Requirements identification for migrating egovernment applications to the cloud.

Evangelos Gongolidis[1] Christos Kalloniatis[1] and Evangelia Kavakli[1]

[1] Cultural Informatics Laboratory, Department of Cultural Technology and Communication, University of the Aegean, University Hill, GR 81100 Mytilene, Greece
vgogol@aegean.gr, chkallon@aegean.gr, kavakli@ct.aegean.gr

Abstract. Increasing citizens' participation in the use of eGovernment services is one of the main goals that governments all around the world are aiming to satisfy. While the number of Internet users is increasing rapidly and the percentage of the use of ICT services follows the same increment it is obvious that governments are seeking to take advantage of the modern alternative technological solutions in order to design the next generation of eGovernment systems and services. Without any doubt one of the most advanced solution that offers many advantages both in hardware and software levels is cloud computing. This paper aims on identifying the major functional and non-functional requirements that a traditional eGovenrment system should realise for its safe migration into a cloud environment.

Keywords: eGovernment, Cloud Computing, functional requirements, non-functional requirements, cloud migration

1. Introduction

According to United Nations, eGovernment is defined as the employment of the Internet and the World Wide Web to deliver government services [1]. Cloud computing according to NIST [2], is based on a new model for the delivery of information and service through the Internet, which is based on the concept that involves a large number of computers who are inter-connected and act as one to each request. In cloud computing, software, hardware and network play the main role [3]. The type of request can vary and is based to the user himself but the most important gain in cloud computing is that it is very economic as it is based on large scale architecture concept (the more you build/use/take, the better) and the cloud client can at any time define the amount of sources that wants to use. As a result, eGovernment in all over the world has significantly changed the idea of delivery specific services through a single server and perform all required maintenance on it [4] by moving to the cloud.

However, there are several differences and aspects that needs to be examined and reinstated before moving from traditional server systems to the cloud. Also, during the last years a discussion has started over whether cloud computing is able to host and handle information and requests provided from different types of users (government, companies etc) [5]. The scope of this paper, is to focus on traditional eGovernment systems and present the requirements a porta/system must fulfil in order to be characterized as a functional eGovernment system. Specifically, in section 2 the main functional and non-functional requirements that an eGovernment platform should satisfy in traditional environments are presented and described. All characteristics are treated of equal importance and significance when designing respective services into the cloud. In section 3 a brief description of cloud service and deployment models is presented. In section 4 an analysis of the identified requirements and their role in the cloud-based eGovernment systems is presented along with a matching of every requirement with the respective cloud service models that has an applicability on.

2. eGovernment

From the establishment of ICT technologies, governments all over the world tried to insert ICT into the daily procedures. However, that act was not easy as there were several requirements that should be adopted for each government system and there were also several legislation requirements. As a result almost 80% of the projects in the early 20s were in the failure category [6]. The requirements that are presented below were extracted from reports provided by the European Union for i2010 initiatives [7], United Nations reports for eGovernment Systems characteristics and the Greek Interoperability Framework [8].

2.1 Interoperability

Interoperability is one of the most important characteristics of eGovernment systems. Interoperability can be described as a chain that allows information and computer systems to be joined up both within organizations and then across organization boundaries with other organizations, administrations, enterprises or citizens [9].

Interoperability is defined in 3 layers: technical, semantic and organization.

- Technical is concerned with the technical aspects of connecting computer systems, the definition of open interfaces, data formats and protocols including telecommunication.
- Semantic, is the ability for an external system to be able to realize that the stored or provided information has a specific meaning and is not treated as

raw data. Semantic interoperability is obtained by the common use of predefined standards and prototypes.

- Organizational interoperability is concerned with modelling business processes, aligning information architectures with organizational goals and helping business process to cooperate. The most important part of organization interoperability refers to the ability of different implemented services that take part in a specific government process to be able to cooperate automatically and generate a specific result.

2.2 eInclusion

eInclusion is the characteristic that requires the eGovernment services to be able to be delivered to all people, breaking any technological barrier that could arise. eInclusion has the power to close the gap between developed and less developed countries, can also promote democracy, participation and mutual understanding between different countries or different social parties. It can also empower disadvantaged individuals, such as the poor, the disabled, and the unemployed.

2.3 eAccesibility

eAccesibility refers to the ease of use of information and communication technologies (ICTs), such as the Internet or services provided by the Internet, by people with disabilities. For eGovernment services each service or each portal that provides the government service needs to be developed so that disabled users can access the information. For example:

- for people who are blind, web sites need to be able to be interpreted by programs which can recognize and read text aloud and also describe any visual images.
- for people who have low vision, web pages need adjustable sized fonts with an easy way to increase or decrease the size of the fonts. Also the use of sharply contrasting colors is greatly encouraged.
- for people who are deaf or hard of hearing, audio content should be accompanied by text versions of the dialogue. Sign language video can also help make audio content more accessible.

2.4 User registration

User registration is the procedure that a user needs to follow in order to register to a specific eGovernment system. The procedure must be clearly defined, must not violate

any legislation related to personal data and must also give the user the ability to cancel his account or retrieve a lost password.

2.5 Single sign on – one stop service

This characteristic requires that all implemented systems that are related to eGovernment will use the same account credentials for each government entity that provides eGovernment services. As a result, implemented systems from different government entities of the same country will require the same credentials. Also, it is of great importance for each country to provide their services from a one stop shop which will be declared as the national eGovernment service portal.

2.6 eTransparency

Transparency is related to the act of make open and searchable by all the act of decision and actions related to a government policy. As a result, eTransparency is the use of ICT for handling or providing information or tools for those steps related to transparency flow. eTransparency can also be categorized in the following levels:

- Publication: providing basic information about a particular area of government.
- Transaction: automating some public sector process and generate automated reporting on that process.
- Reporting: providing specific details of public sector decisions/spending/actions (e.g. via performance indicators or via list of spending).
- Openness: allowing users to compare public servant performance against pre-set benchmarks.
- Accountability: allowing users some mechanism of control (e.g. reward or punishment) over public servants.

An interesting aspect of eTransparency is project Diavgeia [10] which was established in Greece since 2009. Diavgeia, aims to solve the publication and reporting level of eTransparency by providing information about public spending made from the greek government sector.

2.7 Adaptivity

Every implemented system or service must be easily adapted, without any great financial cost, to new requirements that are provided by the government entity. Adaptivity is of great importance for matters related to legislation and technology evolution.

2.8 Use of standards / prototypes

Each implemented service or procedure should be based on a trusted prototype. The use of open source standards is also greatly encouraged. Several countries in their eGovernment frameworks also provide the standard that they require to be used for specific services so apart from using a trusted standard the developer must also verify that the developed service is compliant with the country defined standard.

2.9 Scaling

The ability for the systems to easily decrease or extend the current use of hardware so it can easily provide better quality of service to a different number of interested users for with the least financial cost.

2.10 System/Service Availability

All implemented systems or services must be available to the users without any interaction of service. In case of a system or service failure the user must be informed immediately about the reason of failure.

2.11 Fault Tolerance/Auditing/Logging

All implemented systems must provide an automate procedure to recover from failure states and also the system must be able to move to the last good state automatically. Internally, the system must have auditing and logging mechanisms that would keep track on any change or request that is done through the system/service.

2.12 Maintenance / Update

The implemented system or service should be easily maintained and updated when required. Each act must not be related or based on a specific constructor and must be able to be accomplished by anyone related to the government entity.

2.13 Trust of Citizen for proper use of data

EGovernment is based on the use of confidential data for the provision of each service. As a result, each government entity that use data for a citizen must be able to process only confidential data that is related to the service/system state and not all data that is stored.

3. Cloud Computing

Cloud computing was a revolutionary change in the state-of-the-art for the provision of both software and hardware services. Cloud computing can be briefly described as a collection of scalable and virtualized resources and is capable of providing specific services on demand [11]. The main goal of cloud computing is to provide ICT services with the use of shared infrastructure and the collection of many systems. For government the value that is gained from moving to the cloud is especially appealing, given both changing demands for IT and challenging economic conditions [12].

3.1 Cloud Service Models

In order to correlate the above mentioned characteristics of eGovernment with cloud computing we must distinguish the service models of cloud computing. Cloud computing mainly consists of three service models:

- Infrastructure as a Service(IaaS)
- Platform as a Service (PaaS)
- Software as a Service (SaaS)

Infrastructure as a Service can be briefly described as buying or scaling recently bought infrastructure resources using a predefined service model. IaaS can also be classified in two categories: Computation as a Service (CaaS) and Data as a Service (DaaS). CaaS refers to the ability to buy or rent specific resources for a period of time in order to perform difficult computation calculations and is related to processor, RAM or deployed software. DaaS refers to the ability to buy or rent storage space which can either be used instantly or can be delegated to third-party users.

Platform as a Service refers to ability of buy of enhance a predefined platform, which results in providing a set of software and services that can be used to provide a better working environment or a better quality of service. The concept of using PaaS relies on the ability to use a platform which provides specific capabilities (ie the ability to build a website) without already know how to do it. PaaS also lies on the ability to support all required procedures or intermediate steps to get the expected outcome.

Software as a Service (SaaS) is based on the use of software of application, which are hosted in the cloud environment of the provider and are provided on demand to the end-user. As a result, the user does not have to worry about licensing or maintaining costs as the provided software is licensed and upgraded by the provider.

3.2 Deployment Models

Apart from the above described service delivery models, cloud computing is also characterized by how it is deployed and specifically who has access in the cloud environment. The delegation of the above mentioned responsibilities forms up the following cloud deployment models [13]:

Private Cloud: Private cloud refers to those organizations which solely operate the cloud environment, whether it is managed by the same operation or it is managed by a third party. Private cloud is the most closest to the traditional use of ICT as every operation performed in the cloud model must be funded by the organization.

Community Cloud: Community cloud refers to a model where the cloud is operated by organizations which share similar interests and can also be managed internally of externally. As a result, the required costs are spread between the different organizations.

Public Cloud: Public cloud is deployed and operated for the public and can be maintained by one or several organizations. Access to this type of cloud is allowed to everyone.

Hybrid Cloud: Hybrid cloud is a composition of different models which retain their independence but cooperate with a specific manner. The manner that they cooperate must be clearly defined by the cloud provider to all interested parties.

4. Categorization of eGovernment requirements to Cloud Service Models

As a result, eGovernment entities who are willing to move to cloud must first decide how they will handle the above mentioned requirements that are related to traditional eGovernment systems. Moving to the cloud for eGovernment systems is not only a matter of breaking technical obstacles but also finding a methodology that would be compliant with all provided government requirements. The first step of providing a compliant methodology for the cloud migration would be to distinguish in which Service Level each requirements would be delegated.

Interoperability is mainly a matter of data and the way that these data could be used or passed to another system using the cloud. As a result, interoperability could be handled with a SaaS approach that will provide specific data for a simple call or as a PaaS approach where interoperability would be handled inside of a model with specific preconditions and post conditions.

eInclusion and eAccesibility are both requirements that are strongly related and act complementary. EGovernment systems should promote the inclusion of all parties'

regardless of current financial state/ education/ hardware, while eAccesibility cares mostly about the sensitive parts of modern societies. As a result, both could be handled with a three cloud level approach. IaaS would be responsible for providing the required hardware on demand for each request, while PaaS and SaaS would be able to tackle accessibility problems in a platform or service oriented approach.

User Registration / Single Sign on are also similar problems which should be tackled in the same way. Moving to the cloud should be accompanied by a mechanism for authentication which should also be used by other systems simultaneously. As a result, this matter could be solved with a PaaS approach where the platform would xbe dedicated to authorization and rights delegation or a SaaS approach where each required action would be provided as a Service (i.e. logging, access rights).

Transparency is a very important characteristic for eGovernment systems and is decomposed in five levels as described above. As a result, eTransparency could be achieved by a SaaS approach where each step would be treated as a service of a PaaS approach where the concept and the requirements of transparency would be handled in a provided platform.

Scaling is a clear matter of an IaaS approach as it refers to the ability to scale up or down provided infrastructure either automatically or on demand.

Adaptivity is a more complex problem and it refers to several matters in different levels of service provision. All provided services to the end users must be easily adapted to new requirements that are provided. As a result, a service oriented approach could formalize the way the adaptions could be done.

Use of standards / prototypes could be handled as a SaaS or PaaS approach. The SaaS approach would handle and store the prototype that is used by each provided service, while PaaS can also move further and provide the capability of online uploading, validating and use of prototypes that are already stored in the platform.

System Service / Availability and Fault Tolerance are inextricably linked. The system must be online 100% using specific cloud features and also there must be services that would enable the tracking of availability, the use of precaution actions (i.e. reboot) or the ability to roll back system data. The provided solution can be software oriented regarding each subject like logging and auditing or Platform oriented regarding the main subject.

Maintenance /Update is clear a matter of SaaS as the update actions should be provided by a software which would be able to handle and perform update requests on its own.

Security - Privacy/Trust of Citizen is a matter of all service levels. Security and privacy issues are identified specifically for every cloud service model separately [14]. In order for an eGovernment system or individual service to be trusted and protected respective security measures should be implemented in all service models.

An outline of the service level where each concept could be handled is provided in table 1.

5. Conclusions

The transformation from the use and maintenance of traditional services to the cloud can be a long and difficult procedure. For government applications it is even more complex because the transformation should not break or violate the relationship or the legislation that was already adopted by the traditional approach.

Table 1. Matching eGov Requirements with Cloud Service Models

Requirement	IaaS	PaaS	SaaS
Interoperability		X	X
eInclusion/ eAccessibility	X	X	X
User Registration / Single Sign on		X	X
Transparency		X	X
Scaling	X		
Adaptivity			X
Use of prototypes		X	X
System Service Availability and Fault Tolerance		X	X
Maintenance /Update			X
Security-Privacy / Trust of Citizen	X	X	X

In this paper we presented the known requirements that an eGovernment system should satisfy and the way that these requirements could be satisfied from respective service models when migrating into the cloud. It is of major importance to mention here that the government entity could act both as the cloud provider or the end user.

Regarding the concept of migrating eGovernment application to the cloud we must also take into serious consideration that the stakeholder is not only the cloud provider but also the legislation and the political will of the government entity. Finally, it is important to mention that the government entities among countries can be of various levels (ministries, municipalities etc.) and the move from the traditional ICT services to the cloud should also try to bridge the gaps that already exist in communication or in data exchange.

Future work includes the identification of respective technical solutions that can realise these requirements into the cloud and especially for every service model and deployment model correspondently. The definition of protocols in each level will also act as a comparison factor on finding which methodology could be better in terms of

implementation and performance. Finally, we will try to provide a specific cloud framework which could act as a PaaS and provide auxiliary steps to eGovernment entities that are willing to migrate their systems to the cloud.

6. References

[1] D. o. E. a. S. Affairs, "E-Government Survey," United Nations, New York, 2012.

[2] P. Mell and T. Glance, "The NIST Definition of Cloud," NIST, 2011.

[3] Y. L. e. al, "Towards a unified ontology of cloud computing," Computing Environments Workshop, 2008.

[4] A. M. e. al, "Above the Clouds: A Berkeley view of Cloud Computing," University of California, Berkeley, 2009.

[5] L. N, "Is cloud computing really ready for the prime time," *J. of ACM,* vol. 42, no. 1, pp. 15-20, 2009.

[6] H. R, Implemenation and Managing of eGovernment, Vistaar Publication, 2006.

[7] E. Commision, "Jeremy Millard et al," European Commision, 2009.

[8] Information Society, "Greek Interoperability Framework," 2008.

[9] Commision of the European Communities, "Linking up Europe: the Importance of Interoperability for eGovernment Services," 2003.

[10] T. e. al, "Open data for e-government, the greek case," Information, Intelligence, Systems and Applications (IISA), Piraeus, 2013.

[11] F. B. a. Escalante, "Handbook of Cloud Computing," Springer Science, 2010.

[12] D. Wyld, "Moving to the cloud: An introduction to cloud computing in Government," 2009.

[13] B. Z. e. al, "Cloud Computing in eGovernment across Europe," Springer-Verlab , Berlin Heidelberg, 2013.

[14] H. M. V. M. S. I. S. G. E. K. C. Kalloniatis, "Towards the design of secure and privacy-oriented Information Systems in the Cloud: Identifying the major concepts," Computer, Standards and Interfaces, Elsevier, 2013.