

# **A Model for Managing Uncertainty on the Cloud**

**Badie N. Farah**  
**Eastern Michigan University**

*Cloud computing refers to providing computation services over the Internet. These Web-Based services are available to the public over network connections and managed by a third party which guaranties the availability of these services at an appropriate price. In this paper we will discuss the various sources of uncertainty that result from placing data and applications on the cloud. Furthermore, we will discuss counter measures to reduce or eliminate these uncertainties by instituting policies and procedures to decide what application and data to place on the cloud. In addition, we will provide a model for assessing uncertainty on the cloud.*

## **INTRODUCTION**

Cloud computing refers to providing computation services over the Internet. These Web-Based services are available to the public over network connections and managed by a third party which guaranties the availability of these services at an appropriate price. This presents an attractive option for some companies to delivering computing services to their businesses without maintain an IT operation (Yves, et al, 2010).

In this paper we will discuss the various sources of uncertainty that result from placing data and applications on the cloud. Furthermore, we will discuss counter measures to reduce or eliminate these uncertainties by instituting policies and procedures to decide what application and data to place on the cloud.

Cloud Computing is one of the biggest technologies in the IT world today. It evolves from the idea that work done on the clients can be moved to the “cloud” (Veiga, 2009). George Pallis (2010) describes Cloud computing as a coming together of different computing services such as Internet delivery, “pay-as-you-go” utility computing, elasticity, virtualization, grid computing, distributed computing, storage, content outsourcing, security, and Web 2.0. In his article on cloud computing, Pallis(2010) uses the US National Institute of Standards and Technology’s definition for cloud computing:

“Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (for example, networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model promotes availability and is composed of five essential characteristics [on-demand self-service, broad network access, resource pooling, rapid elasticity, and measured service], three service models [cloud software as a service, cloud platform as a service, and cloud infrastructure as a service], and four deployment models [private cloud, community cloud, public cloud, and hybrid cloud]. “(Pallis, 2010)

Daniele Catteddu and Giles Hogben (2009) in their paper on cloud computing suggested that the following characteristics of cloud computing services:

- Highly abstract resources
- Near instant scalability and flexibility
- Near instantaneous provisioning
- Shared resources
- ‘Pay as you go’ system
- Programmatic Management (Cattedu & Hogben, 2009, p 14)

They also stated that the forecast for cloud services in 2009 will be \$17.4 billion and in 2013, it will be \$44.2 billion. (Catteddu & Hogben, 2009, p 4)

### **Uncertainty with Computing on the Cloud**

Cloud computing, however, does not come without uncertainty. When the firm’s data is placed on the cloud, the firm has very limited control over such data. This makes the data exposed to hackers and other breaches. In a survey poll of InformationWeek Analytics, security concerns topped the list of reasons to not use cloud computing services (Shiple, 2010). Shiple (2010) illustrates that even the biggest of cloud providers, like Google, are subject to security breaches and therefore firms have every right to be concerned about their data on the cloud. Furthermore, applications that are hosted by the provider may not be available all the time, and/or they may not present the latest versions of these applications. As such, the client may encounter uncertainties with respect to these applications or the results that are delivered by these applications.

### **Sources of Uncertainty**

There exist a number of sources of uncertainty chiefly among them are:

- Missing information
- Trusting the available information
- Inconsistency of available information
- Irrelevant information
- Interpretable information

### **Potential Uncertainty Treatments**

After sources of uncertainty have been identified and assessed, all techniques to manage the uncertainty fall into one or more of the following categories:

- **Avoidance:** This implies not performing the activity associated with the uncertainty.
- **Reduction:** This involves employing methods that reduces the uncertainty. In the case of deploying applications on the cloud, uncertainty reduction may be achieved by deploying these applications incrementally. Outsourcing could be considered a form of uncertainty reduction if the developer can demonstrate a higher technical capability than the originator of the application.
- **Transfer:** This involves buying insurance where the damages from uncertainty could be compensated for by the insurance provider.
- **Retention:** This involves accepting the uncertainty and budgeting for it.

When selecting a cloud service provider, the “transparency” of the provider should be also taken into account (Shiple, 2010). Shiple (2010) found that some providers like Google were ready and open to questions, while others did not cooperate. Transparency and visibility of the key control features is important to assess areas like cloud provider's quality-assurance processes, service-level agreements, financial health, and dependence on other suppliers.

Shiple (2010) also suggests auditing to look into the security features of the cloud provider. SAS 70 type II audit is a letter of attestation and a report on the control objectives of the provider; but not many

firms are willing to let customers see their report on the control objectives. Shipley (2010) states in his article that an audit named CloudAudit A6, is being prepared to evaluate and assess the cloud providers thus making it easier for customers to access and choose an appropriate cloud provider.

Cloud Computing could benefit from a service level agreement (SLA) between the client and the cloud provider. Furthermore, the client should encrypt its data and use appropriate high security controls for sensitive data on the cloud (ICASA, 2009). According to the organization, the SLA will help cloud clients specify if joint control frameworks will be used, clarify expectation of both parties and state policies for disaster recovery. A strong SLA will be beneficial to both parties (ICASA, 2009).

John Wheeler (2010) recommends the following company's internal key areas to examine before adopting or considering cloud technologies:

- Organizational and Human Resource Security
- Access Control
- Asset Management
- Physical and Environmental Security
- Operations and Change Management
- Disaster Recovery and Business Continuity
- Privacy

Below is a list of some of the uncertainties that a cloud client might encounter depending on the services of the cloud provider and its willingness to grant access to its facilities to the cloud client.

- Governance: A cloud client may become uncertain about the governance of the software resources due to gaps in security with the cloud provider.
- Lock in: A cloud client can become very dependable on the service provider and prevents the client from changing providers. This adds uncertainty to the quality of information that the client receive from the cloud.
- Isolation failure: A cloud client could become uncertain about the separation of storage, memory, and routing between different tenants. The cloud client might not know, or be able to find out if such separation fails.
- Compliance risks: A client uncertainty might manifest itself if the cloud provider does not allow customer to audit it, or if the cloud provide cannot provide compliance with the needed requirements.
- Data protection: A cloud client might encounter another uncertainty about the information it is receiving from the cloud provider if the cloud customer cannot effectively check the data handling practices of the cloud provider or if the cloud provider is not willing to provide that information.
- Insecure or incomplete data deletion: When a client makes request to the provider to delete data, the provider may not truly delete the data because the disk to be deleted might also contain data from other cloud clients. This represents uncertainty about the data to the cloud client (Catteddu & Hogben, 2009, p 9-10).

A cloud client is responsible for dealing with all the uncertainties that are generated from using a cloud provider to handle its data and applications. It is beneficial for a cloud client to take certain precautions before adopting the cloud technology. Taking these precautions will reduce or mitigate the uncertainties that such a client will certainly encounter after adopting the cloud technology. The following are some precautions that could be exercised by a cloud adopter.

- A cloud client should determine if the data is suitable to be put on the cloud. Performing cost benefit analysis will definitely help in the process of classifying which data should be considered as a candidate for the cloud.
- A cloud client should find a cloud provider that does security assessments to determine whether the application or the data is ready for the cloud.

- A cloud client may start with non-sensitive and less valuable data on the cloud. This is an important first step until appropriate measures are considered and implemented to reduce the uncertainty that the cloud introduce into applications and their data.
- A cloud client may evaluate service provider agreements to determine how the cloud provider secures data. This evaluation is detrimental in choosing a cloud provider since it reduces the uncertainty of the client.
- A cloud client should also insist on transparency of the cloud provider so that they understand what's happening underneath the virtual cloud infrastructure. This also goes a great way in reducing the uncertainty of the client with respect to its data on the cloud (HP, 2010).

Some or all of the above precautions may be instituted as policies and/or procedures for farming data and applications to the cloud. A careful draft and adherence to these policies and procedures will go a long way to reducing, or even, eliminating some of these uncertainties.

### **A Model for Assessing Uncertainty on the Cloud**

Applications which are included in the IT portfolio of an organization are usually subjected to cost/benefit analysis, unless it happened to be the result of a directive to comply with rules and regulations. As such, a measure of uncertainty in cloud computing is a function of this cost/benefit analysis for each project.

We could look at such a function as a percent reduction in benefits from the cloud. That is, if the organization expects to save \$X as a result of using cloud services for a particular application, then probably the net saving is

$\$(1-\beta) X$  where  $\beta$  is the fraction of X that is lost due to uncertainty of placing the application on the cloud

As  $\beta \rightarrow 1$ , the savings decrease until they equal to \$0.

For  $\beta = 0$  (no risk) the net savings remains at \$X.

For a portfolio of applications that a business might be interested in placing on the cloud the total net savings (T) that might accrue is given by the following formula:

$$T = \sum_1^n (1 - \beta_i) X_i$$

Where n is the number of applications to be placed on the cloud,

$X_i$  is the savings from application  $i$ , and  $\beta_i$  is the fraction of X that is lost due to placing application  $i$  on the cloud which may be used as a decision variable by management. That is, an application might be a candidate for the cloud if its  $\beta_i \leq c$ , where c is a constant determined by management to be the maximum acceptable level for reduction in the savings for any application.

### **Assessment of $\beta_i$ 's and $X_i$ 's**

Assessing  $\beta_i$  depends on assessing  $X_i$  and the experience of the firm in estimating savings and cost of uncertainty. The value of  $\beta_i$  is dependent on loss as a result of placing an application on the cloud for reasons including compromise of data integrity, downtime of application, degradation of performance of data link connection, availability and dependability of customer service. It further depends on the cost of posting the application on the cloud. And that is a function of the charges (rate and time) the provider requires to post an application. For example, you may have to pay for a (24 by 7) application availability, while your application is not needed (or used) during the weekend. Or similarly, your application is not needed overnight.

Assessing the  $\beta_i$  may be facilitated by considering other people experiences with the considered provider; or different providers. None the less, the better (more accurate) the estimate, the better the

decision of placing an application on the cloud will be. Furthermore, available data about past performance of the provider may play a role in enhancing the estimates of the  $\beta_i$ 's. Sensitivity analysis could be used to assess the robustness of the decision for a varying (or interval) values of the  $\beta_i$ 's.

This approach provides a framework for dealing with the assessment of  $\beta_i$ 's and  $X_i$ 's and could help in reducing the uncertainty about posting applications on the cloud.

$\beta_i$ 's and  $X_i$ 's may be assessed using quantitative methods such as Analytical Hierarchy Process or Decision Trees with monetary values associated with possible outcomes. Alternatively or when quantitative assessment is not plausible, we may use qualitative methods such as rankings rendered by a panel of experts. When it is desirable, both quantitative and qualitative methods may be used. In such a case, a function may be used to augment all measures and produce a point estimate for  $\beta_i$ 's and  $X_i$ 's. In the next section we will describe the variables that may be used to estimate  $\beta_i$ 's and  $X_i$ 's.

### **Determining the Variables that Make $\beta_i$ 's and $X_i$ 's**

#### *$X_i$ Variables*

These variables represent the saving (cost reduction) that might be the result of placing the applications on the cloud. The saving is a function of variables that include: savings from needing less IT staff; the cost of purchasing and updating necessary software (such as Microsoft Office); savings from purchasing, upgrading and maintaining servers, server software; and savings from purchasing database software.

#### *$\beta_i$ Variables*

These variables contribute to the uncertainty of the application being on the cloud and are associated with: the reliability of the application being on the cloud (downtime and loss of business); the security issues associated with the application being on the cloud; cost of maintaining the application on the cloud when the application is not in use (for example paying fees for the provider over the weekend even though the application will never be used over the weekend); availability of the helpdesk 24 by 7 by phone or only email and what is the turnaround time (in essence if a business dismantles its IT department in favor of the cloud, would they still get technical help when needed in a timely fashion?); the cost of customizing an application if necessary; and other variables that the organization deems necessary.

### **SUMMARY**

Cloud computing refers to providing computation services over the Internet. These Web-Based services are available to the public over network connections and managed by a third party which guarantees the availability of these services at an appropriate price. In this paper we discussed cloud computing, the various sources of uncertainty that result from placing data and applications on the cloud, and counter measures to reduce or eliminate these uncertainties by instituting policies and procedures to decide what application and data to place on the cloud. A further analysis of these procedures and policies with respect to their effectiveness and efficiencies is in order. Furthermore, the paper discussed a possible model for managing the uncertainty on the cloud with respect to the saving that might accrue, and the reduction of such saving that might be the result of placing the application on the cloud. We argued that such analysis should be based on data collected from firms that have used, or using, the cloud for their software applications. Instruments for data collection should be designed, firms identified, and these instruments administered in the selected firms. The collected data is then utilized to assess the efficiencies and effectiveness of these policies and procedures, as well as, the measures for assessing the saving and risk of placing applications on the cloud.

## REFERENCES

Bublitz, E. (2010). Catching The Cloud: Managing Risk When Utilizing Cloud Computing. Retrieved November 17, 2010 from <http://www.property-casualty.com/Exclusives/2010/8/Pages/Catching-The-Cloud-Managing-Risk-When-Utilizing-Cloud-Computing.aspx>

Catteddu, H. (2009). Cloud Computing: Benefits, risks and recommendations for information security. *European Network and Information Security Agency*. Retrieved October 12, 2010 from <http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment>

Giard, Y. & Lessard, A. (2010). *CA Magazine*. Toronto, May, 143, (4), 37-39.

HP (2010). Cloud computing security risks. Retrieved November 17, 2010 from <http://h71028.www7.hp.com/enterprise/us/en/messaging/feature-enterprise-cloud-security.html>

ICASA (2009). Cloud Computing: Business Benefits With Security, Governance and Assurance Perspectives. Retrieved November 3, 2010 from <http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Cloud-Computing-Business-Benefits-With-Security-Governance-and-Assurance-Perspective.aspx>

Pallis, G. (2010). Cloud Computing: The New Frontier of Internet Computing (HTML), *University of Cyprus* September/October, 14, (5), 70-73. <http://www.computer.org/portal/web/csdl/abs/html/mags/ic/2010/05/mic2010050070.htm>

Shiple, G. (2010). Cloud Computing Risks. *Information Week*, April, (1262), 20-22, 24. Retrieved October 20, 2010, from ABI/INFORM Global. (Document ID: 2022248671).<http://proquest.umi.com.ezproxy.emich.edu/pqdweb?did=2022248671&sid=2&Fmt=3&clientId=594&RQT=309&VName=PQD>

Viega, J. (2009). Cloud Computing and the Common Man, *Computer*, August, 42, (8), 106-108, doi:10.1109/MC.2009.252 <http://csdl.computer.org.ezproxy.emich.edu/dl/mags/co/2009/08/mco2009080106.pdf>

Wheeler, J. (2010). Dealing with the risks of Cloud Computing. Retrieved November 3, 2010 from <http://www.openpages.com/blog/index.php/dealing-with-the-risks-of-cloud-computing>