Volume 6, Issue 3
August 2013
ISSN: 1946-1836

JOURNAL OF INFORMATION SYSTEMS APPLIED RESEARCH

Special Issue: Cloud Computing

In this issue:

The **Journal of Information Systems Applied Research** (JISAR) is a double-blind peer-reviewed academic journal published by **EDSIG,** the Education Special Interest Group of AITP, the Association of Information Technology Professionals (Chicago, Illinois). Publishing frequency is currently quarterly. The first date of publication is December 1, 2008.

JISAR is published online (http://jisar.org) in connection with CONISAR, the Conference on Information Systems Applied Research, which is also double-blind peer reviewed. Our sister publication, the Proceedings of CONISAR, features all papers, panels, workshops, and presentations from the conference. (http://conisar.org)

The journal acceptance review process involves a minimum of three double-blind peer reviews, where both the reviewer is not aware of the identities of the authors and the authors are not aware of the identities of the reviewers. The initial reviews happen before the conference. At that point papers are divided into award papers (top 15%), other journal papers (top 30%), unsettled papers, and non-journal papers. The unsettled papers are subjected to a second round of blind peer review to establish whether they will be accepted to the journal or not. Those papers that are deemed of sufficient quality are accepted for publication in the JISAR journal. Currently the target acceptance rate for the journal is about 45%.

Questions should be addressed to the editor at editor@jisar.org or the publisher at publisher@jisar.org.

JOURNAL OF INFORMATION SYSTEMS APPLIED RESEARCH

Editors

JISAR Editorial Board

Demystifying the Fog: Cloud Computing from a Risk Management Perspective

Joseph Vignos
jvignos@walsh.edu

Philip Kim
pkim@walsh.edu

Walsh University
North Canton, Ohio 44720 USA

Richard L. Metzer
rick.metzer@lmco.com
Robert Morris University
Pittsburgh, PA 15222, USA

Abstract

Continual advances in technology and product differentiation have led to the dawn of cloud computing where virtually any computerized service – hard or soft – can be outsourced. Now that well-known companies such as Amazon and Google use their spare capacity and specific expertise for this purpose, all small business owners and IT managers must take its offerings into consideration. The potential benefits as well as the risks involved need to be weighed in light of the overall business strategy before deciding which services to engage. There are a great deal of services and applications available and choosing among them requires a multi-factor analysis. Because cloud computing is a young field and involves placing company assets under external control, there is significant risk involved. The manager or CIO must carefully select which aspects of his/r business model are amenable to roam in the cloud and use a variety of criteria to make a final decision. This paper examines an experimental approach to assessing whether organizations are ready for cloud computing.

Keywords: cloud computing, public cloud, software-as-a-service, and risk management

1. INTRODUCTION

Cloud computing continues to draw headlines and forecasts look impressive even in a sluggish economy. Investment is expected to increase to more than $120 billion by 2015. But should companies invest in it? And if so how much? Jumping right in could put businesses at risk, while waiting until it is completely safe could leave the organization playing catch-up with the competition (Loebbecke, 2012).

Officially, the National Institute of Standards and Technologies (NIST) has defined cloud computing 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 & Grance, 2009, p.2).

In plain English, that means either offering or using computer hardware, software and/or

services over the internet. A cloud is an apt metaphor because the internet can be accessed from almost anywhere on earth today, even via a mobile phone. Storing e-mails on a Yahoo! server means you are using and relying on the cloud.

The NIST standards list the five characteristics of cloud computing as 1) On-demand self-service: server time and network storage are always automatically available; 2) Broad network access: computers can be reached through standard and mobile devices; 3) Resource pooling: storage, processing, network bandwidth, virtual machines and more can be assigned to many users simultaneously; 4) Rapid elasticity: capabilities can be quickly scaled up or down to satisfy demand; and 5) Measured service: services are optimized by metering out each service based on actual use (Mell & Grance, 2009)

The model that cloud service providers seem to be following is that of a utility company. Katzan (2010) labels the key characteristics as a) necessity: most of us consider computers and the internet to be necessary today; b) reliability: we expect water or electricity to be available 24/7; c) usability: getting on and off the cloud should be as easy as flipping a switch; and d) scalability: there should be ample resources available, yet users are only charged for actual consumption, and perhaps a small monthly fee. On the other hand, the cloud increases risk because you can be providing unauthorized access to private and proprietary information, which could possibly be mishandled or stolen.

One of the primary decisions a manager will have to make is what type of cloud to use. For this purpose, clouds can be classified into four types (Mell & Grange, 2009).

Private: This is operated for one organization only; it is the most secure and the most expensive. It can be hosted internally or externally, and can be managed either internally of by a third party. Géczy et al (2012) explain that a private cloud is on the organization's own premises and accessed via an intranet.

Public: This is owned and operated by the provider and available to the general public either for free (like Microsoft and Google's e-mail) or on a pay-per-use model. This is less secure than a private cloud, and depends on the levels of security provided by the service provider.

Community: This is shared by several organizations with a common purpose or requirements, thus the cost can be shared. It too can be managed and/or hosted internally or externally.

Hybrid: This is a combination of two of the above working together which share some data and applications. This type of cloud uses both on-site and off-site resources. It is more flexible for using applications, but there is a trade-off between more capacity and less security than with a strictly in-house system.

The four cloud types must be juxtaposed with three general layers of cloud services. The manager must decide which service(s) to use on which type of cloud(s).

Software as a service (SaaS): This is the most common service, whereby the customer uses the internet to access the provider's software hosted on the cloud at any time. A manager may choose to run any number of applications, including those for CRM, HRM, MIS, ERP or accounting.

Platform as a service (PaaS): the customer can use the cloud provider's infrastructure and tools to create and run its own software and applications; however, each provider has a limited set of tools and programming languages, such as Java and .NET. Companies can make their code available to others and lease unused infrastructure space this way.

Infrastructure as a service (IaaS): the processing, storage, networks, etc. are maintained by the cloud service provider, while the customer can choose and control the operating system and applications to run for its particular needs.

SaaS, PaaS and IaaS share several traits. They are all delivered over the web, and services can be accessed in the cloud on demand, usually via subscription fees or in a pay-as-you-go model. At any time, services can be upgraded or downgraded to accommodate current needs. This way they are expensed rather than capitalized.

2. ADVANTAGES

Switching from a traditional IT infrastructure to the cloud is like a manufacturing company changing from steam to electricity 100 years ago (McAfee, 2011). There are several reasons that organizations should consider the cloud.

The most popular reason given is usually cost. Rather than purchase hardware or software off the shelf, a new company can rent these services. This also reduces operating costs for maintaining equipment and paying IT personnel. In one extreme case, the IT manager at Coleman Data Services in Ohio reported his IT costs went from $2000 to $150 per month when he migrated to the cloud (McDaniel, personal communication). McAfee (2011) states that only 11% of a company's IT budget is spent on developing new applications. He suggests focusing on research and development to develop proprietary software, and that equipping employees to navigate the cloud would be a better use of resources (McAfee, 2011).

Another advantage of using the cloud is the provider may have useful software unknown to the customer. When Fairchild Semiconductors was not happy with its ERP package, it went to Workday and chose the standardized options Workday had developed by collaborating with 150 other companies. As users modify the configuration, Workday incorporates their best ideas or adds them as an option (Laudon & Laudon, 2012). The software is always up-to-date because providers are expected to have the most modern equipment. There is no need to constantly update and all members have the same version.

Key to the cloud-based model of IT is the integration of an organization's architecture. When Thomson and Reuters merged in 2008, they decided to use Salesforce instead of their own separate systems. By consolidating their data, they could share client account and other information at a lower cost (Iyer & Henderson, 2012).

Location independence is another advantage, especially for companies spread over a wide area or between countries. The Japanese corporation Fujitsu is in the process of having all 170,000 of its employees in 500 offices move to a private cloud where it can place all its files rather than having to upload them from an FTP server (Laudon & Laudon, 2012).

Businesses can increase worker output as well. Balfour Beatty decided to store company information on Box, allowing employees to access it while working overseas by using a web browser. This method also enabled personnel to manage their own accounts and apps without going through the IT department. This helped end users collaborate and share up-to-date information with both upstream and downstream partners (McAfee, 2011).

With Platform as a Service, users can create their own applications. Apple is the best example of this, offering tools for this purpose on its platform. When doctors at Rehabcare began using their iPads for patient screening, average wait time dropped from 18 hours to under 60 minutes (Iyer & Henderson, 2012).

Another benefit of cloud computing is that some clouds can blend into one another. Businesses can use different clouds for different aspects of their business, such as accounting, HR and production. The Small Business Web is a group of vendors forming an ecosystem of software applications that all customers can use. As long as the customers' APIs are open, they can share apps and information with others (Iyer & Henderson, 2012).

A final example is the San Francisco Bay area public transit authority, which moves 350,000 people/day. In 2009 it replaced its legacy system with Oracle's PeopleSoft applications running on HP servers with a Linux OS. In addition to providing more reliable service, its cloud is eco-friendly, using 20% less electricity (Laudon & Laudon, 2012).

3. DISADVANTAGES

The reason many companies are not jumping on the cloud is because of concerns over privacy, security and reliability. Ryan (2011) discusses the privacy issues that a conference chair must consider when using the cloud like EasyChair to host convention data. There are benefits and risks involved in leaving your data in the hands of others, but the open nature of the technology makes the system susceptible to bribery or coercion. He concludes that while a provider's reputation depends on its service, organizations cannot rely on people's sense of good behavior (Ryan, 2011).

Another major concern is reliability. In 2011 Amazon Web Services went down for three days in some places, causing a significant loss of revenue to many subscribers. When one organization is dependent upon another for critical services like internet access and data storage, then availability and system up-time requirements should be analyzed before migrating to cloud services. Another key element is to have an adequate backup system in place. Netflix developed its own redundant system when it adopted the Amazon cloud and

consequently suffered no loss during the blackout. In general, every organization experiences some downtime, and moving to the cloud does not significantly change this (McAfee, 2011).

Security is the third main issue facing cloud providers. How secure is the cloud? Who has access to your confidential and proprietary data? Does Toyota want its designs in the same network partition that Hyundai uses? While these concerns are legitimate, the same concerns would exist if the organization maintained its own IT infrastructure. All organizations are vulnerable to both internal and external attacks and should consider the appropriate access controls and security policies to ensure their data is secured. Hayes (2008) raises the issue of ownership. Can you take all your data and customized apps with you if you change providers? Can you delete records? And what happens if you can't pay your monthly bill?

4. RISK MANAGEMENT

In a more in-depth analysis, Iyer and Henderson (2012) name five business risks. First, there is a *falling demand* risk due to internal or external factors. This is especially fluid in the pay-per-use model of cloud computing. Second is *inefficiency risk* – companies with higher relative costs will lose out. Iyer and Henderson (2012) believe that outsourcing IT infrastructure and routine tasks makes a business more efficient, as in the case of Fairchild, which saved 15% in expenses and 50% in time when it used Workday. Third is *innovation risk* – the less innovative companies will falter. Even this can be outsourced, as when customers tap into Salesforces' continually expanding number of apps. Fourth is *scaling risk* – the risk that expansion for a new project will not pay off once it is finished. This is like the risk cities take when hosting an Olympics. Finally, *control risk* is the danger of inadequate internal controls to prevent and detect unauthorized access.

Iyer and Henderson (2010) then discuss seven ways that cloud computing mitigates these risks (Appendix 1). By "orchestrating dependencies" they mean a company's ability to match its dependence on various providers with the several needs of the company, such as using Salesforce for CRM. The "Facebook effect" refers to loyalty: designing features around user experience. Facebook carries out extensive testing before it launches a new feature, and then it analyzes user behavior to understand trends (Ivan & Henderson, 2010, p.54), thus anticipating demand.

The seven ways that cloud computing can add business value are:

1. Controlled interface: applications can be used by other services using an application program interface (API) – specifications used by software components to communicate.
2. Location independence: controls access to assets from anywhere within the enterprise
3. Sourcing independence: controls access to services and allows the company to change providers without penalty
4. Virtual business environment: integrated apps and tools that support business needs
5. Ubiquitous access: users' ability to access any service from any platform with a browser
6. Addressability and Traceability: the address of users and the usage of services can be tracked
7. Rapid elasticity: service usage can be scaled up or down automatically (Iyer & Henderson, 2010, p.56).

Ivan and Henderson (2010) indicate how these seven capabilities can control the five risks previously listed (Appendix 2). For example, demand risk can be dealt with by maximizing user access, tracking users and usage to look for causes, and either scaling up service to satisfy customers or scaling it down in order to minimize cost.

5. STRATEGY

Cloud computing greatly lowers the barriers to entry, not only due to lower hardware costs, but because software programs can eliminate the learning curve involved with each service area. Rhoton (2010) warns that it is important to get the right provider because the costs of changing clouds can be high due to incompatible programs or operating systems.

The bargaining power of customers is also increasing as the number of providers and users increases, bringing down prices. The threat of substitutes exists with the constant entry of more providers, who continuously offer more services and new applications. Companies should be very happy with their own apps before they choose to ignore the growing menu on tap in cyberspace.

Rhoton (2010) recommends a focus on product differentiation and believes that cloud computing makes a company more agile. Because

information is more widely available due to global networks, the time from when a new product is designed to when it gets to market needs to be accelerated. Even then the advantage is only temporary; consequently, companies should keep focused on their core competencies of creating new products.

Ultimately, outsourcing cloud services (or "cloudsourcing") can allow a business to change its entire strategy. If internal IT resources are a weakness, it can soon become a strength as the field trends toward XaaS – everything as a service (Rhoton, 2010).

6. SELECTION

If cloud technology is the revolutionary technology many claim, a company must take measures to minimize the risk to its mission and strategy to achieve its goals. Management needs to take an inventory of its business processes and decide which ones can be safely outsourced without losing control over its core competencies. There will also be financial repercussions with changes in cash flow and the shift from capital to operating expenses.

Making financial calculations related to the change to cloud computing is very difficult because it's a new field and the effects are hard to gauge. There is not yet enough data to calculate a discount rate for risk or a standard deviation for variability. Because cloud computing is considered risky at present, banks may charge a higher interest rate than for other projects. Finance managers should take this into account when making scenario analyses for risk and return decisions.

Rhoton (2010) provides a list of the components of an extant IT system which should be compared with the costs of the cloud option, including hardware, network infrastructure and connectivity, software, security, support, operations, service, and contract management. Normally, procurement may only be 25% of the total cost of IT investments. There are also capital costs – installation and maintenance; transition costs – training users and integrating the legacy system with the cloud; and operating costs such as support, overhead, and any license or usage fees.

Most businesses do not want to put everything on the cloud at once. It is advisable to first make an inventory of the software applications in stock and decide which ones are safe and less expensive to put on the cloud. There are many technical considerations which IT personnel should be consulted on, such as the degree of customization needed to interact with the cloud (Rhoton, 2010).

Any new IT projects undertaken by a company involve a number of rent vs. buy decisions. Much depends on the available expertise in the IT department. Unless control over private data is a paramount concern, it may be cheaper to cloudsource many services than to hire new personnel. With so many cloud services offered, most IT personnel need only be concerned with maintenance and security.

Software as a service is the most common use of the cloud. Many services are prefabricated like the web pages hosted by Yahoo. They can be customized for a price, which may be necessary to differentiate a brand. The interaction with the customer is very important and must be monitored closely at the outset.

Infrastructure as a service is the most flexible offering. The company can choose among hardware and network facilities, or separate components of these, such as CPU time. The amount of storage and bandwidth needed can also be priced. Another advantage of cloudsourcing is that many costs are itemized without having to calculate overhead.

Platform as a service is the least developed to date. This includes many tools for application design and development. If the platform is multi-tenant, the number of programming languages and interfaces are strictly limited in order to protect the other tenants. Géczy et al (2012) says this is necessary for small companies that need to integrate with third-party systems or large-scale testing. There is a risk of vendor lock-in whereby material must be left behind when the contract is terminated. One must also check for backward compatibility – that versions do not become incompatible when the platform updates (Rhoton, 2010).

The choice of provider is obviously extremely important. There is an abundance of cloud providers today, but many of them new and unproven. Public companies are considered more reliable since they must publicize information about how they store data and what security measures are in place. Companies may also state whether they follow audit standards like SAS 70, or have ISO or NIST certificates. Rhoton (2010) gives four criteria to take into consideration:

Environment – encompasses the location of the building and its power supply, HVAC and security.

Technical – the amount of capacity and bandwidth available, as well as security concerns such as tenant isolation and a separate encryption key for each business.

Contractual – how usage is measured and billing is determined. The terms of service should specify how the provider will handle incidents such as DoS or hack attacks and viruses. The provider may not want to make these public, but a company needs to know about all of these.

Financial – The status of the company as an on-going concern is quite relevant for a long-term contract. Consult Moody's and other credit raters, and again, public companies are more forthcoming with financial statements and debt level.

Balanced scorecard

A company's balanced scorecard may also be consulted before making the jump to the cloud. This is a group of performance measures intended to evaluate the company vision and strategy. Each item should be noted such that judgments can be made about whether the company is improving. If no scorecard exists, one could be created for the questions raised during deliberation. The Balanced Scorecard (BSC) normally has four perspectives, Internal Business Processes, Learning and Growth, Financial, and Customer (Kaplan & Norton, 1996). Cloud computing could fit as an initiative within each of the four dimensions of the BSC. However, it would be helpful to have a control group not affected by the cloud implementation for comparative purposes.

The most important element is the customer. Placing that client's data and business in the hands of another entity does not diminish any responsibilities of the primary data owner. Customer satisfaction can still be measured by surveys and indicators such as the number of complaints, new customers, and retention rate.

There will be many factors to evaluate in the operations section of the scorecard. The primary factor is the sales numbers, but other factors include response time in the customer service center and throughput time in internal business processes such as manufacturing, processing, and logistics. Learning and growth and human resources will also be affected, so training and value-added performance need to be measured to avoid under or over-staffing.

7. IMPLEMENTATION

Considering the risks involved, managers must plan carefully before moving some of their business processes to the cloud. Iyer and Henderson (2012) recommend short-term experiments. New technologies should be matched with internal needs. Using the scientific approach, a business unit can formulate a hypothesis and assess the outcome of the experiment.

On less expensive public clouds like Amazon, there is very little support. Potential users need to join online user groups where they can find out what the common problems are, share knowledge, and get answers to FAQs. If moving to the cloud gradually, a competent IT team is needed to maintain compatibility between the legacy systems and new architecture.

Decision-makers must also consult with their upstream and downstream partners to understand their plans for the future. The clouds are not all interchangeable, so compatibility could become an issue.

McAfee (2011) also recommends an experimental approach. CIOs first need to meet with their counsels and compliance experts to understand any restrictions on sharing confidential and private data. Infrastructure-as-a-service is mature now and new development projects are a good fit for the cloud. The hardware and software are all ready to plug in and play, so more time can be spent writing proprietary code. Google Maps is one well-known application. One energy company in Queensland used this to map its 150,000 km. of power lines in order to make better environmental impact and risk management decisions (McAfee, 2011).

8. CONCLUSION

Although financial analysts will have their work cut out for them when deciding whether to include a shift to the clouds in the budget, cost is only one of many important factors to weigh. While security and reliability concerns have kept many from taking the leap, risk management also includes the business risks that exist when a company does not keep up with the competition.

Cloudsourcing can be ideal for smaller companies with limited capital and funds to invest in IT infrastructure, or limited human resources with IT expertise to run an in-house platform. There are also many routine IT operations for a medium or large company to outsource, such as accounting entries, data entry, and logistics.

In reality, cloud computing is nothing mysterious and should be seen as a potential way for organizations to do business. It has become almost as common as the internet that ties people to e-mail and e-commerce. Any company that relies heavily on IT for sales or analytics needs to prepare for the day when nearly all services may be provided inexpensively through the cloud by companies such as Amazon and Google. The best strategy for most organizations will be to begin their cloud implementation one incremental step at a time.

9. REFERENCES

Brown, F. (2012, May 27). Personal interview.

Géczy, P., Izumi, N., & Hasida, K. (2012). Cloudsourcing: Managing cloud adoption. *Global Journal of Business Research* (GJBR), 6(2), 57-70.

Hayes, B. (2008). Cloud Computing. *Communications of the ACM*, *51*(7), 9-11.

Iyer, B., & Henderson, J. C. (2012). Business value from clouds: learning from users. *MIS Quarterly Executive*, *11*(1), 51-60.

Katzan Jr., H. (2010). On An Ontological View of Cloud Computing. *Journal of Service Science (19414722)*, *3*(1), 1-6.

Kaplan, R. S. & Norton, D. P. (1996). Linking the balanced scorecard to strategy. *California Management Review*, *39*(1), 53-79.

Kenealy, B. (2012, April 23). Working definition of cloud computing established. *Business Insurance*, Vol. 46, 7.

Laudon, K., & Laudon, J. (2012). *Management Information Systems* (12th ed.). Upper Saddle River, NJ: Prentice Hall.

Loebbecke, C., Thomas, B., & Ullrich, T. (2012). Assessing cloud readiness at Continental AG. *MIS Quarterly Executive*, *11*(1), 11-23.

McAfee, A. (2011). What Every CEO Needs to Know About The Cloud. *Harvard BusinessReview*, *89*(11), 124-132.

Mell, P. & Grance, T. (2009). The NIST definition of cloud computing. *National Institute of Standards and Technology, Special Publication 800-145.*

Rhoton, J. (2010). *Cloud Computing Explained* (2nd ed.). Recursive Press.

Ryan, M. D. (2011). Cloud Computing Privacy Concerns on Our Doorstep. *Communications Of The ACM*, *54*(1), 36-38.

Editor's Note:

This paper was selected for inclusion in the journal as a CONISAR 2012 Distinguished Paper. The acceptance rate is typically 7% for this category of paper based on blind reviews from six or more peers including three or more former best papers authors who did not submit a paper in 2012.

APPENDIX 1

Table 1. Benefit Patterns and the Business Risks They Help Mitigate

	Business Risks				
Business Benefits	Demand	Inefficiency	Innovation	Scaling	Control
Increased business focus			√		
Reusable infrastructure	√	√		√	√
Collective problem solving		√		√	√
Business model experimentation	√		√		
Orchestrating dependencies	√	√			
Facebook effect	√				

Iyer & Henderson, MIS Quarterly Executive, 2012, Vol. 11 Issue 1, p.55

APPENDIX 2

Table 2. How Cloud Computing Capabilities Can Mitigate Business Risks

	Business Risks				
Cloud Computing Capabilities	Demand	Inefficiency	Innovation	Scaling	Control
Controlled Interface			√		√
Location independence		√			
Sourcing independence		√		√	
Virtual business environment		√	√		
Ubiquitous access	√	√	√		
Addressability and traceability	√		√		√
Rapid elasticity	√			√	

Iyer & Henderson, MIS Quarterly Executive, 2012, Vol. 11 Issue 1, p.57