**Managing Cloud Complexities – Boosting Operational Coherences for Global & Diversified Projects**

# 1. Introduction

Cloud computing is a technology that uses the internet and central remote servers to host data and applications. It allows individual consumers and businesses to use applications without installation and also offers personalized data storage on remote servers, to access their files from any computer with internet access. This technology allows for much more efficient computing through the distributed computing architecture and by centralizing storage, memory, processing and bandwidth. Anything that involves delivering hosted services over the Internet is generally termed as ‘cloud’. In the marketing field, cloud computing is a term for technologies that provide computation, software, data access, and storage services that do not require end-user knowledge of the physical location and configuration of the system that delivers these services.

According to Jin et al.’s article (Jin, et al., 2010) on tools and technologies for building clouds, cloud computing refers to the hardware, systems software, and applications delivered as services over the internet. Cloud computing serves to describe a new supplement, consumption, and delivery model for Information Technology services based on Internet protocols. It typically involves provision for dynamic scaling of virtualized resources. Cloud computing providers deliver applications via the internet, which are accessed from web browsers on desktop and mobile apps, while the business software and data are stored on servers at a remote location. But here, it is to be noted that the broader concept of infrastructure convergence and shared services lie at the foundation of cloud computing. Making use of this type of data center environment, enterprises can now get their applications up and running faster, with easier manageability and less maintenance, thereby enabling IT to more rapidly adjust their resources (such as network bandwidth or storage) to meet fluctuating and unpredictable business demand. Not all applications benefit from deployment in the cloud; Issues with latency, transaction control, and in particular security and regulatory compliance are of primary concern (Sosinsky, 2011).

# 2. Cloud Computing as a Business Solution

According to Laszewski and Nauduri, the basic premise of cloud computing is that users can get access to any IT resource, including storage, CPU resources, memory, and software, over the internet whenever they want, and can pay for their actual use of the resource rather than incurring capital and operational expenditures in order to own and operate the IT infrastructure (Laszewski & Nauduri, 2011). Many businesses have now taken a good look at cloud computing and have decided whether some form of cloud would be an ideal solution to part of their need for IT. A company's business situation is either a problem or an opportunity for which it seeks a solution that includes IT enablement. It sees cloud computing as a technological possibility that is the way to solve the problem, or seize the opportunity thereby making cloud computing its IT architecture vision. For example, an international retailer might have a vision that "We will cope better with peak business demand by deploying our applications software on cloud computing platforms which can be accessed through the internet from any part of the world." However, it is to be taken note here that cloud computing is often confused with other similar paradigms. Examples of common computing models that are not cloud computing are: peer-to-peer networks, Service-Oriented Architecture (SOA), grid computing, and network asset sharing (Harding, 2011).

The next question that is often posed by organizations that look forward to move into the cloud is, "Which particular cloud service should we use?" There are now many competing services, and there are complex factors, including functionality, performance, manageability, security, and compliance with regulation, that must be considered in making the choice.

In a business environment, the business processes are how work gets done. They are supported by applications that manage information content and perform transactions. These are in turn supported by a platform and infrastructure that provide storage, processing, and communications. Cloud computing enables businesses to create and use services on demand, through cloud *SaaS* (Software-as-a-Service), *PaaS* (Platform-as-a-Service), and *IaaS* (Infrastructure-as-a-Service). Examples of such services include business services, application software services, integration and development services, and infrastructure services. The applications, platform and infrastructure layers of a business, thus can be replaced by cloud services, as shown below in Figure 1.

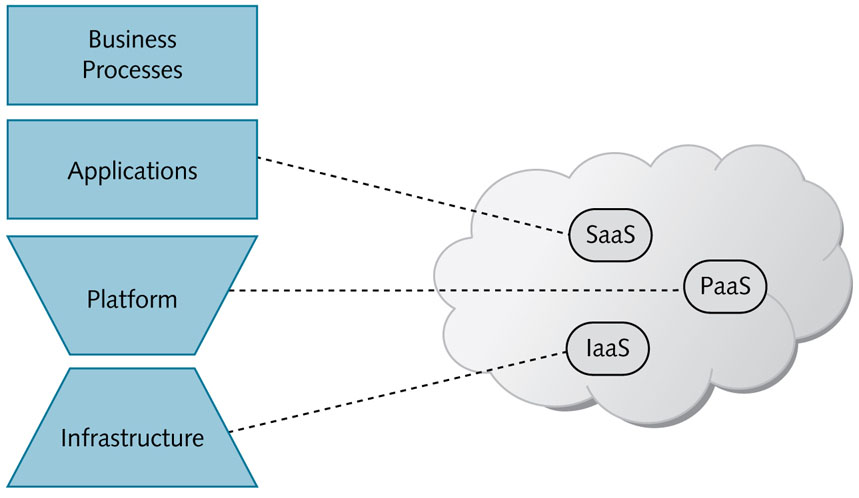


Figure 1: Cloud Services

Cloud computing enables providers and consumers of products and services to interact much more easily, because they are freed from the expensive task of providing the necessary IT support. This encourages the creation and growth of ecosystems in which companies co-operate effectively to meet the needs of society. The benefits of cloud computing extend not just to individual businesses, but to business as a whole.

# 3. Cloud computing – Current and future trends

Cloud technologies contribute to the enhanced functionality for the federal workforce to improve interoperability, feedback, collaboration, and dissemination of information. By using commercially available cloud technologies, offered government services can be more cost-effective and can provide a better Quality of Service (Chang, Abu-Amara, & Sanford, 2010). A forecast of Cloud services (Business Process as a Service, Software as a Service, Platform as a Service and Infrastructure as a Service) from 2011 to 2020 is shown in Figure 2. Forrester, an analyst firm predicts that it will generate greater revenue potential which can clearly be seen from Amazon Web Services (AWS), the undisputed commodity IaaS revenue leader. Investment bank, UBS reported that AWS earning statement could jump from $550 million in 2010 to $750 million in 2011. This year, AWS reveals that its *S3* storage service hosts doubled as it now hosts more than 262 billion objects. Rackspace, the second largest commodity IaaS provider also reveals an increase in its revenue. With its Cloud Servers and Cloud Files, it reported an 18.1 percent increase from $31.4 million to $37.1 million for the first quarter of 2011. Both AWS and Rackspace’s rapid revenue growth can be credited from the growing usage of the IaaS. Commodity IaaS will continue to shape up and take on more enterprise workloads. Enterprise-focused clouds will look to further specialize their offerings, in providing cloud solutions to businesses.

The huge financial investment that PaaS gained in the past years proved that is continues to gain popularity. Microsoft’s Windows Azure platform is at the center of its cloud efforts that has attracted a number of customers. Among them are Toyota, the Associated Press and Intuit. Microsoft’s success with Windows Azure suggests the possibility of success for VMware, Red Hat and Salesforce.com as they continue to use PaaS application platforms. It is also interesting to see Google App Engine as PaaS adoption picks up. Google promises that more features will make their way into the standard App Engine.

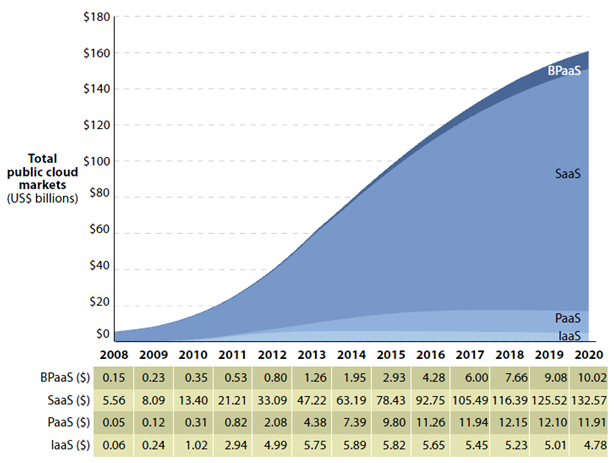


Figure 2: Forecast - Global Public Cloud Market Size, 2011 to 2020 (Pola, 2011)

In terms of users and revenues, Software as a Service, has the biggest share. One good example is the CRM service of Salesforce.com’s multi-billion-dollar business. SAP and Oracle are also embracing SaaS for their heavy-duty applications. Some organizations have reported that SaaS has inspired *everything* as a Service, where any IT process or application or business function is available as a service. Gartner estimated SaaS to reach $10.7 billion in 2011. Another analyst firm, IDC, predicts a $72.9 billion cloud services market by 2015. As SaaS use grows, data virtualization can pick up its momentum by incorporating data from mobile devices and other end-user derived sources. SaaS providers must also find ways to work tightly in integrating data among applications.

Cloud storage is currently being used to backup data, although it also serves as primary file- or content-storage option for web applications, like for Amazon’s Simple Storage Service (S3). The innovation on cloud storage will focus on primary storage for enterprise applications in the cloud. As vendors such as HP and Dell have storage businesses and public clouds, they could benefit from leveraging their storage expertise to make primary cloud storage a reality. Private cloud is considered as the delivery model choice of large enterprises and other risk-averse businesses. Over the past years, these four most-prominent private cloud startups – Nimbula, Eucalyptus Systems, Cloud.com and Abiquo – have raise a combined total of $73 million. Private clouds are here to stay whether as a whole or part of a hybrid cloud environment. For private cloud vendors, choosing to rely on their partners or building their own features will be a big decision.

# 4. Problems associated with virtual (cloud) projects

So far, in this paper, the basic concepts involved in cloud computing along with present and future market trends that project its growth have been discussed. Cloud computing is rapidly evolving making standardization difficult leading to vendor lock-in (Sitaram & Manjunath, 2011). Going forward in this paper, let us focus our analysis on some of the major problems that require our attention and identify possible solutions that can help us overcome these negativities associated with cloud computing.

## 4.1 Data Security

Having your own information, on your own hardware and between your own four walls, provides a level of comfort that you lose in the cloud. According to Mather et al., an organization’s information security policy should provide management direction and support for information security in accordance with business requirements and relevant laws and regulations (Mather, Kumaraswamy, & Latif, 2009). Regarding data protection, cloud computing raises a number of interesting issues.

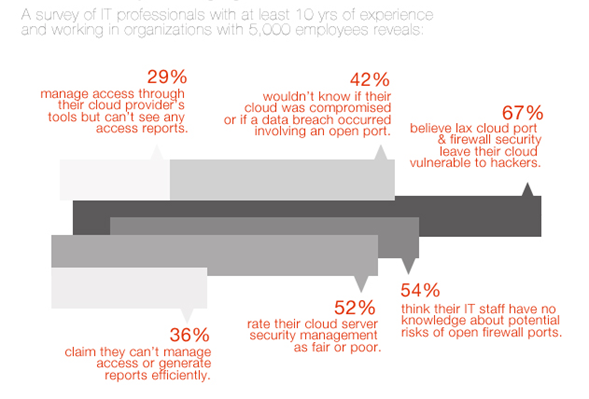


Figure 3: Cloud Security - Managing Firewall Risks

Data protection law is based on the premise that it is always clear where personal data is located, by whom it is processed and who is responsible for data processing. Cloud computing appears to fundamentally conflict with this evidence. For example, if a customer uses a data storage service based on cloud computing, the customer's data can be stored anywhere in the world, depending on where the servers on which the necessary storage capacity is available are located. Different services supplied by a wide range of providers are regularly bundled to produce an end-user proposal. For example, a mail service provider obtains the storage capacity required to store its customers' data from other providers. Therefore, with cloud computing it is no longer possible to say where the data is at a certain moment and by whom and how it is being processed. This means that it is doubtful whether those responsible for data processing, in accordance with data-protection regulations, are in a position to effectively assume their responsibility at all.

If the data circulates freely around the globe via the internet, it is also no longer clear which data-protection authorities at which location are responsible for ensuring the observance of the principles of data protection. A graphical representation of a survey conducted among IT professionals with at least 10 years of experience and working in organizations with 5,000 employees or above is shown in Figure 3.

In a cloud, the cloud computing system needs to provide a strong and user friendly way for users to access all kinds of services in the system. When a user wants to run an application in the cloud, the user is required to provide a digital identity (Yan, Rong, & Zhao, 2009). In part, there is a demand that the applicable statutory provisions regarding data protection be adjusted in order to find an appropriate arrangement for cloud computing. Whether statutory adjustments are necessary was the subject of a hearing conducted by the US Federal Trade Commission (FTC) in March 2009, although whether new data protection provisions should be drawn up is questionable, in particular because the market for cloud computing services is still very young and in its early stages of development. At such an early phase it is difficult to ascertain the right legal framework for effective and appropriate data protection.

Since providers centrally pool services such as e-mail, database applications, or security solutions for a large number of users, they tap into vast economies of scale and can pass these savings on to customers (Molen, 2010). However, issues involving data protection are eclipsed by aspects of competition law on account of the market power of providers such as Google or Amazon, which cannot be challenged by an individual customer, who does not have adequate negotiating power at his disposal to negotiate contract terms and conditions effectively.

## **4.2 Possible infringement on proprietary or copyrighted software**

An organization seeking to set up a SaaS to run its business operations is forced to share its software with the company that provides a ‘cloud’ solution. In spite of several technological improvements which are attainable using a cloud computing architecture, it is almost impossible to ascertain the complete security on software that is copyrighted or exclusive for the use of that particular organization. Since cloud computing makes use of a distributed computing architecture, several non-relevant hosts can simultaneously access the same server that is being used by a proprietary software which can lead to infringement or exploits. Different motivations are now emerging for online attacks. Recently we have seen the emergence of 'hactivism', when a group of hackers attack a website or company with the purpose of making a stand or getting a point across. This has added to the concerns of those looking to make the internet a more secure environment.

One possible solution to mitigate this risk is to set up dedicated clouds that are operationally and physically kept aloof from the rest of the users who wish to use other services provided by the cloud vendor. Although this can increase operational and infrastructural costs, exclusive or sensitive software can be operated without fear of being exploited on these cloud servers.

## 4.3 The Cloud Network Dependency Problem

In all our discussions placed above, we realize that a cloud solution can completely alter the way in which we do business. Either data or software or infrastructure or all of these can be built into the cloud so as to eliminate IT workloads within the organization. However, access to these services is almost completely dependent on the network services offered by the cloud provider. In case of disasters, a business can be completely washed clean of all its records if no proper disaster recovery solutions have been setup by the cloud provider. Cloud-based disaster recovery (DR) services first started appearing at the end of 2009, which means that most of these solutions are merely a year old. Many of these should really be described as replication-as-a-service because they do not yet provide full DR capabilities.

Because of the immaturity of replication-as-a-service, few large or even mid-sized organizations have been willing to risk going down this route, not least because they are concerned about boxing themselves into a niche market stocked by relatively few vendors. To this end, they either employ services from dedicated vendors such as SunGard or use the replication services offered by infrastructure- or software-as-service companies as part of a broader recovery package after moving the application to the cloud.

Further, most cloud-based DR vendors provide infrastructure based on commodity Windows or Linux-based systems and databases. Consequently, these vendors may simply not be able to replicate data and update databases from older, non-web based applications without developing a customized system. A key reason that vendors are only providing replication-as-service rather than full DR capabilities, is the lack of bandwidth, in particular relating to data upload speeds. As a result, cloud-based replication services are most feasible today for either small companies with up to 50 staff, which do not have much data or for large corporates that do not suffer from bandwidth constraints - but not those in between.

Finally, the cloud provider relies on a combination of network, equipment, application, and storage components to provide the cloud service. If one of these components goes down, end users (individuals, organizations, customers, etc.) will not be able to access their information. Therefore, it is important to understand how much can be done without a certain kind of information before a decision is made to put it on the cloud. For example, an online retailer would expect his customer order entry system to be up and running all throughout the year with absolutely no tolerance for downtime or failures. It is important to weigh the level of tolerance for unavailability of information against the cloud provider’s guaranteed uptime.

## 4.4 Lesser privacy protection under the law

Cloud computing implies entrusting data to information systems that are managed by external parties on remote servers "in the cloud." Webmail and online documents (such as Google Docs) are well-known examples. According to Pastoriza and Gonzalez, the most important issues that can hold back the widespread adoption of Cloud are security and privacy. Both concepts are very close to each other in Cloud, as there can be no privacy without security (Pastoriza & Gonzalez, 2010). Cloud computing raises privacy and confidentiality concerns because the service provider necessarily has access to all the data, and could accidentally or deliberately disclose it or use it for unauthorized purposes. Enterprise executives must weigh the risks and benefits of cloud computing and analyze both the provider being used and the information being put in the cloud.

Obviously, the technology has evolved faster than privacy laws, which don't address the unique cloud computing privacy challenges. The geographical location of the cloud provider is decisive in the determination of the laws that will apply to the data stored. The data (residing on the cloud) may have been replicated so that they exist in different places in the world at the same time and therefore might be subject to different data privacy laws (Baun, Kunze, Nimis, & Tai, 2011). Information stored in the cloud is much more accessible by a private litigant or the government. The reason is that traditionally, if an enterprise has information in its possession that a government wants, the government must come directly to the owner of the information to get it. But if it is in the hands of a third party, the information potentially could be released without the owner's knowledge. In such a scenario, the owner of the information would not have been able to object to the disclosure let alone even know their information had been released.

# 5. Conclusion

Cloud computing also offers an on-ramp to new computing advances such as non- relational databases, new languages, and frameworks designed to take advantage of new innovations. Close to half of U.S. IT professionals say that the risks of cloud computing outweigh the benefits. Virtual workplaces and inter-organizational projects are changing the business landscape. More and more companies are looking to the cloud to give them broader capabilities and greater application access. Anyone (an individual or an organization) considering the cloud should take the time to educate themselves so they understanding the offering, the cost and how information is protected. Issues and solutions discussed in this paper may be effective for most IT organizations; however project managers should perform diligent and regressive research before choosing a cloud based business platform.

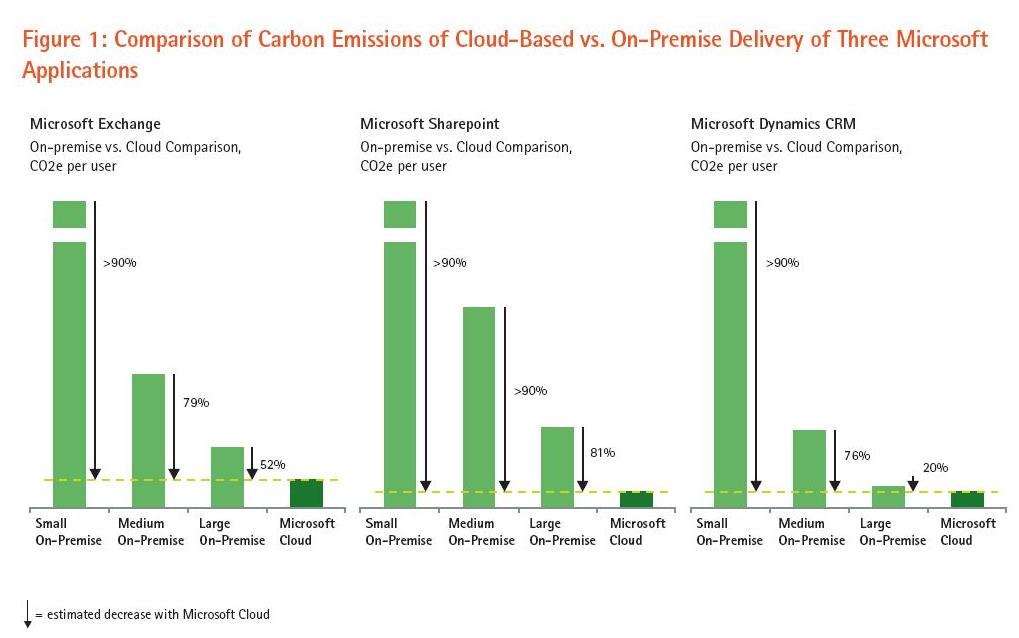


Figure 4: Comparison of Carbon Emissions of Cloud-Based vs. On-Premise Delivery of Three Microsoft Applications (Microsoft Corporation, 2010)

To conclude this paper on a positive note, shown above is a comparison of carbon emissions of cloud-based vs. on-premise delivery of three Microsoft applications on Figure 4. Usage of cloud solutions when viewed from a different perspective, can help the earth in its own way, walk towards a greener environment. Cloud based business solutions hold a lot of promises, and I believe that it is likely to be a major influence on hosting services and business applications that revolve around the virtual world.

# Bibliography

Baun, C., Kunze, M., Nimis, J., & Tai, S. (2011). *Cloud Computing: Web-based Dynamic It Services.* Springer Publications.

Chang, W. Y., Abu-Amara, H., & Sanford, J. (2010). *Transforming Enterprise Cloud Services.* Springer Publications.

Harding, C. (2011). *Cloud Computing for Business: The Open Group Guide.* The Open Group.

Jin, H., Ibrahim, S., Bell, T., Qi, L., Cao, H., Wu, S., & Shi, X. (2010). *Cloud Computing Principles, Systems and Applications.* Springer Verlag London Limited.

Laszewski, T., & Nauduri, P. (2011). *Migrating to the Cloud: Oracle Legacy Client/Server Modernization.* Elsevier Inc.

Mather, T., Kumaraswamy, S., & Latif, S. (2009). *Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance.* O'Reilly Media, Inc.

Microsoft Corporation. (2010, November 5). *Cloud Computing Can Cut Carbon Emissions by 30% to 90%*. Retrieved from environmental LEADER: http://www.environmentalleader.com/2010/11/05/cloud-computing-can-cut-carbon-emissions-per-user-by-30/

Molen, F. v. (2010). *Get Ready for Cloud Computing.* Van Haren Publishing.

Pastoriza, J. R., & Gonzalez, F. P. (2010). CryptoDSPs for Cloud Privacy. *Web Information Systems Engineering* (pp. 428-439). Hong Kong, China: Springer Publications.

Pola, S. (2011, May 21). *Are YOU Ready for the CLOUD Revolution? It’s a WIN-WIN for All!* Retrieved from INGurus: http://www.ingurus.com/are-you-ready-for-the-cloud-revolution-its-a-win-win-for-all/

Sitaram, D., & Manjunath, G. (2011). *Moving To The Cloud: Developing Apps in the New World of Cloud Computing.* Elsevier Inc.

Sosinsky, B. (2011). *Cloud Computing Bible.* Wiley Publishing, Inc.

Yan, L., Rong, C., & Zhao, G. (2009). Strengthen Cloud Computing Security with Federal Identity Management Using Hierarchical Identity-Based Cryptogrphy. *CloudCom* (pp. 167-177). Beijing, China: Springer Publications.