

Oates (2006) essentially highlights the process of reading through the transcripts carefully several times for ensuring that it all is included; this was repeatedly made after these three segments were created. As the segments related to the security aspects was the focus during the process, they needed to be understood and highlighted. The hermeneutical circle illustrated in the research perspective (section 2.1) was used as a tool when analyzing the data. The importance of it is to prevent satisfaction within an early stage and instead approve a higher chance of interpretation on an in-depth level (ibid). The next step presented by Oates (2006) was to categorize the segments of data, by writing in the margin. The data should be categorized according to the choice of approach, whether deductive or inductive, that has been applied to the research. As this research has taken an inductive approach (section 2.2) the categorization of data was made while reading through the material, it is important to allow the data ‘to speak to you’ (ibid). The categorized data, the documents and collected material were all part of an inductive approach (ibid). Sub categories were created after refining the categories chosen in the previous step (ibid). The categories were interconnected with the segments in order to identify significant patterns (ibid).

A visual table was created for perceiving a clear and structured pattern, it contains statements from Case 1 and 2, with a connection to one of the created security aspects. This was mainly created for a clear insight of how the connection was made. It was important to find these security aspects from the empirical data, because there is no research in this area. By

understanding the data and interpreting it the last step was fulfilled according to Oates (2006), and the theory came to be based on the collected data. The purpose with this connection was to strengthen the identified security aspects with already known security problems within cloud computing. The textual analysis is a starting point for the hermeneutics (Kvale 1996). Kvale (1996) states that in a textual analysis it is appropriate to adopt a certain way of thinking related to the hermeneutical circle. It often starts with a vague understanding as a whole as the different parts are gradually interpreted with time (ibid). It is explained as a back and forth process (ibid). The purpose is not to distance oneself from the hermeneutical circle when explaining the meaning, the purpose is to become a part of it accurately (ibid). According to Kvale (1996) the transcribed interviews needs to be carefully read through during the analysis, which was made in this research in order to obtain an overall picture. Kvale (1996) means that the central themes and certain expressions is preferred to be labeled, especially the ones relevant for the research. In this research important parts were highlighted for categorization.

3.7 Evaluation method

To be able to evaluate the research, Bryman and Bell (2015) mentions a set of criteria, that function as tools for this. The presented and commonly used ones are reliability, validity, and generalizability (ibid). The main purpose of an evaluation method was to evaluate the research after it was done. Despite that these three are commonly used, Bryman and Bell (2015) suggest a more suitable choice for this type of research, which are according to authors more suitable for quantitative research; trustworthiness and authenticity. Bryman and Bell (2015) discuss it as two criteria: trustworthiness and authenticity that as well will become the criteria for evaluating this research.

By applying these criteria, an improved and more accurate evaluation was made. The research purpose is to interpret and collect deep-level knowledge and therefore the methods presented by Bryman and Bell (2015) was the best way of evaluating the research. It is important that the evaluation process is correct and that the research will be presented in a way that shows these two criteria. Both trustworthiness and authenticity have underlying criteria that will be further defined. The choice of adopting trustworthiness and authenticity as evaluation methods relies in the criteria (Bryman & Bell 2015).

3.7.1 Trustworthiness

Trustworthiness is by Bryman and Bell (2015) described as a set of criteria for assessing the quality for a qualitative research. Credibility is the first criterion, which parallels internal validity (ibid). Transferability is the second criterion that is parallel with external validity (ibid). The third criterion is dependability and is parallel to reliability (ibid). The fourth and last criterion for trustworthiness is conformability, and has parallels to objectivity (ibid). All these four criteria have been considered during the whole research, the purpose was to meet them.

Trustworthiness was a significant factor when evaluating and acquiring a truthful research. This is possible by considering it while doing the research. The purpose and research question where according to Bryman and Bell (2015) also needs to be considered during this part. The four criteria are credibility, transferability, dependability and conformability.

Bryman and Bell (2015) explains that credibility is essential when writing and evaluating a report. It is important that the data and literature is credible, otherwise it is impossible to create a good report (ibid). This criterion may be particularly central as there is no existing literature within the field of the focus of this study, which implicates its essentiality and why it must be extra credible (ibid). Different types of techniques can be applied to for assuring the credibility of the research, such as respondent validation and triangulation (ibid). This research will adopt a respondent validation in order to attain a credible research (ibid). The credibility is therefore only controlled by the respondents, as they are the only ones who decide whether this research is credible or not (ibid). The focus is to obtain internal validity, which has the purpose to ensure that this study will test and measure the information intended (ibid).

Transferability is the criteria that Bryman and Bell (2015) explain as it will display if the data of the research can be transferred to further settings. Qualitative research is commonly an intense study as its findings are often oriented into the contextual uniqueness and significance of the subject that is being studied (ibid). Therefore, qualitative research is encouraged to produce an outcome referred to as a thick description with rich details (ibid). Bryman and Bell (2015) describe this thick description as a database for other research. So the transferability ensure that the content can be applied into other studies. Bryman and Bell (2015) explain dependability with the purpose of arguments with an idea to establish a worthy research by applying the trustworthiness criteria. This in turn will provide the researcher to adopt an 'auditing' approach (ibid). It is important that records and notes are saved for every part of the research, as it will deliver dependable data to the research (ibid). Its focus is related to reliability, and ensures that the methods applied are connected.

Meanwhile, Confirmability is when recognizing that the research is entirely objective according to Bryman and Bell (2015). For a research to obtain total objectivity is more or less impossible, however it is discussed by Bryman and Bell (2015) that the possibility equals the impossibility. The purpose is that the research will not be shown in the report, which has been a difficult task as the human mind is always displaying in one way or another (ibid). They further explain that it is important that nor personal feelings or values should be exposed to fulfill the criterion (ibid).

3.7.2 Authenticity

Authenticity is presented as a complement to trustworthiness by Bryman and Bell (2015), which involves a set of criteria that concern a wider political impact from a broader set of issues. These will as well become a complement to trustworthiness in this research. There are five criteria presented by Bryman and Bell (2015):

1. Fairness is the criterion that concerns fairness towards different members, in different viewpoints and from different types of social settings.

2. The second criterion is ontological authenticity, which will help the members to obtain an improved understanding of the social setting.

3. Whether the members learned to appreciate the other members from different perspectives is explained as educative authenticity.

4. Catalytic authenticity is whether the research has worked as a force towards the members, if they have changed their circumstances.

5. The last criterion is tactical authenticity which evaluate if the research has empowered the members for them to be able to take necessary steps engaging in action.

3.8 Summary of research methods

The chosen methods and approaches for this research provided an opportunity to achieve the aim of the research. The combination of a hermeneutical perspective, inductive approach, and qualitative research made it possible to focus on texts and words and from the collected data create a theory. The case study design and conduction of semi-structured interviews made it possible to dig deeper within the two organizations and ask questions based on the respondent's answers. The textual analysis provided these tools with a form of analysis that had its basis in texts and words and was therefore an appropriate choice. The purpose of choosing trustworthiness and authenticity as evaluation tools was to ensure that the research was accurately evaluated with fairness regarding all parts of the research. The combination of these applied methods and approaches are closely connected to each other and have set a stable base for the entire research.

4 Empirical Study

The collected data from the two organizations that participated in this research will be outlined in this chapter. As defined by Kumar (2014) a case can be an individual, a group, a community, a subgroup of a population, an event an instance, an episode or a city. Therefore, both companies and respondents will be referred to as cases in this research, with an identifying number for separating the two organizations.

4.1 Case 1

4.1.1 Background

The first interview was conducted with a company that will be referred to as Case 1 with a business operating in the fish industry. Case 1 produces, sells and manages different variations of fish and seafood, from seas and lakes. The range of the additionally provided products includes sauces, pates and salads. The company is family owned and was established in 1880, that in 1980 came to be fused with another company. Case 1 is most known for its fish stores in Gothenburg that along with their sister company in the group, composed with further companies operating within the same field. The offered products are mainly sold to large retail chains, but to institutional kitchens and schools as well. The distribution reaches the entire country of Sweden, including large exports to Finland and Russia. Currently Case 1 has approximately 60 employees, but it is indicated that it depends on the season and therefore it could slightly vary.

4.1.2 The respondent

The interview was conducted with the company's IT manager referred to as Case 1. The interviewee has been employed within the company for 16 years with 28 years of work experience within the IT field. The previous positions included handling several large IT systems with roles such as consultant, systems administrator and database administrator. The working experience even included managing a self-owned company at one point. The role as IT manager within Case 1 includes major tasks within IT that concerns the whole group of companies because of the shared resources.

4.1.3 Current IT system

According to Case 1 the company has currently an in-house solution for managing the IT department. This solution was created several years ago that has remained as it is delivering and meeting the needs of the organization. The solution is placed in two computers in two different computer rooms, in prospect of the company. The IT systems are operated from five large servers as the data storage and its data is replicated inside the computer room. Case 1 is currently using a 100 percent virtual desktop infrastructure (VDI) solution, where one physical server visualizes one of the economy assistant's computers. The VDI and Citrix are combined with Microsoft and Windows 7 where they have 60 clients. The solution obligated today is functioning and structured in a manner suitable for the business and its processes and

tasks within the industry. The determination for Case 1 is to continuously strive for improved and faster solution for the IT system.

4.1.4 Security and cloud computing

Case 1 claims that their system is secure in relation to the safety of their operation system as it is an important factor for their company. The reason for its importance is because of them handling fresh products such as seafood, therefore the availability is crucial. Case 1 explains that the function of the system must be 99, 99 percent. The possibility of one computer room to stop functioning for different reasons is high, however there is the other computer to rely on, whether automatically or manually and is therefore used as a backup. It is further explained that if a problem with the system occurs, it will affect and have consequences on the production department and knowing whom to deliver to. If the system crashes there is a need for Case 1 to handle all the fresh seafood themselves, which can result in high expenses. As a solution to this problem the management team within the company has decided that the IT system cannot be out of operation for more than 4 hours to prevent and mitigate these types of situations. Case 1 clarifies that without IT the organization would not function, and that almost every part of the organization is in need of IT in order to function. This includes telephony, accessibility of cards, ability to open gates and doors in the building. During the last 16 years the system has stopped functioning four times. The reasons have been because of infrastructure problems like floods, fire in a cabinet which caused errors in the data storage and problems with refrigeration units. It is highlighted that the system itself has never caused any problems. The current system is a combination of servers that are four years old with data storage since two years back. Similar solutions have been implemented before but provided by different manufacturers, the reason for the change has been because the demand of more space for storage and that therefore resulted in purchasing new ones.

Case 1 mentions their investigating and evaluating of what available cloud solutions there are today. The idea has always been to implement it; however, no decisions have been made. The main reason why the search after different cloud solutions started was related to the services concerning security. The reason also included services linked to email and office packages. For a long time, the options were evaluated due to the interest for solutions regarding backup and data storage. Case 1 reached a realizing with the awareness of that there are pros and cons with the cloud's provided services. The main issue was the financial part; it was over Case 1's budget. It was soon to be acknowledged and realized by Case 1 that it was too expensive for that type of service compared to their current system. Another reason that is indicated by Case 1 is the importance of control. Today Case 1 is managing its own IT system, which permits total control. Case 1 gave an example that if the Internet access somehow became disconnected it would not completely stop the company from running their business, at least not for a short period of time. By adopting a cloud solution this would be impossible in Case 1's opinion. The full control would be mitigated and the system would be impossible to operate without any Internet connection. Another factor is related to the flexibility as the cloud solution provided for Case 1 was not viewed as flexible enough. Case 1 explains that the idea of backup on a cloud was dismissed because they realized early in the process that this came to be an uncertain factor. Today they have control over the backup and became unsure of the cloud solution. Four parameters are mentioned by Case 1 that outwaits the use of in-house. The parameters are: economy, control, performance and flexibility. Case 1

complements that as for their organization the disadvantages weigh greater than the advantages.

A general thought was why Case 1 decided to search for different cloud solutions, but it then came to be explained that there will always be open-mindedness regarding new ideas and solutions. As the current system is in-house, the financial part will always be considered. There is no indication of the dismissal for not adopting cloud computing solutions in the future. According to Case 1 different cloud services will be overviewed as they may be optional for their choice of cloud solution which will guarantee their operations running. Case 1 stated that if the economic allowed, they would prefer to outsource small parts of the IT system such as security, anti-virus or anti-spam. However, it is further stated that this business contains a critical issue as data storage and instincts are hard to switch to a cloud service because of flexibility, reliability and control.

What was mentioned by Case 1 several times was the control. It was explained that the current system, allows full control as well as the entire IT environment, which is indicated as extremely important. Case 1 sees a large amount of disadvantages with cloud computing and states the main ones: flexibility, economy, and availability. Case 1 explains that a high rate of availability is necessary for the daily work and that it would result in a major security problem when a cloud solution cannot guarantee that. With a cloud solution, it would be necessary to have two internet connections to guarantee the availability, which will double the costs compared to what Case 1 is using today. Regarding the performance, Case 1 clarifies that every part of the system is in control, which with a cloud solution will affect the ability of tracking. Case 1 exemplifies a scenario that is used every day, connected to the largest IT part in the company, the production IT. There is a need of special hardware for the products, which therefore is not as flexible as solutions like an office computer. The hardware needs to be connected with the industry associates with a must of providing quick response time. This is a major problem for Case 1 because a cloud cannot guarantee the demanded quick response time, which could result in a security issue for the organization.

Case 1 further explains that there is no industry espionage and that the existing data is not considered as that sensitive. However, they still have requirements regarding the security in the cloud. One of the problems associated with cloud is the transfer of data when changing cloud from one supplier to another. Today this may in specific cases be possible but it is overpriced and not guaranteed safe, as the company is being charged depending on the amount of transferred data. If adopting a cloud solution one of the requirements will be a safe and effective process of transferring data. This type of service is in general expensive for all the involved parties, when transferring data. Case 1 mentions that with some flexibility it would be easier to change over time.

Case 1 explained in the beginning of the interview that most parts of the system are in-house, but that small parts are outsourced, within the economic department, which includes the billing system. During the last few years many different solutions have been considered, but there is still a massive lack of control and flexibility, which is overpriced.

Case 1 explains that they are one of few companies that are not using Microsoft products for email and exchange, and that adopting a cloud mail would annually cost them 70-80 000 Swedish crowns. This is at the moment a too high expense, especially as Case 1 has an own functioning email. By moving all the company's computer clients to the cloud and change everything would be too expensive for Case 1, as their expenses for Internet and data storage

are not viewed as high as they might become if deciding to move to the cloud. Case 1 is not considering it necessary to change the system and is therefore not a priority. It is explained that despite if the future cloud provider would decide to meet their financial demand, it would not be enough as the costs are important. It is further explained that the same is with the other way around, if the price is improved and the company's need is still not fulfilled the adoption will not take place.

Case 1 explain how it is believed that the future regarding this area would appear and think that they still will have most parts in-house, because the need of control. This might be the safest way to ensure that the daily procedures will function all the time. Case 1 probably would adopt cloud services for excellence and services that are not as business critical for them. The main idea in the future is to adopt a hybrid solution where both in-house and cloud is combined. With adoption of such parts as applications which are not profitable to make in-house and also standardized services. To be moving Case 1 completely to the cloud is currently not being reflected.

4.2 Case 2

4.2.1 Background

The second interview was conducted with a shipping company that is nearly exclusively providing wind energy throughout Europe; they are referred to as Case 2. Case 2 operates with an array of multipurpose that particularly drives high-speed aluminum catamarans out for wind turbines. The company was founded in 2008 and has since then grown increasingly with a current staff of approximately 150 employees. The offered services are being provided to North Europe, which is described as 'driving a bus on the water'. Techniques are being driven out along with belonging materials that are included in both the construction and maintenance phase. Case 2 has offices in Gothenburg, Sweden and Copenhagen, Denmark. Today they are leaders in servicing offshore wind farms in Europe; the segment makes up the main client base and continues to grow. According to Case 2 their mission is to provide services of the highest standard regarding all the four most important criteria: health, safety, environment and quality.

Case 2 explains that they have four values to daily navigate in life. The first is to be business minded. Gaining profit is needed to secure the company's future. This leads to the possibility of adding the values efficiency and flexibility. This further adds value to their customers. In order to be efficient and flexible in a meaningful way, there is a need of skills to be delivered professionally, such as high education and trustworthiness. All the mentioned values combined together build the fourth value, which is trust.

4.2.2 The respondent

The person interviewed is a man that has been employed as IT manager at the company for 4 years. The IT manager is originally employed by an IT company in Gothenburg but is hired by Case 2 to be in charge of their IT. The interviewee, who is representing the company and will be referred to as Case 2, is not highly educated within the IT area explains that the experience has been taught through the practical way of learning.

4.2.3 Current IT system

The current system of Case 2 is outsourced and managed by an IT company in Gothenburg that is hired to organize the task regarding IT. The data is stored on site in server rooms located at the head office in Gothenburg. Some of the company's documents are currently stored in a cloud service. Case 2 is pleased with the current system, as long as it is functioning as it should. All their structured files and documents are stored in a KMA (kvalitet, miljö & arbetsmiljö) system, which is a system for quality, environmental and working environment. Case 2 always strive for an improved, fast and more efficient system. One disadvantage with the current solution is when the demand requires restarting the servers, which is not appreciated within the company. However, the search for new solutions for improving the system is always sustained. Case 2 states that the company itself is partly against the cloud because of its uncertainty regarding the security within specific areas. One reason why is because it is not within their control as there is a lack of availability. The concern further relies within the lack of information regarding who is managing the system, as it is managed by a third part supplier. The insecurity relies within authorizing an unidentified part with unknown intentions with the responsibility to control the system.

4.2.4 Security and cloud computing

The entire company is dependent on the IT system and the network, without the system the company will not function. The IT system is a significant part of the daily activities of the business. As exemplified by Case 2, if the network disconnects, it results in the staff to finish their working day as even the telephones are controlled and affected by the system. Case 2 has considered the adoption of the cloud several times, mostly as a comparison to the current IT solution. Mainly the solutions of Microsoft and Amazon have been evaluated, however their solutions were still not entirely convincing. One of the main reasons for deciding not to adopt a cloud solution was the economy. It has not been an economically possible to adopt a cloud solution for the entire company, which may be optional in the future. Case 2 explains that the IT world is commonly being attacked by network terrorists and the attacks are increasing. Therefore, the reason behind the rhetorical question "Is it actually safe to be on the cloud and to allow us being available for this?". Case 2 discusses that it might be one reason why companies may avoid cloud solutions, or that it is the reason why companies decide to move to the cloud. It is stated as a mystery. There is a possibility that the adoption of a cloud solution for each part within the company will not be fulfilled. If a hacker intrudes a cloud, numerous companies would be exposed. On the other hand, a traditional solution with a fire disaster would erase all the data on the servers. This would not occur in a cloud, therefore the reason why Case 2 are feeling double sided regarding this question.

Case 2 explains that the IT Company they decided to hire, is in a near future for providing their own cloud solutions for their customers. The services Case 2 needs to have provided from a cloud would be offered by the same company that manages their IT today. This service will not be offered within at least two years. Case 2 explains that there are existing advantages with applying a cloud solution, but that there are numerous disadvantages as well. One of the main disadvantages according to Case 2 is the uncertainty. As cloud computing is a rather new area it is believed by Case 2 that there is a gap in the field that need to be filled before they enter the cloud community. By remaining the traditional system of storing information inside a company this uncertainty will almost be reduced, because the company itself has the entire control.

Case 2 was recently exposed to a cyber-attack through an email. These types of attacks have been exposed quite often for Case 2 lately. These particular viruses have been sent from emails claiming to be DHL or other post services, as one of the employees has agreed to the mail. Case 2 are currently attempting to reach the data from the backup as current data have been destroyed. Case 2 believes that they probably would be more vulnerable within a cloud, but that they at the same time cannot know for sure. An additional explanation illustrated by Case 2 is if ten companies share a cloud and one of them become hacked the possibility that the virus would reach all the companies in the cloud is greater than in a traditional system. The insecurity is believed to be the most concerning factor. Case 2 further explains that the reason why they been hacked is not because of the company and its system, it is viewed as a coincidence as random viruses always are sent to companies.

Case 2 has during a short period of time grown enormously with a data that is considered to be sensitive. The reason is not because it is a threat towards the company in the sector, mainly because of a competitive matter or that data thieves find it interesting of how they achieved this great progress which has resulted in them becoming leading in Europe. The company has recently finished a few drastic changes within the industry, and it is still under development. Case 2 mentions that when the cloud is proven to be totally secure, they might consider locating their sensitive data on a cloud. In Case 2's opinion it firstly has to be entered by other organizations so that the attacks may be exposed and identified before they enter the cloud. Case 2 believe that nothing is completely solid regarding data security. It is further explained that it is essential to protect their two most sensitive departments in relation to data. These are the purchasing and sales department within the company which contains data that needs to be protected.

Despite all the benefits the company perceives about cloud computing the disadvantages weighs more than the advantages, but it might come to change in the future. One advantage with cloud computing is that the company never has to update or replace hardware. As for now, when the hardware becomes old, they need to replace it themselves. There are other factors that are needed to be considered in this case.

According to Case 2 they are always regarding solutions that would be possible to adopt, but currently there is no need of change. The requirements Case 2 requested from a cloud solution were many. The most important factor Case 2 sensed was missing was availability and that it must not be left with a gap. Without an IT system, the daily operations cannot function, which is currently not completely assured in a cloud solution. Case 2 states that most of the requirements on the current system equal the same requirements that would be required from a cloud system. Another factor that has a major role in the decision is the price, which today is too expensive in parallel to the demand. Case 2 believe that there is too little information available regarding the solutions offered for similar companies as their business operating within the same industry. It is not claimed that the information does not exist, rather the explanations and descriptions of the cloud systems are too briefly to be convincing as an option. The main requirement is the control. During the whole interview Case 2 mentioned several times that they feel insecure and are curious and insecure of how the data is managed in the cloud. Control is a main part of Case 2 and without it they believe problems might occur or that it could discontinue their business growth. In the nearest future it may happen that after adopting a cloud solution, they will adopt an in-house solution or create their own cloud if the resources are demanded by the organization. This decision might affect the business growth as it is essential for the data to be secure; therefore it is believed that the best

way of finalizing that is by managing it themselves. Case 2 states that nothing has been decided yet and that these are only ideas and thought that have been discussed. As Case 2 is currently not in a cloud environment, it is however being considered. The optional solutions cannot meet the demand, which mostly concerns security problems. Therefore, Case 2 will wait until these requirements are solved.

5 Analysis & Discussion

5.1 Analysis

Recker (2013) indicates that qualitative research builds on interpretive analysis that stands for a characteristically subjective activity, which is dependent on the researcher. The research was conducted with the assistance of analysis method explained in the data analysis method (section 2.5). The purpose was to analyze the data collected from the semi-structured interviews, link it to the theoretical framework and from that create a theory. The creation of a theory aims to answer the research question "*What security aspects are identified by potential Swedish users focusing on data storage when implementing a cloud solution?"*. As explained in section 1.3, there is no current research about what security aspects is required by companies when adopting a cloud solution. However, there is current research regarding the security issues that might occur in a cloud. The main focus is therefore in this analysis to analyze the data collected from the two case studies.

The analysis is derived from the data outcome from the two cases in the empirical study by applying a textual analysis method illustrated by Oates (2006). As the strategy of this research is inductive (section 2.2) the focus will be on the data that has been collected in order to create a theory.

5.1.1 Case 1

Case 1 presented an in-house solution where no part of the system lies outside the company. The awareness of cloud computing and its beneficial services where observed by Case 1, but in their opinion their current system are a better solution for them today. Case 1 stated that they are pleased with the functions the system provides for them today. But Case 1 explained that occasionally they have searched for other suitable options, provided from cloud providers, but declined the idea mainly because of the security issues. A cloud solution would to a certain extent provide them with appropriate services needed, but that one of the reasons why the idea of adopting a cloud solution was declined was mainly related to the security issues. The purposeful reason behind the decision of the structure for the empirical data collection combined with case studies and semi-structured interviews, was to receive an in-depth meaning in order to understand the company's feelings and thoughts related to the problem area. Case 1 described that they have not been considering adopting a cloud solution for their entire company; instead it is desirable to adopt solutions regarding specific services with front edge competence. Case 1 stated that they are aware of the beneficial aspects of deploying cloud and are frequently searching for optional solutions, striving for a faster and more efficient system. They view their in-house solution as a secure system; despite the occurrence of problems with one of the servers it can easily be managed by moving their backup. The cost of entering a cloud is an essential factor according to Case 1, which is one of the reasons for keeping the system they have today as it will overdraft their budget. The reason behind the decision of searching for alternative options on the cloud was related to their backup. However, they quickly came to realize the uncertainty within the fields finance, control and security.

5.1.2 Case 2

Case 2 presented an outsourced solution as their current system. An IT company is in charge of managing and maintaining the system that today has most of the control. Equivalent to Case 1, they are aware of the beneficial services that can be provided towards them from a cloud solution. Case 2 explained that they are pleased with the system they have today, as long as it functions. What they further explain that they occasionally have searched for other suitable options that can be provided through a cloud. Case 2 mentions that a cloud solution could provide a certain extent for them with appropriate services needed, but that the idea of cloud solution has been declined mostly because of its security issues and high expenses. The purposeful reason behind the decision of the structure for the empirical data collection combined with case studies and semi-structured interviews, was to receive an in-depth meaning in order to understand the company's feelings and thoughts related to the problem area. Case 2 is more navigated towards the idea of adopting a cloud solution than Case 1, that will substitute their entire system. Their IT department is currently managed by an IT company that within a near future will launch their own cloud services. The development is still in progress. They further state that it is not current at the moment because of problems that need to be solved before entering the cloud. Case 2 explain that the disadvantages of cloud computing weights greater than traditional computing but that it might come to change with time. One of the advantages mentioned is not having to update the software or changing the server when it is out of date. Despite the highlights of the advantages the disadvantages are considered superior.

5.1.3 Security aspects based on empirical data

It has been explained by the two cases that they currently are satisfied with their existing implemented systems, which is sensed as a secure choice. Regarding the features and layout of the current system both organizations are pleased, despite their consideration to apply a cloud solution. As long as the system is functioning there will be satisfaction, however according to Case 2 it might reach a certain point when the awareness of missing fragments will be awakened. Case 1 shared a similar explanation but with a supplementary citation: "From a security and availability perspective, our system is a very good system". Case 2 additionally explains that they want and need a cloud system that has been practiced and tested before considering the adoption. This is mainly because they believe new problems will arise and come to be discovered that concerns the security and features. Particularly as they view cloud computing as a relatively new area. Their clarification is that other organizations will adopt clouds and discover its problems, rather than them primarily carrying out the mistakes. When they eventually decide to deploy a cloud solution, most of the problems will therefore be exposed and eventually solved. Case 1 also explained that the security aspects are only one of the factors for deciding not to implement the cloud solution; the financial part came to have a large impact. As cited by Case 1: "Economy, control, performance and flexibility are the main reasons why we decided to continue with our in-house solution".

Concerning Case 2, who are not managing their own IT department and has instead decided to outsource it to an IT company, indicates that they lack the wide knowledge required for operating their own IT department. The knowledge within IT is essential for the organization's management and performance. This has resulted in allowing an IT company operating the essential part of their company. As stated by Case 2 they are dependent on the

IT drift to function properly or else the consequences will be that the staff will leave for the day.

The IT manager within Case 1 has been employed at the company for many years, with additional experience from earlier positions at different companies managing other systems. The indication refers to the case's different experience of IT including the employee controlling its department. What concerns both cases are the sense they have regarding cloud computing. Case 2 expresses the uncertainties about who will manage and be able to observe the data if a cloud solution would be applied. The worries are as well related to the location of data, where it will be stored, which in turn is unknown in a cloud. They have been attacked by hackers and therefore suspiciousness to the idea with implementing clouds has been awakening. It is for the simple reason that when adopting a cloud solution, the cloud will be shared with other cloud users, and if one user would be exposed to a hacker it can easily affect the remaining users within the same cloud. As this situation is an existing issue, Case 2 believes an essential attentiveness is needed and further protection must be applied towards this direction. With this current problem, it would be necessary to reflect in this direction, as there is a need of further protection. Case 1 confirms another anxiety that includes the transfer of data when changing from one cloud to another. That if they would decide to store their data on a cloud, but after a while decide to change to a new provider, the transfer of the data between these two might result in difficulties of transmission. Although it might be possible, it is extremely expensive as the cloud provider charges depending on the amount of data that needs to be transferred. It is viewed as a security concern, as they might not be pleased with the first solution that then complicates transferring all their data transferring it to a cloud provided by a different provider.

The general outcome of the interviews indicates that both companies are dependent of their IT system. Without an IT system their daily activities cannot be managed. Neither Case 1 nor Case 2 can therefore continue with their operations properly without the availability of the system. Therefore, the need and performance of the system is essential for the organizations by allowing them to continue functioning purposefully. Case 1 explained that because they manage fresh products there is a need of them being sold the same day as problems might occur if the system would stop functioning and not be accessible. If the necessary information is not reachable of whom the products should be delivered to might result in them recompensing for the cost themselves, which can be very expensive. The products are weight by customized scales that are complexly connected to their current system. This specific service is currently not possibly provided by cloud providers. It is explained as a significant factor, in which is essential for the management of the daily activities within Case 1. The necessity of control within a system is explained by Case 2 as a feature they daily strive for. Within a cloud they think the control of the system will decrease in order for them to feel safe and comfortable enough. Similarly, is mentioned by Case 2 that view upgrades and control of the server as a major problem. Despite that a contract will be signed with the cloud provider, both cases will not be convinced and ensured enough. Case 2 view their data as extremely sensitive, mainly because it is still a young company and has during the last years grown tremendously. They are concerned of attacks, not because there is a suspicion that the industry itself will be attacked, but if that was the case then it certainly will be them. It has been previously explained that they have been attacked with virus that encrypted their whole system and stated that the possibility would be even bigger in a cloud, just because of their data. The system they have today is hard to intrude, but is aware that it can be easier in a cloud. Case 1 on the other hand explains that their data is not sensitive; therefore, the location of the stored data is not an issue as they are not concerned about potential hackers or attacks.

The concern relies within how the data can be reached rather than what data they have. The satisfaction has been specified by both companies regarding their current systems. As both have considered the idea of adopting a cloud solution, they have come to decline it mainly because of its security issues.

5.1.4 Security aspects

Oates (2006) suggests to create categories from the data that has been collected, which for the cases included in this research analysis will be based on the security aspects that has been defined. Based on the data that is presented in previous section and in the empirical chapter as well, there is a need of interpretation. It has been outlined that both companies are satisfied with their current system as they believe it is functioning well. The reason why they think that might be related to a safety matter, they do not want to change their current comfortable and well-known management for a completely new one. For Case 1 it may be a more essential factor, because it is a well processed organization that has existed for over 140 years. They have created their own system and added all the essential features themselves that has been formed after the organizational needs and processes. Therefore, they will not easily substitute their current system for a solution that might not meet the organizational needs. However, they are continuously searching for a suitable applicable solution better than the current one. As their business is strongly established and under control the choice of changing their system is viewed as vital. Case 2 is an organization with a solid growth that has led to a leading position in Europe within a few years. Their needs are not as clear as Case 1, because of their constant expansion that will require changes. The IT Company that currently is managing their IT department and system may not be knowledgeable of the company's future plans and all the included changes. Therefore, their current system might be their best of choice to begin with. With a continued growth it might create problems by deciding to preserve the current system without further developments and changes, especially because their data is highly sensitive. A company with an increased growth as Case 2 is in need of upgrading the system and to remain open for new options suitable for the organization. The previously presented factors are connected to a safety aspect.

Case 2 mentioned their need of a system that is well tried and secure by allowing others to make the mistakes first. This symbolizes a security aspect that relates to their lack of trust towards solutions that presently are provided and offered. Trust involves psychological feelings that are difficult to satisfy by only a contract between the parties, as it is an important factor. According to their statements and explanation as they partly are waiting until other companies have made the mistakes before they decide to deploy a cloud solution, clearly demonstrates that there are problems regarding the trust.

As the respondent in Case 1 was an experienced IT manager with extensive knowledge of the company itself and general IT systems, Case 2's decision of hiring an IT company to manage their entire IT department is from a security aspect considered as ignorance. Mainly because their system and IT department is not controlled by the organization itself, instead by the employed IT company that has been given all the responsibilities concerning the IT section. One of the main security aspects are related to the uncertainty of cloud solutions. Case 2 had special concerns about who will view and manage their data, and clarified it as an insecure factor. They are not aware of where the data will be located, which might be related to the security aspect of ignorance, but is more related to the insecurity factor as an unauthorized stranger that is not supposed to, will access their data. Case 1 generally

presented their concerns regarding the transfer of data between two cloud suppliers rather than the data will be viewed and accessed by someone unauthorized. They have explained it as one of their major insecurity towards the cloud.

A concern presented by Case 2 includes the insecurity to share a cloud with other users. This is essential because their previous virus attacks have led to bad consequences affecting the company and its operations. Therefore, in their opinion the possibility to be attacked in the cloud is greatly higher as it is shared by several users. The mentioned factors indicate that their security aspects are based on the organizational need and situation. The need of an IT system is another security aspect presented by both cases. Without their IT system there are difficulties to manage the rest of their system, which in turn affects the operational features. As Case 1 explained with them managing fresh products and the scale for weighing their products as a given example, they are aware of that this solution is not available and therefore not provided by a cloud provider. However, they are in a daily need of this function for their organizational operations. Without this feature to be functioning it will lead to financial loss and arising problems. This type of solution is therefore essential. Even Case 2 are in great need of a functioning IT system, although they are not managing any fresh products and scales. However, they need it for controlling which ship should be sent to which location, as this can affect the trust built between them and their customers that might lead to financial losses. Both cases have indicated their concerns regarding the control of their system. Case 1 explained it as one of the major problems and a reason for why they have not adopted a cloud solution until now. The need of control is as well indicated by Case 2 that currently has no control of their IT system. How their current system is managed might not be similar to a cloud solution as the employed IT Company is highly trusted and provides them with frequent updates during regular meetings. By choosing to adopt a cloud solution the trust might be continued as the IT Company are soon providing their own cloud solutions. For the company to trust a new party and allow them to manage their sensitive data and system is not that different from what they currently have.

Case 1 is not viewing their data as sensitive, and the chances for them to be attacked are therefore small. Case 2 outlines that their data is extremely sensitive, essentially because of their fast growth. This can also be categorized as a security aspect, as they view their data as vulnerable. Their concerns are related to that the data will be located, changed or destroyed. One of the main security aspects is their cautiousness that might be interpreted as exaggeration, more than needed. Both cases would probably prefer, in certain parts of the company, to adopt a cloud solution. They are both satisfied with their system, but the question is if they have done their research properly, and if they are fully aware of the availability of the optional solutions. Some of the features required by the cases are currently not possible to acquire from a cloud solution. Case 1 explained that their future or long-term goal is to have a hybrid solution, where in-house is used for those services that are safer to have in-house and implement cloud solutions for the remaining parts. Currently there are applicable solutions available that might be adopted as some parts can be kept in-house. The same refers to Case 2 as they have already given away the responsibility of managing their IT. What might be asked here is; why not a cloud solution? The reason might either be because of the fear for changes or that they simply are comfortable and satisfied with what they are familiar with and currently using.

Oates (2006) explains that one way to clarify the findings of an analysis is to illustrate them in different types of tables or diagrams. Therefore, a table has been created to show not only the connection between different statements to the security aspects, but also to strengthen the

analysis part and make it more trustworthy. The text above explains how the security aspects have been created, but there are no exact statements cited by the respondents from the case studies. The main purpose of Table 5.1 is to illustrate and present the close connection that occurred between these two factors. It is important to illustrate that these identified security aspects are found and interpreted from the statements.

Table 1: Statements and Security aspects

Statement	**Security aspect**
Case 1: "We are very satisfied with the system we have today and how it is structured. Of course we always strive for a faster and more efficient system."	Comfortability
Case 1: "We want flexibility when changing cloud supplier so that the data can be transferred safely. This is possible in certain cases, but is however too expensive."	Uncertainty
Case 1: "We are not able to work without the system."	Demand
Case 1: "As we are working with fresh fish there is a need for them being sold the same day, otherwise it will cost us highly as we have to pay for it ourselves. We need a system that is available 99 percent of the time."	Demand
Case 1: "The managing team has decided that the system can only be out of function for maximum four hours."	Demand
Case 1: "We are using an industrial type of scale, which we daily use for weighing our fish. We have special hand computers with special hardware that allows this. Right now this solution is not available within a cloud"	Demand
Case 1: "We are in need of great control, without it, the daily functions are severe to control."	Demand
Case 1: "In my opinion, we do not have sensitive data. A problem might occur when transferring data between cloud suppliers. I do not believe our data will be attacked by anyone."	Sensitivity and vulnerability
Case 1: "The future for us may be similar to a hybrid solution, as some parts will include cloud solutions."	Cautiousness
Case 2: "We are very pleased with the system we have today, as long as it always functions."	Comfortability

Case 2: "We always strive for a faster system and always think it is too slow, although it works"	Comfortability
Case 2: "We want the systems to be tried and tested. This way the problem will firstly occur within other companies before they reach us."	Trust, dependency
Case 2: "We do not have any IT department or manager in this company; therefore, we hire a IT company to manage it for us. We are in need of improved control if a cloud solution would be applied."	Inexperience
Case 2: "Our company is slightly against the cloud. We cannot touch it and are not aware of which servers that are used."	Uncertainty
Case 2: "Another factor to consider is that we are not sure who we will be sharing the cloud with."	Uncertainty
Case 2: "If ten companies share the same hardware, and one of the companies becomes hacked by a Trojan the risk of it to be transferred to the rest of the users in the cloud is very high."	Uncertainty
Case 2: "I believe we have very sensitive data within our company. We have grown quickly during the last few years and other companies or persons would find it interesting of how we made it this far. The sell- and purchase department has particularly sensitive data."	Sensitivity and vulnerability
Case 2: "With all that is happening in the world of network-terrorism that is becoming larger and more common. It might result in unsafe for companies to be placed in clouds."	Cautiousness

What can be generated from the table 5.1 is that the security aspects are not randomly chosen, instead they are outlined from the personal knowledge and feelings of the participants regarding the security field. Based on the presentation of the statements and the security aspects in this table, a few security aspects were created, highlighted and interconnected. These security aspects are an important part of the whole research in order to answer the research question.

5.2 Discussion

By analyzing the generated security aspects in relation to the highlighted security issues presented in the theoretical framework, it is being interrelated to the literature in order to strengthen the identified aspects. An aspect is defined in section 1.4 as the way that a person or company view a certain object. A few of the companies' views towards the issues with deploying cloud computing have been identified as discussed and outlined in the table above. The security aspects that have been identified are:

- Comfortability of current system
- Dependency and trust of the IT system
- Inexperience of IT systems
- Uncertainty of the cloud's functions and accessibility
- Demand of the functions of the IT system
- Sensitivity and vulnerability regarding data
- Cautiousness before implementation

Both cases are currently using a self-hosted infrastructure, which by Molnar and Schechter (2010) was presented as a much safer solution than the cloud. That the usage of self-hosted infrastructure is safer than the cloud is agreed by both cases. Organizations nowadays have higher requirements regarding cloud solutions than traditional systems. Traditional computing allows greater control, and is therefore one of the reasons why both cases are pleased with their current system. (Molnar & Schechter 2010) As mentioned by both cases, they desire a faster and more efficient system, but are however pleased with their current implemented solution. A cloud solution would probably provide them with this efficiency and quickness but they may be too pledged to the idea of that nothing might be better than their current solution. A cloud solution provides a wide range of services in which offers the opportunity to only pay for what have been used (Rajaraman 2014). Case 1 that have created their own system that functions properly, believe the costs are too high as their system already functions well. Regarding Case 2, they have decided to agree to an external part managing their system.

Availability is a well-known security issue in a cloud environment according to Ogigau-Neamtiu (2012) that might have problematic effects such as mismanaged operations. It is described by both cases that the system is severe for the functioning management within the company; it cannot be operated without it, chiefly because the system controls everything. The security aspect with relation to how reliant they are on the system can therefore be connected to the availability which is described as one of the main security issues in cloud computing. The need and importance of the system is closely related to its availability. Through availability the system can be reached and therefore functioned to be able to firmly operate the organization's daily activities. As Case 1 mentioned, they need the system to be able to weigh their fresh products. The need of control is another factor that is discussed by both cases, which connects to the confidentiality explained by Zissis and Lekkas (2010). Confidentiality concerns whom is authorized to reach the data, it is an essential part for operating the business (ibid).

One idea why both cases feel uncertain regarding cloud solutions might be because of the problems related to reliability. The cloud is not as reliable as their current systems that might become a threat for them and their organizations. The uncertainty reflects on identical problems such as the fear of unavailability, or fear of not being able to obtain integrity and confidentiality. As stated by Ogigau-Neamtiu (2012), the insecurity if the data will be safe and confidential within a cloud is preventing organizations from adopting a cloud solution.

Hackers, described as one of the main threats to organizations by Srinivasan (2012), are related to the sensitive data that could be found within Case 2. Despite that Case 1 states that they do not have any sensitive data, there is still a chance for them to become attacked by hackers, as well as any other company. As stated by Case 2, when a cloud is shared by several users the possibility of one being attacked or infected by a virus is larger although another company was originally targeted. The data's sensitivity is related to reliability, as the system

needs to be reliable and trusted to protect the sensitive data. As generated from the case studies, there is a significant fear- and cautiousness exhibited by both companies regarding moving to the cloud. This might be an outcome of lack of trust, that the available solutions cannot be fully trusted that in turn relates to the integrity. Particularly as the trust towards cloud computing is frequently highlighted.

The inexperience can be related to Case 2's lack of knowledge regarding managing the IT within the company. Their choice of employing an IT company reflects their trust towards them despite the fact that they claim to dismiss cloud solutions for the exact same reasons. The frequent attacks by hackers, although it is seen as accidental mistakes from the staff, might be seen as lack of updates and security within the company. The reason why they are not updated and well protected is mainly because lack of knowledge. The ignorance of the essentiality of keeping the IT system and its data secure is being ignored by Case 2. This in turn affects the staff with consequences that open doors to attacks and viruses.

Cloud Security Alliance (2009) provides different guidelines for securing the cloud for users. It is explained as having no requirements, rather to help the organizations to protect their cloud solutions (ibid). The purpose of this document is to enlighten organizations to adopt these recommendations that are provided from them, for free (ibid). This would not be a solution for the security problems that might occur if these two organizations decide to move to the cloud, but it can provide help for mitigating the risks of these problems to occur. These descriptions are for five essential characteristics: on-demand self-service, broad network access, resource pooling, rapid elasticity and measured service (section 3) (ibid). Both Case 1 and 2 explain that they will not consider the idea of moving to the cloud until their requirements about the security issues are met. Case 2 however might still consider the adoption, mainly because the IT company that manage their data is creating their own cloud solution, particularly as there already is a built trust between the two parties. A suggestion for the organizations to minimize the risks and problems is to apply the recommendations presented by the Cloud Security Alliance (2009). They illustrate that there is lack of trust towards the cloud solutions, but by using these standards, both cases can reassure that these recommendations will provide a slightly more secureness, than without them.

It has been illustrated that the security aspects discussed and explained by the two companies has a close relationship to the already known security problems. These security problems are in the introduction chapter explained as one of the main reasons why companies decide not to move to the cloud, and can therefore be seen as a threat for the cloud providers and the users. During the two conducted interviews in this research, none of the respondents were informed about these existing problems that might occur in a cloud environment. The statements that they presented has a concern towards the security in a way themselves, maybe never thought about. Their decision for not adopting a cloud solution was based on that it was not safe enough for their business. The security aspects that were interpreted from the statements are more personal than the security problems that were presented in the theoretical framework (section 2). What can be concluded from these aspects is that organizations do not trust a cloud solution, and are afraid. Case 1 explains that they do not have any sensitive data, but it feels more that they are afraid of taking the step to change their business, because they are pleased with their current system. Meanwhile, Case 2 is a fast growing company that, according to themselves has sensitive data, would perhaps loose more and should therefore have larger concerns regarding it than Case 1. But the concerns they have towards cloud computing, and what is illustrated from the security aspects is that all their concerns are actually problems that today can happen to both of them. So to conclude this analysis, the

security aspects that were discovered are closely related to the actual security problems that can occur in a cloud solution.

6 Conclusion

6.1 Conclusion of the results

What have been generated from the analysis chapter were primarily seven security aspects that were outlined based on the empiricism with a connection to the interrelated issues. The purpose was to obtain a deeper understanding of what security aspects companies have regarding a cloud solution. But also to provide knowledge about familiar security issues that might be related to the security aspects. The aim is therefore to answer the research question; *What security aspects are identified by potential Swedish users focusing on data storage when implementing a cloud solution?* The seven security aspects that have been identified are:

- Comfortability of current system
- Dependency and trust of the IT system
- Inexperience of IT systems
- Uncertainty of the cloud's functions and accessibility
- Demand of the functions of the IT system
- Sensitivity and vulnerability regarding data
- Cautiousness before implementation

These aspects are essentially highlighted as they are set by analyzing the empirical study. Based on the presented statements, interpretation was made and the security aspects were identified. It was discovered that the presented security aspects had a close relation to the already known security problems that can occur in a cloud solution. What can be outdrawn is that even if users follow guidelines or suggestions regarding how to protect their data and their cloud solutions, they are not as protected as they would want to. There are still no solutions to these security problems and the time duration until the problems will be completely solved is viewed as long. What can be outdrawn is that organizations often are highly aware of the risks. A reason why companies may not enter the cloud environment until this day is because of these problems. What also can affect the decision is related to the financial part, the type of system required is too expensive for companies today. The impression perceived is that the economical factor might be the largest issue to companies that unitedly relates to their requirements, requirements that today are viewed as impossible to fulfill.

The security aspects mainly concerned the uncertainty and trust which is related to their comfortability of keeping their current solution and system in fear of new changes. Although a contract is signed by both parties, the concerns still exist that chiefly relates to the fact that they may not reach their system when required. The lack of knowledge might be an excuse among the potential users for not contacting the Cloud Security Alliance that provides guidelines for organizations regarding the security of their business and data. Despite the choice of including two companies in this research, there are many organizations that might recognize the outlined security aspects can be closely generated within any business as their security issues are the same.

What can be concluded from this research are the findings of the security aspects that organizations might have towards entering a cloud environment. The main concern is related to the uncertainty of what is being received from a cloud solution, but also that there is a lack of trust towards the services of the cloud. From the conducted security aspects, a close relationship can be identified to the already known security problems. The problems will

therefore strengthen the meaning of the security aspects, and that they are based on real concerns that can be connected to real problems.

6.2 Contribution to the field

The contribution of this study, to the field of Informatics is the identified security aspects. The findings of this research can contribute as a complementary knowledge to why companies decide not to implement a cloud solution. The security aspects, that have not been outlined by either current or potential users in any other research, are proven to be closely related to the outlined security issues with cloud computing. Cloud computing and its security risks are still a rather new topic and it is therefore essential to find and highlight companies' thoughts and feelings regarding this field. Despite the fact that organizations choose to enter the cloud environment, many decide not to deploy it because of its security issues. Although the potential users are aware of its beneficial aspects, there must be reasons for them not to enter the cloud.

6.3 Method evaluation

In this research, different methods and approaches have been applied as discussed and outlined in previous chapters. Each applied method has been serving a different and specific purpose. By applying a hermeneutic approach made it possible to interpret both literature and the empirical data. This has led to the possibility of creating a perspective about the topic area based on the gathered data. The main reason behind the decision of applying an inductive approach in this research relied within the fact that there is no creation of a hypothesis; instead the empirical data was needed in order to create one. In this case it was suitable as the importance is more outstanding because there was no research within the area of what companies require. The result of the research created a theory that was supported by the approach directed towards the outcome. The decision by choosing a qualitative research is currently, after the research has been conducted, still viewed as the most appropriate one.

The qualitative approach provided the opportunity to receive a deeper understanding within the companies with focus on the text, instead of focusing on the collection of large amount of data. With focus on collecting large amount of data, might in particular cases become a more suitable choice if the research would include more participants and be differently intended with interviews conducted by asking more general questions. What might have been an enhanced solution is the gathering of a larger amount of data generated from more than two companies. Despite its awareness, this research is based on security aspects collected from two organizations that might be considered as insignificant, have a keen and noteworthy content, which was the reason why it was considered as enough collected data. The focus in this research was directed towards the case studies with its significant role as the research has a need of deep interpretation with a further understanding of the processes and management within the organizations including their thoughts and ideas about the security aspects. A further understanding was interpreted with explanations behind the motives of their choices.

For this reason, two interviews were conducted, which in turn were assisted by the choice of semi-structured interviews. The decision to apply this type of interview contributed with the opportunity to ask more open-ended questions when necessary. It allowed higher flexibility both for the prepared questions and for the respondents. After the research has come to an

end, it appears that the choice of including focus groups could have been an option, as to include different employees within the company. However, an employee engaged within the IT department is to be expected considering other aspects as their roles require knowledge within the IT field. Despite that decision making tasks are not included in the role within the company, it might have been an interesting contribution to the field of study. This could have resulted in obtaining different perspectives from diverse positions within each organization's IT department regarding the security aspects.

The way of choosing the two companies to participate in the case studies were made based on a range of criteria, to make an appropriate sampling. This was necessary to be sure that the interviews would provide information that would be relevant for this research, but also that the company would be a good choice. This became an effective method of choosing both companies and respondents. The companies that participated met the set of criteria and assisted the finding of an appropriate interviewee within the organization to interview. An existing sampling method would have been an appropriate decision; however the customized criteria set for this research were of a more suitable choice.

The data collection method made it possible to answer the research question, which is the primarily task in a research. Through the collection of data, the textual analysis was applied with the help for analyzing the data. This type of analysis is closely related to all of these approaches, particularly the hermeneutic one that allowed the opportunity to interpret the texts. The tools are essential, depending on the findings and can be explained as puzzle pieces to be able to reach and obtain the result of the research.

6.4 Result evaluation

6.4.1 Trustworthiness

Trustworthiness is explained as one of the alternatives of how to evaluate the findings in a qualitative research. The need for evaluation is necessary to be able to note how worthy the research is. The set of criteria that are included are; credibility, transferability, dependability and conformability. Most guidelines of this research have been used through trustworthiness.

To be able to create a good report it is important that the information is credible as it must be considered within a research. A technique that has been used in this research is named respondent validation. This has been conducted by sending the participated companies regarding what have been said and written down during the interviews. The entire report has been sent out to the participants for an opportunity to reflect upon what has been mentioned. By deciding to send the research to the participants, it created a chance for a second opinion regarding the empirical collection. Through this cooperation it created a closer relation to the participants which in turn lead to the assurance that the empirical chapter is credible.

The transferability of the research is applicable as complementary in other contexts. There is a possibility that this research can be used as there is an existing database with the purpose of evaluating the accurate judgement and worthiness of the research's content. The fact that the different organizations, referred to as cases, identified similar security issues that resulted in the findings of security aspects is not a coincidence. Despite that their operational management differs, their issues and requirements were more or less similar.

Regarding the dependability of the research, the importance of consistency and opportunity to be repeated is requested, which is an element that has been considered during the conduction of the research. All its records from all phases are saved to ensure this.

As this research is qualitative and interviews have been conducted it created difficulties for neutrality. This research needed to be subjective as the interviews must have been interpreted on a depth level. The analysis of the collected data also had to be analyzed therefore the need of subjectivity. Both these factors had an essential role in this research in order to answer the research question, therefore total objectivity was impossible.

6.4.2 Authenticity

Authenticity is a supplement to the criteria of trustworthiness, it contains the sub criteria; fairness, ontological authenticity, educative authenticity, catalytic authenticity and tactical authenticity. The authenticity criteria have not been the main focus; therefore, it has resulted in a role as an underlying factor during the conduction of this research. Its focus is described how faithful and fair the researchers have been described.

Many viewpoints have been considered regarding the criterion fairness. Particularly when deciding upon the respondents and companies that participated in the case studies. The respondents were obligated to have knowledge about cloud computing, but also experienced within the company to be able to answer the interview questions.

To receive more help in order to attain an enhanced understanding is ontological authenticity, which assists to understand the social settings. Through this criterion the understanding was achieved as it was improved, as well as the social settings were possible to comprehend. Educative authenticity has been assisted by appreciating enhancement to the perspectives. The research has considered the criterion catalytic authenticity and made the research more motivational for a change to the circumstances. Meanwhile, the tactical authenticity factor has facilitated for members to take steps for engaging in action.

6.4.3 Further research

The focus in this research has been what requirements companies obligate regarding the security. Therefore, it would be convenient to conduct further research by interviewing more companies to find out if there are any similarities or patterns of the requirements between different organizations. Organizations can be chosen depending on which industry they operate in, with the aim to find similarities or contrasts. For future research this study can be used as an underlying base for the security aspects that already have been required by users.
This research is based on the requirements set by potential customers that have been considering the adoption of a cloud solution. An idea of conducting future research is to compare their requirements with current cloud users and their requirements and view of security aspects.

An additional way to conduct further research would be to understand the cloud suppliers' perspective regarding this matter and if they have any explanations or answers for the potential and current users. The future research can also be based on specific services

provided within the cloud, and what requirements there are depending on each service. The perspectives can be viewed both from a user and a supplier.

- From a user perspective, further research can be conducted of how a cloud can provide protection for the users since these security issues already have been identified, in relation to the security aspects prioritized and requested by potential users.

- From a supplier perspective, further research can be conducted concerning potential solutions provided by the suppliers to the users.

As mentioned by Case 2, cloud computing is still a new field and therefore the existence of problems, but the findings of the problems are comparatively easier than developing solutions for the issues.

7 Reference

Balasubramanian, R. & Aramudhan, M. (2012), "Security Issues: Public vs Private vs Hybrid Cloud Computing", *International Journal of Computer Applications,* vol. 55, no. 13.

Barnatt, C. (2010). A Brief Guide to Cloud computing: An essential guide to the next computing revolution. London: Constable & Robinson Ltd.

Bryman, A. (2012), *Social research methods,* 4.th edn, Oxford University Press, Oxford.

Bryman. A, & Bell, E. (2015) *Business Research Methods*. 4th ed. New York: Oxford University Press.

Chowdhury, R.R. (2014), "Security in Cloud Computing", *International Journal of Computer Applications,* vol. 96, no. 15, pp. 24-30.

Cloud Security Alliance (2009). "Security Guidance for Critical Areas of Focus in Cloud Computing",
https://cloudsecurityalliance.org/guidance/csaguide.v1.0.pdf

European Commission (2003), "Commission Recommendation" nr. C (2003) 1422) *Official Journal L 124, 20/05/2003 P. 0036 – 0041, p.*

Ficco, M., Palmieri, F. & Castiglione, A. (2015), "Modeling security requirements for cloud-based system development", *Concurrency and Computation: Practice and Experience,* ol. 27, no. 8, pp. 2107-2124.

Ganesh Olekar, V.S. (2013), "Cloud Computing: Migration from Traditional Systems to the Cloud", International Journal of Advanced Research in Computer Engineering & Technology (IJARCET), vol. 2, no. 3, pp. 1128-1131.

Hedman, J & Kalling, T. (2002). *IT and business model – Concepts and theories*. Malmö: Liber

Jangwal, T. & Singh, S. (2012), "Cost breakdown of Public Cloud Computing and Private Cloud Computing and Security Issues", *International Journal of Computer Science & Information Technology,* vol. 4, no. 2, pp. 17-31.

Karnwal, T., Sivakumar, T. & Aghila, G. (2011), *Cloud Services in Different Cloud Deployment Models: An Overview*, Foundation of Computer Science, New York.

Khan, S.N. (2014), "Qualitative Research Method - Phenomenology", *Asian Social Science,* vol. 10, no. 21, pp. 298.

Kumar, R. (2014), *Research methodology: a step-by-step guide for beginners,* 4thition. edn, Sage Publicatons, Thousand Oaks, CA.

Kumar, S., Kumar, P., Singh, S.P. & Saxena, A. (2013), "A New Approach for Providing Security Mechanism in Cloud with Possible Solutions and Results", *International Journal of Computer Applications,* vol. 67, no. 12.

Kvale, S. (1996), *Interviews: an introduction to qualitative research interviewing,* SAGE, Thousand Oaks.

Kvale, S. (1996), *Interviews: an introduction to qualitative research interviewing,* SAGE, Thousand Oaks.

Kvale, S. & Brinkmann, S. (2009), *InterViews: learning the craft of qualitative research interviewing,* 2.th edn, Sage Publications, Los Angeles.

Lourida, K., Mouhtaropoulos, A. & Vakaloudis, A. (2013), "Assessing database and network threats in traditional and cloud computing", *International Journal of Cyber-Security and Digital Forensics,* vol. 2, no. 3, pp. 1.

Molnar, D. & Schechter, S. (2010). Self hosting vs. Cloud hosting: Accounting for the security impact of hosting in the cloud. *Microsoft Research. The Ninth Workshop on the Economics of Information Security (WEIS 2010).* Available: [2012-04-20] http://weis2010.econinfosec.org/papers/session5/weis2010_schechter.pdf

Neuman, W.L. (2006), *Social research methods: qualitative and quantitative approaches,* 6.th edn, Pearson/Allyn and Bacon, Boston.

Noy, C. (2008), "Sampling Knowledge: The Hermeneutics of Snowball Sampling in Qualitative Research", *International Journal of Social Research Methodology,* vol. 11, no. 4, pp. 327-344.

Oates, B.J. (2006), *Researching information systems and computing,* SAGE, London.
Ogigau-Neamtiu, F. (2012), "CLOUD COMPUTING SECURITY ISSUES", *Journal of Defense Resources Management,* vol. 3, no. 2, pp. 141.

Ogigau-Neamtiu, F. (2012), "CLOUD COMPUTING SECURITY ISSUES", *Journal of Defense Resources Management,* vol. 3, no. 2, pp. 141.

Olekar, G., Sreekumar, V. (2013), "Cloud Computing: Migration from Traditional Systems to the Cloud", *International Journal of Advanced Research in Computer Engineering & Technology (IJARCET),* vol. 2, no. 3, pp. 1128-1131.

Patton, M.Q. 1990, *Qualitative evaluation and research methods,* 2.th edn, Sage, Newbury Park, Calif;London;.

Payne, G. & Payne, J. (2004), *Key concepts in social research,* SAGE Publications, Thousand Oaks, Calif;London;.

Potdar, A., Patil, P., Bagla, R. & Pandey, R. (2015), "Security Solutions for Cloud Computing", *International Journal of Computer Applications,* vol. 128, no. 16, pp. 17-21.

Rajaraman, V. (2014), "Cloud computing", *Resonance,* vol. 19, no. 3, pp. 242-258.

Recker, J. & ebrary, I. (2013), *Scientific research in information systems: a beginner's guide,* Springer, Heidelberg;Berlin;.

Robson, C. (2011), *Real world research: a resource for users of social research methods in applied settings,* 3.th edn, Wiley, Chichester.

Ryan, M.D. (2013), "Cloud computing security: The scientific challenge, and a survey of solutions", *The Journal of Systems and Software,* vol. 86, no. 9, pp. 2263.
Shipman, M.D. (1997), *The limitations of social research,* 4.th edn, Longman, London.

Sinjilawi, Y.K., Al-Nabhan, M.Q. & Abu-Shanab, E.A. (2014), "Addressing Security and Privacy Issues in Cloud Computing", *Journal of Emerging Technologies in Web Intelligence,* vol. 6, no. 2, pp. 192-199.

Srinivasan, M. (2012), "BUILDING A SECURE ENTERPRISE MODEL FOR CLOUD COMPUTING ENVIRONMENT", *Academy of Information and Management Sciences Journal,* vol. 15, no. 1, pp. 127.

Subashini, S. & Kavitha, V. (2011), "A survey on security issues in service delivery models of cloud computing",*Journal of Network and Computer Applications,* vol. 34, no. 1, pp. 1-11.

The National Institute of Standards and Technology (2010). *"NIST Cloud Computing Program",*
http://www.nist.gov/itl/cloud/

Vairagade, R. S., & Vairagade, N. S. (2012), "Cloud Computing Data Storage and Security Enhancement", *International Journal of Advanced Research in Computer Engineering & Technology (IJARCET),* vol. 1, no. 6, pp. 145-149.

Younis, Y. A., Kifayat, K. & Merabti, M. (2014), "An access control model for cloud computing", *Journal of Information Security and Applications,* vol. 19, no. 1, pp. 45-60.

Zissis, D. & Lekkas, D. (2010), "Addressing cloud computing security issues", *Future Generation Computer Systems,* vol. 28, no. 3, pp. 583-592.

8 Appendix: Interview guide

Opening questions

- Are you approving for allowing us to record the interview?
- Describe the organization briefly.
- How many employees are there currently in the organization?
- What is your role within the organization?
- How long have you been employed at the organization?
- What previous experiences have you acquired within the IT field?

General questions

- What is the organization's current IT solution?
- Are you currently pleased with the functioning of the traditional storage of data?
- Is the organizational data sensitive in your opinion? How sensitive?
- Have you ever considered adopting cloud services? Why/Why not?
- What was the reason for not adopting a cloud solution?
- If a cloud solution was to be adopted which solution would it be? Why/Why not?
- How aware are you of the risks of cloud computing?
- There are studies that indicate that one of the main reasons why enterprises decide not to adopt cloud services is because of its security issues. Do you agree? Why/Why not?
- What are the demanded requirements for deploying a cloud solution in relation to its security?
- Do you believe that traditional computing overweighs cloud computing or vice versa? Define.

Closuring questions

- Are there any further comments you would like to add?
- Can we contact you for additional questions, if needed?

University of Borås is a modern university in the city center. We give courses in business administration and informatics, library and information science, fashion and textiles, behavioral sciences and teacher education, engineering and health sciences.

In the **School of Business and IT (HIT),** we have focused on the students' future needs. Therefore we have created programs in which employability is a key word. Subject integration and contextualization are other important concepts. The department has a closeness, both between students and teachers as well as between industry and education.

Our **courses in business administration** give students the opportunity to learn more about different businesses and governments and how governance and organization of these activities take place. They may also learn about society development and organizations' adaptation to the outside world. They have the opportunity to improve their ability to analyze, develop and control activities, whether they want to engage in auditing, management or marketing.

Among our **IT courses**, there's always something for those who want to design the future of IT-based communications, analyze the needs and demands on organizations' information to design their content structures, integrating IT and business development, developing their ability to analyze and design business processes or focus on programming and development of good use of IT in enterprises and organizations.

The **research** in the school is well recognized and oriented towards professionalism as well as design and development. The overall research profile is Business-IT-Services which combine knowledge and skills in informatics as well as in business administration. The research is profession-oriented, which is reflected in the research, in many cases conducted on action research-based grounds, with businesses and government organizations at local, national and international arenas. The research design and professional orientation is manifested also in InnovationLab, which is the department's and university's unit for research-supporting system development.

UNIVERSITY
OF BORÅS

VISITING ADDRESS: JÄRNVÄGSGATAN 5 · POSTAL ADDRESS: ALLÉGATAN 1, SE-501 90 BORÅS
PHONE: + 46 33 435 40 00 · E-MAIL: INST.HIT@HB.SE · WEB: WWW.HB.SE/HIT