UNIVERSITY OF VAASA
FACULTY OF TECHNOLOGY
DEPARTMENT OF COMPUTER SCIENCE

Sami Niskanen

DESIGNING A COMPUTER SYSTEM FOR REMOTE OFFICES: TRADITIONAL SYSTEM VERSUS CLOUD SYSTEM
Case: Church council of the Evangelical Lutheran church of Finland

Master's thesis in

Computer Science

VAASA 2012

VAASAN YLIOPISTO

Teknillinen tiedekunta

Tekijä: Sami Niskanen

Tutkielman nimi: Suunnitelma tietokonejärjestelmän rakentamiseksi etäpisteisiin: perinteinen järjestelmä verrattuna. pilvipalveluna ostettuun järjestelmään. Case: Suomen evankelis-luterilaisen kirkon Kirkkohallitus.

Ohjaajan nimi: Merja Wanne

Tutkinto: Kauppatieteiden maisteri

Oppiaine: Tietotekniikka

Koulutusohjelma:

Opintojen aloitusvuosi: 2008

Tutkielman valmistumisvuosi: 2012 **Sivumäärä:** 54

TIIVISTELMÄ:

Tässä työssä vertaillaan keskenään kahta mallia rakentaa tietokonejärjestelmä. Vastakkain ovat perinteinen malli ja pilvipalvelun malli. Työssä käydään läpi viitekehys eli kirkon ja Kirkkohallituksen tietotekniikan historiaa, nykyisyyttä ja tulevaisuutta. Sen lisäksi tutustutaan järjestelmien historiaan, nykyisyyteen, tietoturvauhkiin ja hinnoitteluun. Tutkimus on tyypiltään konstruktiivinen.

Aineistoa työn kirjoittamiseen oli käytettävissä todella paljon. Pääosa aineistosta löytyi yliopiston Nelli- tietokannan aineistohaulla ja aineisto ja lähteet kuvaavat ja tukevat hyvin työn kulkua. Työssä on mukana myös kirjoittajan oman kokemuksen myötä syntyneitä ajatuksia ja faktoja kirkon tietotekniikasta, ja arvokasta apua saatiin myös tietohallintoyksikön johtajalta haastattelun muodossa sekä yhteistyökumppaneilta.

Yllättävää oli se, että vaikka pilvipalvelut ovatkin puhutuin uusi asia IT-maailmassa juuri nyt, niistä ei juuri löytynyt yleistieteellistä tietoa, muuten kuin tietoturvan osalta sekä joitain yksittäisiä suppeaan alaan keskittyviä tutkimuksia. Esimerkiksi palveluiden hinnoittelun määrittäminen oli hankalaa. Pilvipalveluiden hinnoittelusta esitellään työssä kuitenkin joitakin malleja.

Tutkimustulos, eli johtopäätös, oli se, että nykyisillä tiedoilla on järkevämpi rakentaa järjestelmä perinteisellä mallilla. Syynä tähän ovat käytettävissä olevat resurssit, käyttäjien ja IT-henkilökunnan tietotaito sekä pilvipalveluiden hinnoittelun vaihtelevuus.

AVAINSANAT:

Pilvi, palvelu, järjestelmä, suunnittelu, etäpiste

UNIVERSITY OF VAASA

Faculty of technology

Author: Sami Niskanen

Topic of the Master's Thesis: Designing a computer system for remote offices: traditional system versus cloud system. Case: Church Council of the Evangelical Lutheran church of Finland.

Instructor: Merja Wanne

Degree: Master of Science in economics and administration

Major subject: Computer science

Degree programme:

Year of entering the University: 2008

Year of completing the Master's Thesis: 2012 **Pages:** 54

ABSTRACT:

This thesis is about a comparison between two models for building a system, a traditional model versus cloud model. The thesis looks through the framework which is the history, present day and the future of the It in the church and the Church Council. It also takes a look at the history, the present day, security threats and costs of the systems. The type of this study is constructive.

There was a lot of material in use. A major part of the material was found through the university's Nelli database search and the material and references describe and support the thesis well. There are also thoughts and facts about the information technology in the church, rising from the writer's own experience. Valuable help was also received via an interview from the manager of the ICT-Management Unit, and also from partners who are in cooperation with the church.

Despite being the most talked about subject in the IT world, there was not much generally scientific information about cloud services, only some researches covering a small specific area. For example, defining the costs of the service was difficult. However, there are some pricing models introduced in this paper.

The conclusion was that given the present information, it is more reasonable to build the system the traditional way. The reasons for this are the resources in use, the know-how of the users and the IT personnel and the variance of the cost of the cloud services

KEYWORDS:

Cloud, service, system, design, remote office

TABLE OF CONTENTS **page**

1. INTRODUCTION

The purpose of this thesis is to investigate what are the costs, possibilities and threats when building a computer system for remote offices of the Church Council of the Evangelical Lutheran church of Finland. This paper also states different aspects of building the system the traditional way compared to using cloud services. This thesis also investigates, would the costs intersect and also what other factors should be considered when building the system in question. The system is to be designed to help the remote offices cope with most of their daily computer-related problems or to possibly remove the problems altogether. The computer system would consist of a server serving the workstations and users for file services, DHCP-service for distributing IP addresses for workstations (also network hardware and multifunction copiers), a virus protection and its administration service and a service for software updates.

The system can later be expanded to include Virtual Local Area Network (VLAN) and Wireless Local Area Network (WLAN) services for external users and guests of the organization in the remote offices. The server or servers can also be used to control information security issues within the network, such as Network Access Protocol (NAP) and for distributing software and updates.

The remote offices mentioned in this thesis are the ones currently under the IT support provided by the ICT-Management Unit of the Church Council. These are the Department for Advanced Training in Järvenpää, the Church Research Institute in Tampere, the Office of the Archbishop in Turku, the Diocese of Espoo and the Diocese of Porvoo, which is maintained by the Department of Activities In Swedish and the IT support and IT related development of which is appointed to the Swedish speaking IT consultant.

Other remaining dioceses, 7 altogether, may be incorporated later, depending on the decisions made by the Central Church Fund and the ICT-Management Unit. At the moment, preliminary plans have been made about incorporating them into the IT domain of the Central Church Fund, starting from the first half of 2012. This would mean a great amount of more work for the IT support team and the ICT-Management Unit. Therefore a system to help the remote offices as well as the dioceses would be extremely beneficial. Also, the possible training of the personnel to take care of some issues should be taken under consideration. According to the enquiry in May 2011 and charting in January and February 2012, the IT support in the dioceses is the responsibility of their personnel. Some have also hired 3rd parties to take care of the support and other issues. If or when all the dioceses are incorporated, the IT support provided by the IT support team of the Church Council would become a valuable addition to the existing arrangement.

1.1. Description of the problem

The need for developing such a system rises mainly from the problem of network traffic generated by the use of bandwidth to save files and other data to a server located in Helsinki, even as the reliability and speeds of network connections have improved over the years. Depending on the network traffic during the busiest hours of the day, retrieving and saving these files can be extremely slow. Furthermore, workstations and network devices in the remote offices use static IP addresses, which makes administering and maintaining them difficult. Also, the frequent updates for Microsoft Windows based systems can be large; especially the service packs for operating systems and office programs. These issues and the fact that some dioceses have old and unreliable hardware in use, lead to a need to develop a system that is reliable, user-friendly and less expensive.

Because of arrangements described above, IT support persons travel frequently to the remote offices to solve problems which could be solved remotely from the main office or perhaps even avoided altogether. IT support travels to remote offices also to install programs that could install automatically. Furthermore, by creating a small system with a server, the use of workstations in the remote offices would be smoother and the load of network traffic to and from the main office would decrease, even significantly. Due to the new system, both the IT support and also the personnel in the remote offices could save considerable amounts of time and effort.

There are two alternatives to be considered when building this computer system. It can be built either the traditional way, when all hardware and software are bought and the system is designed to serve users as long as its capacity is adequate. When more capacity is needed, the servers and workstations alongside the network hardware are renewed or updated to meet the new requirements. The second way to build the system is to buy it, or parts of it, as a service. Nowadays, cloud computing is what the computer world -and users- are excited about. Software and services, and even hardware can be bought or rented as a service from a service provider and they can be managed, updated and grown virtually. All happens in a matter of seconds, and when it comes to server capabilities, virtual servers can be updated almost without limits. They are also very easy to maintain with remote desktop connections. Cloud computing is growing as the costs decrease and as new service providers enter the field.

1.2. Research approach

The approach in this study is constructive. It means that the system in question is being designed at the same time as this thesis is written. A considerable amount of findings, basic knowledge about the information technology used in the church and conclusions are the writers own. Naturally, scientific references are used as a base and as sources of theories and they are mentioned as needed.

At first, this thesis was supposed to introduce a timeline in which the costs of the traditional system and the cloud system would have been introduced and it would have shown if the costs would meet at any point. From that point on, it would have been less expensive to continue using the cloud system compared to a traditional system. However, time and other limitations molded the thesis towards its current appearance.

The motivation for this thesis rises also from the fact that the information technology used inside the church and the Church Council is fundamentally quite simple. This is in its part due to the fact that most of the personnel are not computer specialists, but normal office workers. It is not possible to have personnel perform very challenging tasks and the ICT professionals of the Church Council do not have the time to take care of every task. The system is being designed to help these tasks and possibly automate some of them, and also to reduce the time between a request for assistance and a solution.

1.3. Previous researches

There are not any major researches made inside the church in this field. Of course, there are literally hundreds of researches about system design and computer systems made worldwide, and the amount of researches on cloud computing is overwhelming. This is naturally a good thing, especially regarding the writing process of this thesis. There are also several researches about clouds and their fundamentals, security and characteristics. There will be references to these researches along the way, but here is a quick look at them. Finding the research papers was not a problem. Credits for this go to the university library's excellent Nelli -database. There were even too many papers to choose from and it took a while to read the abstracts of each one to determine whether or not it qualified.

The real problem was that it was quite hard to know what search terms to use to pick out the relevant researches. Hardest part was without a doubt finding contemporary researches about client/server technology, as the technology itself dates back to early 1990's. The basic idea behind it is however still valid today.

Zhang, Zhang, Chen and Huo compared the difference between grid computing and cloud computing in 2010, and Kantarcioglu, Bensoussan and Hoe published a research paper about the risks of cloud adoption in 2011.

1.4. Composition of the thesis

This thesis constructs of seven main sections and their subcategories. In the first one, the subject of the thesis and main problem are introduced and defined. The second one focuses on the framework, in other words the organization and the environment where the system in question is to be built and on the history and development of that environment.

The third section discusses the design of the system, when it would be designed and built the traditional way using both existing or purchased hardware and software, along with specification of costs and possible threats to the system. The fourth section introduces the design made with cloud technology, including the threats and some cost models. The fifth section brings the conclusions and findings to light, sixth section is for the references and the seventh one lists the appendixes.

2. CHURCH ORGANIZATION

Today, about 78 per cent of Finnish people are members of the Evangelical Lutheran Church. This, among other things shows that the church is a respected institution in Finland. Most Finns come into contact with the Church every year due to family occasions like weddings, burials and confirmation but many Finns attend church only a few times a year, usually at Christmas and Easter. (Evl.fi 2011.)

Today Finland no longer has a state-church structure in the exact sense of the term. The system has been dismantled to give greater internal independence to the Lutheran Church. It consists of 9 dioceses and 449 parishes (as of January 1st 2011). Each parish is an independent working unit. The Church is responsible for its own finances and the parishes receive some 75 per cent of their total income from church taxes. (Evl.fi 2011.)

Some speak of the Evangelical Lutheran Church of Finland as a state church, while others call it a folk church. However, both labels are somewhat misleading, but if they are used in the correct context, they remain useful as they still give a rough picture not only of the position of the church in Finnish society, but also of the relationship between the church and the state. (Evl.fi 2011.)

To totally understand the current religious situation and church politics in Finland, it is important to bear in mind Finland’s strong state-church oriented tradition. The continuous state church situation has not only been a feature of the legal relationship between the church and the state, but in its time it set the tone for the nature of the state. (Evl.fi 2011.)

The Lutheran Church’s autonomy in internal affairs is further protected by the fact that the national Parliament, which ultimately ratifies church law, has no right to alter the content of the proposals it receives from the Synod. All proposals must be either accepted in their original form or rejected altogether. (Evl.fi 2011.)

The most significant change has been the introduction of a new procedure for Episcopal appointments. As a result, the bishops are no longer appointed by the President of the Republic. The new procedure involves an election consisting, if necessary, of two rounds of voting, after which the winning candidate receives an official letter of appointment from the diocesan chapter. (Evl.fi 2011.)

Another significant area of contact is the system of guarantees for the church's financial position. Based on its public rights in state legislation, the church is entitled to collect taxes. In addition to church members, societies and corporations are also required to pay church taxes, with the exception of registered religious organizations and so called "free-thinker" societies. (Evl.fi 2011.)

The church itself, in providing certain social services, is nurturing an ongoing relationship with the state. This is seen most clearly in that parishes continue to take responsibility for maintaining census registration data concerning their members, and for their funeral services. (Evl.fi 2011.)

In spite of the abundant and diversified contacts between the church and the state, Finnish Lutheran Church should not be classified as a traditional state church. The most decisive reason for this lies in the great internal autonomy of the Lutheran Church. State authorities cannot become involved in decisions concerning the church's internal affairs. Therefore, local parishes have broad economic independence and autonomy, as does the Synod. (Evl.fi 2011.)

2.1. Implementation and management of information technology in the church and in the Church Council

Like many organizations, also the Church Council existed long before any kind of information technology was available. Nonetheless, the employees had to communicate to the outside world somehow. Letters were written with mechanical typewriters, some by hand, and landline telephones were used to reach people faster.

There have been computers and some sort of computer support in the Church Council since the 1980's, and in the early 1990's a group of church officials decided that the Church Council needed to keep up with the rest of the world. They hired a manager for the computer team and at first, in 1994, the team consisted of just two people, a manager of the team and a designer. Later that year, a few more people joined the team and during that year, a total of five people worked in the unit: a computer specialist, the manager of the team, two temporary PC support persons and a secretary. (Karjalainen 2012.)

The unit grew slowly and in 1998 there were five persons with permanent contracts in the unit: manager of the unit, an analyst, two designers and a secretary. In the year 2000, a concern about the well-being of the unit's employees due to massive work load was brought up, and two more positions were declared open and later filled, totaling the number of the unit's employees to seven. As the writer of this thesis joined the unit in 2001, there were ten persons in the unit. An interesting point is that in the whole church, there were five or six full-time IT professionals in 1994. Today there are 130-150 of them. (Karjalainen 2012.)

In the end of 2011, there were 15 persons working in the ICT-Management Unit. The unit is responsible for developing and maintaining the computer systems that help the church in its main actions, economy and administration and for supporting the personnel in using them (Sakasti 2011).

This was and still is the leading thought with the ICT-Management Unit, only today it has focused on larger projects like the system for membership of the church and the IT coalitions of the parishes and parish unions. Nevertheless, it is very important also to develop and maintain the basic ICT infrastructure within the Church Council.

The information technology and the IT architecture used in the Church Council today is rather modern, but is based on a practical client/server system like in most organizations. The Church House was equipped with computer cabling in the early 1990's, before that there was none or it was mishmash, to say the least. After the implementation of the network, all the employees got new personal computers, despite the recession in Finland during late 1980's and early 1990's. The users even had an email application in use. All this was due to a data administration strategy, which had been compiled since 1993. Re-writing this strategy was the first task of the present manager of the ICT-Management Unit, when he entered the Church Council (Karjalainen 2012).

The strategy included the construction of the CHURCHnet, the churches own network into which all parishes are connected. The need for building such a network rose from requirements from the Finnish Population Register Centre. In 1994 and 1995 there was some discussion between the state and the church about the role of the parishes in the population census in Finland. The government's opinion was that all the work done with pens and papers in the parishes had to be digitalized. The registry offices felt that it was extremely difficult and time consuming to handle the hand-written papers sent from the parishes, when 40000-50000 children were baptized every year and the papers were sent to the registry offices. (Karjalainen 2012.)

Slowly the amount of parishes attached to the CHURCHnet grew, and in 1999 the Finnish parliament ratified a census law reform. The church was given a five-year transition period, and all parishes were obliged to do their share in the population census digitally by the end of 2004, communicating with the Population Register Centre via the CHURCHnet. (Karjalainen 2012.)

In the end of 1994, the government had launched a strategy concerning data networks. The strategy stated that the networks were to be built by ISO's OSI standards, and at the same time, the IP technology was taking over the world. The church in Finland chose to start using IP technology in their networks, as well as with email applications. (Karjalainen 2012.)

Most computer users have up-to-date laptops with wireless and mobile, e.g. 3G network capabilities and working from home or remotely is made possible via a simple login page, although there is a sophisticated and complicated system behind it. In October 2011 all users in the church Council were registered in a new domain which makes working remotely possible and easy. Also the mobile phones have email applications and work email in general can be read from any computer connected to the Internet. There are about 370 workstations in use, most of them being laptops with docking stations and large 23- or 24-inch displays. Most of these workstations are located in the Church House. During the first half of 2012, all workstations are being renewed. All of them are going to be laptops with docking stations and large wide screen displays.

The Church Council has some fifteen servers in use. Some servers are located in Katajanokka, inside the Church House and some are located in the service providers' locations. These servers have different tasks, for example print server, DHCP server for managing and distributing IP addresses and domain controllers, through which the employees log in to the private corporation network.

The private network has changed a few times, the latest being a migration from an old Active Directory domain to a new one. This migration was carried out in 2011, and it included the Church House, the Department of Advanced Training, the Church Research Institute and the Diocese of Espoo. Also the IT coalitions around the country carried out similar migrations. All of these Active Directories in the church are a part of a larger forest, so that different domain controllers of the IT coalitions (of the parishes and parish unions in different parts of Finland) can have trust relationships between them. This then again means that where ever a church employee goes, he or she has a specified username with what they get most of the same services anywhere, which they get when logging on to their home network. This username follows the user through their career within the church, and is erased when he or she leaves the organization.

The future of the church is in the hands of the citizens. This might sound rough, but as the activity of the church in Finland is dependent on its members and their tax money, it is obvious that the church must prepare for the future. This of course means that if and when the money doesn’t flow in as it used to, the church and the Church Council must decrease the largest expenditure; personnel (Karjalainen 2012).

With the help of information technology, the personnel that is facing more and more challenges can survive. Personnel and travel costs can be reduced by letting technology take care of some operations and also by enabling the personnel perform operations remotely. New, reliable technology and coalitions between different units can also help smaller units cope with challenging times. (Karjalainen 2012.)

In the figure below, there is an organizational chart of the Church Council. The ICT-Management Unit was a part of the Administration Department until the beginning of 2008 when it was transferred to be a part of the Finance Department.

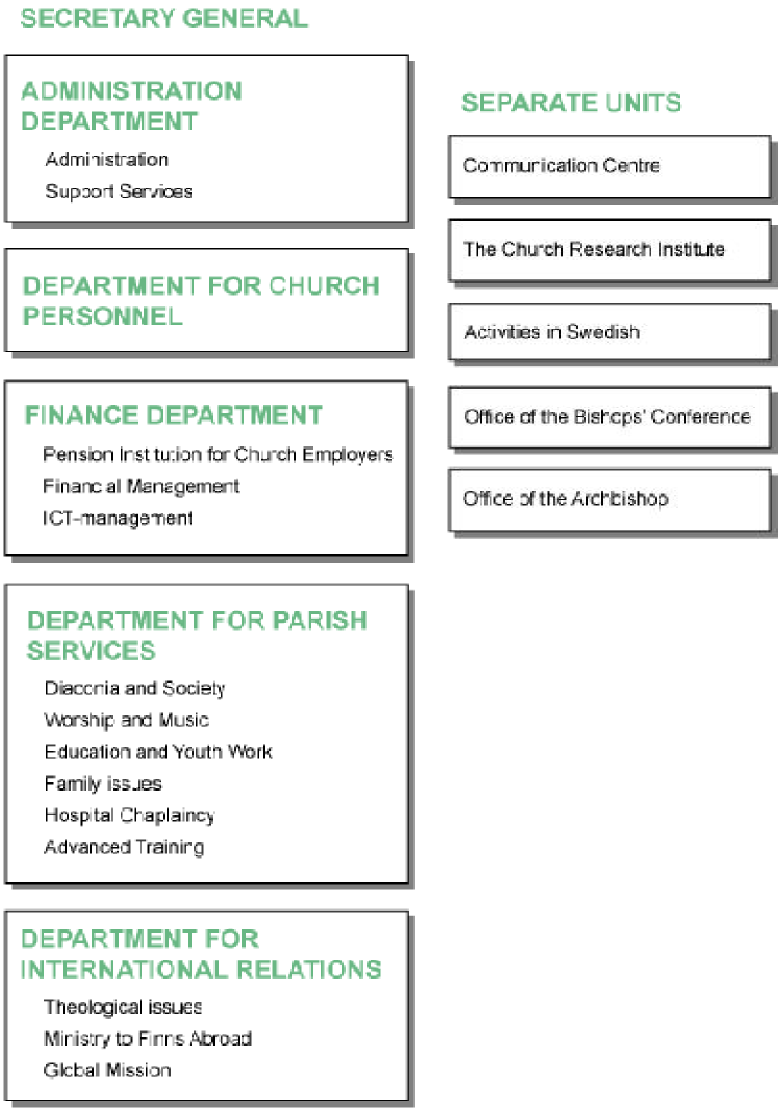


Figure 1. Church Council’s organizational chart.

2.2. Development of the information technology and operating environment in the Church Council

As mentioned earlier, the ICT Management Unit is quite young in general but still, when it started to operate, the applications and technology of today was far beyond anyone’s expectations. For example, the CHURCHnet (KIRKKOverkko in Finnish), a Wide Area Network (WAN) for all parishes and dioceses, was slow and rather unreliable. Parishes had only a few, if any, computers each and there were much less email addresses, compared to some 17500 today. In 2004, the number of email addresses reached 10000 and the holder of the 10000th address was rewarded (Lehtinen 2012).

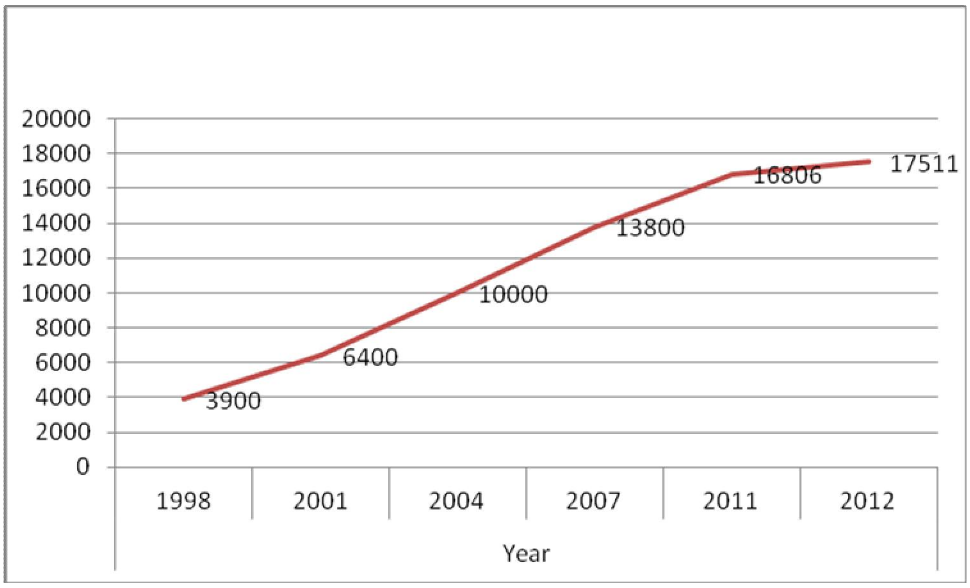


Figure 2. The number of email addresses within the church during certain years of operation.

As the world –and also the church– started looking forward to the 21st century, computers and different applications became more common, and at the same time the need to save and keep electronic files grew. The Church Council went from IBM OS/2 –based hardware and software (1994-1998) through Windows 3.11, Windows NT networks (1998-2001) and Windows 2000 (2001-2008) to Microsoft Windows Vista or Windows 7 (from 2008 onwards) workstations and Active Directory based on Microsoft Windows Server 2008 –technology where it stands today (Karjalainen 2012).

Also the CHURCHnet is about to face its third generation. It also needs to change, as the IT coalitions of parishes and parish unions need more reliable and more simplified networks to better serve their customers, the people of the parishes. The AD migration in 2011 also brought new requirements to the CHURCHnet.

2.3. Remote offices

The IT support group of the Church Council is responsible for supporting users within Church Council. This means that while there are about 200 people working in the Church House in Katajanokka, there are also several dozens of people to assist located in different remote offices, like the Department for Advanced Training in Järvenpää, the Church Research Institute in Tampere, and the Office of the Archbishop in Turku.

The Diocese of Espoo was founded in 2004 when the Diocese of Helsinki was divided in two. The other one, which is the Diocese of Helsinki today, had and still has IT support provided by their own employees and the IT support for the Diocese of Espoo was appointed to be a part of the Church Council's responsibility. The arrangement is somewhat special of a kind, as the diocese has its own budget for IT equipment and they also make their own decisions regarding the equipment, but listen to the specialists' opinions and recommendations. This of course is essential as the IT support only supports certain kind of hardware and software.

Incorporating other dioceses means that they will be equipped with similar workstations as in the Church Council. Some may have their own server, maintained by their own personnel and some may leave it up to the Church Council's ICT-Management Unit to decide what kind of server they would start using and where it should be located. These servers have tasks like file storage, print server or DHCP-server.

3. IMPLEMENTATION AS A TRADITIONAL MODEL

Implementing a new system can be, and often is, a tricky task. Fortunately, there is a lot of support and know-how to be found. Some support comes as so called "silent knowledge", where more experienced individuals share knowledge and advice younger ones, and provide strong, experience-based information. Some support comes from books and articles of the field in question, most of them being easily available from different Internet databases. Based on both of these, a simple diagram of a model is explained and shown in this thesis. The model features a simple but usable and reliable system. As always, it is good to know the facts about building such a system and also a little about the history. Network and computer security is naturally a very important issue when building a new system and also when renewing an old system.

Quite like the client/server system used in the Church Council, the system to be built should also include a server, network hardware and a multifunctional printer/copier in addition to the workstations. Remote offices have these, but as mentioned earlier, they often use servers located somewhere else than their own premises. This generates unnecessary network traffic which could be avoided by setting up a server closer to the actual users. In many dioceses, the server is located under premises, but the technology sometimes being outdated, a renewal of these servers is a very considerable option.

3.1. System security

In this thesis, the system being designed is based on the old system. In fact, there is not an immediate need for the system, as the old system works. But the system should be re-planned and re-organized or even re-built because the systems in the remote offices are built ages ago, especially if they are analyzed from usual IT equipment's life span perspective. Re-building any system also raises questions about security, especially network security. Users in the remote offices are members of a domain, and they have usernames and passwords with which they log in to the network. But how can they be sure that this information is secure?

Yue, Chen and Wang (2009) show that network safety has 4 characteristics: integrity, confidentiality, availability and controllability. *Integrity* means that data cannot be changed, unless it is done by people who are authorized to do so and are capable of determining whether or not it has been changed. *Confidentiality* means that data is not leaked to unauthorized people or entities or to their use. Encryption is often used to ensure this. *Availability* means that access to data is authorized by an entity and is made available for use on demand. *Controllability* means that the flow of information is controlled by a system, and it can also control who can access data, and authenticate users.

Main threats to a network security are the following: 1) unintentional human error. This includes vulnerabilities in security configuration and users with poor or non-existent security awareness, 2) man-made attacks, which are divided into two groups, active attacks and passive attacks, 3) loopholes, or “back doors” in software, and 4) non-authorized access, where networks or computers are used for illegal operations. (Yue et al. 2009.)

As computer technology has advanced, for example federal agencies in the United States and their nation’s critical infrastructures such as power distribution and water supply have become increasingly dependent on computerized information systems. These systems carry out their operations and process, maintain and report essential information. Public and private organizations rely heavily on computer systems to transfer increasing amounts of money and sensitive information. They are also used to conduct operations and deliver services. (Wilshusen 2011.)

The security of these systems and data is vital to protecting national and economic security, as well as public health and safety. On the contrary, ineffective information security controls can result in major risks, including the loss of resources like payments and collections. Another great risk is inappropriate access to sensitive information, such as national security information or even personal information of citizens. It could even disrupt critical operations supporting critical infrastructure, national defense, or emergency services. (Wilshusen 2011.)

Threats to systems that support critical infrastructure and information systems are evolving and growing. US government officials are concerned about attacks from both individuals and groups, such as criminals, terrorists, and foreign nations. Federal law enforcement and intelligence agencies have identified multiple sources of threats to United States' critical information systems, including foreign nations through espionage and information warfare. These groups and individuals have a variety of attack techniques at their disposal. These techniques can be used to find vulnerabilities and enter certain systems. (Wilshusen 2011.)

The connection between information systems and the Internet creates opportunities for attackers to disturb and destroy telecommunications, electrical networks and other critical services. In May 2008, it was reported that the Tennessee Valley Authority's (TVA) corporate network contained security weaknesses. It could lead to the disruption of control systems networks and devices connected to that network. TVA concurred with the recommendations made by a security corporation and has taken steps to implement them. (Wilshusen 2011.)

Incidents like the one depicted above, put sensitive information at risk. Identifiable personal information about U.S. citizens has been lost or stolen, potentially exposing those individuals to loss of privacy, identity theft, and financial crimes. Different agencies have experienced a wide range of incidents involving data loss or theft, computer intrusions and privacy breaches, showing the need for improved security. Furthermore, reported attacks and unintentional incidents involving critical infrastructure systems show that a serious attack could be devastating. (Wilshusen 2011.)

When these incidents occur, agencies are supposed to notify the United States Computer Emergency Readiness Team (US-CERT). The reported incidents have increased dramatically, from 5500 in 2006 to about 42000 incidents in 2010. This is a more than 650 percent increase. The three most common types of incidents and events reported to US-CERT during 2010 were malicious code, improper usage and unauthorized access. (Wilshusen 2011.)

According to McGee, Vasireddy, Xie, Picklesimer, Chandrashekhar, and Richman (2004) the four types of security threats to a network that can be caused by intentional or unintentional actions are interruption, interception, modification, and fabrication.

Interruption: An asset of the system becomes lost, unavailable, or unusable. This is an attack on availability. Examples include malicious destruction of a network element, erasing a software program or data file, cutting a communication line, and malfunction of an operating system file manager so that it cannot find a particular disk file. (McGee et al. 2004.)

Interception: An unauthorized party gains access to an asset. The outside party can be a person, a program, or a computing system. This is an attack on confidentiality. Examples of this type of attack are “wiretapping” to obtain data in a network and passive listening to a wireless radio transmission. (McGee et al. 2004.)

Modification: An unauthorized party tampers with an asset. This is an attack on integrity. Examples include changing the network configuration values in a database and modifying data that is being transmitted in a network. (McGee et al. 2004.)

Fabrication: An unauthorized party gains access to and fabricates counterfeit objects on a network. This is an attack on authenticity. Examples include unauthorized access to the network, untraceable malicious activity on the network and the addition of records to an authentication database. (McGee et al. 2004.)

The section above depicts examples of what a critical system must prepare for. Church network might not be the most critical system, but nonetheless, it may offer at least a plausible passage to government and public networks that contain critical information, and the fact that church in Finland does collect census data about its members, is a viable cause to protect the network properly. Networks are protected by firewalls and other devices that monitor and restrict network traffic from a network to another. Also an anti-virus software and hardware are critical. They prevent malicious software from entering the protected network.

According to a research by Yue, Chen and Wang (2009) firewalls can be divided into three groups:

1) Packet filtering type firewall, also known as filtering router or network –layer firewall. It works at the network layer and transport layer and is based on a single data packet network control, according to IP source address of the packet received and IP

destination addresses. It also has a user access control list to compare whether the data is in line with pre-established security policy. It is designed to control the internal hosts of the network. It may allow direct access to the external network, while the external network access to hosts in the internal network will have to be restricted. The advantages of such a firewall are that it is a simple, convenient, fast and transparent and has little impact on performance. Unfortunately it lacks the user logs and audit information and due to different operating environments, it may have poor compatibility. (Yue et al. 2009.)

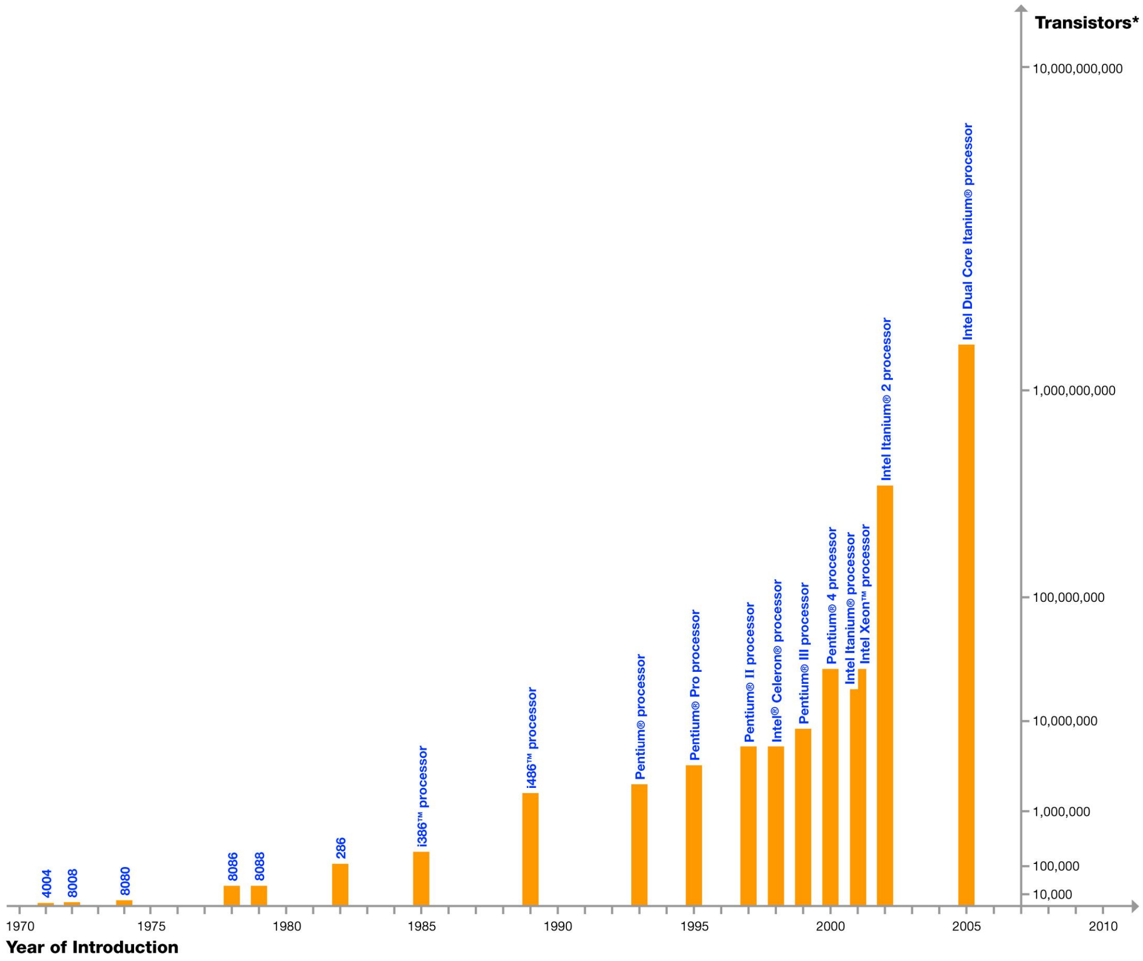
2) Proxy server-based firewall. These kinds of firewalls run on the host through the proxy server program, reporting directly to a particular application layer service. It is also known as application-oriented firewall. A proxy server is actually a specific network gateway to connect two networks. For each different application services, there must be a corresponding agent, and to establish a connection between the internal and external network it must be made through a proxy in the middle of the conversion. The internal network only accepts service requests made by the proxy. (Yue et al. 2009.)

3) The composite firewall. Because of higher security requirements, usually packet filtering and proxy services, functions and characteristics of the system together, constitute a complex firewall system. The host is called a bastion host, and it is responsible for agency services. (Yue et al. 2009.)

Various types of firewalls have their own advantages and disadvantages. The current firewall products are no longer single type of packet filtering firewalls or proxy server type, but rather a variety of security technologies that are combined to form a hybrid multi-level firewall, a system in order to enhance flexibility and security. Hybrid firewalls generally use techniques like dynamic packet filtering; user authentication, internal information hiding, intelligence logs, auditing and real-time alerts and firewall interoperability. (Yue et al. 2009.)

3.2. System design

In 1992, Chang and Kwong presented one of many models to construct a computer system. Their system consisted of workstations and a server, and the network was built with Ethernet cabling. Even today, systems are still built the same way, at least on a principal level. Chang’s and Kwong’s system, being from the beginning of the PC era, represents a system which was typical at the time, with 80286/AT, 80386/AT or 80486/AT chipset PC’s but the principal and basics of building a system where a server serves several workstations, is still valid today. This is the principal the system in question in this thesis is built with, but as we can see in the figure by Intel (2012) below, there are almost five hundred times more transistors in the modern era CPU, than in the Intel486 processor, which was introduced in 1989. This means that the computing power has increased at the same rate. It has been estimated, that in 2050 the computing power of computers exceeds the power of 10 billion human brains. Be that as it may, the today’s computers will do the same as the computers of 1995, only several hundred times faster.



*Note: Vertical scale of chart not proportional to actual Transistor count.

Figure 3. The count of transistors on a single microprocessor. (Intel 2012)

G. Edward Bryan explained in his research paper (1995) that a client/server computing is a style or architecture for distributed computing. According to him, there are two classes of computers on the network: client and server. Client computers are in the hands of end users; servers provide shared services available to all users. Client/server systems are usually distributed geographically over a wide area: a building, a town, a country, or even the world. They are able to connect together because of the use of standard agreements on interfaces. Without the agreed standards, connection would not be possible. (Bryan 1995.)

Standards became available in the 1970's, which resulted in extensive change and explosive growth in the computer business. The existence of standards makes client/server systems possible, but standards have not made them problem-free. Clients always provide for the user system interface, and it is through clients that the user makes requests for service. (Bryan 1995.)

For example, for an airline reservation system a request for a seat is a short transaction that must be sent to the system where the seat record is kept. It wouldn't be a very good idea to have a copy of the database in several places and risk selling the seat more than once. (Bryan 1995.)

Today most clients are PC's that provide independent processing of user applications such as word processing, spreadsheets, presentation creation programs, scheduling and calendar programs and personal databases. Server computers generally handle central functions needed by all users of the client/server computer network system. Servers, which provide these shared services, are larger, more powerful systems with larger memories and more disk storage, and sometimes with backup tape drives and other peripheral devices. (Bryan 1995.)

They provide and control central services such as database storage, print service and high-capacity computational service which all the users of the system share. There are often multiple servers providing different network services or providing added capacity. Distributed systems originally used central systems with "dumb" terminals connected through an often proprietary network. These were "timesharing" systems, since all computing was done on the mainframe which was multiplexed or timeshared among them. (Bryan 1995.)

There were no concerns about where the data was, but if the machine broke down everyone was affected. In client/server systems the failure of a single client is not such a bad thing, except, of course, to the owner of the failed system or users of the failed server. (Bryan 1995.)

The figure below explains the basics needed for the system in question.

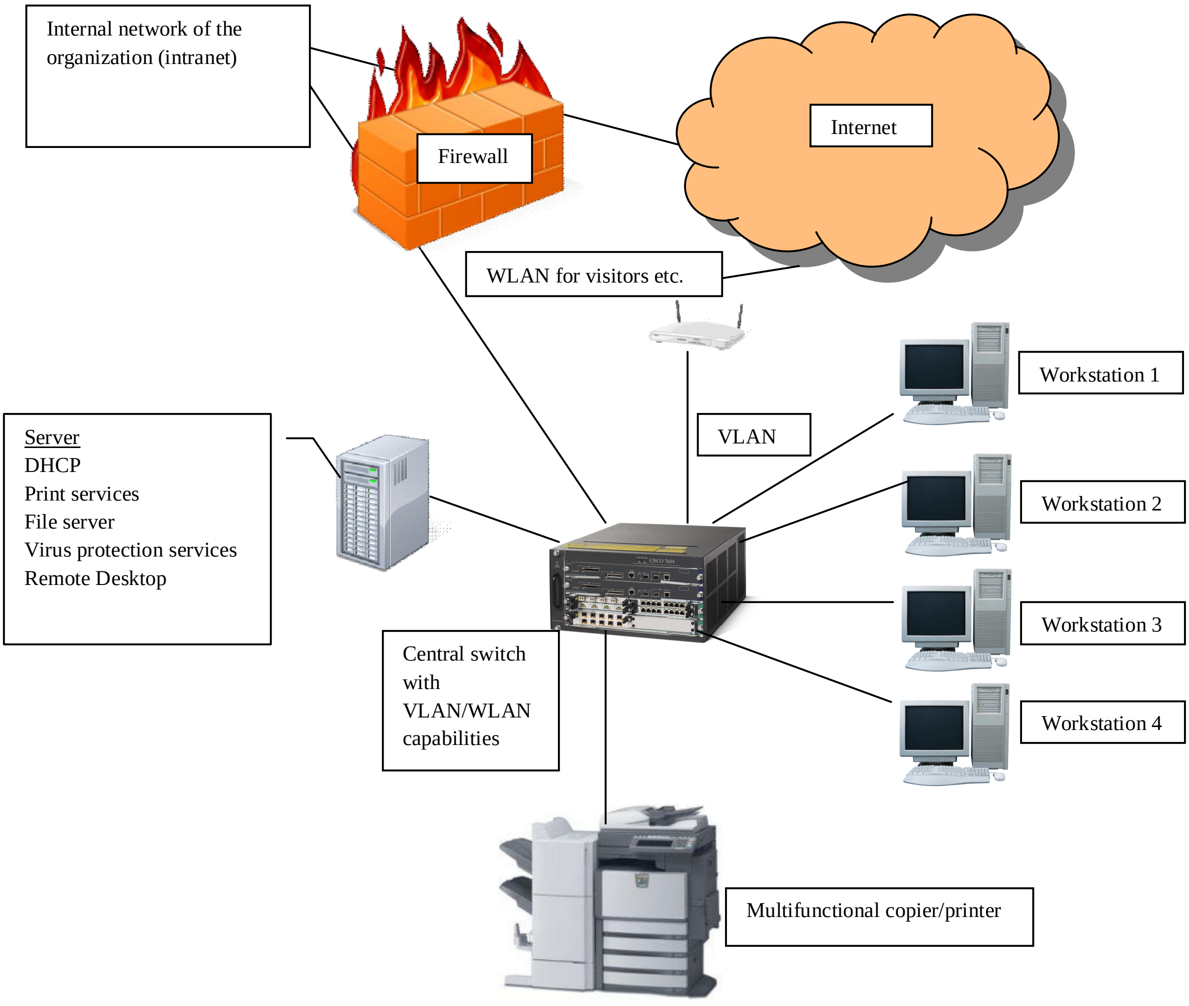

Internal network of the organization (intranet)
Firewall
Internet
WLAN for visitors etc.
Workstation 1
VLAN
Server
DHCP
Print services
File server
Virus protection services
Remote Desktop
Workstation 2
Workstation 3
Central switch with VLAN/WLAN capabilities
Workstation 4
Multifunctional copier/printer

Figure 4. A basic model for a system.

3.3. Advantages and disadvantages of a traditional system

When thinking of the advantages and the disadvantages of a traditional system, which here means something other than a cloud system, many people think of the costs first. Of course, it is essential, especially in an organization that runs on taxpayer's money. In the tables in the next sections, there are some costs gathered up. But costs are not the only thing that is to be concerned. Personnel resources for building the system must be figured out also, and one important thing is that how much outside assistance (consultants etc.) is needed. One major advantage is that most of the building can be done with existing human resources. There is enough know-how in the ICT-Management Unit for it and also, if planned correctly, workload should not be too heavy for one or two individuals, who take the hardware to a predetermined place, install the software and start and test the system. The workstations are pre-installed with an image that contains the operating system, office programs and other essential software, and therefore only the server software is to be installed onto the server hardware. Below is a table where most apparent "pros and cons" are listed.

The costs featured here are per year, the first year being the most expensive because acquisitions are added to a yearly cost. These acquisitions include the hardware and new software, so that existing software contracts are have been taken into account. For example, the price of the workstation OS is already included in the price of the workstation and the price in the tables is the price of the upgrade, for example from Windows Vista to Windows 7. Furthermore, as mentioned before, some old hardware can be used, but the cost tables in this paper show the scenario where all hardware and needed software are purchased as new. In the section 3.6., there are two tables, tables 4 and 5. Table 4 sums up the yearly cost for the first year and table 5 shows the costs for years two, three and four.

Personnel costs, being hard to measure, are left out of the costs. The personnel are appointed to this project as a part of their daily duties, so they present no extra cost. If any extra, for example construction work is needed for cabling etc., they require very specific contracts and are therefore left out of the cost tables.

Table 1. Known advantages and disadvantages when building a system.

Issue	**Explanation**	**Advantage/Disadvantage**
Know how	Personnel are capable of determining needs and building the system.	Advantage
Human resources	Personnel are willing and able to take on the building, no extra workforce needed.	Advantage
Itemized work - cabling works - electrical works	If any cabling (that demands construction work) or electrical works are needed, a 3rd party certified professional is needed.	Disadvantage
Transportation of hardware	The hardware must be transported to a site; either delivered there directly or by transporting it there by the personnel.	Advantage/Disadvantage
Premises	The hardware must be kept safe behind locked doors.	Disadvantage

3.4. Founding costs

In the table below, there are a group of devices and their extra features mentioned needed to build a basic system. The prices are near estimates, a part of them are based on real contracts, and a part is gathered from vendor websites. The sums are rounded for clarity.

Table 2. Hardware for a system.

Hardware	**Needed**	**Cost in euros**
Server HP, suitable for small businesses or remote offices, includes 4-core CPU, 4 Gb memory, no hard disks	Yes	1200
- server extra memory, 4Gb x 3	Yes	3x75=225
- server extra hard disks (HP 2Tb disk, 7200 rpm, 3,5”)	Yes	500
- server network interface card, 1Gb	Yes	200
Workstations		
- laptops, incl. docking station, mouse, keyboard, 23” display, and a 4-year guarantee.	Yes	1500
Switch, scenario 1	No, existing used	-
Switch, scenario 2	Yes	650
Router	No, existing or none used	-
Cabling, scenario 1	No, existing cabling used	-
Cabling, scenario 2	Yes	Depending on the need
Copier/printer	No, existing used	

Table 3. Software for a system.

Software	**Needed**	**Cost in euros**
Server OS	Yes	450
Workstation OS, upgrade	Yes	170
Office programs	Yes	170
Anti-virus software, workstations	Yes	15
Anti-virus software, servers	Yes	15

3.5. Maintenance costs

During the four-year period, which is covered by the guarantee of the workstations and servers, there should be no major extra costs due to maintenance. Of course, nothing is ever completely certain, so the organization should be prepared for costs that are caused by surprising events, like a breakage of hardware uncovered by a guarantee. Any delay costs, direct or indirect, for example long waits due to breakage when employees have to wait for repairs, are difficult to measure but have to be taken into account.

The costs for ISP (Internet Service Provider) services are included in the maintenance cost, but these costs have been going on before the first year investments and they will go on after that. The listed price in the cost tables is an estimate, although it is based on a real contract. The price consists of the network maintenance, hardware maintenance and general costs that are related in those.

3.6. Combined costs for a four year period

In table 4 below, there are the first year costs combined. This example shows the costs for a remote office that has 10 workstations, a server, and a central switch, the software for workstations and the server and anti-virus programs for workstations and the server. Also, the price of the server consists of the server itself and the extra memory, upgraded network interface card and a large capacity hard disk. The table also includes the cost for the ISP services, which includes maintenance and other, for example email services

Table 4. First year costs combined.

Item of expenditure	**Cost in euros**
Server	2125
Workstations, 10 pcs	15000
Switch	650
Workstation software, OS + office programs + antivirus	3550
Server software, OS + anti-virus	465
ISP service	2500
TOTAL	**24290**

Table 5. The costs for years 2, 3 and 4 combined

Item of expenditure	**Cost in euros**
Workstation software, office programs + antivirus. Only office and anti-virus licenses needed.	5100
Server software, only anti-virus license needed	45
ISP service	7500
TOTAL	**12645**

As we can see from the tables above, the costs peak the first year but the following three years *combined* make only about a half of the first years investment.

4. IMPLEMENTATION AS A CLOUD SERVICE

Several people and businesses alike think that cloud computing will change the way we do business. One of them, president of Twist Image Mitch Joel, writes in his blog February 14th 2012 that if the cloud isn’t on your businesses mind, it should be. He firmly believes that it will change everything. According to him, it’s a revolution as big as the microprocessor and as relevant as the desktop computer. It is to be seen what the future brings, especially with the cloud. (Joel 2012.)

But why is it so important, then? Putting it simply, a cloud is a just a term for the Internet as a storage facility. But isn’t this an old concept already? In fact, it is old. The first steps were made in 1960, when a computer scientist called John McCarthy stated that “Computation may someday be organized as a public utility” and in 1965 Western Union had a dream about the company being US-wide “information utility”. (Marston et al. 2011.)

In 1969, Leonard Kleinrock, one of the chief scientists of the original Advanced Research Projects Agency Network (better known as ARPANET) said:” As of now, computer networks are still in their infancy, but as they grow up and become sophisticated, we will probably see the spread of *computer utilities* which, like present electric and telephone utilities, will service individual homes and offices across the country.” This vision of the computing utility based on the service provisioning model anticipates the transformation of the entire industry in the 21st century, where computing services will be available on demand much like many utility services are available today (Buyya et al. 2009).

Cloud computing is becoming a promising alternative to the traditional in-house IT computing services. Cloud computing is a form of computing in which providers offer computing resources like software and hardware on-demand. All of these resources are connected to the Internet and they are provided dynamically to the users. Cloud providers are able to provide computing services to both enterprise and personal users. (Sahinoglu & Cueva-Parra 2011.)

Some companies see this form of computing as a single major type of service which will be demanded extensively in the next decade. In fact, companies like Google, IBM, Microsoft, HP, Amazon, and Yahoo among others have already made investments not only in cloud research but also in establishing cloud computing infrastructure services. (Sahinoglu & Cueva-Parra 2011.)

Cloud computing services fall into three major categories: 1) infrastructure as a service, IaaS, (2) software as a service, SaaS, and (3) platform as a service, PaaS. In IaaS virtualized servers, storage and networks are provided to the clients. SaaS is focused on allowing clients to use software applications through web- interfaces. A service targeted to developers who focus primarily on application development only, without dealing with platform administration (operating system maintenance, load balancing, scaling, etc.), is called PaaS. (Sahinoglu & Cueva-Parra 2011.)

Advances in virtualization, distributed computing, and high-speed network technologies have given further push to cloud computing. The major advantages are scalability, flexibility, resilience, and affordability. However, as users whether it is companies, organizations or individual persons, turn to cloud computing services for their businesses and commercial operations, there is a growing concern from the security and reliability perspectives as to how those services actually rate. The serviceability measurement can be categorized into three areas: performance, reliability, and security. Performance and reliability are two characteristics related to the condition of the providers' infrastructure and the way they maintain and update them. Security, more precisely data protection and disaster recovery, on the other hand, is one aspect that is more difficult to measure (Sahinoglu & Cueva-Parra 2011).

Both cloud computing providers and users need a way to measure the quality of this service, mainly in the area of reliability and security. This metric can provide the sending and receiving end-users with a better sense of what both parties are getting for their return of investment. Also, it gives providers a concrete numerical reference, rather than just vague attributes, so they can improve the quality of the current service. However, despite evident benefits, cloud computing lacks precise analysis regarding its quality of service. In general, the quality of cloud computing services is difficult to measure, not just qualitatively, but most importantly quantitatively. (Sahinoglu & Cueva-Parra 2011).

Cloud computing may mean a fundamental change in the way information technology services are invented, developed, deployed, updated and scaled, as well as maintained and paid for. Computers continue to become exponentially more powerful as the cost per unit falls significantly, so much so that computing power is widely seen as a commodity. This presents a paradox, because at the same time, as computing becomes more pervasive within organizations, the ever increasing complexity of managing the whole infrastructure has made computing more expensive than ever to an organization. (Marston et al. 2011.)

Cloud computing promises to deliver all the functionality of existing information technology services, and more, at the same time dramatically reducing the costs that hinder many organizations from implementing new services. These promises of course have led to great expectations. According to AMI partners, small and medium sized businesses are expected to spend over 100 billion US dollars on cloud computing by 2014. (Marston et al. 2011)

In addition, in the figure below, we can see that according to Gartner (2010), the cloud-based applications are estimated to grow from approximately 6 billion US dollars to approximately 20 billion US dollars between 2009 and 2014.

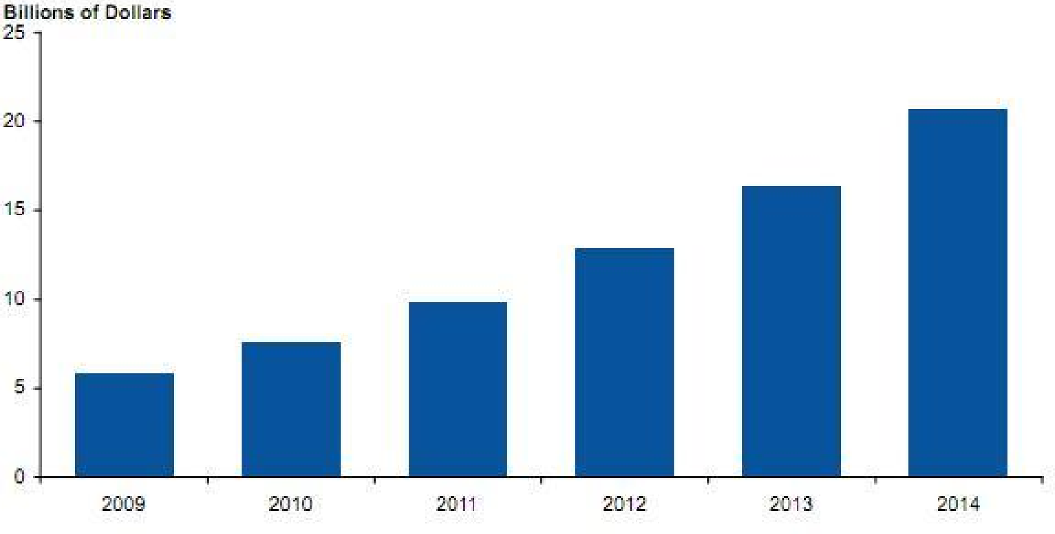


Figure 5. Growth of cloud-based applications. (Gartner 2010)

4.1. Advantages and disadvantages of a cloud service

Cloud computing is a flexible, cost- effective and proven delivery platform for providing business or consumer IT services over the Internet. Computing services, ranging from data storage and processing, to software such as email handling, are now available instantly, commitment-free and on-demand. Cloud computing can be compared to the early days of electricity networks. Homes, businesses and towns did not want to produce or rely on their own source of power. They began connecting in to greater power grid, supported and controlled by power utilities. (Tripathi & Mishra 2011.)

Along with this utility connection, came time and cost saving, in addition to greater access to, and more reliable availability of power. Similarly, the new concept of cloud computing offers dynamically scalable resources provisioned as a service over the Internet and therefore, promises a lot of economic benefits to be distributed among those who adopt the service. Email, instant messaging, business software and web content management are among the many applications that may be offered via a cloud environment. (Tripathi & Mishra 2011.)

The main focus of cloud computing, from the provider’s view points, is to have extra hardware connected to support down time on any device in the network, without a change in the user’s perspective. The cloud computing allows users to avoid upfront hardware and, software investments gain flexibility, collaborate with others, and take advantage of the sophisticated services that cloud providers offer. (Tripathi & Mishra 2011.)

Distinct layers can be defined based on the resources provided by the cloud. The bottom layer provides infrastructure services such as CPUs, memory, and storage and is known as Infrastructure-as-a-Service (IaaS). The middle layer provides platform-oriented service, enabling the usage of hosting environments tailored to a specific need and is known as Platform-as-a-Service (PaaS). For example, a PaaS service may enable to deploy and dynamically scale python and Java based web applications. The top layer provides users with ready to use applications and is known as Software-as-a-Service (SaaS). All these layers reduce capital expenditures, e.g., IaaS layer reduces hardware costs and license cost is reduced in all layers. In spite of these benefits, cloud computing raises a number of important policy issues regarding how people, organizations, and governments handle information and interactions in this environment. (Tripathi & Mishra 2011.)

The figure below explains what the cloud service consists of.

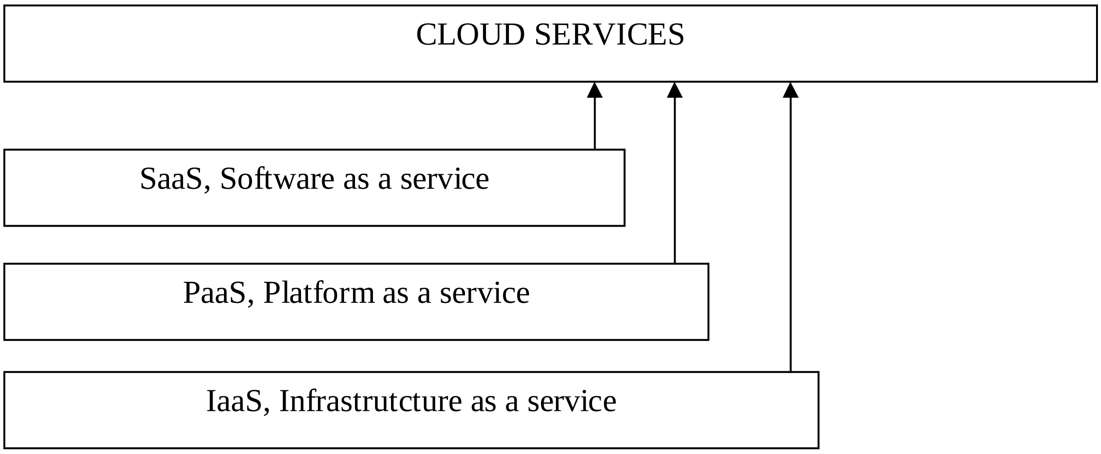

CLOUD SERVICES
SaaS, Software as a service
PaaS, Platform as a service
IaaS, Infrastrutcture as a service

Figure 6. Cloud computing services.

Cloud computing also raises severe concerns, especially, regarding the security level provided by such a concept. There are three important things to be mentioned about cloud security. Firstly, cloud security is almost exactly like internal security. The security tools that are used nowadays to protect the internal network cloud, also used to protect data in the cloud. Secondly, for remaining financially competitive, some of these security technologies should be moved to the cloud. Thirdly, if a quality cloud service provider is selected, the security in the cloud will be as good as or better than the current security in most cases. (Tripathi & Mishra 2011.)

4.2. Security issues

Tripathi and Mishra (2011) also define some risks in their paper:

1) VM-Level attacks.

The cloud computing is based on VM technology. For implementation of cloud, a hypervisor such as VMWare, vSphere, Microsoft Virtual PC, Xen etc. are used. This threat arises because of the vulnerabilities appearing in these hypervisors due to some facts being overlooked by developers during the coding of these hypervisors. The threat arising due to VM-Level vulnerabilities can be mitigated by monitoring through IDS (Instruction Detection System)/IPS (Intrusion Prevention System) and by implementing firewalls. (Tripathi & Mishra 2011.)

2) Abuse and nefarious use of cloud computing.

This threat arises due to relatively weak registration systems present in the cloud computing environment. In cloud computing registration process, anyone having a valid credit card can register and use the service. This facilitates anonymity, due to which spammer, malicious code authors and criminals can attack the system. According to Tripathi & Mishra (2011) this type of threat can be mitigated in following ways:

- by implementing stricter registration process and validation process.
- by credit card fraud monitoring and coordination.
- detailed introspection of user’s network traffic.
- network blocks through monitoring public black lists.

3) Loss of governance

The client gives up control to the cloud provider on a number of issues while using the cloud infrastructure. The service Level Agreements (SLA) may not have commitment on the part of cloud provider, to provide such services, thus having a gap in security defenses affecting security. This loss of control may lead to a lack of confidentiality, integrity and availability of data. Unfortunately there are no publicly available standards specific to cloud computing security. Thus organizations considering cloud services need to exercise persistent and careful efforts for the execution of Service Level Agreements. (Tripathi & Mishra 2011.)

4) Lock-in

Lock-in means inability of the customer to migrate from one cloud service provider to another .This is due to loss of portability of the customer data and programs. Presently, there are few tools, procedures or standard data formats which provide data, application or service portability. This prevents customers or organizations from adopting cloud computing. To mitigate this, standardized cloud Application Programming Interface

(API) should be used. This standardization will ensure cloud computing to be more fully accepted. (Tripathi & Mishra 2011)

5) Insecure interfaces and API's

Customers use a set of software interfaces or APIs to interact with cloud services. The provisioning, management, orchestration and monitoring of the cloud service are generally done using these interfaces .If the weak set of interfaces and APIs are used, this may expose organizations to various security threats, such as anonymous access, reusable tokens or password, clear-text authentication or transmission of content, inflexible access controls or improper authorizations, limited monitoring, and logging capabilities. To mitigate the above threats, the security model of cloud provider interfaces should be analyzed. Strong authentication and access controls should be implemented. Encryption should be used for transmission of content and, dependency chain associated with the API should be clearly understood. (Tripathi & Mishra 2011.)

6) Isolation failure

The services are delivered in cloud computing by sharing infrastructure .The components that are used to build Disk partitions, CPU cache, graphics processing units etc are not designed to offer strong isolation properties or compartmentalization. The hypervisors, that are basic building blocks for cloud computing, have exhibited flaws that enable guest operating system to gain unauthorized control .Due to this isolation failure, the attackers focus on to impact the operations of other cloud customers to gain unauthorized access to data. Strong compartmentalization should be employed so that the individual customers do not impact the operations of other customers .This can be enforced by implementing best practices for installation, configuration, monitoring environment for unauthorized changes/activities, promoting strong authentication and access control, patching the vulnerabilities and conducting vulnerability scanning and configuration audits. (Tripathi & Mishra 2011.)

7) Data loss or leakage

Data loss or leakages have an adverse effect on the business. The brand or reputation is completely lost and the customers' morale and trust are eroded. This data loss or leakage may be due to insufficient authentication, authorization and audit controls, inconsistent use of encryption and software keys, disposal challenges, a data center reliability, and disaster recovery. The threats arising due to data loss or leakage can be mitigated by encrypting and protecting integrity of data in transit, analyzing data protection at both design and runtime, implementing strong key generation, storage and management. Contractually demanding provider to wipe persistent media before it is released in to pool and contractually specifying provider backup and retention strategies. (Tripathi & Mishra 2011.)

8) Account or service hijacking

The above threat occurs due to phishing, fraud and software vulnerabilities .Attackers can steal credentials and gain access to critical areas of deployed cloud computing services, resulting in compromise of the confidentiality, integrity and availability of these services. To mitigate the above threats, sharing of account credentials between users and services should not be allowed, multi-factor authentication techniques should be used wherever possible, strict monitoring should be done to detect unauthorized activity, and security policies, as well as SLA's of the cloud provider, should be clearly understood. (Tripathi & Mishra 2011.)

9) Management interface compromise

The customer management interface of the cloud provider is accessible through the internet .In cloud computing, larger set of resources are accessed through these interfaces than traditional hosting, since cloud computing provides remote access to customers through these management interfaces. This may pose a serious threat if web browser vulnerabilities are present. To mitigate threats arising due to remote access, secure protocol should be used to provide access. Also, web browser vulnerabilities should be completely patched before providing remote access. (Tripathi & Mishra 2011.)

10) Compliance risks

This threat arises due to lack of governance over audits and industry standard assessments. Due to this, customers of cloud services do not have a view into the processes, procedures and practices of the provider in the areas of access, identity management and segregation of duties. Organizations that seek to obtain certification, may be put at risk because cloud computing service providers may not be able to provide evidence of their own compliance with the necessary requirements or may not permit an audit by cloud customer. To lessen this threat vendors' internal audit process should be reviewed. How often it is audited by external agencies and, whether or not, it is open to being audited for compliance. (Tripathi & Mishra 2011.)

11) Malicious insiders

This threat is well known to most organizations .Malicious insiders' impact on organization is considerable. Given their level of access, they can infiltrate organizations and assets and do brand damage, financial losses and productivity losses. Therefore, it is critical for customers of cloud services as to what controls have been provided by cloud providers to detect and defend against the malicious insider threats. The Malicious insider threats can be mitigated by specifying human resources requirements as part of legal contracts, conducting a comprehensive supplier assessment, providing transparency into overall information security and management practices, as well as compliance reporting and determining security breach notification processes. (Tripathi & Mishra 2011.)

4.3. Design and costs

The design of a cloud system can vary from very simple to a very complicated one. In this thesis the design is quite simple. This is due to the fact that everything cannot be implemented as a cloud service, in contrary of the promises. This was learned when talking to a Microsoft specialist in the Microsoft TechDays 2012 event in Helsinki 8th and 9th of March 2012.

This naturally raises concerns about the adaptability and suitability of a cloud system for the remote points. Their need is in short to use, modify and save files during the work day and possibly continue the next, communicate via email and use either web-based or local services.

Also, as several researches show, the pricing and cost models or predictions are difficult to make, due to the nature of the cloud service being full of variables and also due to the very competitive environment.

Many of the current cloud end customers use price as their primary decision criteria. As a result, service providers' offerings tend toward a least common denominator, determined by the realities of providing cloud service at the lowest possible price. At the same time, the cloud computing market is becoming more crowded with large providers entering the playing field, each one of which trying to differentiate itself from the already established players. (Durkee 2010.)

Durkee also discusses in his paper (2010) about the result of many providers competing to deliver very similar product in a highly price-competitive environment. This is termed *perfect competition* by economists. Perfectly competitive markets, such as those for milk, gasoline, airline seats, and cellphone service, are characterized by a number of supplier behaviors aimed at avoiding the downsides of perfect competition, including:

- Artificially differentiating the product through advertising rather than unique product characteristics
- Obscuring pricing through the use of additional or hidden fees and complex pricing methodologies
- Controlling information about the product through obfuscation of its specifications
- Compromising product quality in an effort to increase profits by cutting corners in the value delivery system
- Locking customers into long-term commitments, without delivering obvious benefits.

These factors, when applied to the cloud computing market, result in a product that does not meet the enterprise requirements for deterministic behavior and predictable pricing. The resulting price war potentially threatens the long-term viability of the cloud vendors. The following section shows how perfect competition affects the cloud computing market. (Durkee 2010.)

Advertisements for cloud computing breaking through the previous price floor for a virtual server instance are frequently seen. It makes one wonder how cloud providers can do this and stay in business. The answer is that they over commit their computing resources and cut corners on infrastructure. The result is variable and unpredictable performance of the virtual infrastructure. Durkee also states (2010) that many cloud providers are vague on the specifics of the underlying hardware and software stack they use to deliver a virtual server to the end customer, which allows for overcommitment. According to Durkee (2010) the techniques for overcommitting hardware include (but are not limited to):

a) Specify memory allocation and leave CPU allocation unspecified, allowing total hardware memory to dictate the number of customers the hardware can support

b) Quote shared resource maximums instead of private allocations

c) Offer a range of performance for a particular instance, such as a range of GHz

d) Overallocate resources on a physical server, or “thin provisioning.” Commercial virtualization management software such as VMWare or Virtuozzo offer the ability to overallocate resources on the underlying hardware, resulting in reduced performance during peak loads.

On the other hand, running applications on the cloud gives many technical advantages and results in significant cost savings over running them on local managed servers. Cost saving and low barriers to launch web services using the cloud is significant when considering easy start-up, scalability, and flexibility. One of the biggest advantages of the cloud computing lies in its on-demand, allowing users to start applications with minimal cost. (Han 2011.)

Martens, Walterbush and Teuteberg introduce a total cost of ownership –model in their 2012 paper. According to them, traditional accounting approaches primarily aim at identifying the lowest possible costs, whereas the benefits of the total cost of ownersip (TCO) approach lie in the improvement of customer-supplier communication and the analysis of the whole lifecycle of the IT artifact. (Martens et al. 2012.)

Furthermore, the TCO approach makes it possible to analyze the costs or individual cost components of an IT artifact by means of a predefined scheme. It virtually constitutes a mathematical representation of the “real world”. However, it is not the purpose of TCO models (or of any model) to provide a 1:1 image of reality, but to deliver a simplified, abstract view [10]. Hence, instead of including all relevant costs into the TCO analysis, the complexity of reality can be reduced by working on the basis of assumptions and by including only a limited number of carefully selected cost factors. In spite of this limitation to selected cost factors the TCO model should be able to provide reliable decision support (Martens et al. 2012.)

The next figure shows a simplified model for a cloud service that would suit the needs of the Church Council and its remote offices.

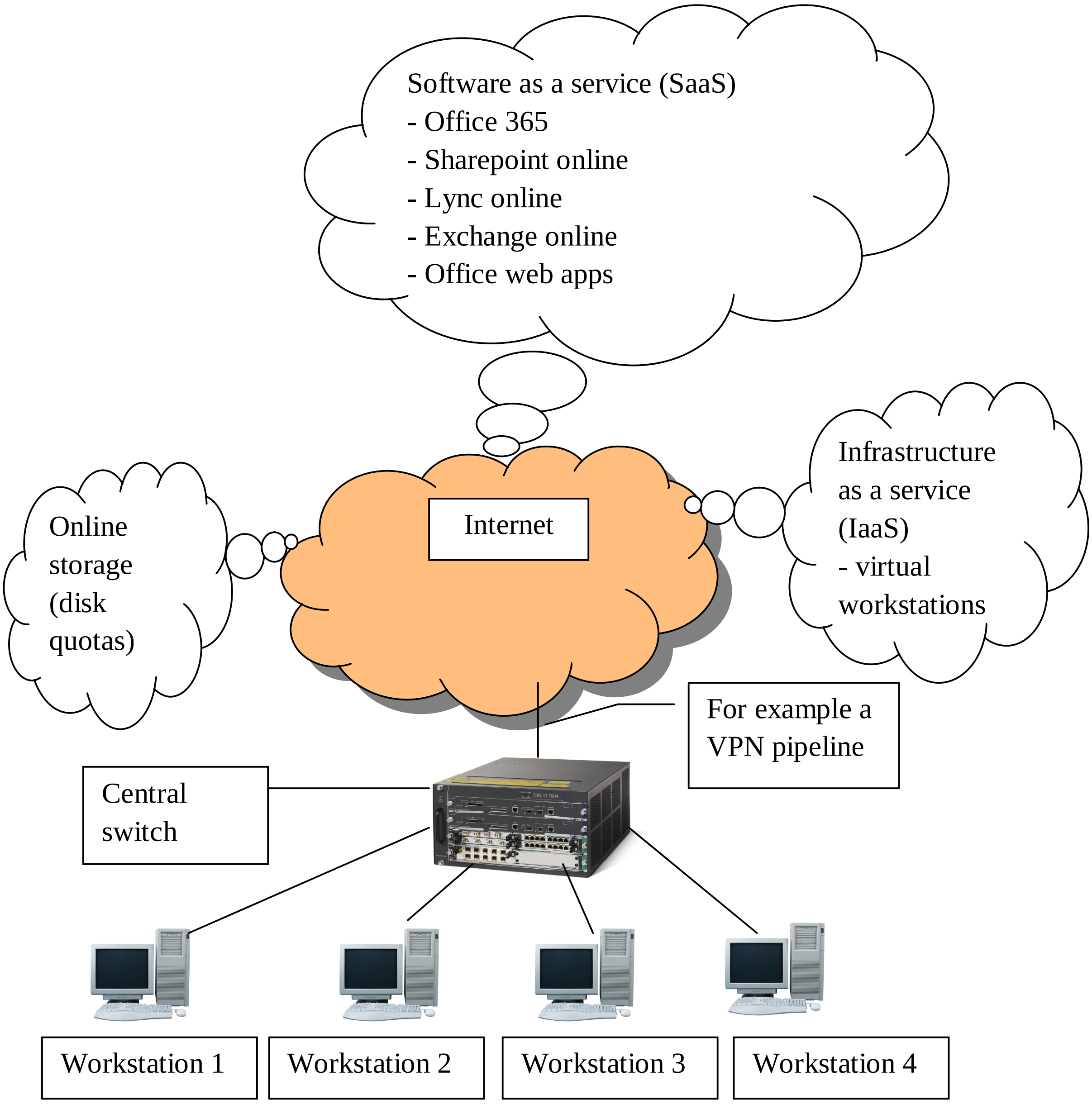


Figure 7. Cloud computing model.

5. CONCLUSIONS

After investigating the need for the system, resources and personnel skills for building it and the technology and costs behind both traditional systems and the cloud systems, the following findings have been made and the following conclusion has been reached. The system for remote offices should be built the traditional way. The reasons for this are the following:

1) Costs

This does not mean it is less expensive to build the system the traditional way, in fact some major savings could be reached by using cloud solutions when implementing the system. It just means that the costs are much more easily untangled, because the costs of a cloud system are very hard to know in advance. In addition, there are several vendors and providers in the market and they all have different models for pricing. The only price easily found out was the price of the Microsoft Office 365, which offers Office programs and other Microsoft software for cloud services.

2) Needs

The needs that the employees have are mostly simple tasks to save, use, modify and store files. This can be very well implemented with traditional systems. In addition to that, most employees work for a certain time every day and do not need to have access to all files all the time with any hardware available. That kind of scenario is extremely rare, and since the employees in the Church Council have the possibility to work remotely anyway, the need for files in the cloud is slender.

3) The scale of the system

In the Church Council, the current system with physical workstations and servers is seen as working, reliable, adequate and familiar. Making major changes to that would cause service interruptions and also would probably cause a need for education of new systems and ways to work. The scale of the system in the remote offices is and has been just right. The one thing that most remote offices are worried about is the bandwidth, which couldn’t be solved with cloud systems anyway.

4) Security

Perhaps the biggest concern about a cloud system is the security. Currently, the users are happy with the security level and instructions. If the users would feel that their data was not secure anymore, or the instructions were to change dramatically, the users would probably start resisting the change. As has been stated earlier, the security of the cloud is a major issue because the data of the users is stored in the Internet. No matter how extensive the precautions, the risk of data loss or tampering is greater in the cloud.

5) Experience and knowledge

The experience and knowledge the IT personnel in the Church Council has, is based on years of working with information technology. Some of the people there have an experience of more than 20 years of IT and they have seen the transition from token ring networks and IBM operating systems to Ethernet networks and Windows workstations and servers. Against that background it is also evident that if the system is built the traditional way, there is going to be no need for external help, unlike in the case of cloud system.

6. SUMMARY

This thesis is about a comparison between a traditional computer system and a cloud system. The system in question is being designed to help the remote offices of the Church Council of the Evangelical Lutheran church of Finland to cope with their daily routines with less problems and delays, and also to lessen the work load of the IT support team of the Church Council.

The writing process started with a quite an ambitious thought. At first, the idea was to compare the two systems solely through the costs and to see if the costs would intersect in time, while taking the reduction of the costs of networking fees and such in to account. This would have required a thorough research among the service providers like IBM, Elisa, Tieto, Microsoft etc. and compare their services, models and prices. However, the time limit was too tight for all this and it would have been uncertain to get sufficient or any information from the corporations.

The main idea changed to comparing the major issues between the two systems, costs being a part of it all. As it turned out, the costs for cloud services are very hard to find, unless the system is actually being built and contracts between the client and the provider have been signed.

First, the thesis introduces the research problems, which are the aforementioned workload of the IT support team and the load on the network by the use of file servers and other services located somewhere else than under the premises of the remote office. From that the thesis moves on to introduce basic knowledge about the church, the Church Council and the environment for the system, alongside with information about the ICT-Management Unit that is responsible for building the system.

Next part introduces the design for the traditional system, along with some history and theory of the systems. The thesis takes a look at the history and essentials of client/server computing, introduces threats to a system and solutions on how to prepare for threats. In the chapters after that the cloud system is introduced. From both systems the risks and opportunities are listed, along with the known yearly costs of the traditional system.

The last part of the thesis brings the conclusions to light. The conclusion was that the system is to be built the traditional way. It is validated with 5 strong arguments all in favor of the traditional system.

However, it must be kept in mind that the cloud services are the future. It is very well possible that the system depicted in this thesis is re-built after 5-10 years, and by that time the cloud services have probably developed and become more safe and reliable, and the system could be built completely as a cloud service.

LIST OF REFERENCES

Bryan, G. Edward (1995). The full cost of client/server computing. *Aerospace applications conference, proceedings, 1995 IEEE , Issue: 0.*

Buyya, Rajkumar, Chee Sin Yeo, Srikumar Venugopal, James Broberg & Ivona Brandic. (2009). Cloud computing and emerging IT platforms: Vision, hype and reality for delivering computing as the 5th utility. *Future generation computer systems.* 25:6, 599–616.

Chang, M. F. & S. Kwong (1992). An implementation of a high performance client-server system. *Singapore ICCS/ISITA 1992: Communications on the Move.*

Church Councils organizational chart (2011). [online] [cited 2011-11-10]. Available from the Internet: <URL: http://evl.fi/EVLen.nsf/Documents/82F558C546FF8E18C22572B400213CEC?OpenDocument&lang=EN>

Church intranet site Sakasti (2011). *ICT-Management Unit.* [online] [cited 2011-11-10]. Available from the Internet: <URL: http://sakasti.evl.fi/sakasti.nsf/sp?open&cid=Content22D242>

Durkee, Dave (2010). Why cloud computing will never be free. *Communications of the ACM.* 53:5, 62–69.

Gartner (2010). Growth of cloud based applications. *Cloud computing: The next generation of outsourcing.* Gartner RAS Core research note G00207255, Ben Pring.

Han, Yan (2011). Cloud computing: Case studies and total cost of ownership. *Information technology and libraries, December 2011.*

Intel (2012). *The count of transistors on a single microprocessor*. [online] [cited 2012-03-10]. Available from the Internet: <URL: http://www.intel.com/pressroom/kits/events/moores_law_40th/index.htm>

Joel, Mitch (2012). *How cloud computing changes everything.* [online] [cited 2012-02-14]. Available from the Internet: <URL: http://www.twistimage.com/blog/archives/how-cloud-computing-changes-everything/>

Kantarcioglu, Murat, Alain Bensoussan & SingRu Hoe (2011). Impact on security risks on cloud computing adoption. *49th annual Allerton Conference, September 28–30, 2011.*

Karjalainen, Aimo (2012). *Interview 2012-03-16.*

Lehtinen, Paula (2012). *Email discussions from 2012-02-12 to 2012-03-13.*

Marston, Sean, Zhi Li, Subhayoti Bandyopadhay, Juhen Zhang & Anand Ghalsasi (2011). Cloud computing – the business perspective. *Decision support systems.* 51. 176–189.

Martens, Benedikt, Marc Walterbusch & Frank Teuteberg (2012). Costing of cloud coputing services: A total cost of ownership approach. *2012 45th Hawaii International Conference on System Sciences.*

McGee, Andrew R., S. Rao Vasireddy, Chen Xie, David D. Picklesimer, Uma Chandrashekhar, & Steven H. Richman (2004). A Framework for Ensuring Network Security. *Bell Labs Technical Journal*. 8:4, 7–27.

Sahinoglu, Mehmet & Luis Cueva-Parra (2011). Cloud computing. *Wiley interdisciplinary reviews: Computational statistics*. 3:1, 47–68.

The Evangelical Lutheran Church of Finland. (2011). *Church in a nutshell.* [online] [cited 2011-11-10]. Available from the Internet: <URL:

http://evl.fi/EVLen.nsf/Documents/0E829455D4B83A5CC22572B400213CCB?OpenDocument&lang=EN>

Tripathi, Alok & Abhinav Mishra (2011). Cloud computing security considerations. *2011 IEEE International Conference on Signal Processing, Communications and Computing, September 14-16, 2011.*

Wilshusen, Gregory (2009). Cyber threats and vulnerabilities place federal systems at risk. *Testimony before the subcommittee on government management, organization, and procurement; House committee on oversight and government reform*. May 5, 2009.

Yue, X., Wei Chen & Yantao Wang (2009). *The research of firewall technology in computer network security. 2009.* Second Asia-Pacific Conference on Computational Intelligence and Industrial Applications.

Zhang, Shuai, Shufen Zhang, Xuebin Chen & Xiuzhen Huo (2010). The comparison between cloud computing and grid computing. *2010 International conference on computer application and system modeling (ICCASM)*

APPENDIXES

APPENDIX 1: GLOSSARY

Cloud system/cloud computing: Cloud computing is a general term for anything that involves delivering hosted services over the Internet.

Computer system: A functional unit, consisting of one or more computers and associated software.

CPU: Central Processing Unit. The key component of a computer system, which contains the circuitry necessary to interpret and execute program instructions.

DHCP: Dynamic Host Configuration Protocol. A protocol that provides means to dynamically allocate IP addresses to computers on a local area network.

Disk quota: Limits the amount of disk space that can be used.

Email: a system for sending messages from one individual to another via telecommunications links between computers or terminals.

Firewall: A firewall is a set of related programs, located at a network gateway that protects the resources of a private network from users from other networks.

IaaS, Infrastructure as a service: a provision model in which an organization outsources the equipment used to support operations.

IBM OS/2: IBM and Microsoft's successor to the MS-DOS operating system for Intel 80286 and Intel 80386-based microprocessors.

IP address: Internet protocol address: the numeric code that identifies all computers that are connected to the Internet.

Packet filtering: the process of passing or blocking packets at a network interface based on source and destination addresses, ports, or protocols.

Proxy: a server that acts as an intermediary between a workstation user and the Internet.

PaaS, Platform as a service: a way to rent hardware, operating systems, storage and network capacity over the Internet.

SaaS, Software as a service: a software distribution model in which applications are hosted by a vendor or service provider via the Internet

TCP/IP: Transmission Control Protocol/Internet Protocol: the basic communication language or protocol of the Internet.

VLAN: VLANs are used to segment the network into smaller broadcast domain or segments.

WLAN: Acronym for wireless local-area network. A type of local-area network that uses high-frequency radio waves rather than wires to communicate between nodes.