INTERDEPARTMENTAL PROGRAMME OF POSTGRADUATE STUDIES

(I.P.P.S.) IN INFORMATION SYSTEMS

MSc Dissertation

CLOUD COMPUTING IN EGOVERNMENT

by

ELENI G. DERMENTZI

Submitted as a prerequisite in fulfillment of the requirements for the acquisition of the postgraduate degree in Information Systems

February 2013

Acknowledgments

I would like to thank my supervisors, Professor Dr. Konstantinos Tarabanis and Assistant Professor Dr. Efthimios Tambouris for their trust and continuous help whenever needed. I would especially like to thank Dr. Tambouris for his advice, suggestions and constructive criticism that helped me to improve this work.

Abstract

The purpose of this MSc dissertation is to examine the adoption of cloud computing in eGovernment. An extensive literature review of related research papers and case studies was conducted to discover the current state of knowledge in the topic and identify areas that need further research. The results of the literature review were used to form a theoretical stage model for cloud computing adoption in eGovernment that could help governments to identify their progress in the field. The proposed model measures the degree of cloud computing adoption and the organizational and technological complexity that this involves. It consists of four stages: “Ad-hoc eGov Cloud Solutions”, “Cloud-based Public Services”, “eGov Cloud(s)” and “eGov Cloud Policy”.

Table of Contents

Acknowledgments ii

Abstract iii

Table of Contents iv

List of Figures vii

List of Tables viii

1. Introduction 1

1.1. Problem Statement 1

1.2. Research scope and objectives 1

1.3. Structure of the thesis 2

2. Theoretical Foundations 4

2.1. Introduction 4

2.2. The concept of eGovernment 4

2.2.1. What is eGovernment? 4

2.2.2. Types of eGovernment 4

2.3. Cloud Computing 5

2.3.1. Defining Cloud Computing 5

2.3.2. Cloud Computing Architecture 6

2.3.3. Service Models 7

2.3.4. Deployment models 7

2.3.5. Essential Characteristics 8

2.4. Summary 9

3. Methodology 10

3.1. Introduction 10

3.2. Literature Selection Strategy 10

3.3. Organizing the literature 11

3.4. Summary 12

4. Literature Review 13

4.1 Introduction 13

4.2 The Conceptual Framework 13

4.3. Examining the adequacy of cloud computing in eGovernment 15

4.3.1. Benefits 15

4.3.2. Risks and Challenges 17
4.3.3. Focus on specific cases 19
4.4. Migration Strategy 21
4.4.1. Specialized frameworks and models 24
4.4.2. Use Cases and SWOT Analysis 32
4.5. Implementation 39
4.5.1. Cloud architectures for eGovernment 39
4.5.2. Cloud–based Platforms for Public Services 48
4.5.3. Open Data in the Cloud 50
4.6. Discussion 51
4.7. Conclusions 57
5. Case Studies 58
5.1. Introduction 58
5.2. Case Studies from North America 58
5.2.1. US Government- USA.gov 58
5.2.2. US Government- Apps.Gov 59
5.2.3. Department of Defense (DoD), Defense Information Systems Agency (DISA) – USA 60
5.2.4. National Aeronautics and Space Administration (NASA) - USA 60
5.2.5. City of Edmonton- Canada 61
5.3. Cases Studies from Asia 62
5.3.1. Japan 62
5.4. Case studies from Europe 63
5.4.1. United Kingdom 63
5.4.2. Germany 65
5.4.3. Greece 65
5.5. Findings of the Case Studies 66
5.6. Conclusions 69
6. A Stage Model for Cloud Computing Adoption in eGovernment 70
6.1. Introduction 70
6.2. Stage models in IT and eGovernment research 70
6.3. The Proposed Stage Model 73
6.3.1. Stage 1: Ad-hoc eGov Cloud Solutions 75
6.3.2. Stage 2: Cloud- based Public Services 76

6.3.3. Stage 3: eGov Cloud(s) 77
6.3.4. Stage 4: eGov Cloud Policy 78
6.4. Conclusions 79
7. Conclusions and future work 81
References 84
Appendix A: Related articles that did not meet inclusion criteria 98
Appendix B: Cloud Computing Use Cases 101
B.1 Business use case templates (Deussen et al., 2011) 101
B.2 Business use cases defined by NIST (2011b) 102

List of Figures

Figure 1: Cloud computing architecture (Zhang et al., 2010) 6
Figure 2: Proposed Conceptual Map for Cloud Computing in eGovernment Literature 14
Figure 3: Classification Framework for IaaS (Repschlaeger et al., 2012) 26
Figure 4: Component Group: User (Mutavdzic, 2012) 27
Figure 5: Component Group "Compute" (Mutavdzic, 2012) 27
Figure 6: Component Group "Database" (Mutavdzic, 2012) 28
Figure 7: Component Group "Fabric" (Mutavdzic, 2012) 28
Figure 8: Application pattern: Government Portal. An example of how proposed decision framework works (Mutavdzic, 2012) 29
Figure 9: Application pattern: Software+Services. An example of how proposed decision framework works (Mutavdzic, 2012) 30
Figure 10: Government to Cloud (Deussen et al., 2011) 30
Figure 11: Government to Cloud to Enterprise (Deussen et al., 2011) 31
Figure 12: Government to Cloud to Citizen (Deussen et al., 2011) 31
Figure 13: Government to Cloud to Government (Deussen et al., 2011) 31
Figure 14: An Example of a Legal Use Case (Deussen et al., 2011) 33
Figure 15: The C-Government concept (Zhang and Chen, 2010) 39
Figure 16: Proposed cloud architecture (Sharma and Kanungo, 2011) 40
Figure 17: eGovernment with cloud data center (Chuob et al., 2010) 41
Figure 18: Proposed eGovernment architecture based on Hadoop (Mukherjee and Sahoo, 2010) 42
Figure 19: eGovernment based on cloud computing with Knowledge-based expert system (Chanchary and Islam, 2011) 42
Figure 20: Cloud Computing Architecture of Taiwan EPA (Hung et al., 2011) 43
Figure 21: The Private Cloud of Taiwan EPA (Hung et al., 2011) 43
Figure 22: Architecture for a DWH in the Cloud (Breil et al., 2012) 44
Figure 23: Architecture for a Mediator- Wrapper based data integration in the Cloud (Breil et al., 2012) 45
Figure 24: Sharing Cloud Architecture for eGovernment (You et al., 2012) 46
Figure 25: Cloud Polling System (Vidhya, 2013) 47
Figure 26: Municipal Shared Services Cloud Ecosystem (Hobson et al., 2011) 50
Figure 27: Open Government Data Cloud (Zhang, 2010) 51
Figure 28: Apps.Gov Portal (https://www.apps.gov/cloud/main/start_page.do) 59

Figure 29: A "mash-up" map in Edmonton's Open Data Catalogue (http://data.edmonton.ca) 62
Figure 30: The Kasumigaseki Cloud (Wyld, 2010a) 63
Figure 31: CloudStore of G-Cloud (http://gcloud.civilservice.gov.uk/cloudstore/) 64
Figure 32: Components of G-Cloud (Cabinet Office, 2011) 64
Figure 33: Plotting the Cloud Maturity Model (Oracle, 2011) 72
Figure 34: A Stage Model for Cloud Computing Adoption in eGovernment 73

List of Tables

Table 1: Benefits, disadvantages and risks of SaaS (Janssen and Joha, 2011) 21
Table 2: Migration strategies for public sector organizations 22
Table 3: SWOT analysis for Public Cloud (ENISA, 2011) 35
Table 4: SWOT analysis for Private Cloud (ENISA, 2011) 37
Table 5: SWOT analysis for Community Cloud (ENISA, 2011) 38
Table 6: Summary of studies focused on specific use 52
Table 7: Specialized frameworks and models 54
Table 8: Comparison of cloud architectures/frameworks suggested for eGovernment . 55
Table 9: Comparison of cloud-based platforms 57
Table 10: Case Studies - Findings 67
Table 11: Main differences among stages 74

1. Introduction

1.1. Problem Statement

Most governments around the world use Information and Communication Technology (ICT) to provide services in a more effective way. Although the benefits from adopting Electronic Government (eGovernment) are clear, its implementation is restricted by some important barriers, such as high costs (Ebrahim & Irani, 2005; Pokharel & Park, 2009; Tsaravas & Themistocleous, 2011a), absence of experts (Ebrahim & Irani, 2005; Pokharel & Park, 2009), heterogeneous and incompatible information systems and security and private issues (Ebrahim & Irani, 2005; Tsaravas & Themistocleous, 2011a).

With the rise of cloud computing, the first scholars examining the potential use of cloud computing in eGovernment appeared. Cloud computing can solve many of the aforementioned issues that can limit eGovernment expansion, but has some risks, too. That has initiated research in the topic since scholars and government organizations try to determine ways to assure the successful adoption of cloud computing in the public sector. At the same time, governments make the first steps towards adopting cloud computing, with the United States being the first to launch a cloud strategy.

Since cloud computing is a relatively new concept, the research for cloud adoption in eGovernment is novel. At the time this study started, there was no review of the related literature. That raised the following research questions: What are the results of related research and are there any areas that require further study? Should cloud computing be used in eGovernment and how? Are there any governments around the world that have adopted cloud computing, and in what ways?

1.2. Research scope and objectives

The purpose of this study is twofold. First, to analyze and organize the results of research that has been conducted in the field and establish a conceptual framework that will map the current research and enable the easy identification of research gaps. Second, to propose a stage model that will rank the different uses of cloud computing in eGovernment and can be used to evaluate the progress of governments in cloud computing adoption.

The study is focused exclusively on the use of cloud computing in eGovernment. Therefore, the use of cloud computing in relative fields, such as eHealth or eLearning, is not examined. Also, subjects that are too technical, such as the establishment of security systems based on encryption algorithms or statistical models, are not examined in detail. However, there is a short reference to them in case the reader wants to search further these subjects.

The contribution of the dissertation lies to the fact that hitherto it is the only literature review of the topic. A previous attempt made by Tsaravas and Themistocleous (2011b) was limited to analyzing case studies in which cloud computing was used by public organizations, due to the absence of adequate research studies in the field at that time. In addition, the theoretical stage model for cloud computing adoption in eGovernment presented in this study is the only stage model in the related literature so far.

1.3. Structure of the thesis

The overall structure of the thesis takes the form of seven chapters, including this introductory chapter.

Chapter 2 presents the basic concepts of eGovernment and cloud computing. Definitions, the types of eGovernment, and the service and deployment models of cloud computing are presented so the reader can understand the rest of the study.

Chapter 3 describes the methodology that was followed in order to conduct the literature review.

Chapter 4 presents the literature review of the studies about the use of cloud computing in eGovernment. The conceptual "map" of the literature that was created from the analysis of the studies is presented here.

Chapter 5 can be considered as an extension of the previous chapter since it analyzes the case studies that were found during the literature review. It appears as a separately chapter though, since it contains some cases that have not presented in literature before and were found from further search.

Chapter 6 includes a brief review of stage models that have been proposed in IT and eGovernment research and presents the proposed stage model for cloud computing adoption in eGovernment.

Chapter 7 is dedicated to the conclusions, recommendations and limitations of the study, and the suggestions for further research.

2. Theoretical Foundations

2.1. Introduction

This chapter presents the basic concepts of eGovernment and cloud computing. Section 2.2 discusses the definitions and the different services of eGovernment. Section 2.3 examines what cloud computing is and which are the cloud deployment and service models. Finally, Section 2.4 presents the summary of the chapter.

2.2. The concept of eGovernment

2.2.1. What is eGovernment?

Various definitions of eGovernment have been proposed over the years. United Nations & ASPA (2002, p.1) defined eGovernment as "utilizing the internet and the world-wide-web for delivering government information and services to citizens". OECD (2003) provided a broader definition, according to which eGovernment is "the use of information and communication technologies, and particularly the Internet, as a tool to achieve better government". Fountain (2001, p. 4) uses the term of "virtual state" for eGovernment and realizes it as the "government that is organized increasingly in terms of virtual agencies, cross-agency and public-private networks whose structure and capacity depend on the Internet and web".

Hu et al., (2009) on the other hand extracted a widely shared definition of eGovernment, which is conceptualized by six elements, by analyzing vocabulary frequently used in eGovernment literature. According to them eGovernment deals with "(1) the major initiatives of management and delivery of information and public services; (2) taken by all levels of governments (including agencies, sectors); (3) on behalf of citizens, business; (4) involving using multi-ways of internet, web site, system integration, and interoperability; (5) to enhance the services (information, communication, policy making), quality and security; and (6) as a new key (main, important) strategy or approach".

2.2.2. Types of eGovernment

There are primarily four types of eGovernment services (Alshehri & Drew, 2010; UNESCO, 2005):

- Government- to- Citizen (G2C), refers to the communication and interaction between government and citizens that supports accountability, democracy and

improvements to public services. Citizens can access instantly and conveniently government information and make transactions like obtaining certificates and paying taxes, from everywhere, anytime.

- Government- to- Business (G2B), refers to services exchanged between government and businesses. It includes services such as distribution of policies and regulations, licenses renewal, payment of taxes and registration of new businesses. It can also mean the establishment of e-marketplaces for government purchases and e-procurement initiatives.
- Government- to – Government (G2G), refers to the communication and cooperation among government departments, organizations and agencies at national, provincial and local level. The services included in this category can be sharing of databases, resources and information about benefit policies, training opportunities and civil right laws.
- Government– to - Employee (G2E), refers to the interaction between government and civil servants. Services that fall into this category are online applications for an annual leave, reviewing of payment records, work guidelines and information for employment opportunities.

2.3. Cloud Computing

2.3.1. Defining Cloud Computing

One of the most cited definitions of cloud computing comes from U.S. National Institute of Standards and Technology (NIST) that defines it as "a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction" (Mell and Grance, 2011). Schubert (2010) has given a more general definition of "a cloud" as: "an elastic execution environment of resources involving multiple stakeholders and providing a metered service at multiple granularities for a specified level of quality (of service)".

Armbrust et al. (2009), on the other hand, use the term "Cloud" in order to refer to the datacenter hardware and software only, while they use the term "Cloud Computing" to

encapsulate both the applications delivered as services over the Internet and the datacenter hardware and software.

Klems et al. (2009) focused on the business perspective of cloud computing and gave the following definition: "Building on compute and storage virtualization technologies, and leveraging the modern Web, Cloud Computing provides scalable and affordable compute utilities as on-demand services with variable pricing schemes, enabling a new consumer mass market".

2.3.2. Cloud Computing Architecture

As can be seen in Figure 1, Cloud computing architecture consists of four layers (Zhang, Cheng and Boutaba, 2010):

- The Hardware layer, which manages the physical resources of the cloud (physical servers, routers, switches, power and cooling systems) and typically is implemented in data centers.
- The Infrastructure layer (also called virtualization layer), which partitions the physical resources using virtualization technologies in order to create the pool of storage and computing resources.

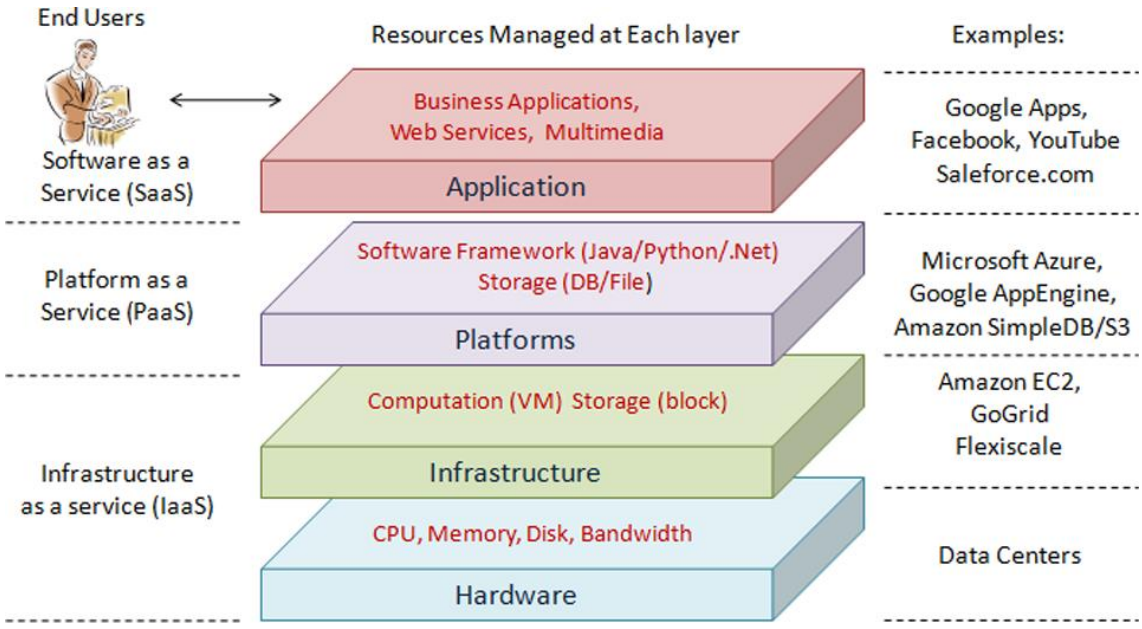

Figure 1: Cloud computing architecture (Zhang et al., 2010)

- The Platform layer, which includes operating systems and application frameworks so the burden of deploying applications directly into VM containers is minimized.
- The Application layer, which includes the actual cloud applications.

In contrast to the traditional computing architecture, the architecture of cloud computing is more modular and allows each layer to evolve separately since each layer is loosely coupled with its adjacent layers.

2.3.3. Service Models

The cloud computing business model is based on services which can be grouped into three categories: Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS) (Mell and Grance, 2011; Zhang et al., 2010). In 2012, the International Telecommunication Union (ITU) added two more service models: Communications as a Service (CaaS) and Network as a Service (NaaS).

- Software as a Service (SaaS): refers to on-demand provision of applications that run on a cloud infrastructure. The applications can be accessed by cloud service users through a web browser or a program interface.
- Platform as a Service (PaaS): in this model, the cloud service user can deploy user-created or acquired applications onto the cloud infrastructure through platform tools that cloud service provider supports. Although the service users cannot control or manage the cloud infrastructure, they control the deployed applications and sometimes the configuration settings of application-hosting environment.
- Infrastructure as a Service (IaaS): refers to on-demand provision of processing, storage, network connectivity and other computing resources of the cloud infrastructure where the user can run operating systems and applications. Again, the user does not control the cloud infrastructure, but the operating systems, the storage and the deployed applications.
- Communications as a Service (CaaS): the cloud service user can use real-time communication and collaboration services such as voice over IP, instant messaging and video conferencing.
- Network as a Service (NaaS): on-demand provision of transport connectivity services and inter-cloud network connectivity services.

2.3.4. Deployment models

Clouds can be hosted and used in different ways according to the requirements of each case. There are four deployment models of cloud computing that can be identified (Mell and Grance, 2011; Schubert, 2010):

- Private Cloud. The cloud infrastructure is dedicated to the needs of one organization that consists of multiple units. The Cloud may physically reside on or off premises and the owner and operator of it may be the organization itself, a third party, or a combination of them.
- Community Cloud. The cloud infrastructure is dedicated to the needs of a community of organizations that share the same interests in terms of mission, security requirements, policy and regulatory compliance. The Community Cloud does not differ from a Private Cloud in terms of hosting or ownership and administration.
- Public Cloud. The cloud infrastructure is open to general public. The owner and operator of a Public Cloud may be a business, academic, or government organization, or some combination of them. The Cloud resides on the premises of the cloud provider.
- Hybrid Cloud. The cloud infrastructure consists of two or more distinct cloud infrastructures (private, community, public) that although they are unique entities, they are closely connected through standardized or proprietary technology that enables data and application portability.

2.3.5. Essential Characteristics

The basic characteristics of cloud computing that differentiate it from traditional computing are (Mell and Grance, 2011; Zhang et al., 2010):

- On-demand self-service. The provision of cloud services is automatic without the need of human interaction with the service provider.
- Broad network access. Since Clouds use the Internet for delivering services, they enable access to cloud services from various thin clients such as mobile phone, tablets and laptops.
- Resource pooling. A pool of computing resources is offered by the infrastructure provider so multiple consumers can be served using a multi-tenant model. In that way, the providers can assign the computing resources in a flexible way and manage their own resource usage and operating costs more effectively.
- Rapid elasticity. Capabilities can be obtained and released on the fly and are often perceived by consumers as being unlimited and available in any quantity at any time.

- Measured service. Cloud computing offers transparency for both the provider and the consumer of the service since the resource usage can be monitored and controlled. That allows also the use of a pay-per-use pricing model.

2.4. Summary

This chapter presented the basic concepts on which the following chapters are based. Apart from the definitions, the different types of eGovernment and cloud computing models were discussed. The basic characteristics of cloud computing were also presented in an attempt to give the reader a better idea of how cloud computing differs from the traditional computing.

Although the above topics are briefly explained, this introductory chapter provides all the basic information that a reader, who is not familiar with the field, will need, in order to understand the rest of the thesis.

3. Methodology

3.1. Introduction

In an attempt to conduct a complete literature review in the emerging field of "Cloud Computing in eGovernment", the methodology proposed by Webster and Watson (2002) was followed. Unlike the author-centric approach that some authors adopt, the methodology used in this study is concept-centric, with the concepts determining the organizing framework of the review. In the subsequent pages of this chapter, the steps taken to indentify relevant literature are presented, along with the results of this procedure. A brief review of stage models was also conducted in order to choose the appropriate approach to form the stage model, and is presented in a separate chapter (Chapter 6) along with the stage model.

3.2. Literature Selection Strategy

Based on the approach of Webster and Watson (2002) that suggest that a literature review should not be limited to one methodology, set of journals or geographic region, in the first phase, the articles were selected by using the most well known databases and search tools (Scopus, Web of Science, Science Direct, CiteSeer and Google Scholar). Several combinations of the following keywords and phrases were used: "cloud computing", "public sector", "e-government", "public administration", "e-governance", "cloud", "electronic government", "government", "eGov", "eGovernment".

The second step was to review the citations of the articles identified in the first phase, in order to find more relevant articles. In this step, apart from articles, there were also found white papers published from well known organizations (the White House and European Commission were among them). Considering that the topic of the review is not just a theoretical concept, but it is of practical application, it was decided that white papers should also be included in the review, giving a more complete view of the developments in the field. Finally, the Web of Science was used to discover more articles related to the topic that were citing the key articles selected in the previous steps.

This procedure resulted in a group of 98 publications. The summaries of them were read in order to exclude articles irrelevant to the topic. Articles concerned eHealth and eLearning were also excluded since they were beyond the scope of this study. The following inclusion criteria were applied to each of the remaining publications:

- The articles had to be written in English.
- The papers should be in international peer-reviewed journals or conference proceedings, published by reliable publishing organizations (such as Springer, ACM and IEEE association). Papers of poor quality that did not meet international standards for scientific journals, and non-scientific articles, were not considered in the review.
- In case of white papers, the publisher should be a well-known organization with international presence or impact.

The 61 publications that matched the aforementioned criteria were used in the analysis stage that is described below. A list with the articles that are relevant to the topic, but were not eventually included in the review, can be found in Appendix A.

3.3. Organizing the literature

The study of the selected publications and the detection of repeating themes among them, led to the identification of several basic subjects in related literature. The subjects or "concepts" that were observed are:

- Benefits of cloud computing in eGovernment
- Risks and challenges of cloud computing in eGovernment
- Case studies
- Focus on specific application of cloud computing
- Specialized frameworks and models for cloud computing in eGovernment
- SWOT analysis of different deployment models of cloud computing for public sector
- Cloud computing use cases for eGovernment
- Cloud architectures for eGovernment
- Cloud-based platforms for public services
- Open data in the Cloud
- Design of security a system for eGovernment based on cloud computing

The above concepts were used to organize the papers and create the structure of the review. The descriptions of these concepts and the presentation of possible relations among them can be found in the next chapter.

3.4. Summary

Following the structured and concept-centric approach proposed by Webster and Watson (2002), a number of publications related to the use of cloud computing in eGovernment were gathered. Further examination of them led to the detection of concepts, in which the structure of literature review was based.

4. Literature Review

4.1 Introduction

This chapter presents the results of the literature review and the conceptual framework that was formed based on them and was the first goal of this study. It also includes a discussion section where the various views and opinions of authors are summarized and compared. The chapter closes with the conclusions in subsection 4.7.

4.2 The Conceptual Framework

The conceptual map that follows (Figure 2) was designed in an attempt to link the concepts that appear in related literature. It is intended to work as a tool for researchers, mapping the current research in the topic and facilitating the identification of potential research "gaps". Since the adoption of cloud computing by public organizations is a relatively new phenomenon, and research is at an early stage, the proposed conceptual map cannot be considered as completed, but rather as a work in progress. New topics that might appear can be added as new "branches" in the map.

Based on the idea that the various topics that can be found in literature, refer to different steps of cloud adoption by eGovernment, it is proposed that research topics should be grouped accordingly. Thus, "benefits" and "risks and challenges" of cloud computing in eGovernment, "case studies" and "focus on specific applications" can be considered as parts of the first stage of cloud adoption, which is to examine whether cloud computing is suitable for eGovernment or not. "Specialized Frameworks and Models", "SWOT Analysis" and "Use Cases" can be considered as parts of "Migration Strategy", and so on. Furthermore, the security systems that are proposed for cloud-based eGovernment systems, are embedded in the cloud architecture, therefore "Design of a Security System" is considered to be part of "Cloud Architectures for eGovernment".

The arrows that link the different groups indicate the dependency relationship among them, since the research in one group/step can promote the research in the next step.

The present chapter is structured in line with the proposed conceptual map. The only exception is that the case studies found in literature are examined in the next chapter along with the case study of Greece.

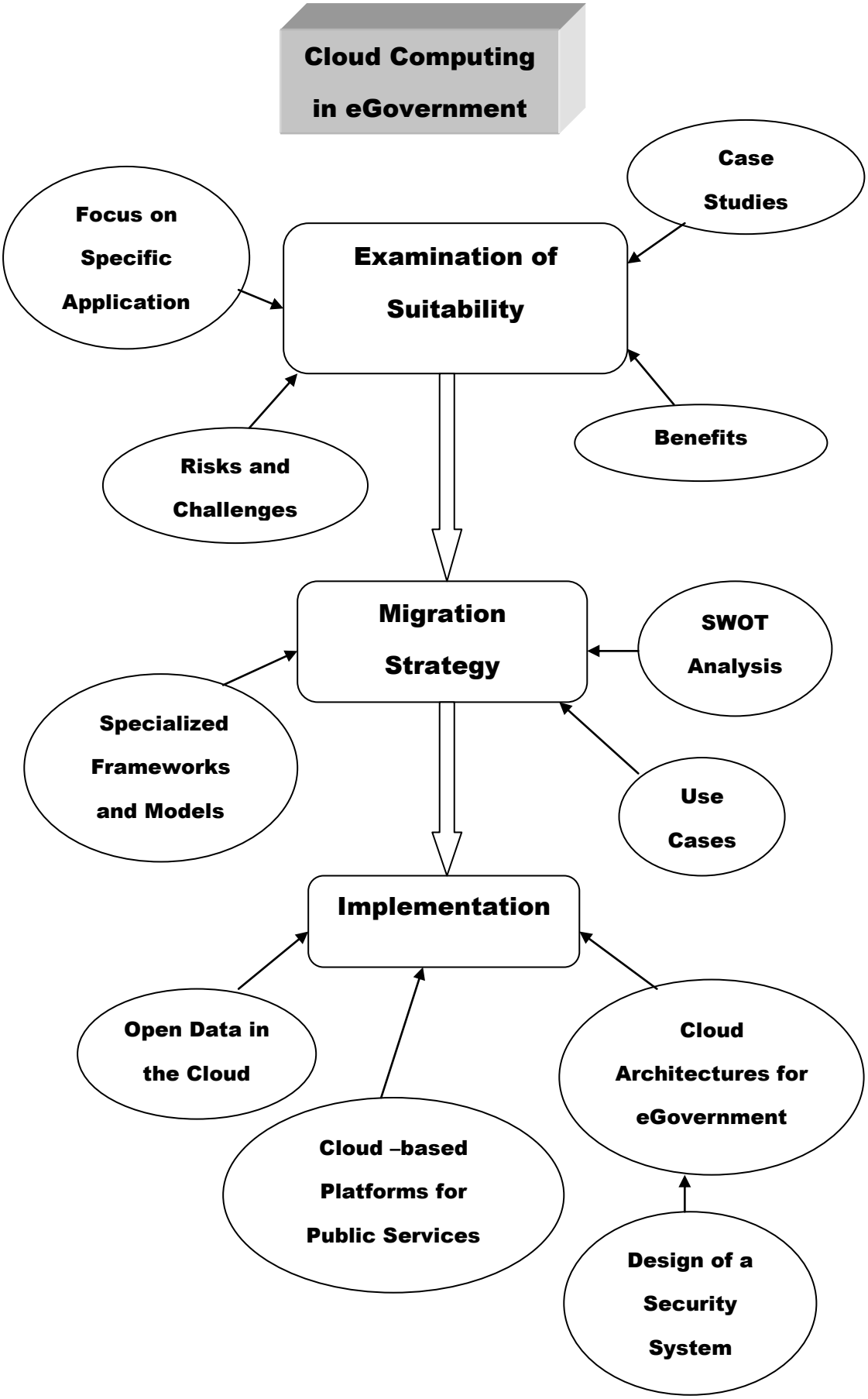

Figure 2: Proposed Conceptual Map for Cloud Computing in eGovernment Literature

4.3. Examining the adequacy of cloud computing in eGovernment

A basic research question in related literature is whether cloud computing is suitable for eGovernment or not (Tsaravas &Themistocleous, 2011a), or in other words, if the benefits a government can reap from cloud computing are more than the risks and challenges that accompany cloud adoption. Several scholars have addressed the topic of adequacy of cloud computing, either in eGovernment generally, or in a specific case (i.e. focus on the eGovernment system of a particular country or on a specific service model of cloud computing, such as SaaS).

4.3.1. Benefits

The benefits of cloud computing in eGovernment fall into four categories:

1. Agility and adaptability
    - Scalability: cloud computing offers the scalability required to meet growing numbers and demands of citizens (Bhishikar, 2011; Das et al., 2011; European Commission, 2012b; Liang, 2012; Kundra, 2011; Macias & Thomas, 2011a; Tripathi & Parihar, 2011; Zissis &Lekkas, 2011)
    - Speed of implementation: no time spent in purchasing hardware or installing software (Das et al., 2011; Frost&Sullivan, 2011; Liang, 2012; Macias & Thomas, 2011a)
2. Cost reduction and control
    - Improvement of utilization of resources: the utilization of IT resources is improved and that results in less expenditure (Bhishikar, 2011; Cellary & Strykowski, 2009; Kundra, 2011; Liang, 2012)
    - Auditing and logging/Better manageability: cloud computing can help in auditing and logging, detecting fraud and fighting corruption, through analyzing huge volumes of data (European Commission, 2012b; Tripathi &Parihar, 2011)
    - Professional maintenance and administration: costs that are related to maintenance and administration of hardware and software (such as salaries of IT specialists) are reduced, since these tasks are undertaken by cloud vendor (Bhishikar, 2011; Cellary & Strykowski, 2009; Elbadawi, 2011; Pokharel & Park, 2009; Zissis &Lekkas, 2011)
    - Reporting and intelligence: the analyzing capability that Cloud offers, can result in better reporting and business intelligence features, that managers in

public sector can use in order to make better decisions (European Commission, 2012b; Liang, 2012; Tripathi &Parihar, 2011)

- Higher performance: cloud computing provider offers high performing hardware, that a government agency may not afford buying if the need for such hardware is not constant and appears only occasionally (Cellary & Strykowski, 2009; Das et al., 2011; European Commission, 2012b; Hada et al., 2012; Zissis &Lekkas, 2011)
- Shift from investment cost to operational costs: government pays only for the resources that are actually used and there is no need for extensive investment in IT field (Bhishikar, 2011; Cellary & Strykowski, 2009; Das et al., 2011; Elbadawi, 2011; European Commission, 2012b; Frost&Sullivan, 2011; Macias & Thomas, 2011a; Pokharel & Park, 2009; Zissis &Lekkas, 2011)
- Environmental friendly: cloud computing is considered to be a green technology and can help government to reduce its carbon footprint (Das et al., 2011; Pokharel & Park, 2009)

3. Risk mitigation
    - Resiliency and business continuity: according to some authors cloud computing can guarantee the availability of services, due to deploying data centers at different locations that can act as availability zones, ensuring business continuity in case of disaster (Zissis & Lekkas, 2011)
    - Higher security: security could be enhanced in Cloud due to the fact that will be implemented by qualified staff (Cellary & Strykowski, 2009; Hada et al., 2012; Kundra, 2011; Macias &Thomas, 2011a; Trifonov et al., 2010; Wyld, 2010b; Zissis & Lekkas, 2011)
4. Better services and collaboration
    - System integration/ interoperability: the heterogeneous systems that different government agencies use can be integrated using cloud computing (Kundra, 2011; Tripathi & Parihar, 2011)
    - Dissemination of good practices/improved collaboration: interoperability can lead to better collaboration and dissemination of good practices among agencies (Cellary & Strykowski, 2009; Elbadawi, 2011; European Commission, 2012b; Liang, 2012; Macias &Thomas, 2011a)

- Location and device independence: applications and services accommodated in the Cloud can be accessed anywhere by any device (Bhishikar, 2011; Das et al., 2011; Frost&Sullivan, 2011; Liang, 2012)
- Active engagement of citizens: it is claimed that since cloud computing is location and device independent, the barriers that digitally or socially excluded groups usually face are brought down and that can increase citizen participation (European Commission, 2012b; Zissis & Lekkas, 2011)
- Enabler for innovation: cloud platforms can promote innovation in public services (European Commission, 2012b; Kundra, 2011)

4.3.2. Risks and Challenges

The risks and challenges that a government may face in the process of adopting cloud computing can be grouped into five key areas:

1. Security and privacy
   - Information security and privacy: one of the most important challenges for government is to ensure that the government cloud and the sensitive data that accommodates, are safe from cyber attacks (AlAjmi, 2011; Clemons & Chen, 2011; Craig et al., 2009; European Commission, 2012b; Hada et al., 2012; Liang, 2012; Macias &Thomas, 2011b; NIST, 2011a; Paquette et al., 2010; Tahamtan et al., 2011; Trifonov et al., 2010; US Department of Defense, 2012; Wyld, 2009; Wyld, 2010b; Zissis & Lekkas, 2011)
   - Isolation failure: risk of failure of mechanisms separating storage, memory and routing among different tenants in case the government uses a public or a community cloud (Kundra, 2011; NIST, 2011a; Trifonov et al., 2010)
2. Outsourcing risks
   - Portability of data and vendor lock-in: the risk that government may depend on a cloud vendor for services, unable to use another cloud vendor without significant switching costs (Clemons & Chen, 2011; Craig et al., 2009; Hada et al., 2012; Macias &Thomas, 2011b; Paquette et al., 2010)
   - Control and ownership: questions of control and ownership of data may arise with the migration of government data to the Cloud (Craig et al., 2009; Macias &Thomas, 2011b; Kundra, 2011)
3. Availability and performance

- Dependence on internet connection: cloud computing depends on internet connection, which is not considered as a trusted network (AlAjmi, 2011; Tahamtan et al., 2011; US Department of Defense, 2012)
- Service availability/possible outages: the availability of public services will depend on the reliability of the cloud vendor (AlAjmi, 2011; Liang, 2012; Macias &Thomas, 2011b; NIST,2011a; Paquette et al., 2010; US Department of Defense, 2012; Wyld, 2009; Wyld, 2010b)

4. Standards and legal issues
    - Absence of standards: since cloud computing is relatively new, standards are still being developed (AlAjmi, 2011; Clemons & Chen, 2011; Kundra, 2011; Liang, 2012; Macias &Thomas, 2011b; Paquette et al., 2010; Tahamtan et al., 2011; Trifonov et al., 2010)
    - Legislation: in many countries storing government data outside of country's boundaries is prohibited, thus compliance with legislation can be considered as another important challenge related to cloud computing adoption (Clemons & Chen, 2011; Hada et al., 2012; Macias &Thomas, 2011b; Zissis & Lekkas, 2011)
5. Change management and organizational issues
    - Political issues: cloud computing can be considered as a form of globalization and as a result, specific political groups may be opposite to its adoption (Zissis & Lekkas, 2011)
    - Cultural change: objections may be raised by public organizations that are concerned about giving up privatizing their resources (Macias &Thomas, 2011b)
    - Financial risks: the possibility that cloud adoption might fail to deliver expected benefits (Clemons & Chen, 2011; Wyld, 2009)
    - Lack of knowledge about available systems: government should be informed for the current state of systems and technologies that are used in different agencies before adopting cloud computing, a task that can be quite demanding (Tahamtan et al., 2011).
    - Legacy systems and lack of interoperability: the integration of legacy solutions with Cloud may be difficult due to lack of interoperability among technologies used (AlAjmi, 2011; Clemons & Chen, 2011; Macias &Thomas, 2011b; Tahamtan et al., 2011)

4.3.3. Focus on specific cases

While most authors examine the potential of cloud computing in eGovernment generally, some others focus on the eGovernment system of a specific country. Tahamtan et al. (2011) studied the potential of cloud computing in Austrian public sector, interviewing eight ministries and the office of chancellor. The research showed that the most important requirements of the Austrian public sector, related to cloud computing adoption, are "Legal compliance", "Reliability", "Availability", "Compatibility and connectivity", and "Scalability". In addition, "Data security and privacy", "Network security", "Lack of knowledge of available systems", "Previous investments" and "Business continuity", were identified as the obstacles for integration of cloud computing in the Austrian public sector.

Khan et al. (2011) focused on the future integration of cloud computing in eGovernment of developing countries, using as an example the eGovernment system of Pakistan. After reviewing the eGovernment challenges and readiness of the country, the authors proposed that cloud computing can be used as a solution to problems such as digital divide and inadequate funding that developing countries usually face in the context of eGovernment. Cloud computing enables the use of thin clients and implementation of "NoPC projects" in government agencies and public organizations, and as a result government costs will be reduced and the citizens' access to online government services will be enhanced.

Stefanou and Skouras (2012) conducted a survey to find whether companies in Greece would be positive towards using a government's payroll information system based on cloud computing. The Information Payroll System based on cloud computing that authors propose, promises to simplify the bureaucratic procedures related to labor inspection, giving to the State the role of administrator of the businesses database, and therefore enabling distant control of labor issues. Through a questionnaire, companies were asked to choose between the "Integrated Information System" planned by Ministry of Labour and the aforementioned "Payroll Information System" provided by public sector via cloud computing. According to the results of the survey, half of the responses were in favor of the first solution and the other half in favor of the cloud based Payroll Information System. Furthermore, it seems that companies have some reservations about using the cloud based solution, mainly as regards data security, and connection and software issues.

On the other hand, there are scholars that narrow the scope of their study to a specific service model of cloud computing. Leikums and Cevere (2012) for instance, examined the potential use of a SaaS document management system in Latvian public sector. According to them, the main advantages that such a solution has are:

- Avoiding technical decisions – public organizations that lack IT specialists may not be able to choose and maintain an equivalent system within premises. In case of a SaaS document management system, all the relevant decisions are taken by SaaS provider.
- Short implementation period – the implementation period of a SaaS solution may be relatively short compared to a system that is not ready-to-use.
- Following the advantages of good practices – SaaS developers may help public organizations in preparing a transition plan that would cover aspects of information safety, life cycle of the documents and potential costs and risks.
- Document accessibility- SaaS document management system can be accessed from everywhere, as long there is internet connection. That would allow government officers to access documents they need during meetings or when they visit other institutions.

A SaaS document management system has at the same time some disadvantages, which authors identified as:

- Data safety – public organizations have strict data safety requirements that cloud providers are not always ready to accept.
- Emergency reaction time – In case of an error or failure, the time that is needed to report, review and eliminate the problem, is longer when a SaaS system is used than it is when the document management system is within premises.
- Performance – a local software solution is usually faster than software being used via public network.

Janssen and Joha (2011) also focus on the use of SaaS in public sector, but in a broader context. The authors examined the possible benefits, disadvantages and challenges of SaaS in public sector, using interviews with IT managers, outsourcing and SaaS decision- makers and IT experts from a variety of public organizations. The findings of their research are presented in Table 1. The benefits and risks of SaaS in public sector

are quite similar to the benefits and risks that accompany the use of cloud computing generally in eGovernment.

Table 1: Benefits, disadvantages and risks of SaaS (Janssen and Joha, 2011)

SaaS benefits	SaaS disadvantages and risks
Strategic and organizational	
• No installation and maintenance of software • No software expertise necessary • Focus on core business • Sharing of software installation and enrolment risks with SaaS providers • No need for human resource management of IT staff • Solving scarcity of IT staff • Improved time-to-market • Opening up new software applications otherwise out-of-reach and enabling innovation	• Need for contractual expertise • Reliability and long term sustainability of SaaS providers • Lack of technical expertise and experience • Difficulty to switch from provider • Risk of lock-in • Less customization opportunities • Integration of software from various SaaS providers. • Lack of innovation and no grip on further development and standardization
Political and legislative	
• Eliminate the need for an ICT-department • Eliminate the need for the governance of IT • Increased accountability • Increased control • Higher service levels that are required • Transparent payment (per use)	• Quality assurance • Ensuring accountability of service providers • Data ownership • Less influence on developments • Privacy control • Ensuring that SaaS providers follow standards and guidelines • Jurisdiction and applicability of law • Interruption or termination of services due to lack of payment
Technical	
• No complicated license management • No complicated versioning control and update concerns • No patching and other maintenance activities in house	• Problem shift to composing and integration • Assurance that data is back-up and can be recovered • Access control and security • Loss of data in case of bankruptcy of provider
• Get rid of legacy systems • Speed of installation always up-to-date • Reduction of overcapacity of hardware (memory and processes) • Back-up and recovery ensured by SaaS provider • No need for having in-house user support	• Identification and authentication • Information sharing among software from different SaaS providers • Performance management and scalability issues • Users utilizing applications running on the same server
Economic	
• Access to software without needing upfront investments • Economies of scale by spreading the costs of innovative solutions over many customers • Less direct costs • Control and predictability of IT costs	• In the long term higher indirect costs by additional management, control and security efforts • Dependency on SaaS provider resulting in higher (transition) costs

4.4. Migration Strategy

Governments should plan carefully their migration to the cloud, considering all the challenges and risks mentioned above. According to Mauro (2012), United States has published more documents for that reason, compared with European Union. Table 2 presents migration strategies that have been proposed by scholars and organizations.

Table 2: Migration strategies for public sector organizations

References	Migration Strategy
Wyld D. (2010a)	Step 1: Learning Step 2: Organizational Assessment Step 3: Cloud Pilot Step 4: Cloud Readiness Assessment Step 5: Cloud Rollout Strategy Step 6: Continuous Cloud Improvement
Reza M. (2012)	Step 1: Review Mandate Step 2: Define Strategic Options Step 3: Select Service Step 4: Select Cloud Service Model (IaaS, PaaS, SaaS) Step 5: Deploy Service Step 6: Evaluate/Manage Service
Craig et al.- Cisco (2009)	• Identify all potential opportunities • Ensure that in-house infrastructure complements cloud based services • Develop a cost/benefit and risk evaluation framework • Develop a roadmap • Identify which data cannot be held in public cloud • Identify and secure in-house competencies • Designate a cross-functional team • Evaluate technical challenges • Ensure that the networking environment is ready
Kundra V. (2011)	Select • Identify which IT services to move and when ✓ Identify sources of value for cloud migrations: efficiency, agility, innovation ✓ Determine cloud readiness: security, market availability, government readiness, and technology lifecycle Provision • Aggregate demand at Department level where possible • Ensure interoperability and integration with IT portfolio • Contract effectively to ensure agency needs are met • Realize value by repurposing or decommissioning legacy assets and redeploying freed resources Manage • Shift IT mindset from assets to services • Build new skill sets as required • Actively monitor SLAs to ensure compliance and continuous improvement • Re-evaluate vendor and service models periodically to maximize benefits and minimize risks

Frost & Sullivan (2011)	Identify • Identify the various workloads that are Cloud ready • Determine which can move to Public, Community, Private Clouds based on Security, SLA requirements Implement • Aggregate the demand either at a department level or BU level for economies of scale • Ensure integration with existing infrastructure • Have a "user first" policy. Don't compromise on usability and simplicity • Ensure that the SLA's are being met by the providers and right level of security controls are in place Improve • Convey the successes and failures clearly to the users • Change the mind-set from asset acquisition to utility services • Ensure that IT teams are trained in managing vendor relationships and SLA management • Constantly monitor the service providers for compliance and performance improvement
US Department of Defense (2012)	Step 1: Foster Adoption of Cloud Computing • Establish a joint governance structure to drive the transition to the DoD Enterprise Cloud Environment • Adopt an Enterprise First approach that will accomplish a cultural shift to facilitate the adoption and evolution of cloud computing • Reform DoD IT financial, acquisition, and contracting policy and practices that will improve agility and reduce costs • Implement a cloud computing outreach and awareness campaign to gather input from the major stakeholders, expand the base of consumers and providers, and increase visibility of available cloud services throughout the Federal Government Step 2: Optimize Data center Consolidation • Consolidate and virtualize legacy applications and data Step 3: Establish the DoD Enterprise Cloud Infrastructure • Incorporate core cloud infrastructure into data center consolidation • Optimize the delivery of multi-provider cloud services through a Cloud Service Broker • Drive continuous service innovation using Agile, a product-focused, iterative development model • Drive secure information sharing by exploiting cloud innovation Step 4: Deliver Cloud Services • Continue to deliver DoD Enterprise cloud services • Leverage externally provided cloud services, i.e., commercial services, to expand cloud offerings beyond those offered within the Department

It should be noted that whereas the majority of the strategies presented above, is general and can be followed by any government or public organization, the strategy of US Department of Defense is adjusted to the department's needs. It was included though in the present study, on the grounds that, not only is it an interesting example of a customized strategy, but it can also be adapted to meet any other organization's needs.

European Commission (2012a) has adopted a more focused approach too, indicating key actions for cloud migration in Europe. Although it cannot be considered as a full migration strategy, it clearly helps towards that direction, bringing to the fore the following important actions to be taken: "Cutting through the Jungle of Standards", "Safe and Fair Contract Terms and Conditions" and "Establishing a European Cloud Partnership to drive innovation and growth from the public sector".

4.4.1. Specialized frameworks and models

Apart from migration strategies and key steps for cloud adoption by governments, there are also specialized frameworks and models in literature, which aim to act as tools for IT managers of public sector, in different stages of migration procedure.

Kurdi et al. (2011) designed a framework for assessing the readiness of eGovernment systems, focused on the migration to cloud computing. The framework, that provides a modeling and analysis method to guide the assessment, covers four dimensions:

- Technological Block, that refers to ICT, network and security infrastructures and quality of systems and services
- Organizational Block, that consists of structure, culture, size and strategy of organization, along with strategic planning and human resources issues (such as training and staff motivation)
- People/Stakeholders Block, that includes citizens, businesses and government
- Environment and Society Block, that refers to demographic characteristics and social/cultural, political and economic issues of a country

Repschlaeger et al. (2012) presented a classification framework for Infrastructure as a Service that can be used in eGovernment. The three-level framework, depicted in Figure 3, supports governments in classifying cloud providers and selecting the proper one, based on relevant requirements depending on their own strategy. The authors interviewed seven experts from six organizations (including IT service providers, a consulting company and a public organization) and conducted a literature review, in

order to design the framework. It consists of 19 abstract classification criteria (2nd level) and 53 operative classification criteria (3rd level) that are grouped into six target dimensions (1st level): “Flexibility”, “Reliability and Trustworthiness”, “IT Security & Compliance”, “Scope and Performance”, “Service & Cloud Management”, “Costs”. The assessment of different IaaS providers based on these criteria, supports governmental decisions about which provider should be chosen.

Mutavdzic (2012) proposed a decision framework that will help government IT managers to choose the proper PaaS implementation. According to this framework, there are four general groups of components that can be used to deliver PaaS solutions, “Component group: User”, “Component group: Compute”, “Component group: Database” and “Component group: Fabric”. Although each group has one or two entities that can be used, some entities can produce more than one instance, increasing the capabilities of specific component group.

The component group “User” (Figure 4) contains the possible interfaces that can be used for user’s communication with PaaS application:

- Web Browser: chosen in case the application needs to be accessed by browser interface on different computing platforms.
- Mobile Browser: in case the application needs to be accessible by mobile devices
- Managed Application: in case application has to be hosted on PaaS that supports chosen managed language and/or can enable execution in native environment without virtualization of code.

Figure 3: Classification Framework for IaaS (Repschlaeger et al., 2012)

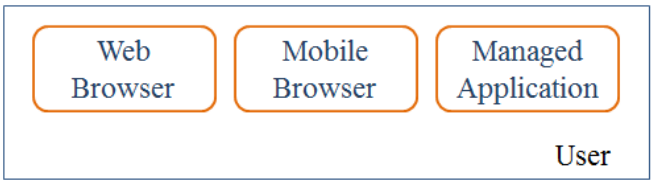

Figure 4: Component Group: User (Mutavdzic, 2012)

The component group “Compute” (Figure 5) contains computing resources that are used to execute applications in PaaS environment:

- Web Role (Page): in case HTTP-based services will be implemented, that generate pages using different execution environments depending on operating systems and web services mentioned below
- Web Role (Service): when there is a need to have externally published web services, accessible by other, third party web services which can relate and communicate the requests for services
- Worker Role: in case there is a need for internally published web services that are accessed by Web Roles, mentioned above
- Table Storage Service: in case application needs mechanisms that store processed information for single request/session in local storage and purge data after the session terminates
- Blob Storage Service: in case application needs mechanisms that store large quantities of binary data for single request/session in local storage and purge data after the session terminates

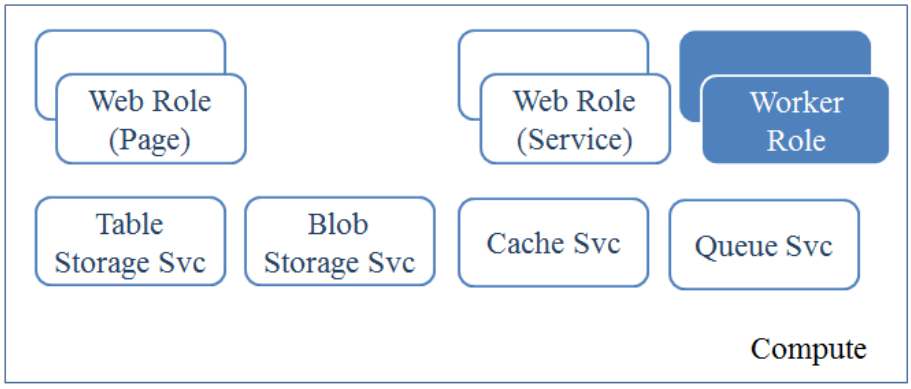

Figure 5: Component Group "Compute" (Mutavdzic, 2012)

- Cache Service: in case application needs a local cache mechanism that will enable reuse of the data in multiple requests

- Queue Service: in case specific requests and objects must be handled in specific order, synchronously or asynchronously

The component group “Database” (Figure 6) contains entities that can store the data used in execution, so they can be manipulated in a number of ways:

- Application Data: use of a relational, hierarchical or integrated data storage model to hold the data for a specified timeframe
- Data Services: need for web services that will enable communication among services and exchange of persisted data
- Business Intelligence Services: in case an analysis that will return an insight into stored data, is needed

Figure 6: Component Group "Database" (Mutavdzic, 2012)

The component group “Fabric” (Figure 7) contains entities that facilitate the connection and exchange of data between the applications implemented in the Cloud and on-premises applications.

- Connection Bindings: in case there is a need for mechanisms that will enable the connection between different protocols and application instance
- Identities and Roles: indicate that security mechanisms are needed that will enable identity management

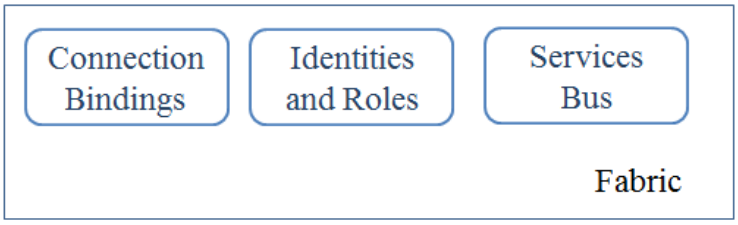

Figure 7: Component Group "Fabric" (Mutavdzic, 2012)

- Services Bus: indicates that service bus mechanism is needed to access and share services and data through platform

Depending on the application model and scenario, IT managers combine components from different groups to decide what type of architecture should be applied for a specific government application scenario. Figure 8 shows an example, where the application scenario is a Government Portal that can be accessed both by web and mobile browsers and is built on PaaS, used for high scalability and availability of services and applications. The arrows show the interactions among the different entities that the application uses.

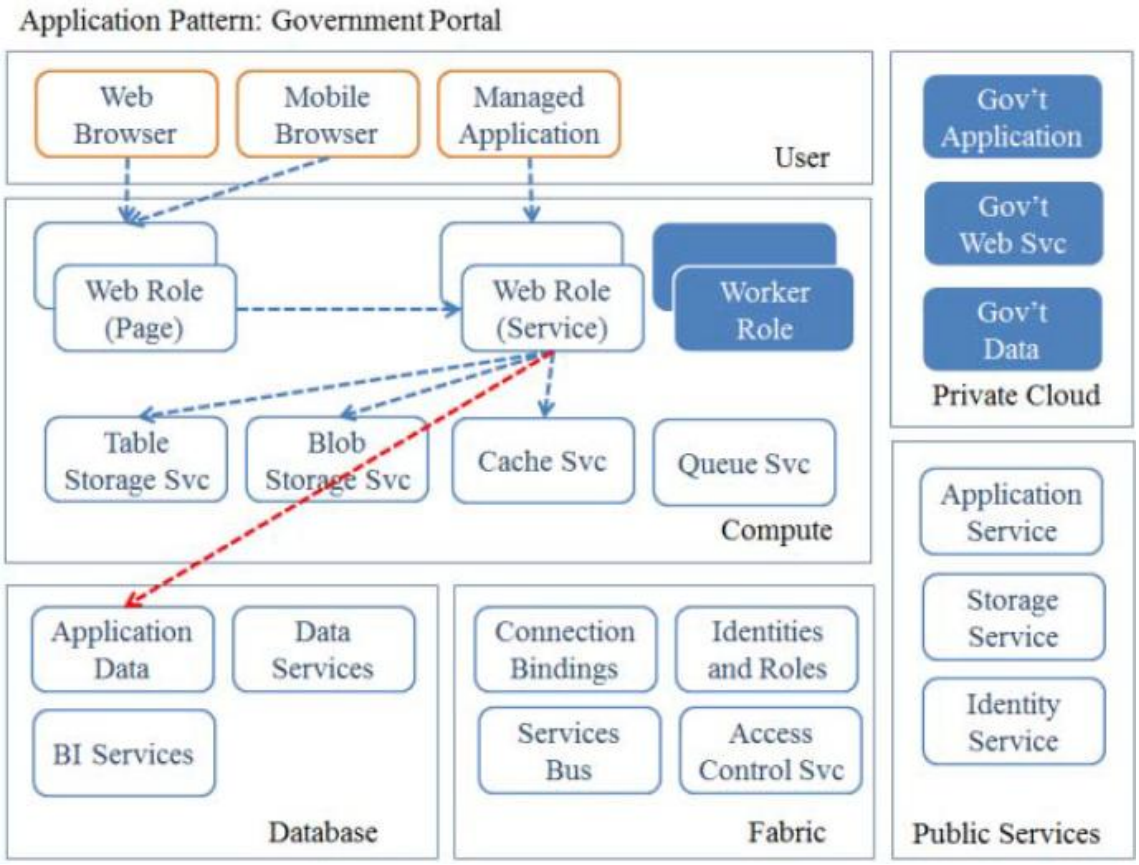

Figure 8: Application pattern: Government Portal. An example of how proposed decision framework works (Mutavdzic, 2012)

Similarly, in Figure 9, another example of the proposed framework is presented. In this case, the aim is to extend the existing on-premises applications of eGovernment through services that are built on PaaS.

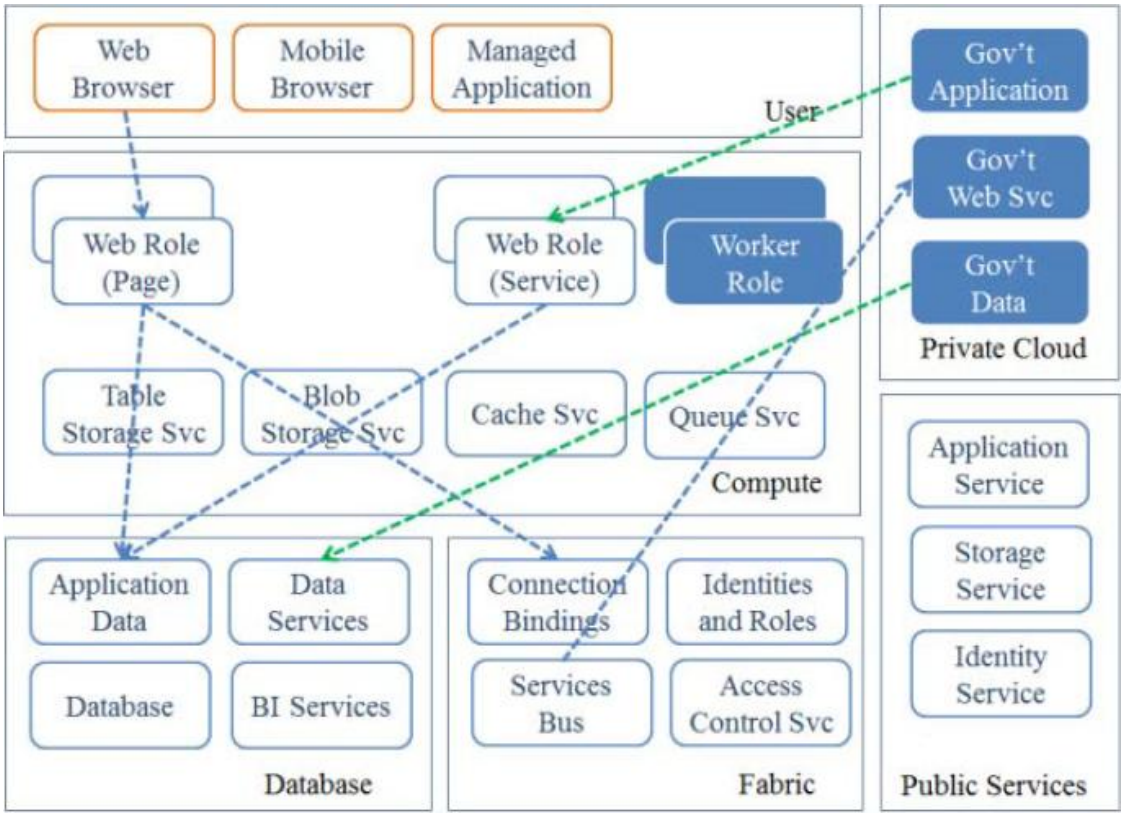

Figure 9: Application pattern: Software+Services. An example of how proposed decision framework works (Mutavdzic, 2012)

Deussen et al. (2011) have followed a more theoretical approach, identifying public sector business models that can be used to refine usage scenarios of cloud computing by governments:

- Government to Cloud (G2Cloud) – citizens are aware that some back-offices services are running in the Cloud, when they use public sector services provided by government agencies (Figure 10).

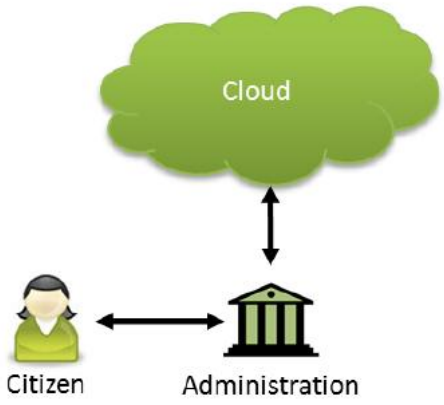

Figure 10: Government to Cloud (Deussen et al., 2011)

- Government to Cloud to Enterprise (G2Cloud2E) – Electronic procurement, applications, notifications, access to open data, processes, and workflows between government and enterprises are performed in the Cloud (Figure 11).

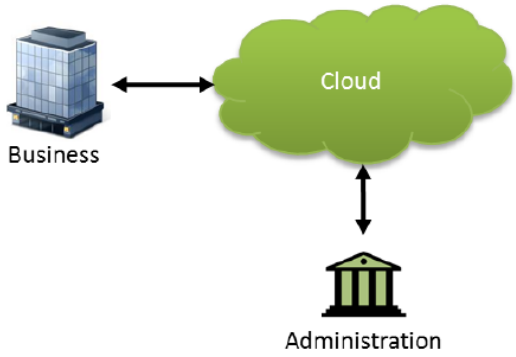

Figure 11: Government to Cloud to Enterprise (Deussen et al., 2011)

- Government to Cloud to Citizen (G2Cloud2C) – Electronic applications, notifications, eParticipation, eCollaboration, access to open data, tax return, and complaint/concern management are performed in the Cloud (Figure 12).

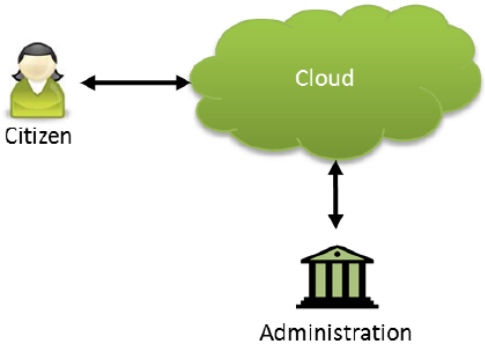

Figure 12: Government to Cloud to Citizen (Deussen et al., 2011)

- Government to Cloud to Government (G2Cloud2G) – Electronic support for federated, cross- governmental process, shared repositories and information systems and the electronic collaboration between public sector agencies in general are performed in the Cloud (Figure 13).

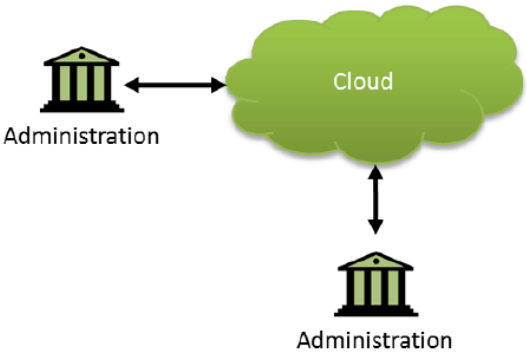

Figure 13: Government to Cloud to Government (Deussen et al., 2011)

4.4.2. Use Cases and SWOT Analysis

While scholars present specialized frameworks and models in order to facilitate cloud computing adoption by eGovernment, institutes and organizations employ common techniques, such as SWOT analysis and business use cases, for the same purpose. The recommendations and conclusions, formed from the analysis of the use cases, can be used in the preparation stage of migration procedure, in order to familiarize public organizations with cloud computing. At the same time, the use case templates that some authors proposed, can be used in the planning stage by organizations and agencies that want to identify the specific organizational and technical issues that appear in case they migrate to the Cloud. SWOT analysis can also be used in the planning stage of migration strategy, facilitating the decision making related to the choice of the suitable deployment model of cloud computing.

Deussen et al. (2011) designed three different use case templates for public sector (can be found in Appendix B), for describing and analyzing legal, organizational and technical issues that arise from governmental use of cloud computing. The authors conducted interviews with eGovernment service providers and used the templates to define a number of use case scenarios about German public sector that served as a basis for the evaluation of benefits and challenges of cloud computing:

- Scenario 1: Open and protected data – this scenario shows that separating between personal and non-personal (open) data, can resolve data privacy issues. Governmental processes that do not rely on personal data can be hosted in a public cloud.
- Scenario 2: Citizen Support Service – illustrates how the employment of a cloud service for storing data in a secure way, can make easier the interaction among administrations, enterprises and citizens, achieve optimization of governmental processes though delivering documents on time, and enable cross-administration processes by the electronic exchange of documents.
- Scenario 3: Business Incubator for SMEs – describes how the interconnection between governmental and enterprise business processes via cloud computing can provide a business incubator for enterprises.

An example of a legal use case, used in Citizen Support Service scenario is illustrated in Figure 14. This use case examines the legal issues that emerge with the governmental use of cloud computing for storing citizens' electronic documents.

Legal Use Case		
UC-Legal	**Document release towards an administration**	
Description	The use case describes how a public administration requests a document from a citizen in the course of an administrative process.	
Actors and Roles	Actor	Roles
	Citizen	Document & EDS owner Document provider
	EDS provider	Safe provider
	Government agency (Administration)	Document consumer
	Certificate Provider	Certificate provider (OCSP)
	PKI provider	Key management provider
Goals and aspirations for the UC	According to German data regulation laws, personal data (which are assumed to be represented by the documents referred to in this use case) are allowed to be collected and processed only if ■ There is a law permitting, or ■ The owner of these data has agreed. Moreover, the administration needs a concrete reason such as an administrative process initiated by a citizen's application. Citizens have the right to be informed which personal data are available to an administration, and for which purposes they are used. The use case describes a process which ensures that these legal requirements are met.	
Legal domain	Data privacy	
Area	Germany	
Legal frameworks, laws, etc., to be taken into account	■ Date privacy laws in Germany (on federal and federal state level) ■ Data privacy directive of the European Union Since documents stored in the EDS provide evidence about the citizen, electronic signatures and certification is required. Hence, a number of additional regulations have to be taken into account. The most important ones are: ■ German Signature Law ■ European Signature Directive	
Required preconditions	■ Citizen registration at EDS provider ■ Application at the administration by the citizen	
Description of procedures to ensure legal compliance	■ Administration requires a certain document from Citizen for a certain purpose. It delivers information about the purpose and the legal foundation of the data collection. ■ Citizen releases the requested document in his/her EDS for access by the administration, and sends access information to the administration. ■ Administration retrieves the document. If necessary, signatures and certificates are validates.	
Compliance criteria	Collection of personal data is done in compliance with German data protection laws. In particular, the user knows about the data collection and processing, is informed about its purpose.	
Related Ucs and those that are pre-requisite	NONE	
Existing specifications to rely on	BSI Baseline Protection Catalogs, privacy protection laws, Signature law.	
New specifications required between the actors	NONE	

Figure 14: An Example of a Legal Use Case (Deussen et al., 2011)

The following recommendations were deduced from the analysis of the use cases:

- Methodology based on use cases can assist the progress of standardization of technical, legal and organizational aspects of cloud computing

- The suitability and feasibility of a specific migration approach planned for a particular application of cloud computing should be instigated with actual demonstrators using existing technology and current related experience
- A better way to demonstrate the benefits of cloud computing is to start the cloud adoption with novel, innovative applications, instead of migrating into the Cloud existing applications that are still functional.

NIST (2011b) has also defined cloud computing business use cases[1] (candidate deployments to be used as examples) to identify business and technical operational scenarios and requirements. These use cases focus on assessment and prioritization of technical and procedural gaps in order to suggest recommendations for mitigation that US government agencies can follow:

- Recommendation 1 - Contribute Agency Requirements: "Agencies should contribute clear and comprehensive user requirements for cloud computing standards projects."
- Recommendation 2 – Participate in Standards Development: "Agencies should actively participate in cloud computing standards development projects that are of high priority to their agency missions."
- Recommendation 3 - Encourage Testing to Accelerate Technically Sound Standards-Based Deployments: "Agencies should support the concurrent development of conformity and interoperability assessment schemes to accelerate the development and use of technically sound cloud computing standards and standards-based products, processes, and services."
- Recommendation 4 - Specify Cloud Computing Standards: "Agencies should specify cloud computing standards as a factor in procuring cloud services and assess cases when multiple vendors offer standards-based implementations and there is evidence of successful interoperability testing. In such cases, agencies should ask vendors to show compliance to the specified standards."
- Recommendation 5 – USG (US Government)-Wide Use of Cloud Computing Standards: "To support USG government requirements for interoperability, portability, and security in cloud computing, in coordination with and under the cognizance of the federal Enterprise Architecture program, the Federal

[1] Examples of business use cases that NIST used for the analysis can be found in Appendix B.

Standards and Technology Working Group should recommend specific cloud computing standards for USG-wide use."

- Recommendation 6 - Dissemination of Information on Cloud Computing Standards: "A listing of standards relevant to cloud computing should be posted and maintained."

European Network and Information Security Agency (ENISA, 2011) has presented SWOT analysis for each cloud model (public, private and community cloud) as far as security, resilience and compliance to legislation are concerned. By comparing the Strengths, the Weaknesses, the Opportunities and Threats of each cloud deployment model, agencies can choose the one that addresses their needs.

Table 3: SWOT analysis for Public Cloud (ENISA, 2011)

Public Cloud for Governmental Organizations – A SWOT analysis	
Strengths • Availability and reliability • Tolerance and elasticity • Patch management • Response time • Business continuity • Physical security • Intrusions prevention and detection • Delay possible subpoenas and e-discovery from law enforcement agencies of other countries	**Weaknesses** • Lack of control over the supply chain • Logging capabilities • Difficulties in accessing forensic data • Lack of bargaining power when negotiating terms of transparency with providers • Legislation that in some countries force public organizations to keep data within the national territory • Degraded performances due to poor quality in the connectivity • Limited local distribution of data centers in EU territory, which can have an impact on the performance of service • Difficulties in transferring data back to the user

Opportunities	Threats
• Risk analysis and assessment • Security testing • Real- time security monitoring • Forensics	• A large public cloud is an attractive target for threat attacks • The impact of attacks from insider threats may be rather large due to the amount of information stored in the Cloud • Isolation failure can open the door to information leakage • Poor definition of requirements and of classification of assets may result in the exposure of assets to other users of the Cloud • Multiple jurisdictions may apply when the sites of the provider are distributed across several nations • A change in the control of the provider may result in the adoption of distinct security strategies • In SaaS or PaaS a proprietary format may be adopted to store data in the Cloud. Moving to another provider can be almost impossible if there is no tool to automatically translate data into the new format

In Table 3 the SWOT analysis for using Public Cloud for government applications is presented, whereas Table 4 and Table 5 present the SWOT analysis for Private and Community Cloud respectively. Hybrid cloud was not considered by authors in SWOT analysis, since it is a combination of public and private clouds. As can be observed, the strengths and opportunities of a Public Cloud result from the abundance of resources and from their geographic distribution, while the strengths and opportunities that a Private Cloud can offer to public organizations, are related to control. As far as threats and weaknesses are concerned, in case of a Public Cloud they are related to the lack of governance, the large number of users in the cloud and the strong negotiating power that cloud provider has in the definition of the contract, while in a Private Cloud are related to lack of flexibility and the exclusively use of the cloud by the government. The

strengths and weaknesses of Community Cloud fall in theory, between those of a public cloud and those of a private one.

Table 4: SWOT analysis for Private Cloud (ENISA, 2011)

Private Cloud for Governmental Organizations – A SWOT analysis	
Strengths • Select the risk assessment practices • Schedule patching • Access control • Control logging • Auditing • Control over availability, scalability, reliability and elasticity • Availability of the management interface • Business continuity plan • Full transparency and control over legal requirements such as data location	**Weaknesses** • The beneficial effect of the economies of scale is likely to be much less compared to public clouds • The possible lack of adequate scale also represents a weakness in the purchase and implementation of security mechanisms • There is potentially less tolerance of malicious attacks than in public cloud, since the available resources may be less adequate • Less flexibility for meeting unanticipated peak demands • The redundancy regime is highly unlikely that will be equal or better than the regime offered by public cloud • Lack of geo-redundancy is a problem as far as continuity is concerned • Sensitivity of reputation
Opportunities • Monitoring • Access control	**Threats** • Politically motivated attacks • The fact that government will be collecting and managing information about citizens could be perceived from end-users as a way to put a surveillance system in place • High volatility in resource utilization could force a private cloud to scale out to into a public cloud • Poor planning • Inadequate definition of contracts with business partners

Table 5: SWOT analysis for Community Cloud (ENISA, 2011)

<table>
<tr><td colspan="2">Community Cloud for Governmental Organizations – A SWOT analysis</td></tr>
<tr><td>Strengths
Common requirements and constraints and risk profile that results in lower overall cost
The configuration of mechanisms and tools to protect applications is simplified due to the common risk profile
Users have more bargaining power as a group
Ability to set the entry criteria for the cloud
Larger scale and better response to high peaks in resource demand (compared to a private cloud)</td><td>Weaknesses
More resource competition between the partners since they have common goals
Compared to a private cloud, a community is a more attractive target for motivated attackers due to larger visibility achieved by successful attacks
Access control and authentication are weakened compared to a private cloud due to the larger number of users
Degraded performance due to poor quality in connectivity may reduce the quality of service for some users in the community</td></tr>
<tr><td>Opportunities
Similar requirements across the community could allow improved security policies, baselines and standards
Common and shared incident management systems can simplify the adoption of mechanisms to store and manage forensics evidence
Larger diffusion of best practices, fine tuned by the most expert community members
Stricter security since security policies and the design and implementation of cloud are shared only within the community</td><td>Threats
Lack of agreement on security baselines and security mechanisms
Communities may either grow quickly, which will eventually decrease the advantages related to flexibility, or grow slowly, which will eventually affect dynamic scalability
Harder to predict resource usage (than in a private cloud)
Failure of isolation mechanisms may result in the leaking of information which is more difficult to control because of the large number of users
It is difficult to identify the legal entity that is responsible for acting against a member of the community when super-national issues are involved</td></tr>
</table>

4.5. Implementation

4.5.1. Cloud architectures for eGovernment

Many scholars have proposed cloud based architectures particularly for eGovernment. Zhang and Chen (2010) defined the Cloud architecture for eGovernment as a stack of the following layers: Hardware, Visualization, IaaS, PaaS and SaaS. The stack is illustrated as a pyramid, with the layer "Hardware" being the base and SaaS being the top. Using their proposed architecture, they designed the conceptual framework of "C-government" (Figure 15) that aims to enhance productivity, efficiency, transparency, participation and collaboration of traditional eGovernment.

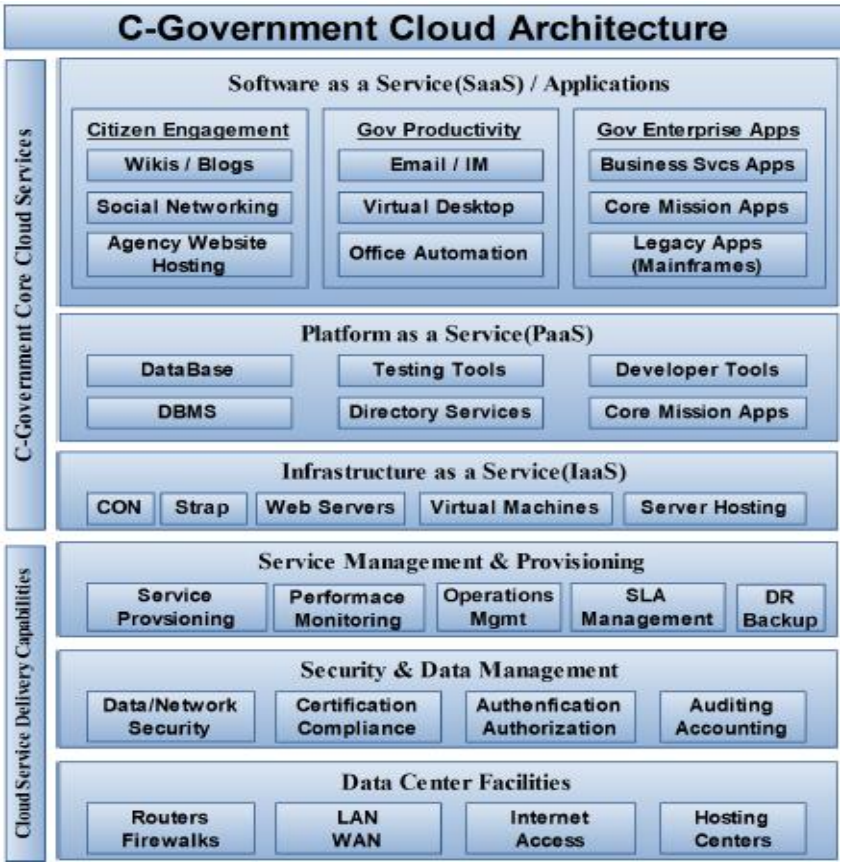

Figure 15: The C-Government concept (Zhang and Chen, 2010)

The cloud architecture for eGovernment introduced by Sharma and Kanungo (2011) has three main entities (Figure 16):

- Master/slave data center: Master data center is located at Cloud provider's administrative premises, where user's accounting on pay-as-you-go basis is completed. Slave data- center are geographically scattered to serve user's requests in minimum physical distance.

- Users/Brokers: Users communicate directly or via brokers to submit requests that automatically reach master data center.
- Service Level Agreements (SLAs): Quality of Service and pricing are settled through SLAs. Master data center scans SLA each time to host needs of the users.

Experiments that were carried out on cloud simulator showed that the suggested architecture based on distributed data centers is energy efficient, eco-friendly and cost-effective for governments.

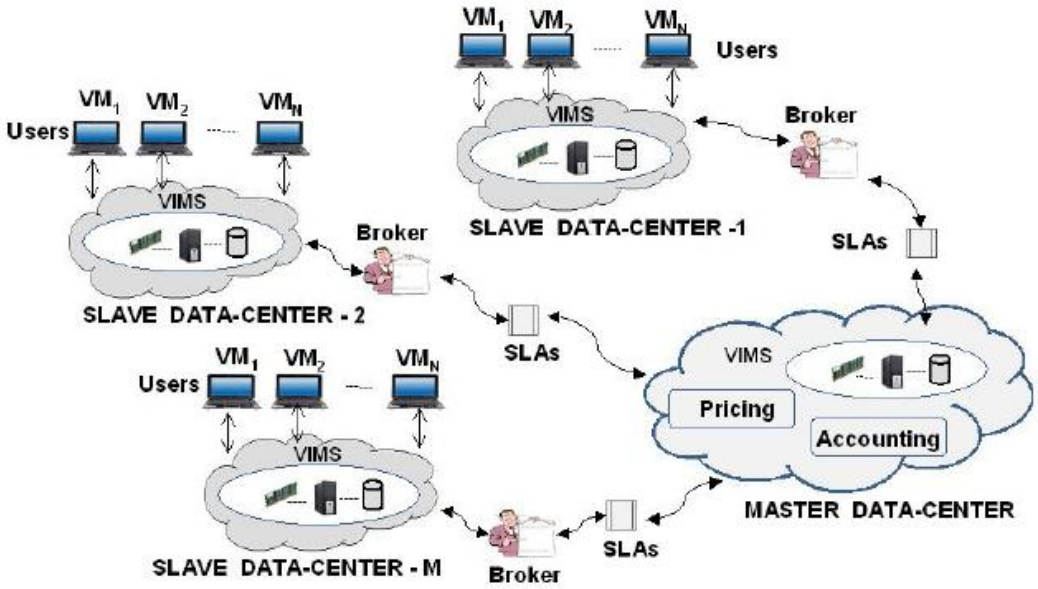

Figure 16: Proposed cloud architecture (Sharma and Kanungo, 2011)

A cloud computing architecture for eGovernment that consists of three parts (eGovernance systems, automation/manual monitoring system and central cloud data center) is discussed by Chuob et al. (2010) (Figure 17). The requests for services from users in each ministry/agency go though the monitoring system that forwards them to the central cloud data center. The Resource Manager searches for the requested services and communicates with the Access Control Management System to authenticate the users. If authentication succeeds the process will continue with the Application Manager.

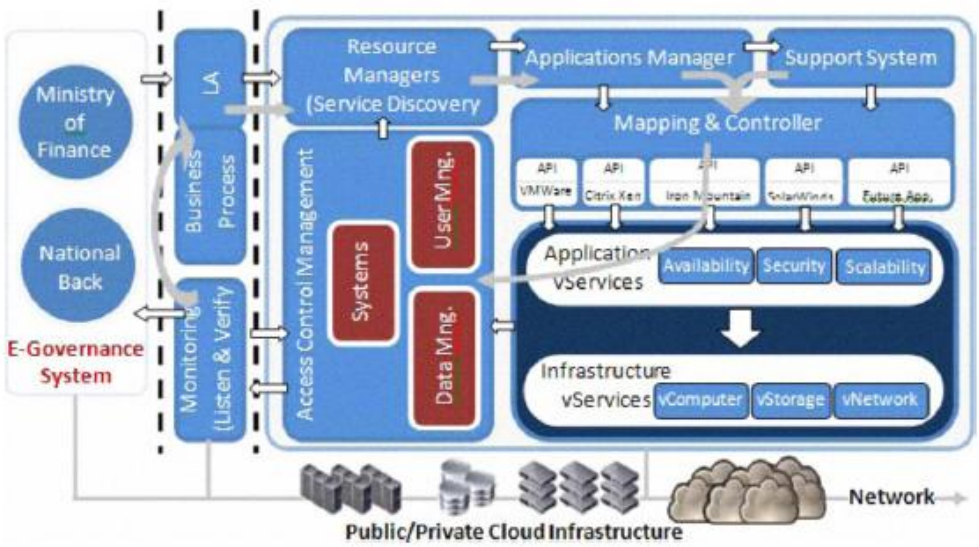

Figure 17: eGovernment with cloud data center (Chuob et al., 2010)

The same authors, in their subsequent work, suggested that a cloud based on Eucalyptus architecture will be more suitable for eGovernment data center, since Eucalyptus platform offers the option to keep the critical government data in private and general data in public (Chuob et al., 2011).

An architecture based on Hadoop (an open source cloud computing environment) can also be found in related literature (Mukherjee and Sahoo, 2010; Patil and Lolage, 2011). Hadoop undertakes tasks like authentication of users, mapping and fetching web services and scheduling the jobs of Passive Commodity Hardware (that consists of volunteer nodes[2]). After the computation process is completed, Hadoop sends the results to users' thin clients/mobiles. In addition, the proposed eGovernment system embodies a Knowledge Base and an Inference Engine (Figure 18) that act as an expert system within one particular field of knowledge.

Kim et al. (2011) on the other hand, used Hadoop to design and implement a Mobile Cloud E-Gov system that aims "to provide high level of integrated e-Gov service to many users, by bringing Web service of each government organization distributed into virtualized Mobile service space".

[2] The idea of volunteer computing is to allow users on internet to donate their idle computing resources to one or more intensive tasks.

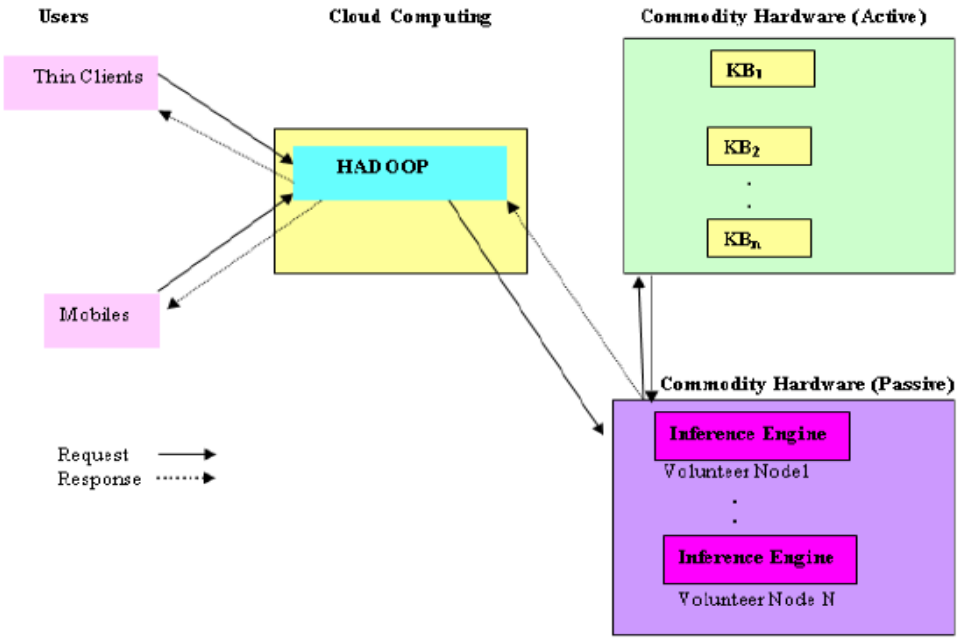

Figure 18: Proposed eGovernment architecture based on Hadoop (Mukherjee and Sahoo, 2010)

The architecture that Chanchary and Islam (2011) recommended for enhancing eGovernment (Figure 19), works in a similar way with the architecture of Mukherjee and Sahoo (2010), with the knowledge-based expert system reducing processing time in major cases and limiting manual workloads in organizations of public sector.

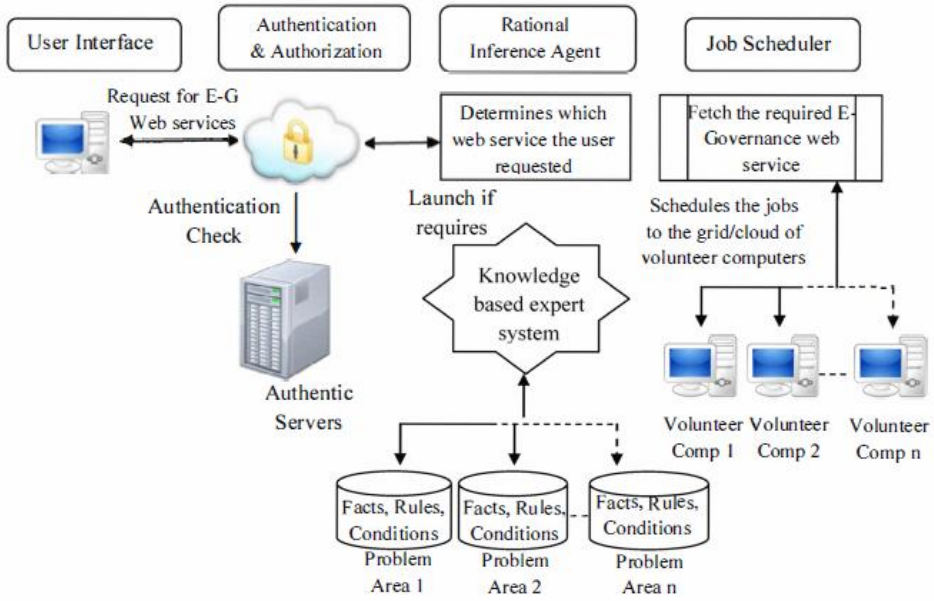

Figure 19: eGovernment based on cloud computing with Knowledge-based expert system (Chanchary and Islam, 2011)

Hung et al. (2011) presented the cloud-based eGovernment architecture that they designed for consolidating IT services and data centers across different agencies of

"Environmental Protection Administration" (EPA), the government department of Taiwan that handles environmental issues (Figure 20). The Private Cloud they built, joined the nine different data centers of the department into the two data centers shown in Figure 21 (the "GSN's Wen-Sin Data Center" is in charge of backing up the data), resulting to the reduction of servers from 130 to 25. According to the authors, due to the employment of the Private Cloud, common devices, such as firewalls and intrusion prevention equipment, were reduced, server management was enhanced and better utilization of resources was achieved.

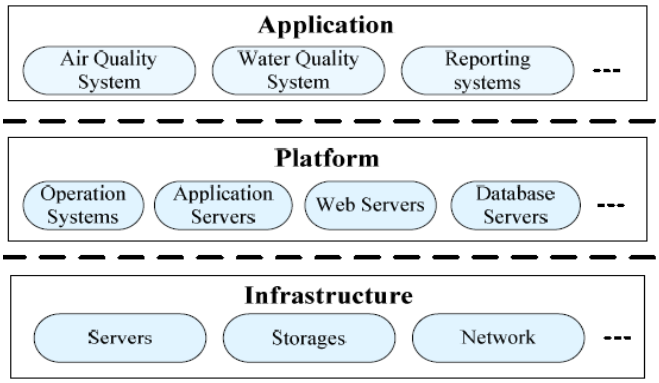

Figure 20: Cloud Computing Architecture of Taiwan EPA (Hung et al., 2011)

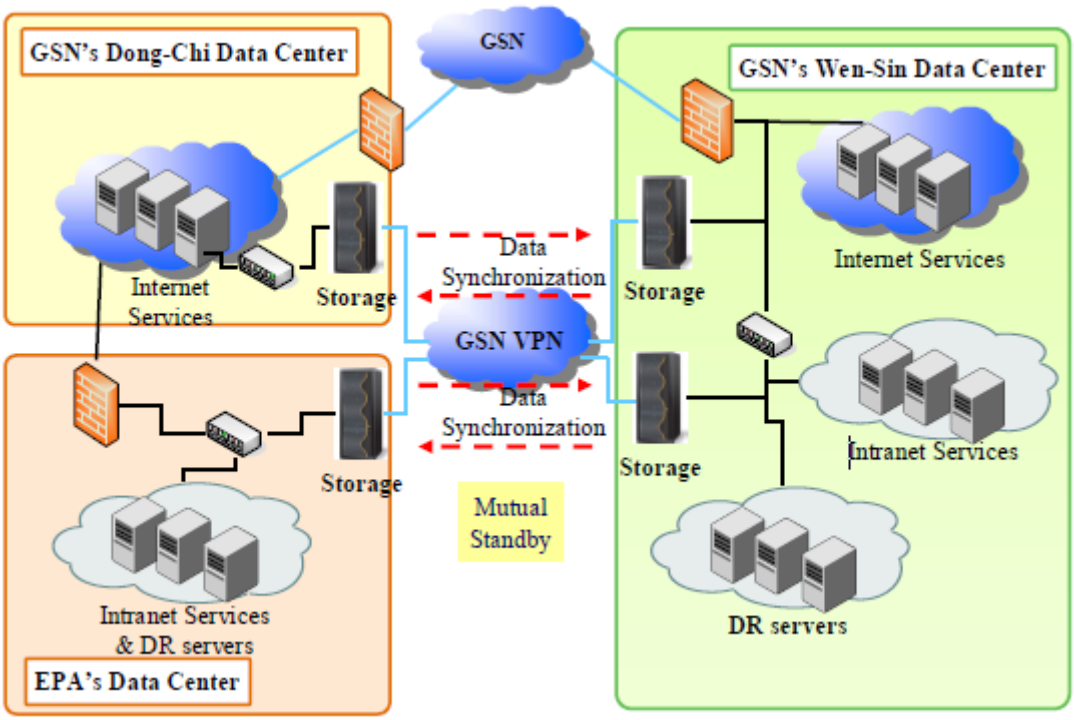

Figure 21: The Private Cloud of Taiwan EPA (Hung et al., 2011)

Breil et al. (2012) analyzed cloud architectures deployed for data integration in eGovernment. The authors examined two possible solutions for data integration:

- Materialized Data Integration, which employs an ETL (Extract, Transform and Load) layer that after it extracts the operational data from their different sources, it transforms it into the DHW- schema and finally loads the transformed data into the Data Warehouse (DWH), and
- Virtual Data Integration, based on Mediator- Wrapper- Architecture that consists of a) wrappers (unique for each source) that transform the source data into a wrapper schema and overcome interface, technical, and schematic heterogeneity, b) the mediator responsible for integrating the different wrapper schemas to global schema, and c) the schema that can be queried by applications that need data from the integrated view.

The cloud-based architectures that the authors presented are shown in Figure 22 and Figure 23. In Figure 22, a cloud- based architecture for Materialized Data Integration is

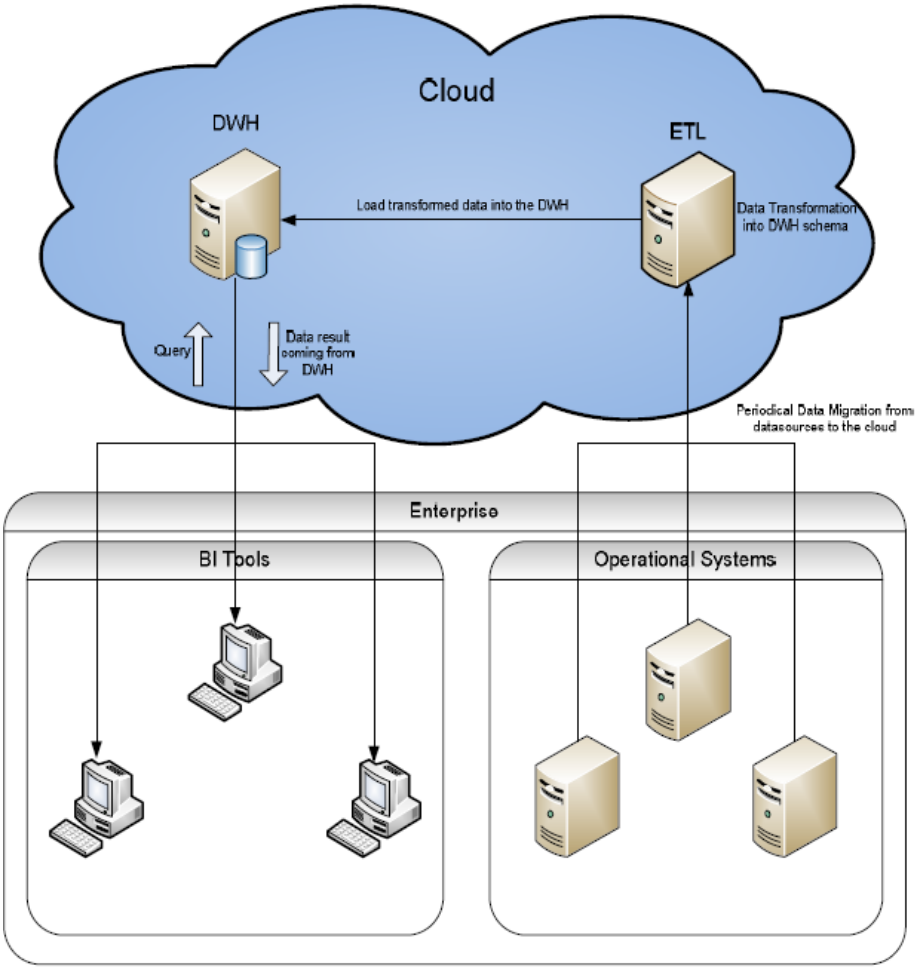

Figure 22: Architecture for a DWH in the Cloud (Breil et al., 2012)

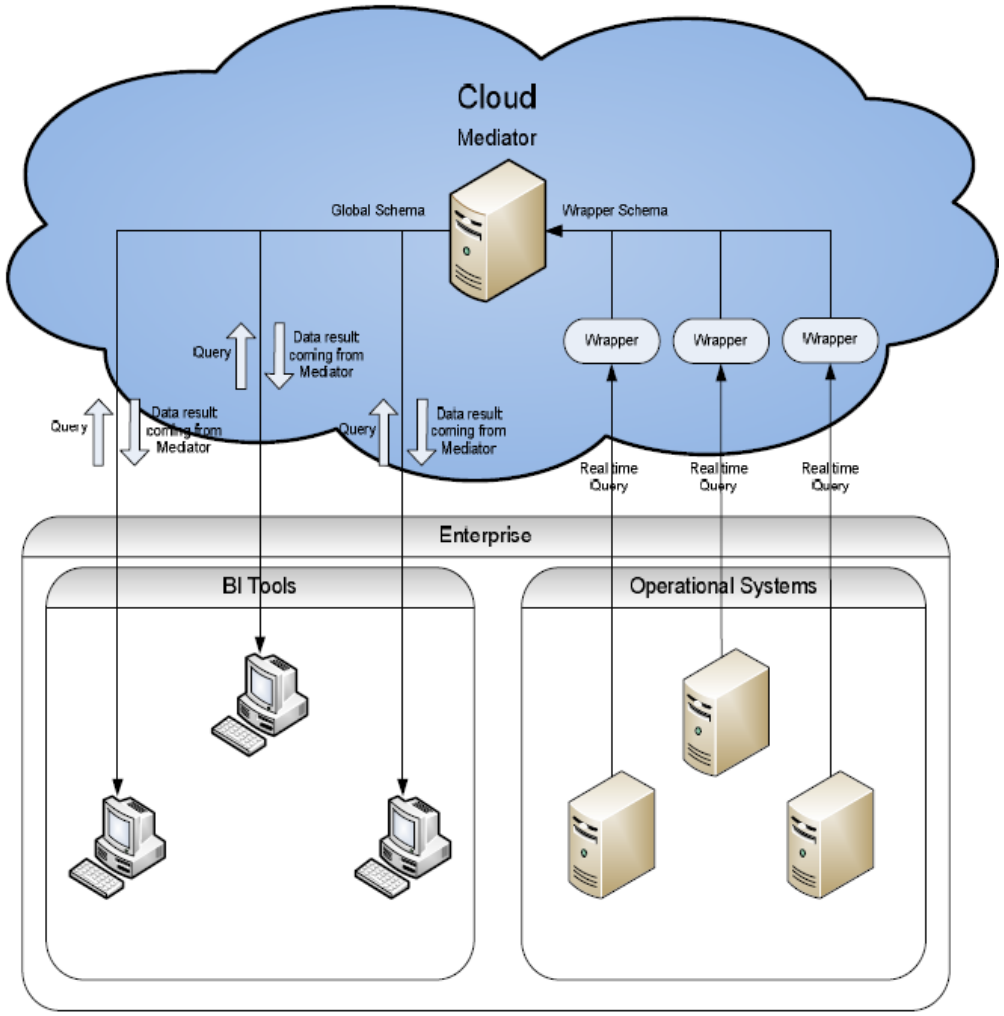

Figure 23: Architecture for a Mediator- Wrapper based data integration in the Cloud (Breil et al., 2012)

presented. In that case, the operational systems and Business Intelligence tools remain on premise, while the Cloud is deployed for the execution of ETL process and storing the data. Figure 23 on the other hand, shows the Mediator- Wrapper architecture. According to this approach, data is retrieved by BI applications through the global schema of the Mediator hosted in the Cloud.

Both approaches follow the Data-as-a-Service design, but in the case of Mediator-Wrapper data is not persisted in the Cloud. For that reason, only in the case of a cloud-based DWH the type of cloud that the organization/agency has deployed, may raise data ownership issues. In case of a private cloud, data ownership is not affected, but if the organization uses a public cloud, data ownership will be lost for all sources. In a community cloud, the data owners are the participating organizations, since the cloud belongs to all of them.

You et al. (2012) introduced a cloud-based architecture for sharing information among agencies (Figure 24).

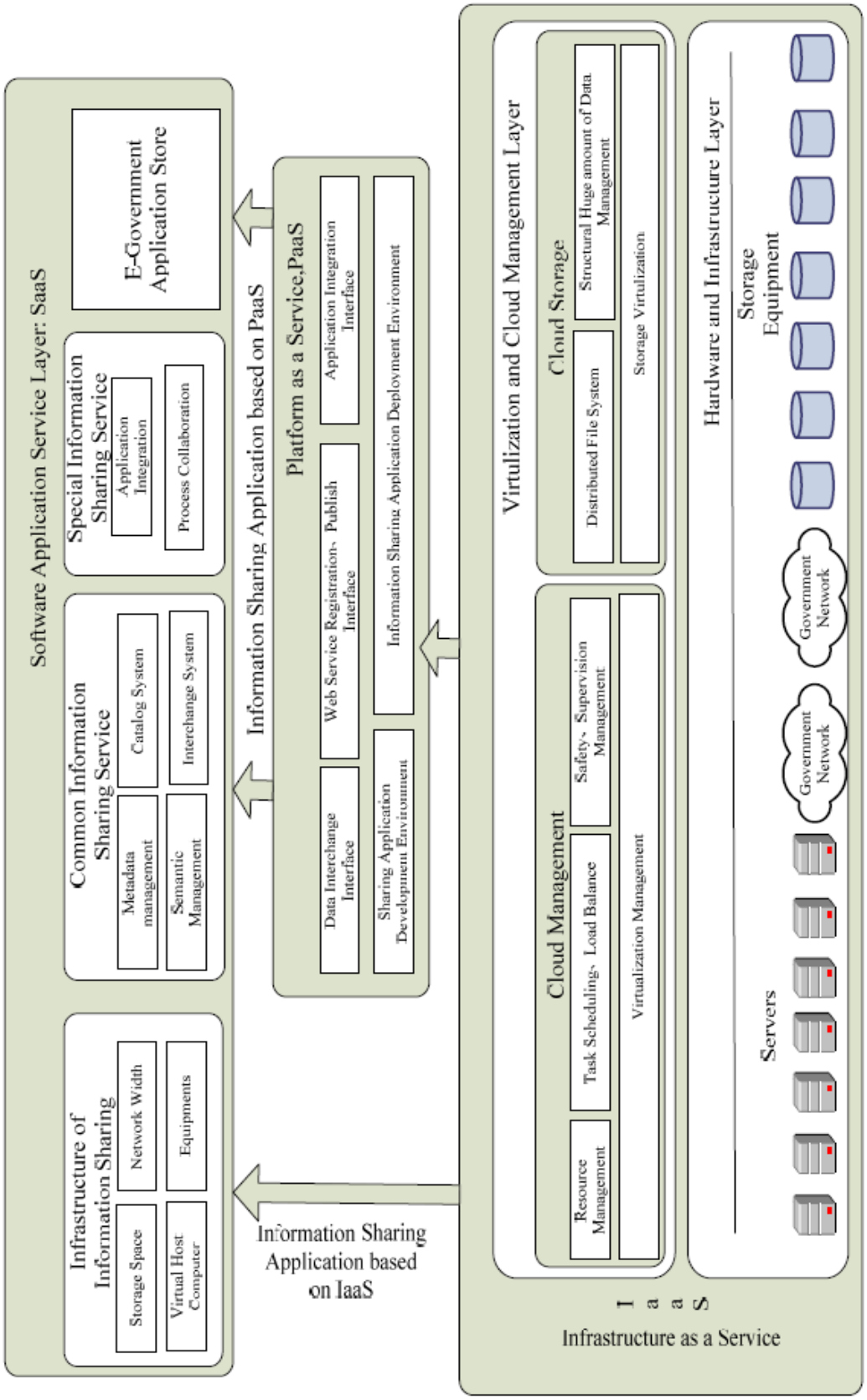

Figure 24: Sharing Cloud Architecture for eGovernment (You et al., 2012)

The IaaS layer provides cloud storage and cloud management services, whereas PaaS provides middleware for all types of eGovernment systems. The SaaS layer includes a variety of sharing application services such as “Common Information Sharing Service” and “E-Government Application Store”, where applications as services for different government departments can be found (related to education, transportation, health, social security etc).

According to the authors, this architecture supports network, system, data and application platforms of information resource sharing, resulting to full integration of IT resources dispersed at different government agencies.

An architecture based on cloud computing that can be used to transform Election Polling in India was suggested by Vidhya (2013).

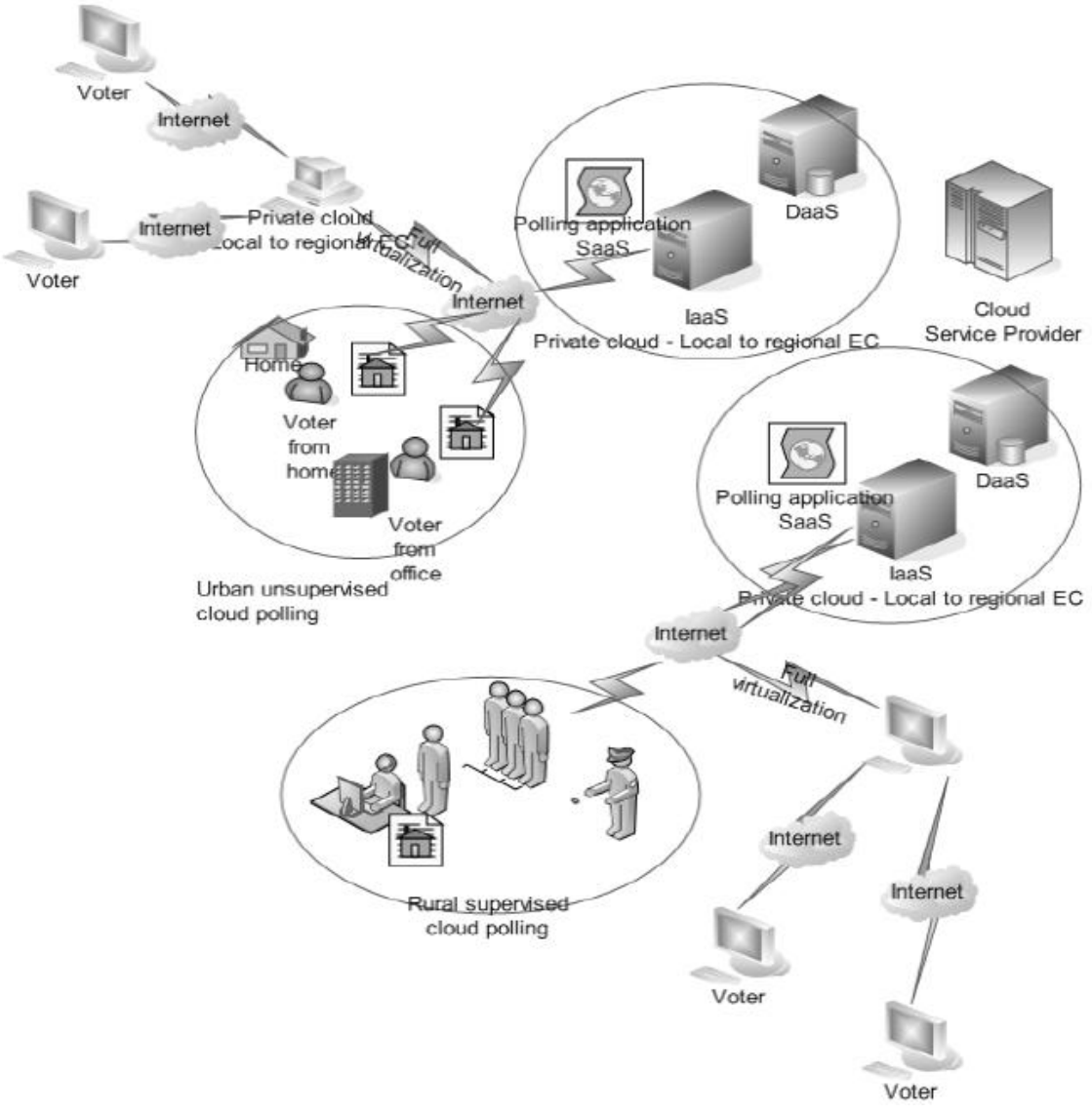

Figure 25: Cloud Polling System (Vidhya, 2013)

The proposed architecture (Figure 25) deploys a private cloud to host infrastructure (IaaS) and database (DaaS) services and replaces the polling application with a SaaS polling service. The polling service can be accessed by voters the day of the election via internet. For citizens that do not have internet access at home/office, there will be supervised limited booths where they can vote. The author believe that among other benefits, the proposed cloud-based polling system will offer the needed scalability for the expanding voting population and significant cost reduction.

Massonet et al. (2011) dealt with the problem of data location compliance that governments face when governmental data are kept in the cloud. They showed that their logging architecture can enable data location monitoring without compromising Cloud isolation. According to their approach, collaboration between the cloud infrastructure provider and the service provider (government agency), with the infrastructure provider monitoring the virtual machines on the service provider's behalf and making the infrastructure level monitoring information available to him, can enable the creation of audit logs required for compliance auditing.

Last but not least, there are scholars that proposed systems that aim to enhance the security of eGovernment in cloud computing environment. Mukherjee and Sahoo (2011) proposed an algorithm for encryption of sensitive governmental data that are stored in the Cloud. Likewise, Guan (2009) introduced a framework for the construction of an intrusion detection system, using statistical modeling. The system is intended to protect privacy in cloud- based eGovernment systems. The aforementioned algorithms are particularly technical, thus a further examination of them is considered to be beyond the scope of this study.

4.5.2. Cloud–based Platforms for Public Services

Considering the fundamental role digital public services have for eGovernment, the particular interest that scholars have shown for cloud-based platforms is understandable. Yeh et al. (2010) have provided a detailed analysis of the values and issues, that accompany the use of cloud- based platform for delivering public services, and affect not only government and society but environment, too.

Marasso et al. (2010) suggested a citizen-centric model based on cloud computing that enables citizens to self-compose their services in a simple way. The authors argued that by following the concept of "mashup" (allow users to deal with content retrieved from external data sources) and principles of Service Oriented Architecture, public

organizations can allow citizens to create services that are tailored on their needs, regardless of their level of familiarization with new technologies.

Taher et al. (2011) designed a cloud- based platform, called "T-Shaped", that aims to support public service organizations in developing and delivering services without the help of experts. The platform consists of two different views:

- Horizontal view: proposes that a reduction in the transparent cost can be achieved by exploiting a number of generic Reusable Services in the public service domain. A Reference Guideline is embedded in the platform to support the customization of reusable services
- Vertical view: proposes that public administrators or service providers may use the Reference Guideline to customize generic public services without the need of being informed about the processes and its related technologies.

Likewise, Charalabidis et al. (2011) introduced a cloud-based platform that follows the principles of Open Innovation. The examined platform should work as an active collaboration workbench for cloud and public administrators, public services and other stakeholders that are interested in creating and delivering public services. It consists of the following main components:

- Composite Services App Store – is a repository where the designed and deployed services that users created, will be stored
- Service Blueprint Registry – stores blueprints of all atomic services deployed in the Cloud. A fully documented catalogue of the building block services that are operated by public administrations can be found there. That allows third parties to re-use these services in order to develop new ones.
- Cloud Registry – a searchable catalogue of all registered clouds that can cooperate with each other and that will contain a list of the deployed public administrations and composite services per cloud. That will help users to locate the services they are looking for.
- Collaborative Design studio – that allows the creation of the composite services

A more "market oriented" cloud-based platform for eGovernment services is presented by Hobson et al. (2011). The "Municipal Shared Services Cloud", as it is called, is an IBM- operated platform that enables independent software vendors to provide services for local governments. The players of this ecosystem (Figure 26) are:

- IBM, the creator and operator of the platform
- Independent Service Vendors (ISVs), that create and manage the software applications running on the platform
- Clients, such as towns and villages that choose to subscribe to application bundles
- Client Relation Owners (CROs) that coordinate the business requirements between clients and the platform owner. Among others, they are responsible for identifying clients that want to subscribe to the platform and for enabling selection of ISV software by clients.

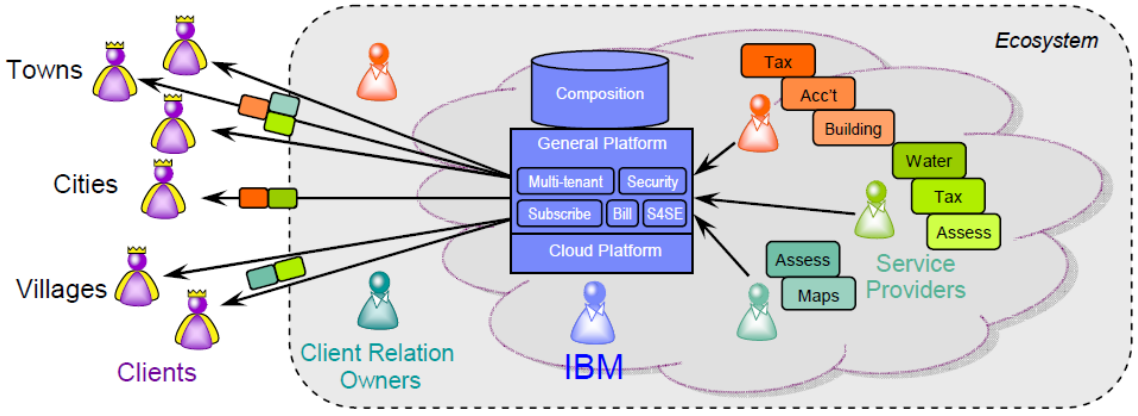

Figure 26: Municipal Shared Services Cloud Ecosystem (Hobson et al., 2011)

4.5.3. Open Data in the Cloud

Apart from the other benefits cloud computing can offer to eGovernment, it seems that it can support the spreading of Open Data policies. Hobson et al. (2011) claimed that the "Municipal Shared Services Cloud", that is mentioned above, can be leveraged as an architecture to collect, aggregate and manage Open Data for governments. Moreover, Open Data may encourage the participation of new Independent Service Vendors in the proposed platform, giving them the opportunity to increase the range of services and their quality. Thus, the collaboration between Open Data and a cloud-based platform for delivering public services can be considered as mutually beneficial.

Similarly, Jiricek and Massimo (2011) discussed the "European Open Government Data Initiative" (OGDI), an open source cloud-based collection of software assets that governments can use, and how cloud computing can generally promote Open Government initiatives. The data repository of European OGDI is based on Windows Azure Platform and aims to offer availability, transparency and added value to

eGovernment services. As the authors point out, the scalability and interoperability that cloud platforms can offer, make cloud computing an ideal solution for hosting government data. In addition, government Open Data is non- Personally Identifiable Information and hence it is not constrained by the legislation that protects sensitive data. Consequently, Open Data can be stored in clouds located internationally.

In the same way, Zhang (2010) suggested that cloud computing is the best choice in order to achieve Open Government and presented a Cloud for Open Government (Figure 27).

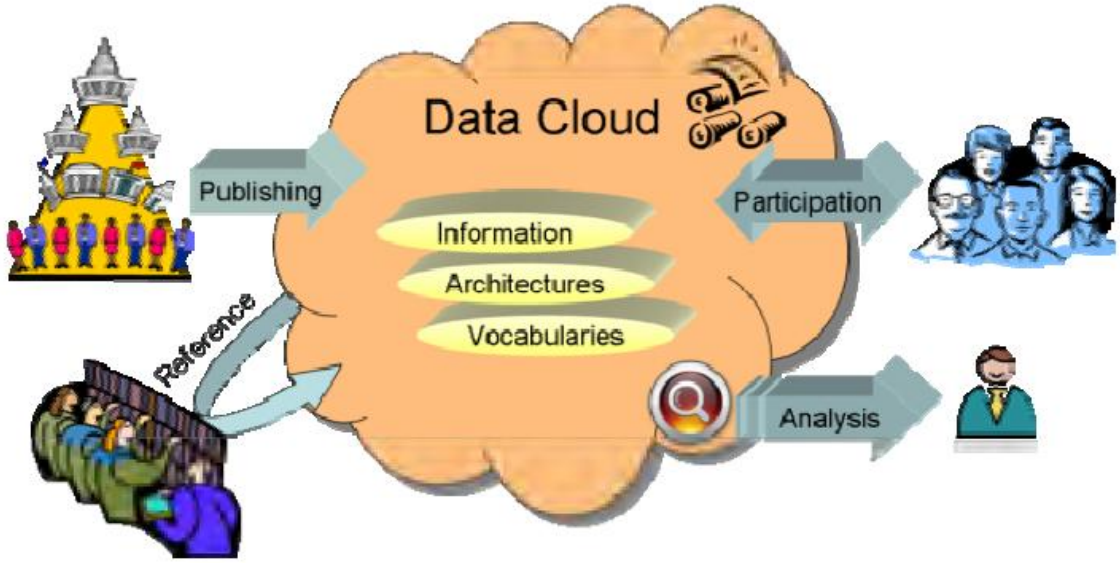

Figure 27: Open Government Data Cloud (Zhang, 2010)

In the author's opinion, the Open Government Data Cloud will enhance visibility, collaboration and participation since it will contain standards based on descriptions of processes, services, information, policies and related government architectures, schema and models. The citizens will have access to information that government and industries publish, along with raw and analytical data that can also be used by other government agencies. Additionally, through social networking technologies, the proposed cloud will operate as a two-way communication channel between citizens and government, facilitating citizens' participation.

4.6. Discussion

The examination of the literature reveals the different aspects from which researchers view the use of cloud computing in eGovernment. Beginning with the examination of suitability, it is interesting to look at the studies focused on a specific case of potential use of cloud computing (Table 6).

Table 6: Summary of studies focused on specific use

Reference	Focus	Method	Results
Tahamtan et al. (2011)	Austrian public sector	Interviews with ministries and office of chancellor	Identification of requirements and obstacles related to cloud adoption
Khan et al. (2011)	Developing countries	Review eGovernment readiness of Pakistan	Cloud computing can solve issues of digital divide and inadequate funding
Stefanou and Skouras (2012)	Government's payroll information system for companies in Greece	Questionnaire, focused on a specific area of the country	Half of the respondents positive towards cloud solution, Data security and connection/softw are issues the main challenges.
Leikums and Cevere (2012)	SaaS document management system	Review advantages and disadvantages of SaaS	Suggestion of advantages and disadvantages of such a solution in Latvian public sector
Janssen and Joha (2011)	SaaS	Interviews with IT managers and experts from various public organizations	Benefits and risks of SaaS

What the studies in Table 6 have in common, although they are focused on a different application of cloud computing, is that their results are consistent with the advantages and disadvantages that have been presented generally in literature. However, they differ in the methodology followed, since some of them are not based on primary research but on related literature. This does not necessarily imply misleading results, but since the use of cloud computing is examined in a narrow context, primary research would be preferable. It is also interesting that only the study of Stefanou and Skouras (2012) concentrates on how the eGovernment service recipients view the cloud computing adoption. The rest of the surveys examine the opinions of public administrators and IT experts, but it would be useful to discover what the other stakeholders think, too.

Differences can be found in the migration strategies presented in this chapter, too, although they share the same aim. One basic difference is that the first two strategies of

the Table 2 (Wyld, 2010 and Reza, 2012) consist of more generic steps, while the others are more detailed. In addition, the first two strategies along with the strategy of US DoD (2012), seem to cover the topic from a broader scope, including steps from the beginning of migration procedure (such as the steps of familiarizing organization with cloud computing and reviewing organization's IT needs), to the end of it (such as the steps of evaluation and continuous improvement). On the contrary, the rest of the strategies either consist exclusively of actions that should be taken before the Cloud adoption (the strategy of Craig et al., 2009), or they give emphasis to the implementation stage and the steps that follow (Kundra, 2011; Frost& Sullivan, 2011).

In an attempt to bridge these different approaches and summarize the steps that have been suggested, the basic steps of each strategy were gathered and grouped under four generic categories:

- **Preparation** – steps that should be taken to "prepare the ground" and support adoption of cloud adoption
  - Learn about/ Familiarize government IT staff with cloud computing
  - Assess government's IT needs – assure that these needs justify migration to the Cloud
- **Planning** – tasks related to readiness assessment and selection of services and service models
  - Present strategic options for adopting cloud computing along with cost/benefit analysis that will help decision making
  - Determine cloud readiness and decide which data and services should be moved to the Cloud
  - Contract effectively to ensure that organization's needs are met
  - Designate a cross-functional team to monitor new services, providers and standards
- **Management** – steps that aim to ensure that new procedures run smoothly
  - Monitor SLAs to ensure compliance and performance improvement
  - Change mind-set from assets to services
  - Ensure integration with existing infrastructure
- **Evaluation and improvement** – steps dedicated to the evaluation of the outcome and continuous improvement
  - Continue to assess the proper use of cloud computing, moving accordingly, data and applications to the Cloud

- Re-evaluate vendor and service models regularly to maximize benefits and minimize risks

The frameworks and models, on the other hand, do not share the same purpose, so an extensive comparison among them would probably be pointless. However, it is important to identify the situations in which they can be used. Table 7 summarizes the frameworks and models found in literature and indicates in which steps of the migration strategy that discussed earlier, they can be deployed. As can be noticed, the use of some frameworks is not limited to one step of migration strategy, but they can be used at different steps in both Planning and Evaluation stages.

Table 7: Specialized frameworks and models

Reference	Aim	Focus on specific service model	Step of migration strategy in which can be used
Deussen et al. (2011)	Identify public sector business model	-	Preparation: Learn about cloud computing
Kurdi et al. (2011)	Assess the readiness of eGovernment systems	-	Planning: Determine cloud readiness
Mutavdzic (2012)	Choose PaaS implementation	PaaS	Planning: Decide which data and services should be moved to the Cloud and/or Evaluation and Improvement: Continue to assess the proper use of cloud computing
Repschlaeger et al. (2012)	Classify cloud providers	IaaS	Planning: Present options for adopting cloud computing and/or Evaluation and Improvement: Re-evaluate vendor

As can be seen from the literature review, a significant number of researchers have worked on technical aspects of cloud computing adoption in eGovernment. The studies focused on cloud architectures could be divided into two main groups: a) the first one would include studies that present an architecture framework on how cloud computing can generally provide the basis for eGovernment, and b) the second one would include studies that examine potential cloud architectures by detail. While the majority of them aim to enhance the whole eGovernment system, the cloud architecture proposed by Vidhya (2013) is designed to support an eVoting system.

Table 8 presents the main cloud solutions presented in this chapter. All the cloud architectures seem to have mainly advantages, which are in agreement with the benefits suggested in literature. It is quite remarkable though, that no disadvantages were noted. This might be related to the fact that only the architectures proposed by Sharma and Kanungo (2011) and Hung et al. (2011) have been tested, the first one through experiments on cloud simulator and the second as an actual implementation (the private cloud of Taiwan's EPA).

Table 8: Comparison of cloud architectures/frameworks suggested for eGovernment

Reference	Presented as	Special characteristics	Potential advantages
Zhang and Chen (2010)	A framework based on cloud computing layers	-	Enhance productivity, efficiency, transparency, participation and collaboration of traditional eGovernment
Sharma and Kanungo (2011)	Master/slave model	Distributed data centers	Experiments showed the architecture is energy efficient, eco-friendly and cost-effective
Chuob et al. (2011)	Deployment of Eucalyptus architecture	Central cloud data center owned by the government	Data privacy
Mukherjee and Sahoo (2010)	Deployment of Hadoop	Volunteer nodes, Knowledge Base and Inference Engine	Can act as an expert system

Kim et al. (2011)	Deployment of Hadoop	Mobile	Integrated eGovernment services to many users
Chanchary and Islam (2011)	Knowledge-based expert system	Knowledge-based expert system	Reduce processing time and limit manual workloads in public sector
You et al. (2012)	A framework based on cloud computing layers	-	Full integration of IT resources dispersed at different government agencies
Vidhya (2013)	Private cloud	Polling system	Scalability and cost reduction
Hung et al. (2011)	Private cloud	Distributed data centers	Reduction of common devices, enhancement of service management and better utilization of resources

Finally, Table 9 presents the cloud based platforms that have been proposed in literature. The platform that Hobson et al. (2011) examine is the only one that is based on a commercial solution and aims to facilitate the provision of cloud based services to governments. The rest of the platforms are supposed to be used for developing digital public services, without the need of specialized IT personnel. In case of the platform proposed by Marasso et al. (2010) citizens have also an active role in the creation of services. Advantages such as cost reduction, active engagement of citizens and innovation that have been suggested in theory, seem to apply in the case of cloud-based platforms. Of course, the number of studies is small, so further research should be conducted to come to firm conclusions.

Table 9: Comparison of cloud-based platforms

Reference	Purpose	Characteristics
Marasso et al. (2010)	Enable citizens to self-compose their services	Citizen-centric, Based on the "mashup" concept, No special IT skills needed
Taher et al. (2011)	Enable public organizations to develop and deliver services	No help from IT experts is needed, Reusable services
Charalabidis et al. (2011)	Work as an active collaboration workbench for developing public services	Open Innovation
Hobson et al. (2011)	Enable independent software vendors to provide services for local governments	Agency-centric, Based on IBM's platform

4.7. Conclusions

The examination of "Cloud Computing in eGovernment" literature has shown that researchers have identified many benefits and challenges of cloud computing in eGovernment, with some benefits being also mentioned as a challenge/risk and the other way around (security for example). This is mainly due to the different approaches of the topic since cloud computing can be applied in several ways in eGovernment (different deployment and service models), and each application can have different effects. Therefore, the general approach of the topic is more useful for intriguing further research on the area, rather than giving an exact answer to the question of cloud computing suitability in eGovernment.

Cloud computing seems to be able to support digital public services and Open Data, but since published studies in this direction are limited, more research is needed. Further research should also be conducted to develop more frameworks and models that will cover the several applications of cloud computing in eGovernment.

It can also be noticed that although "Cloud Architectures for eGovernment" is the topic that so far has drawn most attention among the concepts presented in Figure 2, only few scholars dealt with designing systems that will secure governmental clouds. Considering the important role that security issues play in the Cloud adoption process, more research in this field would be welcomed.

5. Case Studies

5.1. Introduction

As it was mentioned in the previous chapter, one of the key areas in which scholars have focused, is cases of governments or agencies that have already used cloud computing. It was decided that a separate chapter should be dedicated to these case studies, mainly for two reasons. Firstly, there were several case studies found in literature and a separate chapter would allow a more extensive examination of them. Secondly, examining the case studies separately from the rest concepts found in related literature, would permit the comparison with other cases that have not been presented in literature yet (such as the case of Greece) or are only briefly mentioned in the publications used in literature review (so further information was sought from organizations' reports in the official websites).

5.2. Case Studies from North America

5.2.1. US Government- USA.gov

The challenge

USA.gov is the official Web portal of US government, designed to facilitate the communication between citizens and the government. It also operates as a channel for online government services, such as tax forms, driver's license renewal, voter registration and student financial aid (Staten et al., 2009). Due to significant variations in portal traffic users suffered longs delays and downtime. The Federal Government was unable to handle the demand using its own infrastructure, so it was decided to move the platform to the Cloud (Spanish National Institute of Communication, 2012; Tsaravas & Themistocleous, 2011b).

The solution and the benefits

The solution chosen was Terremark's Enterprise Cloud Service since it was estimated that the move to that platform would cut costs by 90%. The other benefits that accompanied that decision were (Spanish National Institute of Communication, 2012; Staten et al., 2009):

- Flexibility and service availability
- Shorter migration period (ten days)

- At normal levels of traffic, only the contracted baseline fee was paid, and additional fees were only charged when there was a need to accommodate large traffic.
- Enhanced security, by using additional security services for system access, communications and platform security monitoring.

5.2.2. US Government- Apps.Gov

The challenge

In order to modernize Information Technology of US Government, President Obama launched in 2009 the Federal Cloud Computing Initiative. The General Services Administration (GSA) participated in this Initiative by implementing projects for planning, deploying and utilizing cloud computing solutions for the Federal Government. One of the aims of GSA was to create a cloud computing "storefront" that will allow agencies to find cloud computing solutions provided by prequalified vendors that had been certified in terms of quality, security and privacy (Wyld, 2010a).

The solution and the benefits

In September 2009, the portal "Apps.Gov" was launched (Figure 28). The portal enabled public sector agencies to acquire cloud services and applications (Frost & Sullivan, 2010; Spanish National Institute of Communication, 2012; Wyld, 2010a):

Figure 28: Apps.Gov Portal (https://www.apps.gov/cloud/main/start_page.do)

- From a wide variety of services that fall into four basic categories (Business Apps, Cloud IT Services- IaaS solutions, Productivity Apps and Free Social Media Apps)
- Without the need of any infrastructure implementation or maintenance costs
- With charge based on pay-per-use model
- From verified vendors

The Apps.Gov Portal closed in December 2012 and all of its services are now available from GSA Advantage[3], the official marketplace of GSA for applications and services. Earlier, in February 2012 GSA had announced the establishment of a new cloud marketplace (Miller, 2012). What will happen and how this new marketplace will operate, it remains to be seen in the future.

5.2.3. Department of Defense (DoD), Defense Information Systems Agency (DISA) – USA

The challenge

The aim of Defense Information Systems Agency (DISA) is to support US and allied fighting forces by providing them with global infrastructure services. Since the computing workload of the agency is variable and occasionally unpredictable events emerge, that need to be handled at once by deploying large scale infrastructure, DISA decided to build its own private cloud infrastructure (Kim et al., 2012; Kundra, 2011).

The solution and the benefits

The private cloud (named Rapid Access Computing Environment -RACE), changed the focus of DISA from asset management to service provisioning. It offers the following benefits (Kim et al., 2012; Kundra, 2011; Paquette et al., 2010; Wyld, 2009):

- Serves more than 3 million DoD users with 18 processing centers, 1400 applications and 4500 servers
- Access to various IT resources within 24 hours of funding approval
- Provides a fast, secure, and automated self-service computing infrastructure

5.2.4. National Aeronautics and Space Administration (NASA) - USA

The challenge

[3] https://www.gsaadvantage.gov/advantage/main/start_page.do

NASA needed a flexible computing solution that would improve performance, security and availability of the agency's web platforms and at the same time would promote transparency and public involvement with space projects (Wyld, 2010a).

The solution and the benefits

Nebula is an open source, cloud computing platform that was developed by NASA Ames Research Center based on Eucalyptus cloud platform. Apart from offering SaaS applications, Nebula can also provide PaaS and IaaS solutions (Wyld, 2010a). The benefits gained are (Spanish National Institute of Communication, 2012; Wyld, 2010a):

- Greater flexibility, use and cost savings
- Reductions in infrastructure operating and maintenance costs
- Significant power savings, environmental sustainability
- Allowing NASA to provide cloud computing services to other federal agencies
- Promoting collaboration and research

5.2.5. City of Edmonton- Canada

The challenge

Following the principles of Open Government, the city of Edmonton in Canada decided to offer census data and other public information online. The need for storing large volumes of data led the municipal government to deploy a cloud computing solution (Tsaravas & Themistocleous, 2011b).

The solution and the benefits

The City's council decided to join the Open Government Data Initiative (discussed earlier, in chapter four) that uses Windows Azure Platform (Jiricek and Massimo, 2011) not only for storing open data, but also for the creation of "mash-ups" and web-based analytics tools (IBM, 2011). An example of a "mash-up" map that depicts Edmonton's Public Schools is presented in Figure 29. By deploying cloud computing, the municipal government (IBM, 2011; Tsaravas & Themistocleous, 2011b):

- Had a fast and a low cost solution
- Enhanced transparency, flexibility and services provided to citizens
- Increased the speed and effectiveness in which the City disseminate information

- Decreased IT procurement cycles, enhanced analytics application lifecycle management (build/test/deploy) and automated the scaling efforts of analytics applications

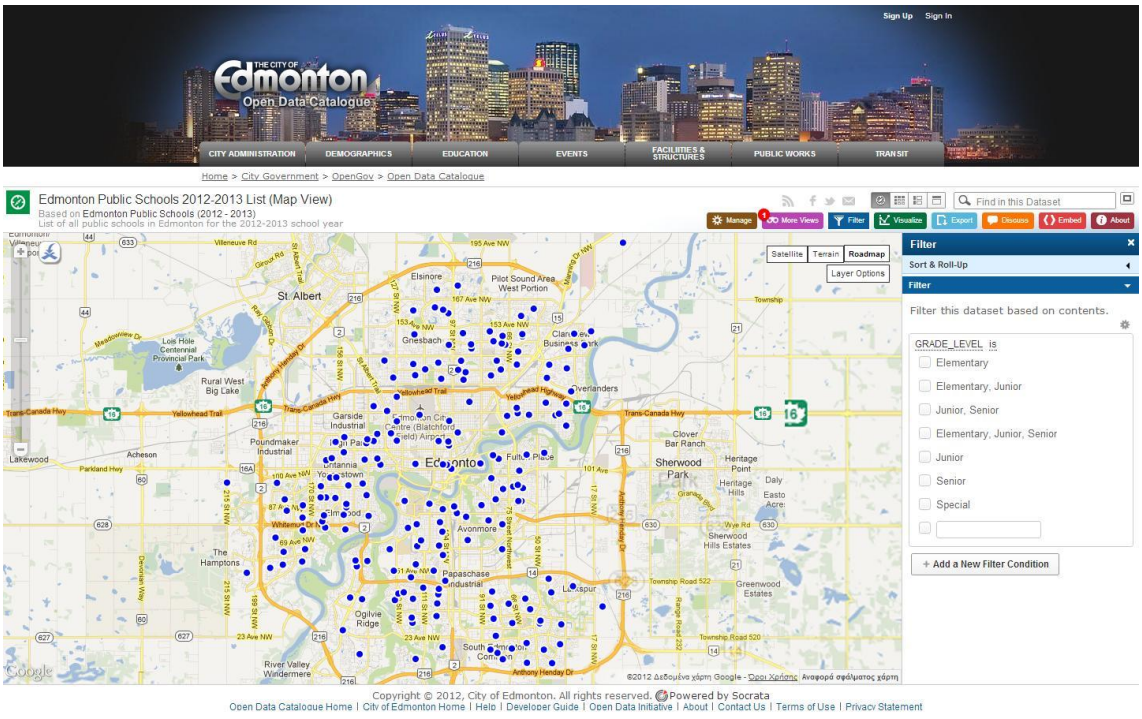

Figure 29: A "mash-up" map in Edmonton's Open Data Catalogue (http://data.edmonton.ca)

5.3. Cases Studies from Asia

5.3.1. Japan

The challenge

In 2009 Japan's Ministry of Internal Affairs and Communications launched the Hatoyama Plan that aims to create new Information and Communications Technology (ICT) markets and support technological management in public sector. This plan includes the creation of a nation- wide Cloud Computing Infrastructure, temporarily called the Kasumigaseki Cloud (Chandra& Malaya, 2011; Frost&Sullivan, 2010; Spanish National Institute of Communication, 2012).

The solution and expected benefits

The Kasumigaseki private cloud (Figure 30) will incorporate services, platforms and infrastructures of Japanese Ministries, promoting information sharing, and supporting standardization and consolidation in Government's IT resources (AlAjmi, 2011; Wyld, 2010a). The benefits that Japanese government expects to gain by 2015, when the project is completed are (Frost&Sullivan, 2010; Spanish National Institute of Communication, 2012; Wyld, 2010a):

- Reduced eGovernment- related development and operating costs
- More environmental friendly IT operations
- Better collaboration
- No need to maintain individual systems for different ministries

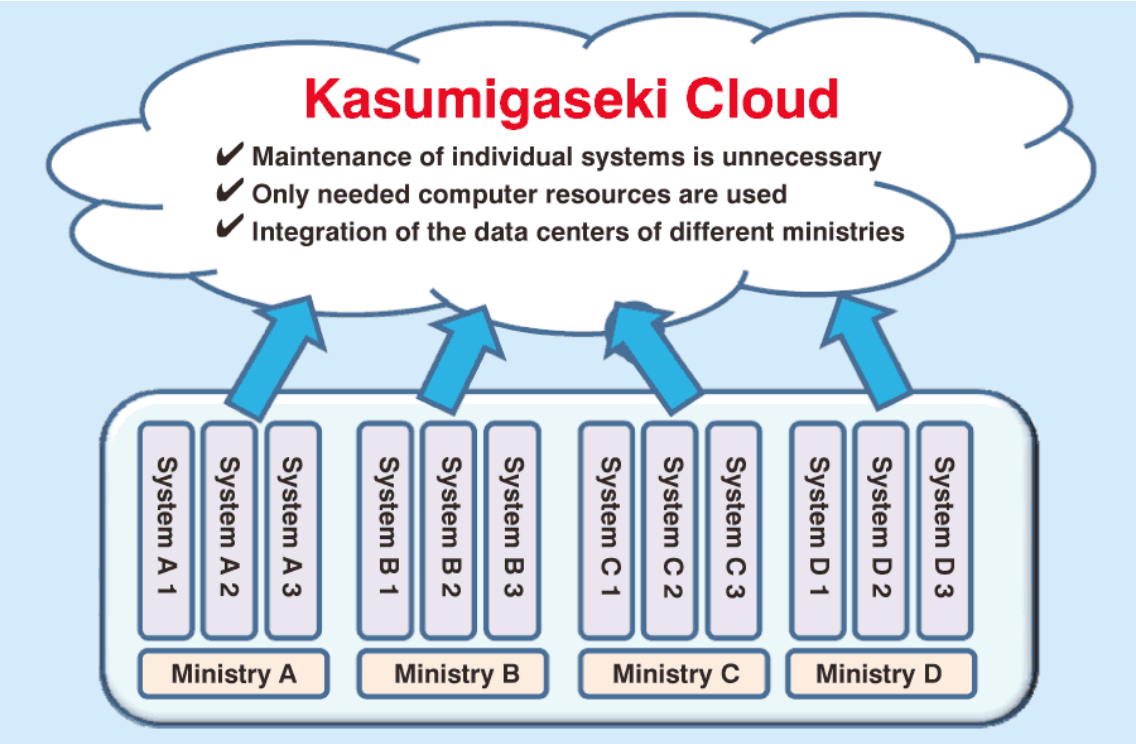

Figure 30: The Kasumigaseki Cloud (Wyld, 2010a)

5.4. Case studies from Europe

5.4.1. United Kingdom

The challenge

The adoption of cloud computing by public sector has been one of the objectives of UK Government since 2009. For that purpose, the Government launched G-Cloud program

that has as an ultimate objective the development of a government cloud computing infrastructure (Kim et al., 2012).

The solution and expected benefits

One of the first steps of G-Cloud program was the establishment of a Government Application Store. The CloudStore, as it is called, operates as a marketplace for British public organizations where they can procure, use and review ICT services offered by certified suppliers. The concept of this digital marketplace is quite similar to "Apps.Gov" US portal, yet in UK's case is still in beta phase (Figure 31).

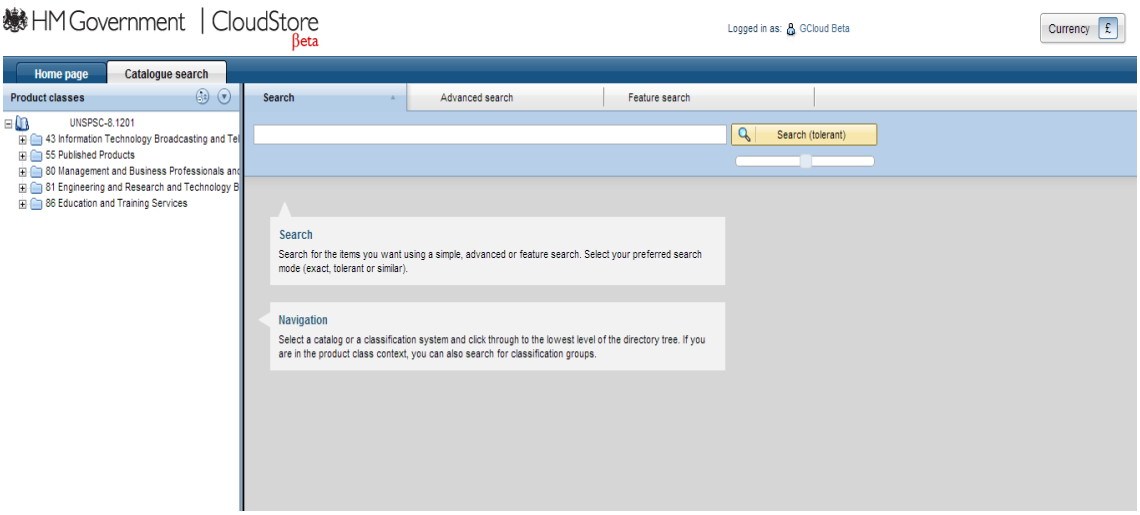

Figure 31: CloudStore of G-Cloud (http://gcloud.civilservice.gov.uk/cloudstore/)

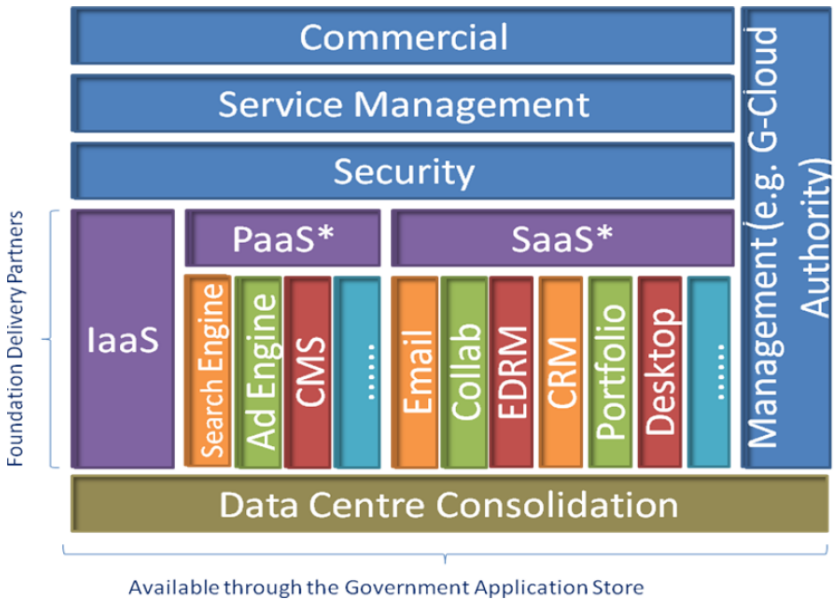

Figure 32: Components of G-Cloud (Cabinet Office, 2011)

As it can be seen in Figure 32, the G-Cloud program will include all kind of services (IaaS, PaaS, SaaS) that will be developed and managed from different public organizations (Foundation Delivery Partners) along with the G-Cloud Authority. According to the UK Government, the G-Cloud program will result in savings of £200 million by 2015. Other significant benefits of the program are (Cabinet Office, 2011):

- Rationalization of existing provision
- Reduced bureaucracy, cost and management overheads
- Greater level of understanding and awareness of the services and how to exploit them
- Transparency and comparison of suppliers

5.4.2. Germany

The challenge

In order to provide a business incubator for small and medium enterprises (SMEs), German Government decided to facilitate the creation of a cloud based business/public sector process integration platform (Deussen et al., 2011).

The solution and expected benefits

The "goBerlin" project, which is being funded by German Government as a part of "Trusted Cloud" initiative, aims to develop a secure and trusted, cloud-based services marketplace for citizens, by enabling the cooperative provision of public and related commercial services. By joining the platform either as a user or as a provider, and extending existing or implementing new processes, a SME can be integrated into eGovernment value chain (Germany Trade& Invest, 2012). The benefits that can be gained from this project are (Fraunhofer-FOKUS, 2012; Germany Trade& Invest, 2012):

- Development of various innovative apps and new online services for citizens
- New forms of collaboration between public sector and companies
- Guaranteed interoperability between different services
- Trustworthy and safe IT services
- Promoting open government idea

5.4.3. Greece

The challenge

Low utilization of IT resources, the need for specialized personnel and high energy consumption were the basic reasons that the eGov ICT Group guided by Cabinet Office of Greece decided to virtualize the old physical systems that were used up until then (Karounos et al., 2012; Prnjat, 2011).

The solution and benefits

The virtualization, for which servers of Greek Research and Technology Network (GRNET) were deployed, resulted to increase of server utilization from 5% to 90%. The next step was the adoption of cloud computing, and more precisely the creation of OpenGov Private Cloud in 2010. So far the Cloud has accommodated 164 "physical" and "virtual" machines and various applications and sites, such as the site of Greek Presidency Office, the site of Cabinet Office and the information system of "Diavgeia" program (Karounos et al., 2012). The full list of the Ministries and agencies supported by OpenGov Private Cloud can be found at List of supported services.[4]

The benefits of cloud computing adoption by Greek Government are (Karounos et al., 2012; Prnjat, 2011):

- Savings of more than € 1,5 million
- Easier migration and disaster recovery procedures
- Improved energy efficiency
- Rapid development of new services

5.5. Findings of the Case Studies

Table 10 summarizes the findings of the Case Studies presented above, indicating the service models that are deployed in each case, along with the chosen solution and the benefits.

[4] https://docs.google.com/document/d/1ZV7LSE1YCRZ3yFivvR_8ySXuYXk3GwGM_PklTUbawfs/edit

Table 10: Case Studies - Findings

Case study	Service Model	Solution	Benefits
US Government-USA.gov	IaaS	Terramark Enterprise Cloud	• 90% saving in operating costs and infrastructure • Shorter migration period • Charges based on the use • Enhanced security
US Government-Apps.Gov	SaaS, IaaS	Various	• Wide variety of cloud services • No infrastructure needed • Pay-per-use model • Verified vendors
DoD- DISA	IaaS	RACE	• Serves a large number of users • Fast access to resources • Secure and automated self service infrastructure
NASA	SaaS, PaaS, IaaS	Nebula	• Flexibility • Cost savings • Power savings, environmental friendly • Promote collaboration and research
City of Edmonton – Canada	PaaS	OGDI, Windows Azure	• Fast and low cost solution • Enhancement of transparency, flexibility, and digital public services • Fast and effective information dissemination • Decreased IT procurement cycles, automated scaling efforts of analytics applications

Japan	IaaS, PaaS, SaaS	The Kasumigaseki Cloud (In progress)	• Reduced costs • Environmental friendly IT operations • Better collaboration • No need for individual systems
UK	IaaS, PaaS, SaaS	G-Cloud (In progress)	• Savings of £200million • Rationalization of existing provision • Reduced bureaucracy and management costs • Greater level of awareness of services • Transparency and comparison of supplies
Germany	PaaS, SaaS	goBerlin (In progress)	• Development of innovative apps and new digital public services • New forms of collaboration between public sector and companies • Guaranteed interoperability between different services • Trustworthy and safe IT services • Promoting open government data
Greece	IaaS	OpenGov Private Cloud-GRNET	• Savings of more than € 1,5 million • Easier migration and disaster recovery procedures • Improved energy efficiency • Rapid development of new services

5.6. Conclusions

The examination of the case studies in this chapter showed that cloud computing has already been adopted by some governments and agencies around the world. Despite the risks that accompany its adoption, most governments do not seem to hesitate to fully incorporate it and they do not limit their use to only one service model or application. On the contrary, some of them promote the overall application of cloud computing in public sector by establishing specialized market places for their agencies (cases of USA and UK).

What can also be noted, is that cloud computing has been employed as a solution for different eGovernment delivery models. For example, in case studies of "Apps.Gov" and "G-Cloud", cloud computing is used for delivering services to government's agencies (G2G), while in cases of Edmonton and "USA.gov" for delivering services to citizens (G2C). There is also the case of "goBerlin", where cloud computing is used for facilitating collaboration between government and companies (G2B).

The benefits that governments and agencies have gained or expect to gain from cloud computing are in agreement with the benefits mentioned in literature, with "costs reduction" being the most common. As far as deployment models are concerned, there is a tendency for public sector to prefer private clouds over public (only city of Edmonton is the exception), mainly for the security and control they offer.

Last but not least, the fact that many projects are still in progress (case of Japan and UK) or have just begun (case of goBerlin) shows that cloud computing adoption by public sector is still in early stages and the full results would be known over time.

6. A Stage Model for Cloud Computing Adoption in eGovernment

6.1. Introduction

From the examination of literature and case studies presented in the previous chapters, it is eminent that there are various ways to apply cloud computing in eGovernment and each country is more or less advanced in that field. The purpose of this chapter is to develop a theoretical stage model for cloud computing adoption in eGovernment that could help governments to figure their progress in the field and decide their next steps. The proposed model is based on the identification of qualitative variables, which delimit the stages by indicating the most likely characteristics of each of them.

In the next sections, a brief review of stage models in IT and eGovernment research is presented, followed by the proposed stage model, the description of its stages and the conclusions.

6.2. Stage models in IT and eGovernment research

Many stage models have been proposed over the years in order to describe various phenomena such as organizational life cycle, product life cycle, change management etc. They are based on the assumption that there are predictable patterns in the growth of organizations, IT maturity, and the growth of living organisms that can be presented as stages or phases (Gottschalk & Solli-Sæther, 2009, p.109). According to King and Teo (1997) these stages are sequential in nature, describe a hierarchical progression that is not easily reversed and include a wide variety of organizational activities and structures.

One of the first stage models presented in IT research is the stage hypothesis of Nolan (1973) which suggested that the activities related to managing the computer resource follow a pattern of growth correlated to four stages of the computer budget: Stage I- computer acquisition, Stage II – intense system development, Stage III- proliferation of controls, and Stage IV- user/service orientation. Individual tasks for managing computer resources were related to each stage in order to describe them.

A model for the stages of growth of end user computing was presented by Huff, Munro and Martin (1988), where the extent of interconnectedness among applications was

considered as an index of growth, defining five different stages: “Isolation”, “Stand-alone”, “Manual integration”, “Automated Integration”, and “Distributed Integration”.

Earl (2000) suggested a six-stage process that corporations are likely to experience during the transition period of becoming e-businesses. The model, which is based on observations and studies on start-ups and companies that wanted to transform into e-businesses, consists of the following stages: “External Communications”, “Internal Communications”, “E-commerce”, “E-business”, “E-enterprise”, and “Transformation”.

Teo and Pian (2004) introduced a model for Web adoption that consists of five levels, by examining organizations’ Internet strategies and the functional characteristics of their Web sites. On the other hand, there are stage models in IT research that were developed by using benchmark variables in order to define each stage of the model. Such examples are the stage models of data warehousing growth (Watson, Ariyachandra and Matyska, 2001), intranet implementation (Damsgaard & Scheepers, 2000) and IT outsourcing relationships (Gottschalk and Solli-Sæther, 2006).

Stage models are quite common in eGovernment research too. Layne and Lee (2001) presented a four-stage model of eGovernment development based on observations of eGovernment initiatives at United States. The model uses the key dimensions “Technological and Organizational Complexity” and “Integration” to explain the four stages of eGovernment growth: “Catalogue”, “Transaction”, “Vertical Integration”, and “Horizontal Integration”. Andersen and Henriksen (2006) proposed an extension of the stage model of Layne and Lee, named Public Sector Process Rebuilding (PPR) model. In contrast to Layne and Lee’s model, the PPR model uses “Activity centric applications” and “Customer centric” as dimensions for explaining the four stages of the model, which are: “Cultivation”, “Extension”, “Maturity”, and “Revolution”.

The European Commission (2009) presented a five-stage maturity model that indicates how public organizations interact with citizens and businesses. The stages that are used to describe governments’ service delivery processes are: “information”, “one-way interaction”, “two-way interaction”, “transaction” and “targetisation”.

West (2004) identified the following stages of eGovernment transformation: “the billboard stage”, “the partial-service-delivery stage”, “the portal stage” and “interactive democracy”. Deloitte Research (2000) on the other hand, suggested that eGovernment transformation goes through the stages of “Information Publishing”, “Official Two-Way

Transactions", "Multi-Purpose Portals", "Portal Personalization", "Clustering of Common Services", and "Full Enterprise Transformation". Another stage model for eGovernment is the one proposed by Hiller and Bélanger (2001), consisting of five stages: "Information", "Two-way communication", "Transaction", "Integration" and "Political participation". Lee (2010) followed a "qualitative meta-synthesis" approach by reviewing and translating the stages of twelve eGovernment stage models. The framework that was synthesized by this procedure has as dimensions the "Citizen/Service Perspective" and the "Operation/Technology Perspective" and as stages the "Presenting" stage, the "Assimilating" stage, the "Reforming" stage, the "Morphing" stage and the "e-Governance" stage.

Stage models are less frequently found in cloud computing research, since the topic is relatively new. Dowell et al. (2011) suggested a maturity model for cloud computing interoperability based on US Department of Defense's LISI Maturity Model. The model focuses on the characteristics of interoperability in cloud computing and aims to assess its maturity. It consists of five levels: "Level 0 – Domain-based interoperability", "Level 1- Enterprise interoperability", "Level 2 – Portability interoperability", "Level 3 –Security interoperability" and "Level 4 – Mobile interoperability". A "Cloud Maturity Model" was presented in a white paper by Oracle (2011) that aims to help companies measure the progress of a Cloud initiative and identify specific capabilities that are needed in order to adopt cloud computing successfully. The model, which measures both maturity and adoption levels of cloud capabilities (Figure 33), defines different levels of adoption ("No implementation", "Discrete Resources", "Across Collections", "Across Pools", "Across Units", "Across Clouds") and maturity ("None", "Ad Hoc", "Opportunistic", "Systematic", "Managed", "Optimized").

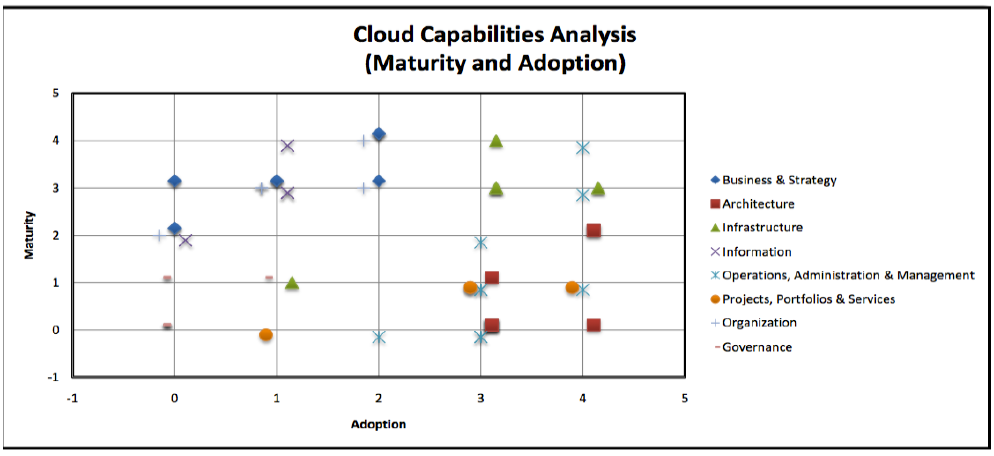

Figure 33: Plotting the Cloud Maturity Model (Oracle, 2011)

6.3. The Proposed Stage Model

The stage model presented in this section, has been developed by following the general principles of stage modeling procedure suggested by Solli-Sæther and Gottschalk (2010). According to them, a suggested stage model evolves to its final state (Revised Stage Model), through a process that has the following intermediate states: "Conceptual Stage Model", "Theoretical Stage Model" and "Empirical Stage Model". While "Conceptual Stage Model" and "Theoretical Stage Model" are based on analyzing case studies and defining benchmark variable respectively, "Empirical Stage Model" is based on survey results. It should be noted that the proposed stage model has not been empirically tested, thus it should be considered as a theoretical model. Its aims are to help governments define their progress in adopting cloud computing and to promote further research in this field.

As can be seen in Figure 34, the proposed model consists of four stages. The horizontal axis represents the degree of cloud computing adoption in eGovernment (in how many agencies/public organizations cloud computing is used and to what extent), and the vertical the organizational and technological complexity of the solutions included in each stage.

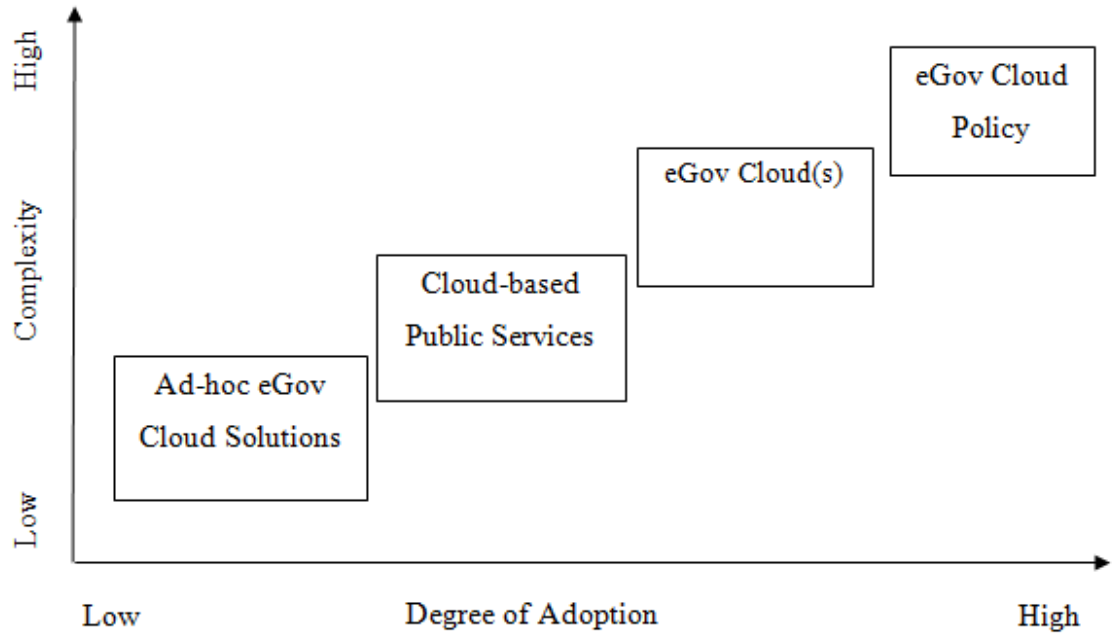

Figure 34: A Stage Model for Cloud Computing Adoption in eGovernment

It should be noted that the model neither depends on time nor presents a "must-go" path. Different agencies or public organizations in a country may use cloud computing

in various ways that fall into different stages of the model, but what this stage model examines is the further a government has gone in adopting cloud computing.

A number of variables have also been defined based on the literature review and the comparison and analysis of case studies. The variables, which are used in order to describe the basic characteristics of each stage, are:

- Type of services – examines whether the services provided with the use of cloud computing are internal (the recipients are government agencies) or public (the recipients are citizens or businesses).
- Provider – examines whether the provider of cloud services is an individual vendor or government department
- Decision level – examines whether the decisions related to cloud computing use are made at municipal/agency or government level
- Degree of engagement – indicates how difficult it is for the agency/government to reverse the decision to adopt cloud computing
- Main change in – indicates the main change that occurs in a stage and differentiates it from the others.

Table 11 shows the main differences among the stages of the proposed model. The detailed description of each stage can be found in the subsections that follow.

Table 11: Main differences among stages

Stages / Variables	Stage 1: Ad-hoc eGov Cloud Solutions	Stage 2: Cloud-based Public Services	Stage 3: eGov Cloud(s)	Stage 4: eGov Cloud Policy
Type of services	Internal (agencies)	External (citizens and businesses)	Internal and External	Internal and External
Provider	Individual vendors	Individual vendors	Government	Government and Individual vendors

Decision Level	Agency/ Municipal	Agency/ Municipal	Agency/ Government	Government/ Federal
Degree of engagement	Very low	Low	High	Very High
Main change in	Procurement of IT services for government	Provision of public services	Architecture of eGovernment systems	Government IT strategy

6.3.1. Stage 1: Ad-hoc eGov Cloud Solutions

At this stage agencies or public organizations use cloud computing only for covering their needs in IT resources and enhancing collaboration with other agencies, and not for providing digital services to citizens or businesses. Since there is no Government Cloud, the cloud services (basically SaaS and IaaS) are entirely provided by individual vendors. In an absence of an official government policy, each agency or municipality decide how and to what extent it will use cloud services on its own. This is the reason why the adoption of cloud computing in this stage is assumed to be sporadic. With no central guidance or familiarity with cloud computing concept, there will be few agencies/public organizations that will attempt to use cloud computing, and probably this use will be limited to a number of pilot services. Thus, the degree of adoption in this stage should be low.

The organizational complexity of this stage is expected to be low too, considering that the change that happens is internal and limited. As for the technological complexity, the organization continues to operate in the way it used to, without any technological change. The provision of cloud services in this stage can be considered as a form of outsourcing. For this reason, the degree of engagement is also assumed to be very low and the agencies can return to the previous situation quite easily. The low degree of adoption combined with the low technological/organizational complexity places this stage of the model near the origin of the axes.

An example of this stage would be the implementation of the “Government to Cloud” or “Government to Cloud to Government” business model (described at §4.3.1.), proposed by Deussen et al. (2011). A more tangible example that belongs in that stage is the case

of “Apps.Gov” portal of US Government. Although in that case there was an involvement of the central government, the agencies were the ones that decided whether they would use cloud services for their internal operations and which services they would procure. The fact that the portal was closed in December 2012 is consistent with the low engagement which characterizes this stage, and shows that that kind of initiatives alone are not enough for the consolidation of cloud computing in eGovernment.

6.3.2. Stage 2: Cloud- based Public Services

At this stage, cloud computing is used by agencies and municipalities in order to provide digital public services to citizens and businesses. The public services are based on PaaS provided by individual vendors and the decisions related to cloud computing are still made at agency or municipal level. The degree of engagement is still low since the government holds also in this stage only the role of the customer of cloud services, but the fact that there are more stakeholders (citizens and businesses) in this case makes the return to the previous state more difficult.

This is the stage where cloud computing can promote Open Innovation and Open Data Initiatives (Charalabidis et al., 2011; Jiricek and Massimo, 2011; Zhang, 2010). Since cloud solutions that appear at this stage are more sophisticated and are not limited to use of SaaS or storage services, there is an increase in technological complexity. Organizational complexity is also increased due to the use of cloud computing for interaction with citizens.

Furthermore, the decision to deploy PaaS solutions for providing eGovernment services implies a higher degree of awareness of cloud computing on the part of government officials. The cloud based platforms for eGovernment services that have been proposed in literature (Charalabidis et al., 2011; Taher et al., 2011) require the active participation of organizations’ administrators in the designing process of the services. This involvement of agencies’ personnel should result in further familiarization with cloud computing and make agencies less reluctant to use it to a greater extent. It should also not be forgotten that the presence of agencies in a government that deliver public services through PaaS, does not prevent the existence of agencies whose cloud use falls into the first stage. It is therefore proposed that the degree of adoption for governments that have reached the second stage is higher than the degree that corresponds to the first

stage. The increase in both organizational/technological complexity and degree of adoption that occurs in this stage places it above and to the right of the first stage.

The business models "Government to Cloud to Enterprise" and "Government to Cloud to Citizen" suggested by Deussen et al. (2011) describe possible examples that fall into this stage. Moreover, as was discussed in the Case Studies section, the City of Edmonton in Canada has already used cloud computing platform in order to offer census data and other public information online.

6.3.3. Stage 3: eGov Cloud(s)

The main change in this stage is the development of one or more government clouds. These private clouds can belong either to the central government or more often, to agencies or government organizations. They are used in order to replace the former eGovernment information systems that the organization had and can support the provision of both internal and public services. The fact that a private cloud offers more security and control than the other deployment models may encourage the organization to use cloud computing more broadly. There are also some cases where the agency handles sensitive government data and the development of its own private cloud is the only way to adopt cloud computing.

The turn of the government from customer of cloud services to owner of a Cloud, increases the organizational complexity along with the degree of engagement. Although it is not impossible in theory to quit the use of cloud computing in the future, it is highly unlikely that the organization will leave its own cloud to turn again to traditional computing. While in theory a private cloud can be operated by a third party, in practice the public organizations choose to build an on-premises cloud. This can be attributed either to their distinctive security requirements, or to the fact that government organizations usually have their own data center and want to utilize its resources.

A lot of technological changes take place in this stage, with the virtualization of the data center being the most significant. The organization is also responsible for the security of the virtualized data center, so technological changes will probably occur in this field too. These changes, which are not found in the previous stages, increase the technological complexity of this stage.

A typical example of a government cloud is the OpenGov Private Cloud of Greek Government that accommodates various applications of eGovernment. At the agency

level, the cases of US DoD and NASA illustrate how cloud computing can be incorporated in public organizations with special needs in terms of security and control.

As the above examples indicate, private clouds are usually developed either by large public organizations that their considerable needs in IT resources justify such a decision or by governments that intend to use cloud computing for hosting their central information systems but they want to have the control of the IT resources they use. In either case, the government or organization will have to follow an organized approach or strategy in order to move its information systems to a cloud environment (the US DoD's Cloud Computing Strategy presented in literature review is such an example). The degree of adoption in this stage is expected to be higher than the previous due to the organized effort and the number of units/agencies that large organizations/governments include.

6.3.4. Stage 4: eGov Cloud Policy

At this final stage cloud computing adoption is fully supported by the central government of a country. While in the other stages the use of cloud computing is usually a result of individual initiatives of agencies and municipalities, here the central government promotes cloud adoption in eGovernment through policies and roadmaps. The coordinated effort for integrating cloud computing in eGovernment that takes place at this stage has as a result a very high degree of engagement.

A special IT strategy is developed to facilitate cloud deployment by all departments of the government, and the government clouds that in Stage 3 were sporadic at this stage are becoming common. In addition, the government encourages smaller agencies and public organizations that have not developed private clouds to procure cloud services from individual vendors, by establishing a cloud marketplace for public sector. In that way, the quality of cloud services can be ensured and the procedure of IT procurement can be easier for agencies. Successful initiatives in this stage should lead to the highest degree of adoption for a government. Even small agencies will be motivated to try cloud computing through the information and guidelines that central government provide.

The diffusion of cloud computing in the whole eGovernment system of a country raises also complexity since the organizational changes that happen in this stage are significant. At this point, the change of mindset from assets to services, which is a step of many cloud adoption strategies (Frost & Sullivan, 2011; Kundra, 2011; US DoD, 2012), occurs. In contrast to the previous stages, the change here refers to the IT culture

of the government. The government should also take steps in order to resolve the legal issues that according to many scholars (Clemons & Chen, 2011; Hada et al., 2012; Macias &Thomas, 2011b; Zissis & Lekkas, 2011) hinder the adoption of cloud computing in eGovernment.

Another important issue that should be resolved in this stage is the absence of standards. As NIST (2011b) recommended, cloud computing standards should be developed and used widely from government agencies to support government's requirements for interoperability, portability and security. In the previous stages, cloud computing is adopted for covering the needs of individual public organizations or central governments and the related decisions do not affect other organizations or agencies outside of organization's/government's direct authority. In this stage, for the diffusion of cloud computing in the whole government, standards are necessary to insure the interoperability of the different information systems. The development of technological standards characterizes the technological complexity of this stage, which is considered to be very high.

Although there are no countries that have reached this stage yet, it seems that United States and United Kingdom, which both have launched cloud initiatives, aim at this direction. EU has also made steps towards establishing a cloud strategy by publishing cloud related roadmaps (European Commission, 2012a).

6.4. Conclusions

In this chapter a stage model for cloud computing adoption in eGovernment is presented. The model measures the degree of cloud computing adoption and the organizational and technological complexity this entails, and defines the following four stages: "Ad-hoc eGov Cloud Solutions", "Cloud-based Public Services", "eGov Cloud(s)" and "eGov Cloud Policy". Unlike other stage models, this one does not suggest that its stages are necessarily sequential in nature. It presents a hierarchical progression in cloud adoption by public sector, as the sophistication and extent of cloud computing use raise. The model can be used by governments to define their progress in cloud computing adoption and decide their next steps. Also it aims to trigger further research at the topic, since it is a relatively new field.

A limitation of the model, which at the same time can be considered as a suggestion for future work, is that it is not validated through empirical work. Further research might

also investigate how the general benefits and challenges of cloud adoption in eGovernment differ from stage to stage.

7. Conclusions and future work

As the research related to the use of cloud computing in eGovernment started quite recently, the number of studies published in this topic is relatively limited. This dissertation presented an extended literature review in order to promote further research in the topic, by mapping the areas in which scholars have already published studies and identifying the areas that are still unexplored. The conceptual map that is presented in Chapter 4 and was the first goal of this dissertation indicates the main areas of current research, which are: the examination of suitability of cloud computing for supporting eGovernment, strategies for adopting cloud computing successfully and implementation of cloud solutions in eGovernment. While some sub-areas have drawn the attention of many researchers, such as the identification of benefits and risks of cloud adoption in eGovernment and the development of cloud architectures for eGovernment, there are other sub-areas that clearly need further research. The frameworks and models that have been proposed so far obviously do not cover all needs of governments. The discussion about open data has been intensified lately, so further examination of how cloud computing can promote open data initiatives would be welcomed. The development of secured cloud architectures for eGovernment is also important, since security is one of the main challenges in cloud adoption by governments.

In regard to the question of whether cloud computing should be used in eGovernment, the unique characteristics of each case should be taken into consideration. The researchers draw attention to the following issues:

- Governments should take steps towards standardizing and ensuring quality of services.
- Although the general migration strategies that have been presented can be applied almost in any situation, it is advisable that each organization develops a strategy that covers its own requirements.
- Cloud computing is not “all or nothing”. Organizations can choose from the four deployment models the one that best suits their requirements. A SWOT analysis can help in that direction.
- Cloud computing will probably bring about more or less changes in the way some services are delivered. The stakeholders should be properly informed in order to accept these changes.

The case studies examined in Chapter 5, answered the other question of the introduction about the ways that governments around the world deploy cloud computing for supporting eGovernment. The analysis of the cases showed that the complexity of the cloud solutions and the extent to which these are applied in eGovernment system, differ from country to country. This finding, in conjunction with the different aspects from which the topic has been viewed in literature, led to the proposal of a stage model that classifies the different ways of adoption. The proposed stage model, which was the second goal of this study, can be used to determine the progress of a government in cloud computing adoption, but is also intended to start a discussion in the topic, since it is the first stage model of this kind.

Limitations

This study is limited in the following aspects:

1. Although there was an attempt to keep pace with new studies that were published after the process of literature research was over, it is possible there are new published papers that have been missed.
2. As it was mentioned in the relative chapter, for the time being the proposed stage model is theoretical and has not been validated by any primary research.
3. The proposed stage model takes into account the government as a whole and realizes the agencies and other government organizations as parts of it. Obviously, an agency could never reach the fourth stage of the model since it does not make centralized decisions and does not publish policies that affect other agencies. Thus, the proposed stage model cannot be used to evaluate cloud adoption at agency level.

Suggestions for further research

Apart from the research gaps that were identified by the literature review and were mentioned at the beginning of this chapter, there are also other topics that can be subjects of further research. The validation of the proposed stage model is one of them. Also, the case studies that can be found in literature come from secondary sources. A primary research, which would include questionnaires or interviews with public administrators, would probably provide more information about the use of cloud computing in the government that would be studied. In that way, the benefits and risks

of cloud computing in eGovernment that have been suggested in literature could be validated too.

References

AlAjmi, K. (2011). Is Cloud Computing Appropriate for Government? Proceedings from EEE2011: *2011 International Conference on E-Learning, E-Business, Enterprise Information Systems,& E-Government*, (pp. 169-175). Retrieved from: http://world-comp.org/p2011/EEE2645.pdf

Alshehri, M. & Drew, S. (2010). E-Government Fundamentals. Proceedings from *2010 IADIS International Conference ICT, Society and Human Beings*, (pp. 35-42). Retrieved from: http://www98.griffith.edu.au/dspace/bitstream/handle/10072/37709/67525_1.pdf?sequence=1

Andersen, K. V. & Henriksen, H. Z. (2006). E-government maturity models: Extension of the Layne and Lee model. *Government Information Quarterly*, 23(2), 236-248. doi: 10.1016/j.giq.2005.11.008

Armbrust, M., Fox, A., Griffith, R., Joseph, A.D., Katz, R., Konwinski, A., …Zaharia, M. (2009). *Above the Clouds: A Berkeley View of Cloud Computing* (Technical Report No. UCB/EECS-2009-28). Retrieved from: http://www.eecs.berkeley.edu/Pubs/TechRpts/2009/EECS-2009-28.pdf

Bhisikar, A. (2011). G-Cloud: New Paradigm Shift for Online Public Services. *International Journal of Computer Applications*, 22 (8), 24-29. Retrieved from http://www.ijcaonline.org/volume22/number8/pxc3873629.pdf

Breil, A., Hitzelberger, P., Da Silva Carvalho, P. and Feltz, F. (2012). Exploring Data Integration Strategies for Public Sector Cloud Solutions. In A. Ko et al. (Eds), Proceedings from *EGOVIS/EDEM 2012, Lecture Notes in Computer Science*, Vol. 7452, (pp.271-278). doi: 10.1007/978-3-642-32701-8_24

Cabinet Office (2011). *Government Cloud Strategy: A sub strategy of the Government ICT Strategy*. [White Paper]. Retrieved from Cabinet Office, HM Government's website: http://www.cabinetoffice.gov.uk/sites/default/files/resources/government-cloud-strategy_0.pdf

Cellary, W., & Strykowski, S. (2009). E-Government Based on Cloud Computing and Service-Oriented Architecture. Proceedings from ICEGOV '09: *3rd*

International Conference on Theory and Practice of Electronic Governance, (pp. 5-10) doi: 10.1145/1693042.1693045

Chanchary, F. H. & Islam, S. (2011). E-government Based on Cloud Computing with Rational Inference Agent. Proceedings from HONET 2011: *High Capacity Optical Networks and Enabling Technologies*, (pp. 261-266). doi: 10.1109/HONET.2011.6149830

Chandra, D.G. & Malaya, D.B. (2011). Problems & Prospects of e-Governance in India. Proceedings from *2011 World Congress on Information and Communication Technologies (WICT)*, (pp. 42-47). doi: 10.1109/WICT.2011.6141215

Charalabidis, Y., Koussouris, S. and Ramfos, A. (2011). A Cloud Infrastructure for Collaborative Digital Public Services. Proceedings from CloudCom 2011: *IEEE Third International Conference on Cloud Computing Technology and Science*, (pp. 340-347). doi: 10.1109/CloudCom.2011.53

Chuob, S., Pokharel, M. and Park, J.S. (2010). The Future Data Center for E-Governance. Proceedings from ICACT 2010: *The 12th International Conference on Advanced Communication Technology* (pp. 203-207). Retrieved from: http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=5440476&url=http%3A%2F%2Fieeexplore.ieee.org%2Fxpls%2Fabs_all.jsp%3Farnumber%3D5440476

Chuob, S., Pokharel, M. and Park, J.S. (2011). Modeling and Analysis of Cloud Computing Availability based on Eucalyptus Platform for E-Government Data Center. Proceedings from IMIS 2011: *Fifth International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing* (pp. 289-296). doi: 10.1109/IMIS.2011.135

Clemons, E.K. & Chen, Y. (2011). Making the Decision to Contract for Cloud Services: Managing the Risk of an Extreme Form of IT Outsourcing. Proceedings of the *44th Hawaii International Conference on System Sciences* (pp. 1-10) doi:10.1109/HICSS.2011.292

Craig, R., Frazier, J., Jacknis, N., Murphy, S., Purcell, C., Spencer, P. and Stanley, JD (2009). *Cloud Computing in the Public Sector: Public Manager's Guide to Evaluating and Adopting Cloud Computing*. [White Paper]. Retrieved from

Cisco website: http://www.cisco.com/web/about/ac79/docs/sp/Cloud_Computing.pdf

Damsgaard, J. & Scheepers, R. (2000). Managing the crises in intranet implementation: a stage model. *Information Systems Journal*, 10(2), 131-149. doi: 10.1046/j.1365-2575.2000.00076.x

Das, R. K., Patnaik, S., Misro, A. K. (2011). Adoption of Cloud Computing in e-Governance. In Meghanathan, et al. (Eds), *Communications in Computer and Information Science,* Vol 133, 161-172. doi: 10.1007/978-3-642-17881-8_16

Deloitte Research (2000). *At the dawn of E-Government: The citizen as customer*. [White Paper]. Retrieved from: http://www.egov.vic.gov.au/pdfs/e-government.pdf

Deussen, P., Eckert, K.P., Strick, L. and Witaszek, D. (2011). *Cloud Concepts for the Public Sector in Germany- Use Cases.* [White Paper]. Retrieved from Fraunhofer FOKUS website: http://www.interoperability-center.com/c/document_library/get_file?uuid=9176f0fa-1ea2-4771-b8e0-a3f9c685199f&groupId=12725

Dowell, S., Barreto, A., Michael, J.B. and Shing, M.T. (2011). Cloud to Cloud Interoperability. Proceedings from SoSE 2011: *6th International Conference on System of Systems Engineering*, (pp. 258-263). doi: 10.1109/SYSOSE.2011.5966607

Earl, M.J. (2000). Evolving the E-Business. *Business Strategy Review*, 11(2), 33-38. doi: 10.1111/1467-8616.00135

Ebrahim, Z. and Irani, Z. (2005). E-government adoption: architecture and barriers. *Business Process Management Journal*, 11(5), 589-611. doi: 10.1108/14637150510619902

Elbadawi, I. (2011). Cloud Computing for E-Government in UAE: Opportunities, Challenges and Service Models. Proceedings from ICEGOV '11: *5th International Conference on Theory and Practice of Electronic Governance*, (pp. 387-388) doi: 10.1145/2072069.2072155

European Commission (2009). *Smarter, Faster, Better eGovernment. 8th eGovernment Benchmark Measurement, November 2009.* Retrieved from: http://ec.europa.eu/information_society/eeurope/i2010/docs/benchmarking/egov_benchmark_2009.pdf

European Commission (2012a). *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions – Unleashing the Potential of Cloud Computing in Europe* (Report No. COM (2012) 529 final). Retrieved from: http://ec.europa.eu/information_society/activities/cloudcomputing/docs/com/com_cloud.pdf

European Commission. (2012b). *Accompanying the document: Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions – Unleashing the Potential of Cloud Computing in Europe* (Report No. SWD(2012) 271 final). Retrieved from: http://ec.europa.eu/information_society/activities/cloudcomputing/docs/com/swd_com_cloud.pdf

European Network and Information Security Agency (ENISA) (2011). *Security & Resilience in Governmental Clouds: Making an Informed Decision*. [White Paper]. Retrieved from ENISA website: http://www.enisa.europa.eu/activities/risk-management/emerging-and-future-risk/deliverables/security-and-resilience-in-governmental-clouds/

Fountain, J. E. (2001). *Building the Virtual State: Information Technology and Institutional Change.* Washington, DC: Brookings Institution Press.

Fraunhofer- FOKUS (2012), "goBerlin – Marketplace for trustworthy governmental and business services". Available at: http://www.fokus.fraunhofer.de/en/elan/projekte/national/go_berlin/index.html (December 2 2012).

Frost & Sullivan. (2011). *State of Cloud Computing in the Public Sector – A Strategic analysis of the business case and overview of initiatives across Asia Pacific.* [White Paper]. Retrieved from Frost& Sullivan's website: http://www.frost.com/prod/servlet/cio/232651119

Germany Trade & Invest (2012), "Public Sector Applications". Available at: http://www.gtai.de/GTAI/Navigation/EN/Invest/Industries/Smarter-business/Smart-systems/public-sector-applications,did=624572.html (December 2 2012).

Gottschalk, P. & Solli-Sæther, H. (2006). Maturity model for IT outsourcing relationships. *Industrial Management & Data Systems*, 106(2), 200-212. doi: 10.1108/02635570610649853

Gottschalk, P. & Solli-Sæther, H. (2009). *E-Government Interoperability and Information Resource Integration: Frameworks for Aligned Development*. Hershey, PA: Information Science Reference.

Guan, Y. (2009). A Statistical CPID Algorithm on Cloud Computing. Proceedings from FCC 2009: *International Conference on Future Computer and Communication*, (pp. 101-104). doi: 10.1109/FCC.2009.27

Hada, P. S., Singh, R. and Goyal, D. (2012). Security Engineering in G-Cloud: A Trend towards Secure e-Governance. *International Journal of Computer Applications*, 46(13), 33-38. doi: 10.5120/6972-9536

Hiller, J.S. & Bélanger, F. (2001). *Privacy Strategies for Electronic Government*. [White Paper]. Retrieved from IBM Center for The Business of Government: http://www.businessofgovernment.org/report/privacy-strategies-electronic-government

Hobson, S., Anand, R., Yang, J., Liu, X. and Lee, J. (2011). Municipal Shared Services Cloud. Proceedings from SRII 2011: *2011 Annual SRII Global Conference*, (pp. 285-292). doi: 10.1109/SRII.2011.39

Hu, G., Pan, W., Lu, M. and Wang, J. (2009). The widely shared definition of e-Government: An exploratory study. *The Electronic Library*, 27(6), 968-985. doi: 10.1108/02640470911004066

Huff, S.L., Munro, M.C. and Martin, B.H. (1988). Growth Stages of End User Computing. *Communications of the ACM*, 31(5), 542-550.

Hung, C.F., Tuan, C.C. and Chu, Y.C. (2011). Constructing a Private Cloud for Government IT Services Consolidation– Taiwan's Experience. Proceedings

from IMIS 2011: *Fifth International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing*, (pp. 561-566). doi: 10.1109/IMIS.2011.102

IBM (2011). *IBM's Smarter Cities Challenge Report: Edmonton*. Retrieved from Edmonton City's website: http://www.gov.edmonton.ab.ca/transportation/SmarterCitiesChallengeReport.pdf

International Telecommunication Union (2012). *Focus Group on Cloud Computing Technical Report Part1: Introduction to the cloud ecosystem: definitions, taxonomies, use cases and high- level requirements* (Version 1.0, 2/2012). Retrieved from ITU website: http://www.itu.int/ITU-T/newslog/Cloud+Computing+And+Standardization+Technical+Reports+Published.aspx

Janssen, M. & Joha, A. (2011). Challenges for Adopting Cloud-based Software as a Service (SaaS) in the Public Sector. Proceedings from ECIS 2011: *European Conference on Information Systems* (paper 80). Retrieved from: http://aisel.aisnet.org/ecis2011/80/

Jiricek, Z. & Di Massimo, F. (2011). Microsoft Open Government Data Initiative (OGDI), Eye on Earth Case Study. In J. Hřebíček, G. Schimak, and Denzer, R. (Eds), Proceedings from *ISESS 2011, IFIP Advances in Information and Communication Technology*, Vol. 359, (pp. 26-32). doi: 10.1007/978-3-642-22285-6_3

Karounos, T., Mpouras, C., Priftis, T., Athanasiou, S., Zamani, T., Karamanolis, G., …Psalidas, M. (2012). Παρουσίαση Δράσεων Ομάδας Ηλεκτρονικής Διακυβέρνησης (in Greek), Presentation of eGovernment Group's activities. [White paper]. Retrieved from http://government.gov.gr/wp-content/uploads/2012/05/Παρουσίαση-δράσεων-Ηλεκτρονικής-Διακυβέρνησης.pdf

Khan, F., Zhang, B., Khan, S. and Chen, S. (2011). Technological Leap Frogging e-Government Through Cloud Computing. Proceedings from IC-BNMT 2011: *4th IEEE International Conference on Broadband Network and Multimedia Technology*, (pp. 201-206). doi: 10.1109/ICBNMT.2011.6155925

Kim, M., Kim, J.S. and Lee, H.O. (2012). Analysis of the Adoption Status of Cloud Computing by Country. In J.J. (Jong Hyuk) Park et al. (Eds), *Embedded and Multimedia Computing Technology and Service, Lecture Notes in Electrical Engineering*, Vol. 181, (pp. 467-476). doi: 10.1007/978-94-007-5076-0_57

Kim, Y.H., Lim, I.K., Kang, S.G. and Lee, J.K. (2011). Mobile Cloud e-Gov Design and Implementation Using WebSockets API. In J.J. Park, L.T. Yang and C. Lee (Eds), Proceedings from *FutureTech 2011, Part I, Communications in Computer and Information Science*, Vol. 184, (pp. 204-211). doi: 10.1007/978-3-642-22333-4_25

King, W.R. & Teo, T.S.H. (1997). Integration Between Business Planning and Information Systems Planning: Validating a Stage Hypothesis. *Decision Sciences*, 28(2), 279-308.

Klems, M., Nimis, J. and Tai, S. (2009). Do Clouds Compute? A Framework for Estimating the Value of Cloud Computing. In C. Weinhardt, S. Luckner and J. Stößer (Eds), *Designing E-Business Systems. Markets, Services and Networks. Lecture Notes in Business Information Processing*, Vol. 22, (pp. 110-123). doi: 10.1007/978-3-642-01256-3_10

Kundra, V. (2011). *Federal Cloud Computing Strategy*. [White Paper]. Retrieved from CIO.GOV website: https://cio.gov/wp-content/uploads/downloads/2012/09/Federal-Cloud-Computing-Strategy.pdf

Kurdi, R., Taleb-Bendiab, A., Randles, M. and Taylor, M. (2011). E-Government Information Systems and Cloud Computing (Readiness and Analysis). Proceedings from DeSE 2011: *Developments in E-systems Engineering* (pp. 404-409). doi: 10.1109/DeSE.2011.33

Layne, K. & Lee, J. (2001). Developing fully functional E-government: A four stage model. *Government Information Quarterly*, 18(2), 122-136. doi: 10.1016/S0740-624X(01)00066-1

Lee, J. (2010). 10 year retrospect on stage models of e-Government: A qualitative meta-synthesis. *Government Information Quarterly*, 27(3), 220-230. doi: 10.1016/j.giq.2009.12.009

Leikums, T. & Cevere, R. (2012). Electronic Document Management Outsourcing and Cloud Computing Possibilities for Public Sector. Proceedings from AICT 2012: *International Conference on Applied Information and Communication Technologies* (pp. 55-61). Retrieved from: http://aict.itf.llu.lv/files/rakstkraj/2012/leikums_aict2012.pdf

Liang, J. (2012). Government Cloud: Enhancing Efficiency of E-Government and Providing Better Public Services. Proceedings from IJCSS 2012: *2012 International Joint Conference on Service Sciences*, (pp.261-265). doi: 10.1109/IJCSS.2012.20

Macias, F. & Thomas, G. (2011a). *Cloud Computing Advantages in the Public Sector: How Today's Government, Education, and Healthcare Organizations Are Benefiting from Cloud Computing Environments*. [White Paper]. Retrieved from Cisco website: http://www.cisco.com/web/strategy/docs/c11-687784_cloud_omputing_wp.pdf

Macias, F. & Thomas, G. (2011b*). Cloud Computing Concerns in the Public Sector: How Government, Education, and Healthcare Organizations Are Assessing and Overcoming Barriers to Cloud Deployments*. [White Paper]. Retrieved from Cisco website: http://www.cisco.com/web/strategy/docs/gov/pscloudconcerns.pdf

Marasso, L., De Maggio, M., Chetta, V., Grieco, M., Elia, C. and Totaro, S. (2010). Allowing Citizens to Self-compose Personalized Services:A Cloud Computing Model. In R. Meersman et al. (Eds), Proceedings from *OTM 2010 Workshops: On the Move to Meaningful Internet Systems, Lecture Notes in Computer Science*, Vol. 6428, (pp. 41-42). doi: 10.1007/978-3-642-16961-8_12

Massonet, P., Naqvi, S., Ponsrad, C., Latanicki, J., Rochwerger, B. and Villari, M. (2011). A Monitoring and Audit Logging Architecture for Data Location Compliance in Federated Cloud Infrastructures. Proceedings from IPDPSW 2011: *2011 IEEE International Symposium on Parallel and Distributed Processing Workshops and Phd Forum*, (pp. 1510-1517). doi: 10.1109/IPDPS.2011.304

Mauro, A. (2012). Cloud Computing: U.S. and E.U. Government/ Military Approach. In F. De Paoli, E. Pimentel & G. Zavattaro (Eds.), Proceedings from *ESOCC 2012*,

Lecture Notes in Computer Science, Vol. 7592, (pp. 277-278). doi: 10.1007/978-3-642-33427-6_24

Mell, P. & Grance, T. (2011). *The NIST Definition of Cloud Computing: Recommendations of the National Institute of Standards and Technology (Special Publication 800-145).* Retrieved from: http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf

Miller, J., "GSA creating cloud marketplace for federal services", FederalNewsRadio, February 16 2012. Available at: http://www.federalnewsradio.com/445/2750996/GSA-creating-cloud-marketplace-for-federal-services (December 16 2012).

Mukherjee, K. & Sahoo, G. (2010). Cloud Computing: Future Framework for e-Governance. *International Journal of Computer Applications*, 7(7), 31-34. doi: 10.5120/1262-1613

Mukherjee, K. & Sahoo, G. (2011). Security Mechanism for C-Governance using Hadamard Matrices. Proceedings from ICCCT 2011: *2nd International Conference on Computer and Communication Technology*, (pp. 485-490). doi: 10.1109/ICCCT.2011.6075133

Mutavdžić, R. (2012). Decision Framework for Building Platform as a Service (PaaS) based Government Services. Proceedings from MIPRO 2012: *35th International Convention* (pp. 1655-1660). Retrieved from: http://ieeexplore.ieee.org/xpl/articleDetails.jsp?reload=true&arnumber=6240916

National Institute of Standards and Technology (NIST) (2011a). *US Government Cloud Computing Technology Roadmap Volume I Release 1.0* (Special Publication 500-293, Draft). Retrieved from: http://www.nist.gov/itl/cloud/upload/SP_500_293_volumeI-2.pdf

National Institute of Standards and Technology (NIST) (2011b). *US Government Cloud Computing Technology Roadmap Volume II Release 1.0* (Special Publication 500-293, Draft). Retrieved from: http://www.nist.gov/itl/cloud/upload/SP_500_293_volumeII.pdf

Nolan, R.L. (1973). Managing the Computer Resource: A Stage Hypothesis. *Communications of the ACM*, 16(7), 399-405.

OECD (2003). *The e-Government Imperative*. Paris, France: OECD Publications.

Oracle (2011). *Cloud Computing Maturity Model Guiding Success with Cloud Capabilities*. [White Paper]. Retrieved from Oracle's website: http://www.oracle.com/technetwork/topics/entarch/oracle-wp-cloud-maturity-model-r3-0-1434934.pdf

Paquette, S., Jaeger, P.T. and Wilson, S.C. (2010). Identifying the security risks associated with governmental use of cloud computing. *Government Information Quarterly*, 27, 245-253. doi: 10.1016/j.giq.2010.01.002

Patil, M. K. & Lolage, R. (2011). Cloud Computing Resource Management for Indian E-Governance. In V.V. Das and N. Thankachan (Eds), Proceedings from *CIIT 2011, Communications in Computer and Information Science*, Vol. 250, (pp. 392-395). doi: 10.1007/978-3-642-25734-6_60

Pokharel, M., & Park, J.S. (2009). Cloud Computing: Future solution for e-Governance. Proceedings from ICEGOV '09: *3rd International Conference on Theory and Practice of Electronic Governance*, (pp.409-410). doi: 10.1145/1693042.1693134

Prnjat, O. (2011). eGovernment and eScience Cloud Initiatives in Greece. [PowerPoint slides]. Presented at Cloud Policy Workshop: "Cloud Technology for e-Government and Beyond", April 13 2011. Retrieved from: http://indico.admin.grnet.gr/indico/conferenceDisplay.py?showSession=all&showDate=all&view=standard&fr=no&confId=15

Repschlaeger, J., Wind, S., Zarnekow, R. and Turowski, K. (2012). A Reference Guide to Cloud Computing Dimensions: Infrastructure as a Service Classification Framework. Proceedings from HICSS 2012: *45th Hawaii International Conference on System Science* (pp. 2178-2188). doi: 10.1109/HICSS.2012.76

Reza, M. (2012). Framework on Large Public Sector Implementation of Cloud Computing. Proceedings from ICCCSN 2012: *International Conference on Cloud Computing and Social Networking* (pp. 1-4). doi: 10.1109/ICCCSN.2012.6215749

Schubert, L. (2010). *The Future of Cloud Computing: Opportunities For European Cloud Computing Beyond 2010*. K. Jeffery and B. Neidecker-Lutz (Eds). Retrieved from: http://cordis.europa.eu/fp7/ict/ssai/docs/cloud-report-final.pdf

Sharma, R. & Kanungo, P. (2011). An Intelligent Cloud Computing Architecture Supporting e-Governance. Proceedings from *17th International Conference on Automation & Computing* (pp. 1-5). Retrieved from: http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=6084891&url=http%3A%2F%2Fieeexplore.ieee.org%2Fxpls%2Fabs_all.jsp%3Farnumber%3D6084891

Solli-Sæther, H. & Gottschalk, P. (2010). The Modeling Process for Stage Models. *Journal of Organizational Computing and Electronic Commerce*, 20(3), 279-293. doi: 10.1080/10919392.2010.494535

Spanish National Institute of Communication – INTECO (2012). *Study on cloud computing in the Spanish public sector*. [White paper]. Retrieved from INTECO website: http://www.inteco.es/file/FKvEuh_D_6xRK6a0e7iZKg

Staten, J., Nelson, L.E., Herald, A. and Yates, S. (2009). *Case Study: USA.gov Achieves Cloud Bursting Efficiency Using Terremark's Enterprise Cloud*. [Report]. Retrieved from Terremark's website: http://www.terremark.com/uploadedFiles/Industry_Solutions/Federal_Government/Case%20Study-%20USA.gov%20Achieves%20Cloud%20Bursting%20Efficiency%20Using%20Terremark's%20Enterprise%20Cloud.pdf

Stefanou, C.J. & Skouras, A. (2012). E-Government: Cloud Solutions in Labor Regulatory Area in Greece. Proceedings from 9th ICESAL 2012: *9th International Conference on Enterprise Systems, Accounting and Logistics* (pp. 390-406). Retrieved from: http://ergatika.gr/wp-content/uploads/2012/07/e-gov-cloud-solutions-9o-ICESAL.pdf

Tahamtan, A., Kern, R. & Tjoa, A.M. (2011). Integration of Cloud Computing in The Public Sector: A Case Study in the Austrian Government. Poster presented at *1st International Conference on Cloud and Green Computing (CGC 2011), Sydney, Australia.* Retrieved from: http://www.ifs.tuwien.ac.at/~tahamtan/Publications/Tahamtan_CGC-Poster.pdf

Taher, Y., Haque, R., Nguyen, D. K. and Van den Heuvel, W.J. (2011). Designing and Delivering Public Services on the Cloud. Proceedings from CLOSER 2011: *1st International Conference on Cloud Computing and Services Science* (pp.471-476). Retrieved from: http://ulir.ul.ie/bitstream/handle/10344/1707/2011_Taher.pdf?sequence=2

Teo, T.S.H. & Pian, Y. (2004). A model for Web adoption. *Information & Management*, 41(2004), 457-468. doi: 10.1016/S0378-7206(03)00084-3

Trifonov, R., Tashev, T. & Toteva, N. (2010). New Approach for Information Security in e-Government. Proceedings from *2010 International Conference on Applied Computer Science (ACS),* (pp. 636-638). Retrieved from: http://www.wseas.us/e-library/conferences/2010/Malta/ACS/ACS-104.pdf

Tripathi, A., & Parihar, B. (2011). E-governance challenges and cloud benefits. Proceedings from *2011 IEEE International Conference on Computer Science and Automation Engineering (CSAE),* (pp.351-354).doi: 10.1109/CSAE.2011.5953237

Tsaravas, C. & Themistocleous, M. (2011a). Cloud Computing & E-Government: Myth or Reality? Presented at *Transforming Government Workshop 2011 London, UK, March 17-18, 2011*. Retrieved from http://www.iseing.org/tgovwebsite/tgovworkshop2011/CRCPDF/tGOV-7/Paper%207.pdf

Tsaravas, C. & Themistocleous, M. (2011b). Cloud Computing and eGovernment: A Literature Review. Proceedings from EMCIS2011: *European, Mediterranean & Middle Eastern Conference on Information Systems 2011*, (pp. 154-164). Retrieved from: http://www.iseing.org/emcis/EMCISWebsite/EMCIS2011%20Proceedings/SCM16.pdf

UNESCO (2005). *E-Government Toolkit for Developing Countries*. [White Paper]. Retrieved from UNESCO website: http://unesdoc.unesco.org/images/0013/001394/139418e.pdf

United Nations & ASPA (2002). *Benchmarking E-government: A Global Perspective*. [White Paper]. Retrieved from United Nations' website: http://unpan1.un.org/intradoc/groups/public/documents/un/unpan021547.pdf

US Department of Defense (DoD) (2012). *Cloud Computing Strategy*. [White Paper]. Retrieved from DISA website: http://www.disa.mil/Services/~/media/Files/DISA/Services/Cloud-Broker/dod-cloud-strategy.pdf?new

Vidhya, P. (2013). Transforming Election Polling from Electronic Voting to Cloud as a Software Service in India. In N. Meghanathan et al. (Eds), Proceedings from the *Second International Conference on Advances in Computing and Information Technology, Advances in Intelligent Systems and Computing*, Vol. 177, (pp.225-232). doi: 10.1007/978-3-642-31552-7_24

Watson, H., Ariyachandra, T. and Matyska, R.J. (2001). Data Warehousing Stages of Growth. *Information Systems Management*, 18(3), 42-50. doi: 10.1201/1078/43196.18.3.20010601/31289.6

Webster, J. & Watson, R.T. (2002). Analyzing the Past to Prepare for the Future: Writing a Literature Review. *MIS Quarterly*, 26(2), pp. xiii-xxiii.

West, D.M. (2004). E-Government and the Transformation of Service Delivery and Citizen Attitudes. *Public Administration Review*, 64(1), 15-27. doi: 10.1111/j.1540-6210.2004.00343.x

Wyld, D.C. (2009). *Moving to the Cloud: An Introduction to Cloud Computing in Government*. [White Paper]. Retrieved from website of IBM Center for the Business of Government: http://www.businessofgovernment.org/sites/default/files/CloudComputingReport.pdf

Wyld, D.C. (2010a). The Cloudy Future of Government IT: Cloud Computing and the Public Sector Around the World. *International Journal of Web & Semantic Technology*, 1, 1-20. Retrieved from: http://airccse.org/journal/ijwest/papers/0101w1.pdf

Wyld, D.C. (2010b). Risk in the Clouds?: Security Issues Facing Government Use of Cloud Computing. In T. Sobh, and K. Elleithy (Eds), *Innovations in Computing*

Sciences and Software Engineering, Vol. 2010, (pp. 7-12). doi: 10.1007/978-90-481-9112-3_2

Yeh, C., Zhou, Y., Yu, H. and Wang, H. (2010). Analysis of E-Government Service Platform Based on Cloud Computing. Proceedings from ICISE 2010: *2nd International Conference on Information Science and Engineering*, (pp. 997-1000). doi: 10.1109/ICISE.2010.5690772

You, J., Sun, Y., Xu, T., Liu, J. and Liu, H. (2012). Research on G2G E-Government Information Sharing Cloud. *Advances in Information Sciences and Service Sciences*, 4(17), 577-586. doi: 10.4156/AISS.vol4.issue17.66

Zhang, Q., Cheng, L. and Boutaba, R. (2010). Cloud Computing: state-of-the-art and research challenges. *Journal of Internet Services and Applications*, 1(1), 7-18. doi: 10.1007/s13174-010-0007-6

Zhang, W. J. (2010). E-Open Government Based on Cloud Computing. Proceedings from EBM 2010: *2010 International Conference on Engineering and Business Management*, (pp. 5442- 5446). Retrieved from: http://www.scirp.org/proceeding/PaperInformation.aspx?paperID=10873&bookID=1272&bookTypeID=2

Zhang, W. & Chen, Q. (2010). From E-Government to C-Government via Cloud Computing. Proceedings from ICEE 2010: *International Conference on E-Business and E-Government* (pp. 679-682). doi: 10.1109/ICEE.2010.177

Zissis, D. & Lekkas, D. (2011). Securing e-Government and e-Voting with an open cloud computing architecture. *Government Information Quarterly*, 28, 239-251. doi: 10.1016/j.giq.2010.05.010

Appendix A: Related articles that did not meet inclusion criteria

Chander, S. & Kush, A. (2011). UID, Cloud Computing & E-Governance. Proceedings from the *5th National Conference; INDIA Com-2011, Computing for Nation Development.* Retrieved from: http://www.bvicam.ac.in/news/INDIACom%202011/75.pdf

Chivukula, S.P., Krovvidi, R. & Chivukula, A.S. (2011). Eucalyptus Cloud to Remotely Provision e-Governance Applications. *Journal of Computer Networks and Communications*, Vol 2011, 1-15. doi:10.1155/2011/268987

Di, R.H., Lv, H., Wang, T., Zhang, X.T. & Xiao, D.M. (2011). Research on the Impact of Cloud Computing Trend on E-government Framework [in Chinese]. Proceedings from *2011 International Conference on E-Business and E-Government (ICEE)*, (pp 1-4). doi: 10.1109/ICEBEG.2011.5886913

Khare, A. B., Raghav, V. & Sharma, P. (2012). Cloud Computing Based Rural E-Governance Model. *Journal of Information and Operations Management*, 3(1), 89-91. Retrieved from: http://www.bioinfo.in/uploadfiles/13316170003_1_18_JIOM.pdf

Mutavdžic, R. (2010). Cloud Computing Architectures for National, Regional and Local Government. Proceedings from the *33rd International Convention MIPRO*, (pp. 1322-1327). Retrieved from: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5533680&isnumber=5533310

Oh, J., Yoon, Y.B., Suh, J.R. & Lee, B.G. (2012). The Difference of Awareness between Public Institutions and Private Enterprises for Cloud Computing Security. *International Journal of Security and Its Applications*, 6(3), 1-9. Retrieved from: http://www.sersc.org/journals/IJSIA/vol6_no3_2012/1.pdf

Prasad, A., Chaurasia, S., Singh, A. & Gour, D. (2010). Mapping Cloud Computing onto Useful e-Governance. *International Journal of Computer Science and Information Security*, 8(5), 129-133. Retrieved from: http://arxiv.org/abs/1009.2314

Prasad, S. R. & Atukuri, V. R. (2012). Cloud Computing Technology for Effective e-Governance. *International Journal of Computer Science and Information Technologies*, 3(1), 3241-3244. Retrieved from: CiteSeer

Rastogi, A. (2010). A Model based Approach to Implement Cloud Computing in E-Governance. *International Journal of Computer Applications*, 9(7), 15-18. doi:10.5120/1399-1888

Sharma, M.K. & Rana, S. (2011). G-cloud (e-Governance in cloud). Proceedings from the *5th National Conference; INDIA Com-2011, Computing for Nation Development.* Retrieved from: http://www.bvicam.ac.in/news/INDIACom%202011/25.pdf

Sharma, R., Sharma, A. & Pandey, U.S. (2011). E – Governance: A Successful Implementation of Government Policies using Cloud Computing. Proceedings from *International Conference on Web Services Computing (ICWSC) 2011*, (pp. 27-29). Retrieved from: http://research.ijcaonline.org/icwsc/number1/wsc006.pdf

Sharma, R., Sharma, A. & Singh, R.R. (2012). E-Governance & Cloud Computing: Technology Oriented Government Policies. *International Journal of Research in IT & Management*, 2(2), 584-593. Retrieved from: http://www.mairec.org/IJRIM/Feb2012/57.pdf

Singh, G.P. & Thapa, R.S. (2011). Cloud Computing Architecture: The Improved Strategy for Good E-Governance. *International Journal of Electronics Communication and Computer Engineering*, 1(1), 1-5. Retrieved from: http://www.ijecce.org/index.php?option=com_jresearch&view=publication&task=show&id=10&Itemid=265

Shekhawat, H.S. (2010). Hybrid Cloud Computing: An Alternative Model for E-Governance with Promised Security and Scalability. *Global Digital Business Review*, 4(1), 125-130. Retrieved from: http://www.vichetsum.com/GDBRFINAL2010.pdf#page=131

Tewari, N. & Sharma, M.K. (2011). Towards e-Governance Framework in INDIA using Cloud Computing. Proceedings from the *5th National Conference; INDIA Com-*

2011, Computing for Nation Development. Retrieved from: http://www.bvicam.ac.in/news/INDIACom%202011/139.pdf

Tian, J. (2011). Research on the Application of Cloud Computing in E-Government [in Chinese]. Proceedings from *2011 International Conference on Computer Science and Service System (CSSS),* (pp. 1630-1632). doi: 10.1109/CSSS.2011.5973937

Vats, K., Sharma, S. & Rathee, A. (2012). A Review of Cloud Computing and e-Governance. *International Journal of Advanced Research in Computer Science and Software Engineering,* 2(2). Retrieved from: http://ijarcsse.com/docs/papers/february2012/volume_2_issue_2/V2I2074.pdf

Wang, P. & Hua (2011). A Model of Government Information Value-added Exploitation Based on Cloud Computing. Proceedings from *International Conference on Business Management and Electronic Information (BMEI),* (pp. 518-522). doi: 10.1109/ICBMEI.2011.5917961

Appendix B: Cloud Computing Use Cases

B.1 Business use case templates (Deussen et al., 2011)

Legal use case template	
ID	**Title**
Description	Short summary of the use case
Actors and Roles	Actors and their roles participating in the scenario, e.g., described using a table as follows: **Actor** / **Roles** Actor 1 / Role 1 for actor 1 Role 2 for actor 1 . . . Actor 2 / Role 1 for actor 2 Role 2 for actor 2 . . .
Goals and aspirations for the UC	Background and main message of the use case
Legal domain	Data privacy regulations, licensing, contracting, etc.
Area	E.g., Europa, US, . . .
Legal frameworks, laws, etc., to be taken into account	Laws, policies, etc. which are of relevance
Required preconditions	Any preconditions necessary to understand the use case
Compliance criteria	Explanation why the use case is an illustration on how legal requirement can be implemented
Description of procedures to ensure legal compliance	Explanation how the use case shows the implementation of legal requirements
Existing specifications to rely on	Specifications and standards already dealing with aspects related to the use case
New specifications required between the actors	**Specifications and standards needed to establish the goals of the use case**

Legal Use Case Template (Deussen et al., 2011)

Organizational use case template	
ID	**Title**
Description	Short summary of the use case
Actors and Roles	Actors and their roles participating in the scenario, e.g., described using a table as follows: **Actor** / **Roles** Actor 1 / Role 1 for actor 1 Role 2 for actor 1 . . . Actor 2 / Role 1 for actor 2 Role 2 for actor 2 . . .
Goals and aspirations for the UC	Background and main message of the use case
Organization domain	E.g., security procedures, data privacy procedures, etc.
Regulations and policies to be taken into account	Policies, standards, best practices to be taken into account
Description of organization procedures	The "workflow" (or procedures) on organizational level used to achieve the goal of the use case
Components and services involved	What components and services of the system in question (described in the usage scenario) are needed/used to realize these procedures
Required preconditions	Any preconditions necessary to understand/implement the use case
Criteria for success	The expected output and the side effects
Failure conditions	What can go wrong
Failure handling	what to do about it
Related Ucs and those that are pre-requisite	May refer to technical UC describing the technical means to implement this UC.
Existing specifications to rely on	Specifications and standards already dealing with aspects related to the use case
New specifications required between the actors	**Specifications and standards needed to establish the goals of the use case**

Organizations Use Case Template (Deussen et al., 2011)

Technical use case template		
ID	Title	
Description	Short summary of the use case	
Actors and roles	Actors and their roles participating in the scenario, e.g., described using a table as follows:	
	Actor	Roles
	Actor 1	Role 1 for actor 1 Role 2 for actor 1 . . .
	Actor 2	Role 1 for actor 2 Role 2 for actor 2 . . .
Primary Actor	The actor who initiates the technical use case	
Goals and aspirations for the UC	Background and main message of the use case	
Platform, tools and the environment needed for execution of the UC	Technical requirements concerning the execution environment	
Description of file formats, wire protocols, in-memory objects, and other artifacts needed for execution	"Artifacts" used in the use case	
Components and services required for execution	What components and services of the system in question (described in the usage scenario) are needed/used to realize these procedures	
Input params needed for initialization	Initial input values for the execution of the use case	
Criteria for success	Expected process, outcome, side effect. Described by sequence charts, etc.	
Failure conditions	what can go wrong	
Failure handling	what to do about it	
Related Ucs and those that are pre-requisite	Relevant use cases for the associated usage scenario.	
Existing specifications to rely on	Specifications and standards already dealing with aspects related to the use case	
New specifications required between the actors	Specifications and standards needed to establish the goals of the use case	

Technical Use Case Template (Deussen et al., 2011)

B.2 Business use cases defined by NIST (2011b)

- **USAID Office Productivity:**

  Delivery Model: Community Cloud

  Service Model: SaaS

  Agency: US Agency for International Development

  FISMA Impact Level: Moderate Internal, Low External

  USAID OCIO plans to use Google Apps service for government to provide cloud-based email and document management service for USAID users. This service is expected to be deployed in an outsourced community cloud and accessed through the VDI or directly through the Internet. The other business applications are expected to be deployed in an on-site private cloud at the beginning and will later be migrated into an outsourced private cloud. These cloud-based applications will be accessed through the cloud-based VDI. The

security infrastructure that enables single-sign-on, two-factor authentication, and identity management is an essential part of the solution and will be deployed in the same on-site private cloud.

- **FGDC Geospatial Cloud**

Delivery Model: Community Cloud, Public Cloud

Service Model: PaaS

Agency: Federal Geospatial Data Committee

FISMA Impact Level: Moderate and Low, depending on need.

The Federal Geographic Data Committee and the General Services Administration (GSA) Cloud Computing Program Management Office operate the GeoCloud project on behalf of a wide range of federal agencies to explore the impact and possibilities of a geospatial computing-oriented cloud. The initiative seeks to define and investigate cloud savings, best practices, and lessons learned by migrating, benchmarking, and operating a set of ten existing public-access geospatial projects from six currently participating agencies –US Geologic Survey (USGS), National Oceanic and Atmospheric Administration (NOAA), Bureau of the Census, Environmental Protection Agency (EPA), Department of Agriculture (USDA), and Department of the Interior (DOI) with interest from the Department of Homeland Security (DHS).

The overall plan is to define, construct, and maintain a set of common geospatial platforms to support the project, using a joint agency platform model. Once platforms are in place and under maintenance, each project team will evaluate their application on its matching platform, document the steps needed to ensure security and performance, and track lessons learned along the way. To date, two platforms have been defined; one has been hardened and constructed and operates on Amazon's AWS public cloud. The project teams are beginning their exploration and sandbox phase to discover and document the processes needed to maintain these existing applications in the cloud.

Some agency geospatial applications, targeted for the public cloud, have data storage or processing needs that appear to make them more cost-effective in a community cloud setting. These applications will be piloted on similar shared platforms in a community facility housed in the US Geologic Survey.