Legal, Privacy, Security, Access and Regulatory Issues in Cloud Computing

Nomusa Dlodlo
CSIR – Meraka Institute, Pretoria, South Africa
ndlodlo@csir.co.za

Abstract: Cloud computing is a sufficiently new research area. Since it is in its development stages, the information on the field is slowly being compiled by the researchers and practitioners from their experiences. Some of the areas in which there is still a gap on reporting on legal, privacy, security, access and regulatory issues. This paper raises an awareness of legal, privacy, security, access and regulatory issues that are associated with the advent of cloud computing. An in-depth literature survey is conducted on these and an analysis is drawn from the issues that are identified through the literature survey. Recommendations are then given on how the issues identified in the analysis can be mitigated. These recommendations centre around the issues of policy interventions, standards, privacy and data protection, traffic and congestion management, business continuity planning, security and regulation. This research is an advancement of knowledge in that field and is meant to initiate further debate on cloud computing

Keywords: cloud computing, security, privacy, regulation, legal issues, interoperability, business continuity planning

1. Introduction

The emergence of very large specialised data centres that host thousands of servers has created a surplus of computing resources that has come to be called the cloud. The cloud is the term for networked computers that distribute processing power, applications and large systems among machines. This means that, computing is no longer on local computers but on centralised facilities operated by third party compute and storage facilities (Foster, 2010). Cloud computing transforms once-expensive resources like disk storage and processing cycles into a readily-available cheap commodity. By deploying Information Technology (IT) infrastructure and services over the network, any organisation can purchase these resources on an as-needed basis and avoid capital costs of software and hardware. By offering enterprises the opportunity to decouple their IT needs and their infrastructure, cloud computing has the likely ability to offer enterprises long-term IT savings, including reducing infrastructure costs and offering pay-for-service models.

One of the definitions of cloud computing given in literature is as follows (Cloud computing, 2009):

> *"Cloud computing refers to both the applications delivered as services over the Internet and the hardware systems and software in the datacentres that provide those services. The services themselves have long been referred to as Software as a Service (SaaS). The datacentre hardware and software is what we will call the cloud. When a cloud is made available in a pay-as-you-go manner to the public, we call it a public cloud; the service being sold is utility computing. We use the term private cloud to refer to internal datacentres of a business or other organisations that are not made available to the public. Thus cloud computing is the sum of SaaS and utility computing, but does not normally include private clouds"*

The National Institute of Standards and Testing (NIST) defines cloud computing under 5 identified characteristics as follows (How cloud computing, 2010):

- On-demand self service, which allows business units to get the computing resources they need without having to go through the IT department
- Broad network access, which allows applications to be built in ways that align with how businesses operate today – mobile, multi-device, etc.
- Resource pooling, which allows for pooling of computing resources to serve multiple consumers
- Rapid elasticity, which allows for quick scalability or downsizing of resources depending on demand
- Measured service, which means that business units only pay for the computational resources they use. IT costs match business success

Kushida, et.al (Kushida, 2010) give the operating definition of cloud computing as:

> *"Cloud computing provides on-demand network access to a computing environment and computing resources delivered as services. There is elasticity in the resource provision for*

> *users, which is allocated dynamically within providers' datacentres. Payment schemes are typically pay-as-you-go models".*

With the advent of the cloud arises legal issues and those of privacy, security, access and its regulation. This paper gives a review of these issues and how they can be mitigated.

2. Problem statement

Since cloud computing is a field that is in its development stages, the information on the field is slowly being compiled by the researchers and practitioners from their experiences. Some of the areas in which there is still a gap on reporting are on are legal , privacy, security, access and regulatory issues. This paper raises an awareness of legal, privacy, security, access and regulatory issues that are associated with the advent of cloud computing.

2.1 Process

An in-depth literature survey is conducted on the legal, privacy, security, access and regulatory issues of cloud computing and an analysis is drawn from the issues that are identified through the literature survey. Literature that is relevant to this article was compiled through Internet searches, and searches of databases of online journals and conference proceedings. The search was done randomly, on the basis of the associated keywords identified. Recommendations as identified from current literature are then given on how the issues identified in the analysis can be mitigated. These recommendations centre around the policy interventions, standards, privacy and data protection, traffic and congestion management, business continuity planning, security and regulation.

2.2 Question and objectives

The main research question in this paper is, " What is the current state of affairs on the soft issues of cloud computing and what does the literature say on the recommended way forward to further the issues of cloud computing."

The objectives are:

- Identify the legal, privacy, security, access and regulatory issues prevailing currently in the area of cloud computing
- Identify recommendations on the way forward on these issues

3. Legal implications of cloud computing

(Legal implications, 2010; Legal issues, 2010; Wisdom of clouds, 2008)

There is the issue of "reasonable security" in the cloud computing context, and potential liability arising out of security breaches in the cloud. A company that provides a service to handle the personal information of another organisation has the responsibility to ensure that there is reasonable security to protect personal and confidential information.

The data centres of cloud service providers are located in various locations all over the world. That means data on the cloud could be stored in any country. The 'physical location' raises the question of legal governance over the data. In case of a conflict between the cloud vendor and the customer the question of which country's court system will settle the dispute comes to the fore. In cases where there is a litigation, an organisation will have to deal with a third party cloud provider to gain access to information relevant to the litigation. Considering the multiple copies of data that may be created, stored, recompiled, reused, dispersed and reassembled, what constitutes a "record" for evidence may be difficult to grapple with the cloud.

The number of trademark filings covering cloud computing brands, goods and services is increasing as companies seek to better position themselves for cloud computing branding and marketing efforts. Therefore ensuring the uniqueness of a trademark with the advent of a cloud has been further complicated.

Sharing and transferring data within the cloud is a problem. Organisations are legally prohibited from transferring personal information to countries that do not provide the same level of protection with respect to personal information. That means cloud providers will not be in a position to make any contractual promises to their clients because in many cases they cannot say which countries data will be transferred to and from.

Systems are vulnerable to damage or interruption from earthquakes, terrorist attacks, flood, fires, etc. Customers have to ensure therefore that they are insured against loss of business due to such potential losses. This is essential. If there is a breach of privacy due to the fault of the cloud vendor, the carrier should be liable for the compensation. Vendors on the other hand should do their level best to meet service level targets committed with any customer.

Ideally, the data that is of the customer's creation is protected under the intellectual property rights of a country. Therefore there should be compensation for infringement. Customers own the data. No vendor can claim ownership of any data that is uploaded or associated with intellectual property. Customer data includes all data maintained by the customer

In one frequently cited scenario (Gurav, 2010), a government agency presents a subpoena or search warrant to the third party that has possession of a customer's data. Had they retained physical custody, the customer might still have been compelled to surrender the information, but at least would have been able to decide for themselves whether or not to contest the order. The third party service is presumably less likely to go to court on behalf of a customer. In some circumstances the customer might not even be informed that their documents have been released.

With the cloud there is lesser privacy protection under the law. To search a house or office (including documents stored on a computer), police need a warrant of arrest. To get the information that is stored on a third party's web server they only need a subpoena, which is easier to obtain. This kind of search can happen without the cloud customer's knowledge.

4. Security issues in cloud computing (hidden risks, 2010)

Due to its distributed nature, the cloud results in weak security systems that are easy to break into. The security of the system is only as strong as the weakest user's set-up. Weak password recovery workflows, phishing attacks, and keyloggers present bigger security risks. In collaborative web applications that are built for groups, like Google Apps or any web-based project management software, any breach of security spreads across all participants.

In cloud computing an organisation's data is locked-in and the third party in control. When you participate in the cloud, you depend on a third party to make decisions about your data and platforms. Cloud computing also comes with chances of server unavailability and account lock-out. When the Internet goes down, access to one's data is cut off. An important measure of security often overlooked by companies is how much downtime a cloud service provider experiences. The client should request the provider's reliability reports to determine whether these meet the requirements of their business. Exception monitoring systems is another important area which companies should ask their service providers about (Binning, 2010).

The biggest concern with cloud computing is that it puts all of a company's data and applications in one place. Businesses should be wary of putting sensitive company information in public clouds. They should instead stick to low-risk, low volume applications and build internal and private clouds to enable collaboration within the organisation and externally with partners.

Security is one of the most often-cited objections to cloud computing (Zhang, 2010). Cloud users face security threats from both outside and inside the cloud. This responsibility is divided among the cloud user, the cloud vendor and any third party vendors that users rely on for security-sensitive software or configurations. The cloud user is responsible for application-level security. The cloud provider is responsible for physical security, and likely for enforcing external firewall policies. Security for intermediate layers of the software stack is shared between the user and the operator. Cloud providers must guard against theft or denial-of-service attacks by users. One last security concern is to protect the cloud user against the provider. The provider will by definition control the 'bottom layer' of the software stack, which effectively circumvents most known security techniques. Users also need to be protected from one another. The primary security mechanism in today's clouds is virtualisation. It is a powerful defence, and protects against most attempts by users to attack one another or the underlying cloud infrastructure.

Virtualisation is the enabler technology for the cloud and uses physical resources such as a server which is divided into virtual resources called virtual machines (VM). Customers cannot protect their VMs on their own. Cloud service providers are making substantial effort to secure their systems, in order to minimise the threat of insider attacks and reinforce the confidence of customers. For example, they restrict access to hardware facilities, adopt stringent accountability and auditing procedures, and minimise the number of staff who have access to critical components of the infrastructure. Security management of virtualisation technologies is required to reduce the risk of security exposures and enable security policy enforcement. A cloud-specific security issue is that of running arbitrary VM images. This is only one aspect of making sure the right data is available to the right user at the right time. The Cloud Security Alliance is directly pursuing in addition, issues of authentication, authorisation, privacy, integrity and non-repudiation and data reliability and availability.

According to Chow et.al. (Chow, 2009), security concerns are categorised as:

- Traditional security
- Availability
- Third party data control

Traditional security concerns involve computer and network intrusions or attacks that will be made easier or possible by moving to the cloud (Chow, 2009). VM-level attacks are a problem because of potential vulnerabilities in the VM technology. There are also cloud provider vulnerabilities. These could be platform level such as SQL-injection or cross-site scripting. Phishers and other social engineers have a new attack vector. The cloud user must protect the infrastructure used to connect and interact with the cloud, a task complicated by the cloud being outside the firewall in many cases. The enterprise authentication and authorisation framework does not naturally extend into the cloud. Traditional digital forensic methodologies permit investigators to seize equipment and perform detailed analysis on the media and data recovered. The likelihood therefore of the data being removed, overwritten, deleted or destroyed by the perpetrator in this case is low.

Availability concerns centre on critical applications and data being available (Chow, 2009). As with traditional security concerns, cloud providers argue that their server uptime compares well with the availability of the cloud user's own data centres. There are more single points of failure and attacks in the cloud. They may lack an assurance of computational integrity.

The legal implications of data and applications being held by a third party are complex (Chow, 2009). Therefore there are many questions that remain unanswered. There is also a potential lack of control and transparency when a third party holds the data. If served a subpoena can a cloud user compel the cloud provider to respond in the required time frame? How can a cloud user be guaranteed that data has been deleted by the cloud provider? Audit difficulty is another side effect of the lack of control in the cloud. Is there sufficient transparency in the operations of the cloud provider for auditing purposes? There are contractual obligation issues also. One problem with using another company's infrastructure besides the uncertain alignment of interests is that there may be surprising legal implications. Cloud provider espionage is the worry of the theft of company proprietary information by the cloud provider. How can a cloud user avoid data lock-in? The data itself might locked in proprietary format and there are also issues with training and processes. There is also a problem of the cloud user having no control over frequent changes in cloud-based services. Another possible concern is that the contracted cloud provider might use subcontractors, over whom the cloud user has even less control and who must also be trusted.

5. Data access and interoperability

The issue of data access and interoperability continues to be an outstanding matter for inherently distributed applications and federated organisations. Common best practices and standards are needed to achieve the fundamental properties of portability and interoperability for cloud applications and environments.

A major challenge of moving applications to the cloud for most organisations is the need to master multiple languages and operating environments (Gurav, 2010). In many cloud applications a back-end process relies on a relational database, so part of the code is written in SQL, or other query language. On the client side, program logic is likely to be implemented in JavaScript embedded within HTML documents. Standing between the database and the client is a server application that might be written in a scripting language (such as PHP, Java and Python). Information exchanged between the various layers is likely to be encoded in some variation of XML. Any web application needs to be available to legitimate visitors from all over the world. A true cloud spans the entire globe, with a server presence in multiple simultaneous locations.

Besides technical issues, a cloud provider could suffer outages for non-technical reasons, including going out of business or being the target of regulatory action. Therefore organisations should be wary of this and put in place measures to ensure business continuity and service availability when outages occur (Zhang, 2010).

Data lock-in by the service provider is a contentious issue for the customer. Software stacks have improved interoperability among platforms, but the storage Application programming Interfaces (APIs) for cloud computing are still proprietary. Thus, customers cannot extract their data and programs from one site to run on another. This has prevented some organisations from adopting cloud computing. Customer lock-in may be attractive to cloud computing providers, but their users are vulnerable to price increases, to reliability problems, or even to providers going out of business (Zhang, 2010).

Applications continue to be more data intensive. Data bottlenecks are likely to occur as more users subscribe to a cloud service. Cloud users and cloud providers have to think about the implications of placement and traffic at every level of the system if they want to minimise costs (Zhang, 2010).

6. Privacy issues in cloud computing

Privacy is a fundamental right enshrined in the UN Universal Declaration of Human Rights. There are various forms of privacy, including ' the right to be left alone" and "control of information about ourselves" (Pearson, 2009). There are different types of information that need to be protected. These include any information that can be used to identify or locate an individual (e.g. name, address, credit card number and IP address). Sensitive information such as personal financial information and job performance information is considered private. Behavioural information such as viewing habits for digital content, user's recently visited websites or product usage history need to be protected as well.

Violation of privacy occurs as a result of a number of cloud dynamics. In the cloud the infrastructure is shared between organisations and is off-premise. Therefore there are threats associated with data being stored remotely and because of virtualisation. Virtualisation is a method of running multiple independent virtual systems on a less physical resource making one computer act as many, and sharing the resources of hosts across multiple environments. The cloud is also a dynamic environment. Services can be aggregated and changed dynamically by customers and service providers can change the provisioning of services anytime. Sensitive data may move around within an organisation and across organisational boundaries. Legal compliance and adequate protection has to be maintained therefore. The speed and flexibility of adjustment to vendor offerings that benefits business and provide a strong motivation for the use of cloud computing might come at the cost of compromise to the safety of data. Cloud computing enables new services to be made available in the cloud by combining other services, e.g. a 'print on demand' service can be provided by combining a printing service with a storage service. This procedure of service combination is typically under less control than previous service combinations carried out within traditional multi-party enterprise scenarios. There may be varied degrees of security and privacy in each of the components.

Privacy risks for cloud computing may also lie in the following (Pearson, 2009):

- For the cloud service user: being forced or persuaded to be tracked or give personal information against their will
- For the organisation using the cloud: non-compliance to enterprise policies and legislation, loss of reputation and credibility
- For implementers of cloud platforms: exposure of sensitive information stored on the platforms (potentially for fraudulent purposes), legal liability, loss of reputation and credibility, lack of user trust and take up.
- For providers of applications on top of cloud platforms: legal non-compliance, loss of reputation, 'function creep' using the personal information stored on the cloud, i.e. it might later be used for purposes other than the original cloud service intention
- For the data subject: exposure of personal information

7. Regulatory issues

In the cloud there are a number of issues that need to be regulated. Potential physical location of data centres could be anywhere, with geography-blind distribution of applications and data. As a practical commercial matter, national regulations should be able to influence the actual deployment of cloud services in countries around the globe.

Without concrete guarantees on the privacy of data held by cloud providers, the diffusion of cloud services may be hampered by the perceived risk in entrusting sensitive data to external cloud services. In the US and Europe the regulations require some cloud offerings to allow users to stipulate the country in which their data will be stored. Non-US firms whose servers are located in the US can have their information accessed by the US government under the US Patriot Act and Homeland Security Act (Carrigan, 2008). This impacts on information privacy policy.

Strongly related to the notion of service level agreements and policy, is that of governance – how to manage sets of virtual resources. At the infrastructure level, applications may consist of many virtual machines, virtual storage and virtual networks. Managing these virtual missions, or virtual data centres, requires policy and enforcement from both the provider and consumer (Lee, 2010).

In a private cloud, the infrastructure for implementing the cloud is controlled completely by the enterprise. Typically, private clouds are implemented in the enterprise's data centre and managed by internal resources. A private cloud maintains all corporate data in resources under the control of the legal and contractual umbrella of the organisation. This eliminates the regulatory, legal and security concerns associated with information being processed on third party computing resources.

In a public cloud however, external organisations provide the infrastructure and management required to implement the cloud. Public clouds have the disadvantage of hosting data in an offsite organisation outside the legal and regulatory umbrella of the organisation. In addition, as most public clouds leverage a worldwide network of data centres, it is difficult to document the physical location of data at any particular moment. These issues result in potential regulatory compliance issues which preclude the use of public clouds for certain organisations or business applications.

According to Enki, et.al (Enki, 2010), the identified regulatory issues in the cloud are in the areas of service level agreements (SLA), service and support and performance. Cloud-computing services define an SLA as some guarantee of how much time the server, platform or application will be available. For example, a cloud provider will provide 99.99% uptime, or five minutes downtime a year, with a 10% discount on charges for any month in which that availability is not achieved. Since its infrastructure is not built to reach this uptime, it is effectively offering a 10% discount on services in exchange for the benefit of claiming that reliability. Another trick is to compute the SLA on an annualised basis. This means that customers are eligible for a service only after one year has passed. The end-user should pay close attention to the details of the SLA being provided and weigh that against what business impact it will have if the service provider misses the committed SLA and regulatory authorities should chip in to level the playing field.

One of the greatest attractions of cloud computing is that it enables computing to be available to a large community. In addition, the elimination of the responsibility for physical hardware removes the need for data-centre administration staff. As a result, there is an increasing number of people responsible for production computing who do not have systems administration backgrounds, which creates demand for comprehensive cloud vendor support offerings and thereby greatly inconveniencing the consumer. Round the clock live support staff costs a great deal.

The cloud is a pervasive federated network in which unregulated personal area networks and local area networks will interoperate with traditionally regulated electronic communication services. Regulators need to carefully monitor the challenges posed by these networks, taking action as necessary to regulate for technical interoperability, consumer protection, support for competition and the appearance of opportunities for the exploitation of market power.

8. Discussion and way forward

This sections draws recommendations from literature on the way forward in cloud computing. These recommendations centre around the issues of policy interventions, standards, privacy and data protection, traffic and congestion management, business continuity planning, security and regulation.

Any large scale deployment needs to adhere to certain standards. The cloud spans multiple industries and differs widely in application scenarios and user requirements. The standardisation of the cloud should cover common communication protocols, at, for example, the carrier level; terminal description and service discovery mechanisms and application data switching mechanisms such as technologies based on XML, SOAP and web services. The latter covers terminal, communication protocols and application specifications.

Concerns over privacy and data protection are widespread. Protecting privacy must not be limited to technical solutions but encompass regulatory, market-based and socio-ethical considerations. There should be a concerted effort involving government, civil society and private sector players to protect these values. One of the hazards of shared infrastructure is that one customer's usage pattern may affect other customers' performance. The cloud must incorporate traffic and congestion management. This will sense and manage information flows, detect overflow conditions and implement resource reservation for time-critical and life-critical data flows.

Policy interventions towards the adoption of cloud computing should include (Etro, 2010):

- International agreements in favour of unrestricted flow of data across borders (since data centres are located in different countries with different privacy laws, data portability remains a key issue for the diffusion of cloud computing)
- Agreements between government and industry leaders on a minimum set of technological standards and process standards to be respected in the provision of cloud computing services to guarantee data security and privacy and promote a healthy diffusion of new technology
- Expansion of broadband capacity
- Introduction of fiscal incentives for the adoption of cloud computing and a specific promotion in particular dynamic sectors (for instance, governments could finance, up to a limit, the variable costs of computing for all domestic and foreign firms that decide to adopt a cloud computing solution)

Some examples of cloud computing risks for the enterprise that need to be managed include (Cloud computing: business benefits, 2009):

- Reputation, history and sustainability of the provider to ensure reliability of service provision
- The cloud provider should take responsibility for information handling and be held liable for loss of confidentiality and privacy
- Business continuity and disaster-recovery plans must be well documented and tested
- Compliance to regulations and laws in different geographic regions can be a challenge for enterprises. It is critical to obtain proper legal advice to ensure that the contract specifies the areas where the cloud provider is responsible and liable for ramifications arising from potential issues.

Business continuity planning is identifying core operational systems and work processes that an organisation requires in order to deliver services and products to their customers. This involves identifying key suppliers, business partners and staff. From an IT perspective this means three things (Cloud computing, 2009):

- Architecting your IT infrastructure and application systems to be distributed with no single point of failure
- Ensuring the systems have built-in data and application redundancy
- Having the ability for these systems to be accessed securely from any location at any time.

The problem that has made business continuity and disaster recovery extremely expensive has always been the need for redundant hardware, both on-site and in remote sites. The advent of cloud computing has made the provision of dynamically scalable and virtualised resources widely and cheaply available.
Security is one of the largest concerns for the adoption of cloud computing. Seven risks a cloud user should raise with vendors before committing are (Foster, 2010):

- 1. Privileged user access: sensitive data processed outside the enterprise needs the assurance that they only accessible and propagated to privileged users
- 2. Regulatory compliance: A customer needs to verify if a cloud provider has external audits and security certifications and if their infrastructure complies with some regulatory security requirements
- 3. Data location: since a customer will not know where her data will be stored, it is important that the cloud provider commit to storing and processing and processing data in specific jurisdictions and to obey local privacy requirements on behalf of the customer.
- 4. Data segregation: one needs to ensure that one customer's data is fully segregated from another customer's data
- 5. Recovery: it is important that the cloud provider has an efficient replication and recovery mechanism to restore data if a disaster occurs
- 6. Investigative support: Cloud services are especially difficult to investigate, if this is important for a customer, then such support needs to be ensured with a contractual commitment
- 7. Long-term viability: your data should be viable even if the cloud provider is acquired by another company.

To avoid customer lock-in, customers would want to see open/standard APIs. Cloud users must not entrust mission-critical applications to cloud service providers so as to avoid outages when cloud service providers go out of business. They should also keep backups of the applications and data on premises. They should also secure favourable service-level agreements from the cloud service provider (Kim, 2009)

9. Conclusion

Cloud computing has transformed the knowledge society by offering enterprises the opportunities to decouple their IT needs and their infrastructure. It has therefore given rise to new business models and given the opportunity for those enterprises that would not have had the resources to compete in the knowledge society a renewed opportunity. As a result the area of cloud computing deserves to be given attention and further developed. This research does exactly that by contributing to the advancement of knowledge in that field.

References

Binning, D., Top five cloud computing security issues, [online], http://www.computerweekly.com/Articles/2010/01/12/235782/Top-five-cloud-computing-security-issues.htm

Carrigan, M., Alex, T., Ward, C., The US Patriot Act deconstruction, Civil Liberties and Patriotism, Journal of Business and Economic Research, Vol. 6, No. 3., pp. 19-30, 2008

Chow, R., Golle, P., Jakobsson, M., Masuoka, R., Molina, J., Controlling data in the cloud: outsourcing computation without outsourcing control, CCSW'09, Novembr 13, 2009, Chicago, Illinois, USA, pp. 85-90.

Cloud computing as a business continuity plan, [online], http://www.tectonic.co.za/2009/05/cloud-computing-as-a-business-continuity-plan/

Enki, D., Why cloud computing will never be free, ACMQUEUE, Distributed Computing, pp. 1-10, 2010.

Etro, F., The economics of cloud computing, [online], http://www.voxeu.org/index.php?q=node/4671

Foster, I., Zhao, Y., Raicu, I., Lu, S., Cloud computing and grid computing 360-degree compared

Gurav, U., Shaikh, R., Virtualisation – a key feature of cloud computing, International Conference and Workshop on Emerging Trends in Technology (ICWET 2010), pp. 227-229, TCET, Mumbai, India, 2010

Hidden risks of cloud computing, [online], http://lifehacker.com/5325169/the-hidden-risks-of-cloud-computing

How cloud computing can transform business, [online], http://blogs.hbr.org/cs/2010/06/business_agility_how_cloud_com.html

Kim, W., Kim, S. D., Lee, e., Lee, S., Adoption issues for cloud computing, proceedings of MoMM2009, December 14-16, 2009, Kuala Lumpur, Malaysia, pp. 2-5.

Kushida K.E., Breznitz,D., Zysman, J., Cutting through the fog: understanding the competitive dynamics in cloud computing, The Berkeley Roundtable on the International Economy (BRIE) Working Paper 190 (Beta), May 1, 2010

Lee, C.A., A perspective on scientific cloud computing, HPDC 2010, June 20-25, 2010, Chicago, USA.

Legal implications of cloud computing – Part One (the Basics and Framing the Issues), [online], http://www.llrx.com/features/cloudcomputing.htm

Legal issues associated with cloud computing, [online], http://www.labnol.org/internet/cloud-computing-legal-issues/14120/

Pearson, S., Taking account of privacy when designing cloud computing services, CLOUD'09, ICSE'09 Workshop, pp. 44-52, Vancouver, Canada, May 23, 2009.

The wisdom of clouds, [online], http://blog.jamesurquhart.com/2008/08/cloud-computing-bill-of-rights.html

Zhang, Q., Cheng, L., Boutaba, R., Cloud computing: state-of-the-art and research challenges, Journal of Internet Serv Appl, Vol 1, pp. 7-18, 2010

Interoperability Monitoring for eGovernment Service Delivery Based on Enterprise Architecture

Badr Elmir[1], Nabil Alrajeh[2] and Bouchaib Bounabat[1]
[1]Université Mohammed V – Souissi, Morocco
[2]King Saud University, Saudi Arabia
b.elmir@daag.finances.gov.ma
nabil@ksu.edu.sa
bounabat@ensias.ma

Abstract: Public administration has to prepare itself to deliver fully integrated eGovernment services. This delivery often requires cooperation via business processes interoperability across two or more departments. In this context, public departments and agencies need to implement interoperability using enterprise architecture techniques to structure business processes, and service oriented models to achieve their integration. Thus, it's quite interesting to adopt enterprise architecture paradigm and techniques to analyse, track and control the evolution degree of processes interoperability from the existing "as-is" state to the future "to-be" state. The present paper proposes a periodic monitoring approach based on an assessment method which considers three main aspects of interoperation: 1. Potentiality, reflecting the preparation to interoperate. The objective is to foster interoperation readiness by eliminating barriers that may obstruct the interaction. 2. Compatibility, referring to interoperation implementation through adequate engineering process. It aims to study the relation between the external interfaces of processes and the surrounding environment in order to ensure effective interaction. 3. Performance efficiency, focusing on monitoring operational performance. It consists of the availability assessment of the communication infrastructure and the supporting system in general. It considers also end users satisfaction of interoperation in use. The proposed method supporting tool, (IMT) for interoperability monitoring tool, assesses interoperability degree periodically through five steps: (i) Delineating the scope of interoperation; (ii) Quantifying the interoperation potentiality; (iii) Calculating the compatibility degree; (iv) Evaluating the operating performance; (v) Aggregating the degree of interoperability. In addition to its capacity to track the evolution of interoperation degree in time, the IMT measures the required effort to reach a planned degree of interoperability. Finally, to better illustrate how to use the proposed interoperability monitoring approach, we present a practical example of integrated public eService. It's a citizen oriented eService proposed by a public hospital that offers special fees for persons covered by social security insurances. It includes government to business collaboration and government to government one.

Keywords: integrated public eService, enterprise architecture, interoperability assessment, periodic monitoring, and eHealth

1. Introduction

Public administration has to prepare itself to provide fully integrated online services for citizens and businesses. In this context, horizontal cooperation in the public domain is a key enabler for eGovernment. Indeed, the delivery of most useful online governmental services often requires cooperation between two or more public administrations or agencies. This cooperation starts from simple information exchange and can reach business processes interoperability among public departments (Klischewski 2004).

The present work focuses on monitoring interoperability between automated business-processes involved in the provision of an integrated public eService. The studied processes may be located within a single organization or across a group of public partners. Therefore, the proposed approach is based on a five step measurement method (Elmir 2010b), and takes into account three main aspects:

- Interoperability maturity level of the environment surrounding the studied eService.
- Compatibility degree between the external interfaces of the involved business processes.
- Operational performance of the support systems used to provide the online service.

The objective of this work is to: (1) Identify the most important characteristics of interoperability used to deliver integrated public services. This work proposes a set of criteria used to assess interoperability in this context considering all aspects of collaboration. (2) Describe a monitoring approach of interoperability. This allows to know what is needed to reach a desired level of interoperability.

In this article, the second section is devoted to eGovernment system interoperability. The third section presents the assessment method based on a set of IT indicators for interoperability measurement. The fourth section proposes the monitoring approach model adopted in this study. This section presents also the platform developed to support interoperability monitoring in the context of integrated public eServices