TDT4520 - Program and Information Systems

Fall 2010

Usage of Cloud Computing for eGovernment services

Simon Litlehamar

Main supervisor: Ole B. Hansen, Accenture

Supervisor: John Krogstie, NTNU

December 15, 2010

Abstract

Cloud Computing as catching the interest of governments around the world. The Cloud Computing model is already in use for eGovernment services in the United States of America with Apps.gov.

There are several benefits for using the Cloud Computing model over conventional hosting. Higher flexibility and greater speed for a lower cost are the three main benefits for using Cloud Computing.

There are also some challenges in running eGovernment Services in the cloud. The most prominent challenges are related to data privacy and data security in addition to vendor lock-in.

Altinn can also benefit from the Cloud Computing model. There are no laws or regulations that present show stoppers. There are two different approaches for putting Altinn in the cloud: using Microsoft's data centers or establishing a national cloud for eGovernment services.

Preface

This report is written as part of the course TDT4520 – Program and Information Systems, Specialization Project in the fifth year of the Computer Science program at NTNU.

The initial project definition was written by John Krogstie with input from Ole B. Hansen and me, Simon Litlehamar.

Ole B. Hansen (Accenture) was the main supervisor for the project.

John Krogstie (NTNU) was also a supervisor for the project.

Simon Litlehamar

Contents

List of Figures

Chapter 1

Introduction

1.1 Motivation

Cloud Computing is a relatively new term within the computer science field. Although a new technology it as gained momentum quickly. Especially within the private sector the cloud computing model has been greeted with open arms. After the financial crisis governments have become more aware of their spending and have started to look for ways to save money.

Many governments have already moved to use digital solutions to increase efficiency of services. Some governments have also started to look at the cloud computing model to increase efficiency even more while lower the spending on IT and utilizing already constructed infrastructure.

Although seeing the benefits cloud computing can have there are some concerns among governments. These concerns include data privacy, security, compliance and legal issues.

The norwegian eGovernment platform Altinn is beginning to explore the possibilities of the cloud computing model.

1.2 Scope

As described in the previous section cloud computing is a growing technology in IT and governments have gained interest in the field. It is interesting to look at the benefits of cloud computing for governments when using it for eGovernment services. The cloud computing model also presents some challenges for governments.

The original project description:

> *Different deployment models for cloud computing has been described, and the student should first look at the literature to describe the different deployment models and architectures and their usage. In particular, the student should look at relevant public services that can utilize a cloud architecture, and possible shop-stoppers in this regard being related to privacy, security, compliance and legal issues (primarily from a Norwegian point of view)*
>
> *If one are able to identify relevant public services, the student should in particular look upon how services that can be provided by Altinn can benefit from using a cloud architecture.*

The central tasks of this project and findings presented in this report are:

1. Describe the concepts of Cloud Computing and eGovernment Services
2. Identify benefits and challenges of using the cloud computing model for eGovernment services
3. Relate benefits and challenges to the use of cloud computing for Altinn

The main task is to look at benefits and challenges for usage of the cloud computing model for eGovernment services. The focus is to look at challenges pertaining to privacy, security, compliance and legal issues that affect eGovernment services in the cloud.

Some governments have already initialized cloud computing initiatives in varying degree. Looking at existing solutions and how they are handling the challenges and mitigating the risks some of the knowledge might be transferrable to a solution with Altinn in the cloud.

The goal is not to solve challenges but identify possible show-stoppers

1.3 Report Overview

Chapter 2 gives a description to the central concepts "Cloud Computing" and "eGovernment Services". The term Cloud Computing is defined using NIST's definition of the term and then described with this as a basis. eGovernment Services gives a definition of eGovernment and then goes on to describe a norwegian eGovernment platform; Altinn. The chapter then describe some eGovernment solutions utilizing the cloud computing model.

Chapter 3 discusses opportunities, challenges and possible show-stoppers for using Cloud computing for eGovernment services.

Chapter 4 follows the structure of Chapter 3 and describes the benefits and challenges for using cloud computing for Altinn and other norwegian eGovernment services.

Conclusion presents the findings of the project along with a section containing further work.

Chapter 2

Presentation of Concepts

This chapter gives a general introduction of the central concepts of the report: Cloud Computing and eGovernment Services. This presentation will be a basis for the discussion in Chapter 3. Together with the two central concepts there are some existing eGovernment services utilizing the cloud computing model that will be introduced.

The first section (2.1) uses the NIST definition to give a general description of the cloud computing model, its key characteristics, service models and deployment methods.

The second section (2.2) gives an introduction to eGovernment services and also to eGovernment services in Norway, specifically Altinn.

The third section of this chapter (2.3) presents some eGovernment solutions that are already utilizing the cloud computing model.

2.1 Cloud Computing

The concept of Cloud Computing started it's development as early as the 1960s when John McCarthy expressed that *"computation may someday be organized as a public utility"*. This thought was further developed in the 1966 book "The Challenge of the Computer Utility"[10] by Douglas Parkhill, where he compared the supply of computational power to the supply of electrical power. This

analogy is oversimplified, i.e. the data transferred over the network contain information, electrons do not, but it gives a basic idea of the concept.

After the dot-com bubble many companies were in a place where they had large data centers which only utilized 10% of their computational power. Amazon saw the potential in this and launched their Amazon Web Service in 2006. IBM and Google together with many universities joined the effort and started on a large research project.

2.1.1 Definition

Cloud Computing is relatively new term within Computer Science and there seems to be no consensus definition.

National Institute of Standards and Technology (NIST) defines Cloud Computing as [9]:

> a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

NIST describes five essential characteristics, three service models and four deployment models [9]. These will be described in detail in the following sections.

The NIST definition does not include the business angle of cloud computing, but as this is not a large drawback with regards to this project, the definition will suffice.

2.1.2 Key Characteristics

The NIST definition of Cloud Computing describes five essential characteristics of cloud computing. On-demand self-service, broad network access, resource pooling, rapid elasticity and measured service.

On-demand self-service Clouds offer automatic scaling of resources without human interaction.

Broad network access Applications hosted in the cloud are often available from thin-clients like mobile devices and web browsers thereby offering great flexibility.

Resource pooling The cloud uses virtualization of resources and therefore appears as one large pool of resources. These resources are dynamically assigned to the users of the cloud. The users of cloud services generally does not know the exact location of the resources being provided, but can in some cases define a location at a higher level of abstraction (e.g. country, continent).

Rapid elasticity Demanded resources in the cloud can be quickly allocated to the customer. The cloud's resources often appears as unlimited from the customers point of view.

Measured service The system automatically monitors and controls the resources used by each customer. The most used method of payment is a pay-per-use model where the customer pay for the resources used. This requires monitoring and control of resources.

2.1.3 Service Models

The NIST definition describes three different service models. The three levels offers different levels of abstraction.

Cloud Software as a Service (SaaS) A customer can rent an application running in the cloud. The application is often accessed via thin clients like web browsers. The customer does not control the underlying cloud structure and not even the application capabilities except for limited configuration settings for the application. Examples of SaaS providers are Salesforce.com and Servicenow.com.

Cloud Platform as a Service (PaaS) The customer is offered a platform where customer created applications can be deployed using APIs offered by and programming languages supported by the service provider. The customer does

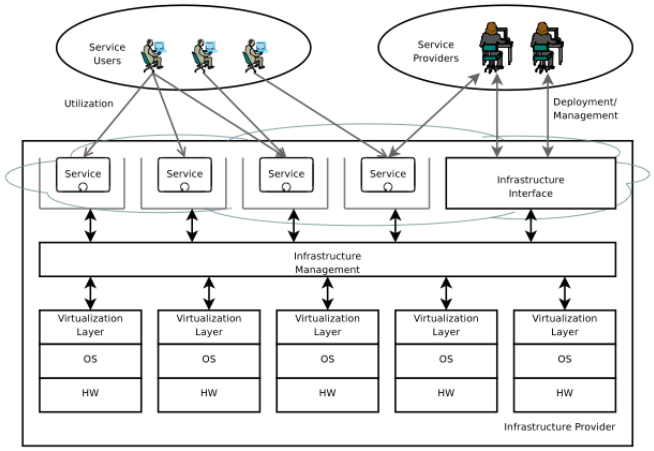

Figure 2.1: This figure illustrates cloud computing. Source: [13]

not control the underlying structure (i.e. operating system, network or storage). An example of this is Microsoft's Windows Azure platform.

Cloud Infrastructure as a Service (IaaS) The cloud infrastructure, usually a platform virtualization environment, is delivered as a service. The customer can control a large part of the platform (i.e. operating system and storage).

2.1.4 Deployment Methods

Customers using cloud computing have different needs when it comes to data privacy and data security. Some have private data that they will not risk being accessed by others, some organizations share privacy concerns and can use the same cloud, while others do not have any concerns with sharing computational resources with others. The NIST definition of cloud computing [9] describes four deployment methods for clouds. A deployment method describes who has access to the cloud. Figure 2.2 illustrates the different methods.

Private Cloud A private cloud is as the name says; private. Private clouds are typical for organizations that have sensitive data that they do no want to risk unauthorized access to.

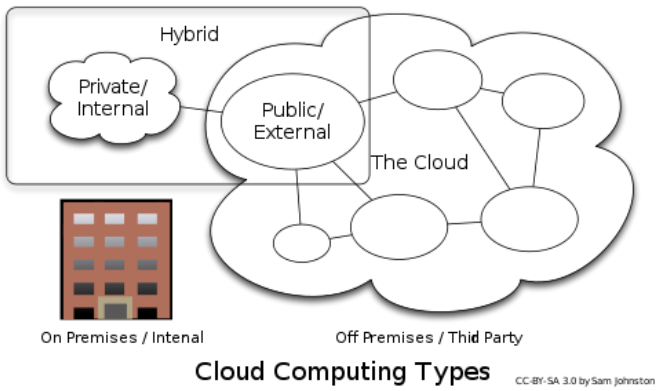

Figure 2.2: This figure shows an illustration of the different deployment methods in cloud computing. Source:m

Community Cloud A community cloud is a private cloud for a larger group. This may be organizations that require the same type of security. They may also use the same type of data in their applications.

Public Cloud A public cloud is a cloud infrastructure that is available to the public. Applications and data can coexist independent

Hybrid Cloud A hybrid cloud is a combination of the previously mentioned cloud types. An organization can run a private or community cloud and utilize the resources of a public cloud if it is needed.

For organizations as large as governments a private cloud does not differ very much from community cloud. For the sake of simplicity the term community cloud will be used.

2.2 eGovernment Services

This section gives an introduction to eGovernment and eGovernment services. In a world where the Internet is central in the way we communicate effectively the development of government services utilizing the possibilities is important. By using eGovernment services governments can offer a higher level of service at the same or lower costs, be more efficient

2.2.1 Definition

The Gartner Group defines eGovernment as[6]:

> the continuous optimization of service delivery, constituency participation, and governance by transforming internal and external relationships through technology, the Internet and new media.

"eGovernance and Developing Countries"[4] describes an eGovernment Model. It defines three main actors that interact through eGovernment services: citizens, businesses and government.

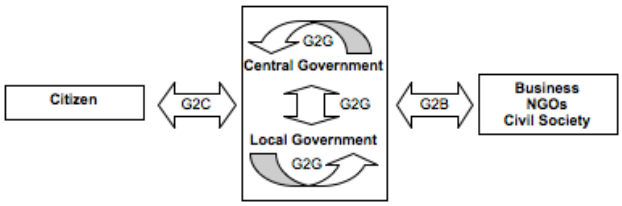

Figure 2.3: The figure shows interaction between the three different groups. Source: [4]

A common way of modeling eGovernment maturity is through a four phase maturity model. The UN's eGovernment Survey[12] identifies the phases as emerging, enhanced, transactional and connected.

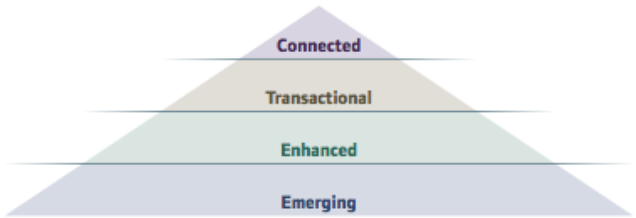

Figure 2.4: The figure illustrates the four phases of eGovernment maturity according to the UN. Source: [12]

Emerging

In the emerging phase of eGovernance governments are in the early stages of utilizing the functionality offered by internet. Relevant information to citizens,

businesses and also government agencies are presented on static governmental internet pages. This is a one-way flow of information.

Enhanced

eGovernment services allow for two-way communication and interaction in addition to static information. Users can download forms and documents, search among government information and ask questions via for example e-mail.

Transactional/vertical integration

The eGovernment services offers complete support for transactions. Users of the service can complete transactions via online services without visiting a government office.

Connected/horizontal integration

All eGovernment services can be reached from one place, a one-stop-shop. All government information systems are integrated.

2.2.2 eGovernment in Norway

Norway is among the top 10 countries in the world when it comes to level of maturity for eGovernment systems according to the UN's eGovernment Survey of 2010 [12]. Norway have several eGovernment services: Altinn.no, norge.no, minside.no and other smaller state and municipal portals. Figure 2.5 illustrates the national infrastructure. It is a three-layered model.

The bottom layer contains agency systems, registries and other information systems in the government. The second layer includes the core components, e.g. forms engine and messaging. The top layer is the presentation layer and includes the websites.

Describing Altinn as an eGovernment service is insufficient. Altinn is a service platform hosting a variety of different services. It works as an interface between government systems and the public, i.e. citizens and businesses. Some of the services included in Altinn are: submission services, messaging services,

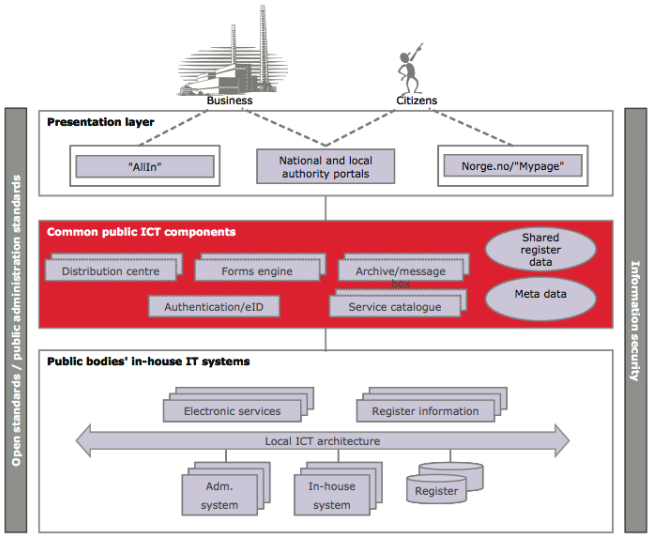

Figure 2.5: The figure shows the national infrastructure of eGovernment in Norway. Source: [2]

information services, link or authorization services, distribution services, and compound services. Altinn also has an authentication service and acts as a centralized user database [2].

The submission service is the core service of the service platform Altinn. The submission service allows for reporting through web forms. Web forms can be pre-populated by information that already exist in the system. Forms can also be collaboratively completed with different actors each contributing different parts. The tax declaration service is the most commonly used service in Altinn.

The messaging service allows the government to send messages to registered users. The messaging service also contains a feature which allow the sender to see if the message has been read. Messages can contain attachments and the registered users can also forward the messages to an external e-mail account.

The information service provide information from central registries.

The link or authorizations service allows for eGovernment services located outside Altinn to be linked. Altinn acts as a proxy for authorization before redirecting the user to the external service.

The distribution service allows for data transfer between government organizations.

The compound service allows for combination of services across processes and process owners. Different actors can contribute at different stages in the process.

The authentication/eID service is also a central part of Altinn and as mentioned also serves as a proxy for other eGovernment services outside of the Altinn service platform.

2.2.3 Types of Data in eGovernment Systems

To understand some of the concerns presented in Figure 3.2 it is valuable to look at what types of data exist in eGovernment systems.

The types of data in eGovernment systems varies with the level of usage and commitment from government agencies and departments, but in most cases some of the information is sensitive either towards privacy of citizens and businesses or national security.

There are different definitions of types of data. The EU/EEA directive (Section 3.2.2) defines personal data as:

> *any information relating to an identified or identifiable natural person ("data subject"); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity;*

Data related to religious beliefs, political opinions, health, sexual orientation, race, and membership of past organizations are regarded as sensitive personal data.

2.3 Existing Cloud Solutions for eGovernment Services

Some governments have already started using cloud technology for different purposes. USA, Great Britain, Thailand and Japan are in an early stage of their cloud computing commitment. Some governments use cloud application for internal administrative tasks. As mentioned in Section 1.2 the focus of this report is eGovernment services pertaining to external actors e.g. citizens and businesses.

The following sections contain a short presentation of different government cloud initiatives. More detailed descriptions of how the different initiatives are handling the challenges that the cloud computing model presents can be found in Chapter 3.

The general strategy of the governments is building a community cloud for government use. Governmental departments and agencies share many concerns pertaining to data privacy and therefore a community cloud makes sense.

Apps.gov seems to be the furthest developed platform for eGovernment services using cloud computing. Great Britain has also made strategies to establish cloud computing services. Some countries in Asia are also in very early stages of implementing cloud computing for use with eGovernment services.

2.3.1 United States of America – Apps.gov

Apps.gov was announced in September of 2009 and is part of the USA's Federal Cloud Computing Initiative. It is one of many steps the American government is taking to lower costs for governmental IT services. The US government spent large amounts of money on IT infrastructure and is hoping that cloud computing will both lower these costs and increase the efficiency of the current infrastructure.

Apps.gov is a storefront offering cloud services to governmental departments and agencies. The service catalog of Apps.gov is large with a variety of services. The services are offered by third party vendors who have a contract with Apps.gov. Both SaaS and IaaS are offered, and PaaS is on the way, and services for most administrative tasks can be found.

2.3.2 Great Britain, Japan and Thailand

Great Britain's G-Cloud is still in very early stages. The goal is to save 20% of the yearly spending on IT.The G-Cloud will in the same way as Apps.gov offer all three service models (Section 2.1.3) and an application store.

Both the asian cloud initiatives are in very early stages of planning. The same arguments as for the G-Cloud are presented.

2.3.3 Google Government Cloud

The Google Government Cloud was announced in September of 2009 and expected launch during 2010. The Google Government Cloud will offer the Google Apps platform to government agencies. For Google to be allowed to offer these services the Google Government Cloud is FISMA-certified. A description of what the FISMA-certification entails can be found in Section 3.2.1.

The Google Government Cloud received the FISMA-certification in July of 2010 and are offering Google Calendar and GMail and other applications supported by Google Apps will be offered eventually.

Chapter 3

Cloud Computing for eGovernment Services

The idea of this chapter is to use the concepts presented in the previous chapter to identify benefits and challenges of using the cloud computing model for eGovernment services.

The first section (3.1) identifies some benefits of cloud computing for eGovernment services and describes the most central benefits, cost, speed and flexibility in detail.

The second section (3.2) describes legislation affecting data security and data privacy. There are three subsections, each describing legislation from different areas, i.e. FISMA, EU/EEA directive and the norwegian personal data act.

The third section (3.3) discusses the challenges of using cloud computing for eGovernment services. The focus is on the most prominent challenge: protecting sensitive personal data; data privacy.

The fourth section (3.4) discusses the different deployment methods described in Section 2.1.4 for use with eGovernment systems.

3.1 Benefits of Cloud Computing for eGovernment Services

The Ministerial Declaration on eGovernment[1] outlines the EU's commitment to eGovernment towards 2015. The declaration states, among other things, that:

- *"We recognise that better public services need to be delivered with fewer resources ..."*
- *"Improve eGovernment services to cater for the different needs of users and deliver them in the most effective way."*

The focus of the EU in regards to eGovernment fits good together with the idea of utilizing the possibilities of cloud computing.

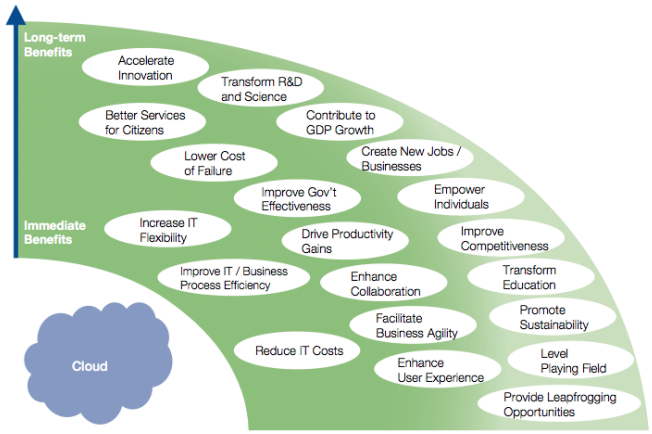

Figure 3.1: This figure illustrates benefits of cloud computing as described by Accenture and World Economic Forum. Source: [7]

Figure 3.1 is based on workshops with cloud computing experts under the direction of Accenture and World Economic Forum and identifies several benefits of cloud computing. The most immediate benefits is increased IT flexibility, improved process efficiency and reduced IT costs. This is also confirmed by the already established cloud solutions for eGovernment services described in Section 2.3. Both the G-Cloud and asian initiatives presented lowered costs as a key argument for the use of cloud computing.

There are also more long term benefits of using the cloud computing model. Among these are Transform R&D and Science and Accelerate Innovation.

There are especially three use cases where the cloud computing model offers advantages compared to conventional hosting [3]:

1. When demand for computational power varies with time
2. When demand is unknown in advance
3. When large amounts of computational power is needed for provisional work, for example batch analysis

Cost

Based on the examples of governments already utilizing some of the possibilities of cloud computing presented in Section 2.3 the most dominant argument is the cost argument.

The most common description of the cloud computing cost model is *"converting capital expenses to operational expenses"*[3]. The most common price model for cloud computing systems is pay-per-use which reflects the previously mentioned description. As described in Section 2.1.2, measuring of service is one of the key characteristics for cloud computing. This allows the service provider to charge the customer for the computational power used.

For government created community clouds the utilization of already existing IT infrastructure is also a focus. The UK government hopes to save 20% of their IT budget by utilizing cloud computing instead of traditional hosting.

Speed

Cloud computing offers easy start-up of new services and easy expansion of existing ones. This is a huge benefit for eGovernment services. Kate Craig-Wood, managing director of a cloud hosting firm, and central in the development of the G-Cloud strategy (Section 2.3.2) says [8]:

> *Local government would be an ideal target for small, customised apps because most county councils have similar needs for tools to monitor*

bins, street light repair and all sorts of things. That's an ideal case for sharing a solution in-house and letting that be scaled up.

For large organizations the change and evolution of processes may take time. The benefit of being able to provide parts of the organization with tools when they are ready for them instead of imposing it on the whole organization will make government departments and agencies more agile and responsive.

Flexibility

A third central focus for governments to utilize the cloud computing model is the flexibility offered. Clouds are well suited for sporadic or temporary high work loads. In Norway for example the tax returns for citizens are released presenting Altinn for high amounts of traffic. Among the characteristics of the cloud model are resource pooling and rapid elasticity (Section 2.1.2), giving a cloud solution the ability to handle these sporadic and temporary high loads.

Other Benefits

By providing better access to national data: economic, census, agricultural, meteorological etc. new applications utilizing these data sets can be developed. These applications might for example combine data sets to find correlations. This is also strongly connected to the the speed benefit (Section 3.1). New applications can quickly be implemented and used in the cloud. This will accelerate innovation and R&D and science may also benefit from this. It may also present new jobs or business opportunities.

3.2 Legislation Affecting the Use of Cloud Computing

Many governments have already identified the challenge of data privacy and security in eGovernment services and have produces laws and regulations for information systems containing sensitive data.

Privacy regulations from the USA and EU/EEA will be used as an example to highlight some of the challenges cloud computing has pertaining to privacy reg-

ulations. The two regions have different takes on privacy laws and regulations. There are different methods of governing the regions and this affects privacy laws and regulations.

3.2.1 Federal Information Security Management Act – FISMA

The Federal Information Security Management Act (FISMA) is a United States federal law.

> *FISMA requires each federal agency to develop, document, and implement an agency-wide program to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source.*

FISMA focus on information security not just for personal and sensitive data, but for all government information systems where as the Data Protection Directive focus more on privacy.

3.2.2 Directive 95/46/EC – Data Protection Directive

The Data Protection Directive is an EU directive regulating the processing of personal data within the EU/EEA. The directive regulates all processing of personal data (defined in Section 2.2.3) where processing is defined as *"any operation or set of operations which is performed upon personal data, whether or not by automatic means ..."*[11].

There are three main principles described by the directive: transparency, legitimate purpose and proportionality.

Transparency *The data subject has the right to be informed when his personal data is being processed. The controller must provide his name and address, the purpose of processing, the recipients of the data and all other information required to ensure the processing is fair.* (art. 10 and 11) [11]

Legitimate Purpose *Personal data can only be processed for specified explicit and legitimate purposes and may not be processed further in a way incompatible*

with those purposes. (art. 6b) [11]

Proportionality *Personal data may be processed only insofar as it is adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed. The data must be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified; The data shouldn't be kept in a form which permits identification of data subjects for longer than is necessary for the purposes for which the data were collected or for which they are further processed. Member States shall lay down appropriate safeguards for personal data stored for longer periods for historical, statistical or scientific use.* (art. 6) [11]

The directive also states that there should be a supervisory authority that will monitor the level of data protection.

All member states of the EU and EEA must implement this directive in national law.

3.2.3 Norwegian Personal Data Act – Personopplysningsloven

The Norwegian Personal Data Act is the norwegian implementation of Directive 95/46/EC and is interesting to describe because it is the main legislation affecting Altinn in an cloud computing environment.

The law implements the three principles described in the previous section. All businesses and actors handling personal or sensitive data are by law required to have procedures for maintaining data security and data privacy. For cloud vendors this would imply that they need employees with adequate level of security competence and also ensure that third party suppliers have equally high level of security procedures.

In Norway the Data Inspectorate is the supervisory unit responsible for monitoring the level of data protection and data privacy. The inspectorate also have other tasks including keeping a record of actors processing personal and sensitive data, handling licenses to process aforementioned data, identify risks and provide information on how to avoid risks and provide advice and guidance.

3.3 Challenges of Cloud Computing for eGovernment Services

As seen in the previous section, cloud computing can offer several benefits compared to traditional hosting, but there are some security and privacy concerns that need to be addressed.

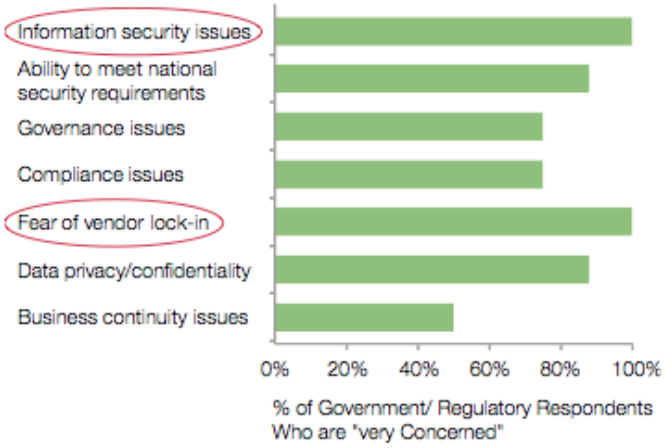

Figure 3.2: This figure shows government concerns pertaining to cloud computing. Source: [7]

Figure 3.2 shows the most prominent concerns of governments pertaining to the use of the cloud computing model. It is based on workshops under the direction of Accenture and World Economic Forum [7].

These concerns will be described in the following sections.

3.3.1 Information Security Issues

In the cloud computing model there are security threats from two sides. The first one being external to the cloud and the second being internal in the cloud.

For external security threats many of the measures user to secure the cloud are similar to the ones used to ensure the security of conventional hosting services. However the responsibility for the information security of the cloud is divided between many parties: the cloud vendor, the cloud user and other third-party vendors involved in for example software configurations. As described in Section

2.1.3 there are three different service models and the user's control over the cloud increases. This also means that for service models which offer extensive control over the cloud the responsibility for information security is shifted to the cloud user.

For internal security threats the cloud provider must guard against denial-of-service attacks and theft of data by other users. One of the central idea of cloud computing is the virtualization of resources (Section 2.1.2). This is also the primary security mechanism in the cloud. There always exist the possibility of bugs in the virtualization software which allow either applications to execute code outside of their virtualized machine and allow other cloud customers to steal data.

A second internal security threat comes from the cloud provider. The provider controls and own the cloud and therefore have physical access to the data. The spying on customer data by cloud providers should be addressed in service level agreements (SLAs). Although one should expect that the provider does not spy on customer data, the customer needs to ensure that hard disks from the data center is being disposed of without wiping the data. These scenarios are should also be covered in SLAs.

Many of these threats are similar to the security threats of conventional hosting. In the case of external threats the cloud computing model can in some cases be more secure [5]. Security measures are cheaper in large scale. Other security benefits mentioned in [5] are multiple locations, audit and evidence-gathering mechanics and more timely, effective and efficient updates.

3.3.2 Fear of Vendor Lock-in

As mentioned in the section presenting cloud computing (Section 2.1) both the term and the technology are fairly new and there is no cloud computing standard developed. There are several suppliers of cloud computing services and many of them are using different APIs for control of the cloud applications and different systems for storage of data in the cloud.

The lack of standardized cloud storage means that customers of cloud computing services can not extract and transfer their data between different cloud providers. This leads to customer vulnerability to the cloud provider increasing prices, reliability problems and even worse if the cloud provider goes out of

business [3].

3.3.3 Ability to Meet National Security Requirements and Data Privacy/Confidentiality

Legislation pertaining to data privacy in Europe and Norway and the legislation pertaining to information security in the USA was presented in Section 3.2 can be used as a basis for looking at security requirements set by the government. The two concerns mentioned in the headline are strongly connected and in a large degree affected by the same legislation.

One of the big concerns of usage of cloud computing for eGovernment services is the geographic location of the data. It is unwanted that data sensitive to national security and sensitive person data can be accessed by unauthorized actors. Especially foreign governments.

As mentioned in the description of the cloud computing model (Section 2.1.2), resource pooling is one of the key characteristics of the model. Situations where data might be transferred over country borders to utilize resources of other data centers is a plausible scenario.

Some governments may limit the type of data that is allowed transferred over country borders. The Data Protection Directive allows for data to be transferred across borders within the EU/EEA and also to countries outside the EU/EEA if the country provide an adequate level of protection. The norwegian implementation of the directive (described in Section 3.2.3) opens for export of personal data to countries that have implemented Directive 95/46/EC (§29).

Governments building national community clouds for government use onshore seems to be the most common solution thereby hindering storage of data offshore. Access to the data is limited to a community with shared concerns for data privacy and security.

The Google Government Cloud is an example of a third party vendor offering cloud services for government use. As mentioned in Section 2.3.3 the Google Government Cloud is FISMA-certified. FISMA (Section 3.2.1) requires Google to develop processes to promote information security.

Some governments may limit the type of data that is allowed transferred over country borders. The Data Protection Directive allows for data to be transferred

across borders within the EU/EEA and also to countries outside the EU/EEA if the country provide an adequate level of protection.

If using a cloud provider that is located in another country a comparison of laws and regulations pertaining to data privacy and security is interesting. If both countries share the same level of required data protection Service Level Agreements (SLAs) can be used to limit access to the data.

3.4 Cloud Deployment Method for eGovernment Services

As presented in Section 2.1.4 there are four different deployment methods for clouds. In this section the choice of deployment model for eGovernment services will be discussed.

The eGovernment services used discussed in the first sections can be assumed to contain personal and in some cases sensitive data. A second case may be governments wanting to share public data, e.g. statistical data. These data can be hosted by cloud storage solutions using a public cloud.

3.4.1 Community vs. Public

As mentioned previously the eGovernment systems can be assumed to contain personal and sensitive data. Section 3.3.1 mentions some risks pertaining to information security of clouds. One of these risks being unauthorized access to application data from other applications. The risk of these data coming into unauthorized hands is not wanted. A solution using a public cloud would probably not be able to meet the expected level of security.

Taking USA as an example the legislation affecting government systems in the cloud is FISMA. Google's Government Cloud is FISMA certified. This is a community cloud for governments. Certifying a public cloud solution for government use is probably unlikely both due to high costs and technical challenges of offering the level of security needed.

3.4.2 Hybrid Cloud

Hybrid clouds would offer greater flexibility. If e.g. in an eGovernment service there are can be scenarios where there are sporadic and temporary increase in load and the private/community cloud is not scaled to handle this load some resources may be used from a public cloud.

The use of a hybrid cloud is a possibility, but it requires the data being processed in the public cloud to not be sensitive. The technical challenge of ensuring data security and privacy is large.

Chapter 4

Cloud Computing for Altinn and Other Norwegian eGovernment Services

Section 2.2.2 contains a description of Altinn and Altinn's architecture in addition to the national infrastructure for eGovernment services in Norway.

The reason for including other eGovernment services in addition to Altinn is that it would make little sense to make a private cloud just to host Altinn. In practice this is just the same as running one application on one or a set of servers. There is also a possibility of using public or community cloud to host Altinn alone. This will be discussed in Section 4.3.

The following sections will use the structure of the previous chapter to describe each of the point in the perspective of the case of using cloud computing for Altinn and other Norwegian eGovernment services.

4.1 Benefits

The benefits described in the following sections will to a greater or lesser extend depend on the deployment method chosen. This is especially true for the Cost benefit. The sections will therefore in most cases contain a general overview and if there are inconsistencies between benefits for the different deployment methods these will be described.

4.1.1 Cost

As mentioned in Section 3.1 one of the largest benefits of the cloud computing model is related to cost. The reason for this is the pay-per-use pricing model. There are some requirements for this to be profitable. Because of the cloud characteristic "infinite" resource pool the data centers must be able to support this illusion. Therefore it is important that computational power is utilized because unused computational power is wasted.

The case of creating a national community cloud to host eGovernment services is discussed in Section 4.3.

4.1.2 Speed

The speed in which new applications can be developed and put in the cloud could definitely be a benefit for Norwegian eGovernment services. Altinn is the main portal for nationwide reporting. What could happen in the future is application being developed to support administrative processes in municipalities.

An other benefit related to Speed is the "Adopt at your own pace" thinking which allows for different rates of adoption between for example different municipalities. This also relates directly to the cost benefit because one would utilize the cloud model benefits rather than needing to scale the hosting service for one specific scenario where for example all municipalities used a service.

4.1.3 Flexibility

As mentioned in Section 2.2.2 the tax declaration service is the most commonly used service in Norway. Tax declaration affects most of the working citizens

in Norway and also businesses. When the tax return calculation is released to the users of Altinn it generates enormous amounts of traffic which the hosting service Altinn uses is not scaled to handle.

Using the cloud computing model the resources available to Altinn could be increased utilizing resources from the resource pool.

4.1.4 Other Benefits

The way Altinn is designed, using a Service Oriented Architecture, makes the fit with the cloud computing model good. As mentioned in Section 3.3.2 there are no standard API used in clouds. Different cloud solution support different programming languages. In such a large system as Altinn using only one type of technology can be complicated. Altinn is built on Microsoft Technology and therefore the Microsoft Azure cloud is very interesting to look at. More about this can be found in Section 4.3.

4.2 Challenges

One can assume that the challenges perceived by governments in [7] also apply for the norwegian government and this section will focus on the following points: information security issues, fear of vendor lock-in and the ability to meet national security requirements and data privacy/confidentiality.

4.2.1 Information Security Issues

There is really nothing separating Altinn from other eGovernment services pertaining to the information security issues described in Section 3.3.1.

4.2.2 Fear of Vendor Lock-In

Altinn is built on Microsoft technology and therefore the Windows Azure platform should be a good fit. This presents a problem pertaining to vendor lock-in and decreased possibilities for competition between cloud actors interesting for Altinn.

The decreased possibilities for competition is not as prominent if Windows Azure can be run on-premises or by other vendors than Microsoft. It will then be, in the right sense, a cloud platform.

The technical challenges of running Altinn on other cloud platforms is no discussed in this report.

4.2.3 Ability to Meet National Security Requirements and Data Privacy/Confidentiality

There are no specific laws and regulations in Norway that inhibit use of the cloud computing platform. There are no big differences between using conventional hosting versus cloud computing when it comes to national security requirements. The same requirements as descried in Section 3.3.3. Norwegian laws and regulations pertaining to storage and processing of personal and sensitive data are described in Section 3.2.3.

4.3 Deployment Method

Seeing that Altinn contain and process an amount of sensitive personal data the use of public cloud would present large security risks. As discussed in Section 3.4 the use of community clouds for eGovernment services seems to be the most used. This includes Apps.gov and Google's Government Cloud and the community cloud method is also central in the british and asian plans.

Other eGovernment services than Altinn could also run in a government community cloud. As mentioned in Section 3.1 one of the main benefits of cloud computing is the simplicity of adding new applications to the cloud and many municipals might have the same needs in software for different administrative tasks.

Chapter 5

Conclusion

In the previous chapters the concepts of Cloud Computing and eGovernment Services have been introduced. Benefits and challenges of using cloud computing for eGovernment services have also been discussed. The benefits and challenges identified have then been extrapolated to the case of putting Altinn, a Norwegian eGovernment service platform, in the cloud.

5.1 Findings

Cloud computing is seen as the future of computing by many governments, as mentioned in Section 2.3 where some national cloud solutions for eGovernments services either have been established or are planned. This also shows that it is technologically possible to do it. Although the services used as an example here are somewhat different from Altinn, the benefits and challenges can be transferred.

Data privacy laws does not hinder the transfer for personal or sensitive data across national borders. At least not between countries that have an adequate level of data protection and data privacy by law.

5.2 Further Work

In Section 4.3 different cloud deployment methods for Altinn are discussed. On of the possibilities mentioned is the establishment of a national cloud infrastructure hosting Altinn and other Norwegian eGovernment services. It would be interesting to look into if this interferes with some legislation pertaining to competition among providers to the government.

Bibliography

[1] 5th Ministerial eGovernment Conference. Ministerial Declaration on eGovernment. Nov 2009.

[2] Gustav Aagesen and John Krogstie. Service Development for National Government Information Infrastructures - The Case of Norway.

[3] Michael Armbrust, Armando Fox, Rean Griffith, Anthony D. Joseph, Randy Katz, Andy Konwinski, Gunho Lee, David Patterson, Ariel Rabkin, Ion Stoica, and Matei Zaharia. A view of cloud computing. *Commun. ACM*, 53:50–58, April 2010.

[4] Michiel Backus. eGovernance and Developing Countries. 2001.

[5] European Network and Information Security Agency. Cloud Computing – Benefits, risks and recommendations for Information Security. November 2009.

[6] Gartner Group. Key Issues in E-Government Strategy and Management. *Research Notes*, May 2000.

[7] World Economic Forum in Partnership With Accenture. Exploring the Future of Cloud Computing: Riding the Next Wave of Technology-Driven Transformation. 2010.

[8] Jemima Kiss. G-cloud would help government save. June 2010. http://www.guardian.co.uk/cloud-computing/g-cloud-would-help-the-government-to-save, retrieved November 15th 2010.

[9] Peter Mell and Tim Grance. The NIST Definition of Cloud Computing. Oct 2009.

[10] D H Parkhill. *Challenge of the Computer Utility*. Addison-wesley, 1966.

[11] The European Parliament and the Council of the European Union. Directive 95/46/EC of the European Parliament and of the Council. *Official Journal of the European Communities*, October 1995. http://ec.europa.eu/justice/policies/privacy/docs/95-46-ce/dir1995-46_part2_en.pdf, retrieved November 15th 2010.

[12] United Nations Department of Economic and Social Affairs. UN eGovernment Survey 2010. 2010.

[13] Luis M. Vaquero, Luis Rodero-Merino, Juan Caceres, and Maik Lindner. A break in the clouds: towards a cloud definition. *SIGCOMM Comput. Commun. Rev.*, 39(1):50–55, 2009.