A Break In The Cloud? The Reality Of Cloud Computing

Chris Rose, Walden University, USA

ABSTRACT

Cloud computing is on the forefront of the technological landscape with Google, Microsoft and Amazon, among others, building up their server capacity to handle the next perceived leap in technological innovation. However, not only does the security of cloud computing have to be seriously addressed, but SOA governance and the capacity in the core, connectivity and fiber layers of the Internet to absorb the increased bandwidth will also have to be considered.

INTRODUCTION

The term "cloud computing" has many different meanings. A discussion at the 2008 IEEE International Conference on Web Services (ICWS), in Beijing, concluded that the definition depends on whom you ask.

- For application and IT users, it's IT as a service (ITaaS)—that is, delivery of computing, storage, and applications over the Internet from centralized data centers.
- For Internet application developers, it's an Internet-scale software development platform and runtime environment.
- For infrastructure providers and administrators, it's the massive, distributed data center infrastructure connected by IP networks (Lin et al, 2009).

Everyone sees the cloud and uses the cloud differently. Some people offload ordinary desktop software and instead use web-based applications, others want on-demand computing with instant availability of extra processing power and extra storage. Nevertheless, the inescapable fact is that companies of all sizes are increasingly using the cloud to increase their businesses, perhaps by enabling remote working or simply to cut costs or even to create entirely new business models (Marshall, 2009).

Cloud computing is not a new invention; it is simply the merging of existing technologies as a method of providing new services. By merging technologies such as networking, virtualization and service-oriented architecture and wrapping it all within an Internet-based delivery model known as software-as-a-service (SaaS) which only charges customers for what they actually use. "*At its most basic, cloud computing is an approach to a shared IT infrastructure in which large pools of computer systems are linked together to provide IT services. It offers a simplified, centralized platform that can be used as needed, thereby lowering costs and energy use*" (Ganek, 2009).

SaaS is a relatively simple concept. Whether it is an application or part of an application, a component, a framework or an environment, everything is delivered on the Web. Even ordinary desktop applications, such as office software are all now offered online. All of these concepts are a part of cloud computing and are available through an ordinary Web browser or through a remote desktop protocol (Erdogmus, 2009).

Many large technology companies, led by Amazon, are building huge server farms to offer cloud computing with virtual applications and business software with self-service interfaces so that customers can use resources when they want and discard these resources when they no longer need them (Brodkin, 2009).

Google has more than a million servers in over 30 data centers across its global network. Microsoft, it says, is investing billions to grow its own physical infrastructure at a whopping rate of 20,000 servers a month. Thus the espoused massive decentralization at the periphery of the cloud is driving massive centralization at its deep center to take advantage of economies of scale in computing power, energy consumption, cooling, and administration (Erdogmus, 2009).

CONSUMER ACCEPTANCE

Acceptance of cloud computing by the average consumer is evidenced in the acceptance of netbooks, small portable, low power notebook computers. Netbooks have limited processing power and storage but have multiple ways to connect to the Internet. Many vendors offer online storage with these netbooks and the very design means that their main purpose is to access email, and browse the Internet. The fact that consumers are willing to give up processing power and internal storage for Internet connectivity and portability, points to a shift in the usage patterns of portable computers. It is thought that netbooks "*will exist alongside cell phones as a means for people to connect to the Internet and communicate. The low price and practical functionality will bring millions of new people into the global web. Netbooks will also become supplemental PCs and ready access points into the cloud of Internet services, media and information*" (Bergevin, 2008).

A recent report stated that netbook sales saw huge growth in the third quarter of 2008, with sales volumes increasing a massive 160 percent vs. the previous quarter. This report predicted that total netbook shipments for 2008 would reach 14 million units in 2008, up from only 1 million units in 2007 (DisplayResearch, 2008). In addition, strong sales of Intel's Atom chip, the CPU in just about ever netbook, accounted for about half of the growth of the entire world microprocessor market in the third quarter of 2008 (Broersma, 2008).

The growth of online software services, such as Google docs, Wrightly or Zoho allows the user to have a complete office suite without the software being installed on their computer. The obvious advantage is that they can access these documents from any computer, anywhere in the world as long as they have an Internet connection. Amazon's Simple Storage Service (S3) allows consumers access to store files on a vast network of Amazon servers in the USA or Europe or even redundantly on both. This very inexpensive storage solution even has a drag and drop interface for the Firefox web browser which allows users to drag and drop files to and from Amazon's servers. However, the long anticipated service from Google called Gdrive should accelerate this acceptance.

Gdrive is thought to be a cloud-based storage that will have two parts, a desktop client and a web interface. The web interface would allow you to access your desktop files anytime, anywhere in the world on any Internet-connected computer. Gdrive would also be tightly integrated with other Google services such as Google docs, Gmail and Picasa web albums (Zibreg, 2009).

SECURITY AND SOA GOVERNANCE

However, moving to cloud computing presents the enterprise with a number of risks perhaps none greater than the security of your information (Cunningham and Wilkins 2009). Cloud computing by its very nature, allows data to be sent and stored anywhere, sometimes data is every shared among locations in different parts of the world. Although dispersing data allows cloud computing to have a performance and cost advantage, unfortunately the data can end up in a storage system in a country where privacy laws are lax or even nonexistent (Edwards, 2009). There are numerous security concerns in cloud computing including data loss and integrity compliance, liability, reliability, authentication and information life-cycle management. Not only is the risk from potential data loss, but also from breaching established regulations. For example, suppose the regulations require encrypting data in storage, but because the data are dispersed, how can customers know whether providers encrypt it or not? In addition, regulations vary from country to country so how can a provider show that data restricted to a particular geographic location by, for example, European Union rules is staying where it is supposed to be when the data can be spread across multiple countries? (Greene, 2009)

SOA (Service-Oriented Architecture) governance, also known as service governance, "*refers to practices and tools for enforcing consistent development, security, performance and other policies across the life cycle of key*

functions, regardless of whether they are hosted internally or provided by outsourcers" (Kobielus, 2009). SOA governance allows organizations to plan, design and modify their distributed environments to ensure that enterprise applications comply with baseline requirements. Cloud computing complicates SOA governance because anyone at anytime can deploy a new cloud service. Without governance, a rogue cloud service could emerge, attempt to pass as a legitimate service, and even try to integrate that service into an existing legitimate service thereby severely undermining the fragile trust inherent in SOA governance. Cloud computing services could make it extremely difficult to enforce governance policies of service, security or management. In fact, cloud computing services are fundamentally different from the regular SOA environment therefore it would be difficult to even determine what best practices should be used in this environment (Kobielus, 2009).

Information security professionals are trying to figure out how to securely move applications and data to the cloud. It is thought that perhaps they could extend directory services authentication outside their environments to manage cloud-based applications and systems. However, what would happen to authentication if the third-party systems were breached? Certain cloud services, such as Amazon's Elastic Compute Cloud, allow companies to apply data encryption within the operating system, application, or database management system running in the virtual instance. However, other services, such as application hosting, require more thought when developing the application to ensure that security measures such as encryption are built in (Ely, 2008).

Security experts now believe that securing systems is an outmoded concept, and that securing the data itself and knowing who is using it and what they are doing with it are better goals (Wittmann, 2009). "*Known to some as enterprise data protection, this always-on, data-centric security strategy works to identify what is at risk and embeds encryption with the data itself, starting with data creation and following data as it is modified, transferred, stored and archived*" (Dunkelberger, 2008).

THE TRAGEDY OF THE COMMONS

A network externality arises from the concept that some goods and services are more valuable when more people consume or utilize that good or service and yet these goods and services have little or no value if they are used without a network (Katz & Shapiro, 1995). Typical examples of these would be telephones and fax machines as people who own these products would form a network to be able to exchange information and provide a way for people to communicate with each other. The more people who have telephones the more valuable this network becomes. Electronic networks such as communication and information networks are said to exhibit positive production and consumption externalities since the value of the good that is a part of the network increases with the number of units sold since each unit complements each other that in turn will increase the value of the component (Rose and Gordon, 2003).

In security it can also be said that an externality is when one person's actions has an effect on others, such as when LoJack is introduced in a city then the theft of cars goes down, since thieves cannot tell if LoJack is installed or not. The attributes of computer security suggests that computer security is an externality, since the lack of security on one machine can adversely affect the security on many other machines, such as when credit card numbers are stolen from an improperly secured machine and are used to commit crimes at other web sites. (Camp & Wolfram, 2000).

William Forster Lloyd, an amateur nineteenth century mathematician, wrote a seminal treatise on the deterioration that would occur in a pasture due to the innate traits of humans. This became known as the "tragedy of the commons" and it was resurrected into mainstream academia by a biologist, Garrett Hardin in 1968. Although Lloyd was examining a shared pasture, his principles can be extended to most shared resources including the Internet (Rose and Gordon, 2003). Basically, if a resource is used at a rate that is near capacity then additional users will only deteriorate the value to all users. This leads to a vicious cycle whereby all users attempt to consume more of the resource so as to be in the same position as they were before the additional user started consuming the resource. Each user is in fact pursuing their own best interest but this ultimately just causes the demise of the resource (Turner, 1993).

For example, a Distributed Denial of Service (DDoS) attacks occur when a number of machines with vulnerabilities are taken over and controlled by hackers and used to flood a specific machine with worthless packets of data. These have become a serious problem since 1999 and they are at the heart of "the tragedy of the commons" since while everyone might be interested in protecting the shared resource of the Internet, the individual had a stronger incentive to cheat by connecting insecure computers (Yan, Early & Anderson, 2000). An individual can do very little to stop a Distributed Denial of Service (DDoS) attack since this type of attack exploits the vulnerabilities of other computers on the network. While someone might be willing to pay $100 to prevent their own computer from being attacked, it is much less likely that they will spend that sum to stop Microsoft or Amazon from being attacked. It might be more rational for that user to keep that $100 in their pocket and hope that they are not one of the small minority that becomes a target (Yan, Early & Anderson, 2000).

However, if cloud computing is examined, it can be seen that one person's actions or inactions can have an effect on others. For example, if there is lax security by one user of the cloud, this can lead to the disruption of service to other users. If some computers become infected because an update or patch was not applied, this inaction by the users will affect every other user of the Internet if their computer is used in a DDoS. Therefore, it can be argued that these users who did not patch their computers are consuming more of the shared resource (the Internet) and are reducing the amount of that resource available to other users which causes a degradation of the shared resource.

Interestingly, if service becomes degraded, it is in the other users own interest to attempt to consume more Internet bandwidth to compensate for the decreasing performance of the Internet. Of course, the result will therefore be an even faster decline in the shared resource, the Internet, and a classic case of the Tragedy of the Commons.

INTERNET CAPACITY

However, the growth of SaaS and the obvious related in growth in consumed bandwidth, also coincides with an ominous report from Nemertes Research which determined that demand for bandwidth on the Internet would exceed its capacity by 2012 since there are more applications that are coming online and that will drive expectations for even higher service quality. Nemertes Research projects that:

Capacity in the core, and connectivity and fiber layers will outpace all conceivable demand for the near future. However, demand will exceed access line capacity within the next two to four years. Even factoring in the potential impact of a global economic recession on both demand (users purchasing fewer Internet-attached devices and services) and capacity (providers slowing their investment in infrastructure) changes the impact by as little as a year (either delaying or accelerating, depending on which is assumed to have the greater effect).

One reason is the growth of virtual workers who work from their homes or virtual offices and another is the growth of high-bandwidth applications gaining in popularity with the home user (Reed, 2008). These applications, such as online gaming and movies also consume enormous amounts of bandwidth. For example, the average DVD movie consumes approximately 2 GB of bandwidth and newer Blu-ray discs consume many times that amount in fact "*4 million households downloading two high-definition movies per month drives the same Internet demand as 50 million households watching 50 YouTube videos per month. YouTube continues to grow at a fast rate, estimated to be 100 petabytes per month*" (Nemertes Research, 2009).

CONCLUSION

If Nemertes research is correct in their prediction, then this growth in Internet usage combined with the inescapable reality of the tragedy of the commons, sounds an ominous warning for the future of cloud computing. If business insist on moving to the cloud, then they have to be aware that not only that they will lose control of the security of their data, but might also find themselves not being able to gain access if some other person or persons either by action or inaction, cause a degradation of the cloud. If their data are stored on servers in countries that have little or no privacy protection, the integrity of their data may also be at risk.

If there is a concerted effort to focus on the security of the data rather than the security of the system this should protect data in countries that lack sufficient privacy regulations. Although nothing apart from regular updates and vigilance can stop a DDoS attack, effort is needed to build out the capacity in the core, connectivity and fiber layers of the Internet to ensure the continuing smooth functioning of the cloud due to the increased bandwidth demanded by today's users. Cloud computing is on the forefront of technological innovations and if sufficient attention is paid to these problems then it will succeed and continue to provide a simplified, convenient, centralized platform that can be used as needed, anywhere in the world as long as there is an Internet connection.

REFERENCES

1. Bergevin P. Thoughts on Netbooks. March 03, 2008. Retrieved April 28, 2009 from http://blogs.intel.com/technology/2008/03/thoughts_on_netbooks.php
2. Broersma M, ZDNetAsia. Intel Atom sales boost global chip market, November 05, 2008. Retrieved on May 1, 2009 from http://www.zdnetasia.com/news/hardware/0,39042972,62047989,00.htm
3. Camp L. and Wolfram C. (2000, October 24). Pricing security. Proceedings of the CERT Information Survivability Workshop, Boston, MA.
4. Cunningham P. and Wilkins J. A Walk in the Cloud. *Information Management Journal*. Lenexa: Jan/Feb 2009. Vol. 43, Iss. 1; pg. 22
5. Display Search (2008). Strong Mini-Note (Netbook) Shipments Buoy Notebook PC Market in Q3'08; Tier One Product Launches Propel Growth. Retrieved on May 1, 2009 from http://www.displaysearch.com/cps/rde/xchg/displaysearch/hs.xsl/Strong_mini_note_shipments_buoy_notebook_PC_Market_Q3_08.asp
6. Dunkelberger P. Secure data — not just systems. *Federal Times*. January 07, 2008. Retrieved May 2, 2009 from http://www.federaltimes.com/index.php?S=3290861
7. Edwards J. Cutting Through the Fog Of Cloud Security. *Computerworld*. Framingham: Feb 23, 2009. Vol. 43, Iss. 8; pg. 26
8. Ely A. Serious About Security. *InformationWeek*. Manhasset: Dec 8, 2008. , Iss. 1214; pg. 24
9. Erdogmus H. Cloud Computing: Does Nirvana Hide behind the Nebula? *IEEE Software*. Los Alamitos: Mar/Apr 2009. Vol. 26, Iss. 2; p. 4
10. Ganek A. The Cloud: a leap created from combining existing technologies. Chief technology officer for IBM Software. FT.com. London: Apr 30, 2009.
11. Greene T. Cloud security fears cast shadow at RSA. *Network World*. Southborough: Apr 27, 2009. Vol. 26, Iss. 16; pg. 1
12. Katz M. and Shapiro C. (1995, June) Network Externalities, Competition and Compatibility. *American Economic Review*.
13. Kobielus J. Storm Clouds Ahead. *Network World*. Southborough: Mar 2, 2009. Vol. 26, Iss. 9; pg. 24
14. Lin G., Fu D., Zhu J, Glenn G. Cloud Computing: *IT as a Service IT Professional Magazine*. Washington: Mar/Apr 2009. Vol. 11, Iss. 2; p. 10
15. Nemertes Research (2009). Internet Interrupted: Why Architectural Limitations Will Fracture the 'Net. Retrieved on May 1, 2009 from http://www.nemertes.com/studies/internet_interrupted_why_architectural_limitations_will_fracture_net
16. Marshall G. Ahead in the cloud. Reporter's notes: *Cloud Computing conference*. Director. London: Mar 2009. Vol. 62, Iss. 8; pg. 54, April 24, 2009. Retrieved on May 1, 2009 from http://news.cnet.com/8301-17939_109-10227573-2.html?tag=newsLatestHeadlinesArea.0
17. Rose C. and Gordon J. (2003) Internet Security and the Tragedy of the Commons, *International Business & Economics Research Journal*, Vol. 1, No. 2, pages 67 – 71.
18. Turner R. (1993, January 21). The tragedy of the commons and distributed AI systems. Proceedings of the 12th. International Workshop on Distributed Artificial Intelligence, Hidden Valley, PA.
19. Wittmann A. Are We Sure This Isn't Clouded Judgment? InformationWeek. Manhasset: Apr 13, 2009. , Iss. 1226; pg. 46
20. Yan J., Early S. and Anderson R. (2000) The XenoService – A Distributed Defeat for Distributed Denial of Service. Proceedings of Information Survivability Workshop, Boston, Massachusetts, USA.
21. Zibreg C. Throw your hard drive away, Google's Gdrive arriving in 2009. Monday, January 19, 2009. Retrieved April 24, 2009 from http://www.tgdaily.com/content/view/41094/140/

NOTES