

Cloud Computing



Gavin O Donnell

Computer Science Department, Letterkenny Institute of Technology, Ireland

Nigel McKelvey

Computer Science Department, Letterkenny Institute of Technology, Ireland

Kevin Curran

University of Ulster, Northern Ireland

INTRODUCTION

Cloud Computing can be described as web service oriented computing that provides an environment which acts as a service in delivering software and information management in a way that would have typically only been available in product format. This is done through personal devices – such as a laptop – that would access the services available through the network of servers that is called the “cloud” (Marston, 2011).

Cloud Computing offers new ways to provide useful services on demand at a much cheaper make-up. The technology is ever developing and there are many cases of ongoing research to further improve this technology which inevitably will change the way businesses operate forever and provide many new opportunities for organisations alike (Mather et al., 2009).

It is important to point out that the idea of Cloud Computing – although it may seem like a new phenomenon – was originally realised in the early 1960’s when John McCarthy foreseen computing in the form of a global network that would act as a public service; which in a sense is how Cloud Computing is commonly viewed since its emergence over the past few years. As more aspects of work and life move online, the Internet is continuing to provide a platform for business and society at a much larger scale as well as the already highly-satisfactory communications means available (Ohlman et al., 2009).

The much talked about cloud environment is continuing to grow and the core principles of Cloud Computing are swiftly entering the curriculum in many Computer Science degrees around the world. This assessment will be widely welcomed in the industry as it can be seen that many organisations are devoting

vast amounts of resources in the development of cloud services. This chapter will take a look into the affects Cloud Computing has on those Businesses, how those businesses go about implementing the technology, the security issues surrounding Cloud Computing and a brief look into what is next for Cloud Computing.

BACKGROUND

The emergence of cloud computing represents a fundamental change in the way information technology (IT) services are developed, maintained, used and paid for. Information technology services within an organisation have become even more complex in recent years, causing the management and the distribution of computing resources to be at such an intricate level, that the software involved had made computing more expensive than ever. However, the promise of cloud computing has allowed organisations to present these computing resources to clients in a way that substantially helps organisations reduce the upfront costs of computing; thus, better align their needs and budgets (Mikkilineni & Sarathy, 2009).

Cloud Computing improves the competitive edge of businesses by providing IT resources immediately which enables them to efficiently meet the needs of customers more than ever. This all-new business agility enables the delivering and processing of new products to reach competent levels even during peak times throughout the year. The implementation of cloud computing services by an organisation will only encourage more innovation amongst staff, as the level of risk is substantially reduced with no huge upfront costs for development and testing. The cloud becomes

DOI: 10.4018/978-1-4666-5888-2.ch098

an adaptive and intriguing method when successfully implemented by organisations, inevitably pulling in the end users for their respective needs.

Regarding the end-user, Cloud Computing has several different models. First of all, there is Software as a Service (SaaS) and this model provides access to software applications over a network. Available to multiple users over the Internet, this model supports applications with their own data centre which allows them to essentially run on the cloud, eliminating the need to install and run the application on a computer. There are many consumer based SaaS services such as hosting and storage services; Dropbox being the most obvious storage service. It is also worth noting that the SaaS services require their own licenses and is responsible for application implementation in the cloud (McFedries, 2008).

Platform as a Service (PaaS) is for software suppliers who want to concentrate on the development of new applications without the cost and complexity of buying and managing the hardware and software needed. PaaS is cloud services with built-in integration of web services and databases; so basically developers use these services to develop their own product from an existing SaaS or develop a new web application. Revenue share mechanisms are in place between the developers and the owners; however the developers usually receive in-and-around 75% of this revenue. Finally, there is Infrastructure as a Service (IaaS). This represents hardware services such as storage, power and memory services are provided also. The best thing about this model is users can pay-as-you-go, so to speak. There is also the option of signing a contract for a specific amount of time. This is mainly because the user is responsible for everything, meaning the users have to prepare the application environment in their virtual machines. The best example of this type of provider is HP's BladeSystem *Matrix* (Weiss, 2007).

In the meantime, there are a lot of steps to be taken for the hype to surround this development to mature into a steady success. Many regulations have to be put in place, the interoperability of already existing cloud environments needs to be developed, and most importantly the flexibility of the technology needs to continue to grow to assist the traditional IT environments which have supported us for years. The key characteristics and variables that these organisations would use to calculate the possible success of cloud computing adoption is still, some-what, up in the air.

Several questions are still being raised about the availability of cloud platforms, as no organisation wants to earn a bad reputation because of downtime.

IMPLEMENTING CLOUD COMPUTING

Cloud Computing is a framework for offering services in new advantageous ways. In a sense, it can be considered as a phase of evolution regarding the expanding and building of the previous successful factors of IT to enable the environment to reach even higher levels of efficiency.

In reality, the planning process regarding the transfer to Cloud Computing will follow the same principles of any planning process. Firstly, the two main questions that need to be answered are; where are you now and where do you want to go? After these questions are answered, we can expand on them and develop a detailed understanding of the requirements needed to complete the process and deliver the service. Fortunately, when moving to Cloud Computing, most of the required applications will already be in place, so it is only a matter understanding the details of the system in place and then building additional requirements to further the system. Implementation details will vary from one application to the next, so it is important to provide solid information in both business and technical aspects. Business requirements includes details of who is responsible for the service in the organisation, the importance of that service to the organisation, and what strategic objective is served by the application. This highlights the services that will run in the cloud and the important requirements for them. Technical, Implementation and Operational Requirements includes details from servers, resources required, platform services, backup requirements, disaster recovery, and compliance issues (Sullivan, 2010).

A move to cloud will open up many new opportunities. For example, additional services could be implemented with the consolidating of already-in-place applications and resources. Long-term, Cloud Computing will continue to influence businesses through the basis of its ability to allow several applications access the single-storage units instead of duplicating several data sets to perform the same job in the traditional IT environment. This gives new advantages from a statisti-

cal viewpoint as with the reduced duplication of data, more accurate estimates can be developed and this will assist in analysing the potential workload needed for the cloud throughout development. Assessing the workload considers the following sub-processes:

- **Capacity Planning:** Estimating the overall capacity the business will need. This helps estimate requirements for peak-periods and the different budgets required.
- **Scheduling:** Not all workloads are predictable, so it is recommended to generate demand patterns to facilitate this process.
- **Cost Recovery:** The goal is to cover the costs and earn a profit (McKelvey & Curran, 2012).

The architectural principles support the fulfilment and utilisation of the computing infrastructure by making it available to a broad range of users through the use of several different applications. These principles are based on:

- **Designing for Scalability:** Addresses the issues of meeting the workload demands, and in the case of customers it surrounds the resources and how effectively they can use them to their advantage. The services used to provide scalable computing resources include the security services, standardised catalogue of applications, and service oriented architecture (SOA).
- **Design for Manageability:** This area is concerned with provisioning and monitoring. Provisioning is the starting of one or more servers on a particular machine. There can be several issues involved when managing this process and it can be even more complex if there multiple instances running different applications. Once these servers are running, they will need to be monitored. This is to realise if there is the need for additional resources and of course to look-out for potential problems.
- **Deploying Layered Technical Services:** Deals with specific hardware issues in the cloud environment by managing low-level operations like virtual memory.

- **Delivering Business Services:** Of course there is need to manage service delivery. The principles surrounding the Cloud Computing service are similar to the day-to-day business requirements, so the policies followed are not too dissimilar either. Such as auditing, security, pricing and cost recovery, and usage rules (Sullivan, 2010).

Arguably, the most important part of the implementation of Cloud Computing is to effectively manage the security in the cloud applications. The rapid growth in the field of Cloud Computing has inevitably brought forward several severe security concerns. Security has remained a constant issue for the Internet, and the cloud environment is a massive sufferer. Therefore, when developing a strategy when pushing a business towards the adoption of cloud services, it is important to include both business planning and the architectural considerations and analyse all the requirements involved and develop realistic workloads to fulfil these requirements (Cox, 2011).

SECURITY

There are of course plenty of security concerns involved with this technology. The problem with Mobile Cloud Computing is that it faces concerns from both mobile device security and cloud security in general. However, smart phones and specific applications have built in security features to protect them for this type of damage, although there is yet a proper solution to be developed for the security Mobile Cloud Computing; easily the most emerging stem of Cloud Computing (Qureshi et al., 2011).

Businesses will have to pay more attention to cloud security as legal repercussions creep in and the increase in big data. Big data is generally cloud-based - private or public cloud. Therefore all the recommended practices applicable to securing data in the cloud equally applies here. Companies should in particular with large data sets due to the multi-tenant nature of a cloud platform pay extra attention to the data lifecycle phases and ensure that aspects such as data destruction is provided and auditable as part of the service. The fact that any company is allowing confidential datasets to reside outside the company network should lead them to

examine how they can robustly protect that data and the answer can be simply a layered security strategy. The core principle to be followed here is the encryption of data. Proper encryption too. A company which does not encrypt sensitive customer data deserves to be fined accordingly. They should ensure that there is complete security built-in, including secure endpoint authentication integrity verification and on-the-fly data encryption. Ideally a minimum of hops or stops in between. We can expect to see more direct I/O offerings as well (Satyanarayanan & Bahl, 2009).

Ultimately, it is critical that businesses implement a layered security strategy regarding cloud services as their company data is more exposed than previously. It is critical to get buy in from upper-management. More so than ever, security breaches can greatly affect a company's public reputation. There are numerous examples in last 12 months - e.g. Skype, Adobe, Sony. Cybercrime is on the rise therefore we should think about security in terms of process, people and technology. This will involve creating security policies with internal departments, performing audits, implementing physical security control and classifying risk. The implementation of Internet-based services and rapid connectivity to external parties has led to increased risks to an organisation's internal assets. Information that is more valuable than ever before is more accessible and easier to divert. Organisations that fail to address the broader security issues that accompany this change will have insufficient controls in place to minimize risks. These risks could lead to significant financial, legal difficulties and reputation risk for these organisations. Appropriate preventive, detective and corrective controls in the form of policies, standards, procedures, organisational structures or software/technology functions and monitoring mechanisms are therefore required to minimise the risks associated with the confidentiality, integrity and availability of information assets within an organisation. These aspects of security should be the underpinnings of any ICT security program (Carlin & Curran, 2011).

The trend however is for increased usage and reliance on cloud services. Ultimately it does make sense. If an organisation of say 5000 employees is served by an IT dept of say 10-15 staff (which is not unusual). Then apart from the usual servicing of client machines/desktops - they also have to ensure the email server and all relevant internal network services are secure. All this must be balanced with daily workloads. On the other

hand, they can offload email to a large multi-national cloud provider with scores of dedicated workers serving that product.....well, only the ignorant would say that the 'firefighting' small IT team are superior. That might be the future. A small pool of Cloud Giants servicing a large pool of minions (Carlin & Curran, 2012).

FUTURE RESEARCH DIRECTIONS

The development of Cloud Computing will inevitably have many benefits for people. However, it will also have a negative effect of people to an extent as well. The traditionalists of the world will see a dramatic effect across several platforms e.g. the ever growing digital library. The traditional publishers and information resources will see an ever decreasing need for them with the constant development of digital print and content for sale. However, they are in the minority; the superior agility of an end-to-end library service would be widely welcomed and the resources will continue to be widely accessible over the Internet.

Now for a more specific benefit. There are many examples over how past few decades have seen major advances in medical technology, and with the emergence of Cloud Computing, it could once more see another massive boost. IT presents an opportunity for universal access to medical transformation at an extremely low cost. Cloud will enable providers to use "eHealth archive services that authorised users could use anywhere in the world through the use of the Internet. This service could provide cost-effective data sharing for several healthcare providers. With the help of this cloud, it will be easier to dissect the latest research, and of course handle it much more efficiently than before which could effectively work as monitoring platform across the world. Standard applications can cover the requirements of large healthcare platforms and hospitals while coordinating their work by sharing data in patients diagnosis and treatment all over the world, thanks to Cloud Computing (Chowdhary et al., 2011).

Another area of computing that is developing just as rapidly as Cloud Computing – if not more – is the development of mobile applications and mobile devices. Mobile Cloud Computing is trying to deal with some of the issues that Cloud Computing currently possess such as making use of the cloud infrastructure to help the performance of the mobile device when using specific

applications that are in demand. Basically, specific tasks are outsourced to the cloud as they happen freeing up other resources on the application.

CONCLUSION

Cloud Computing is certainly changing the way we see, operate and deliver business. This chapter was focused on the aspects of planning metrics, architectures, and characteristics, while touching on the surrounding applications involved. The cloud provides a much improved user experience thanks to the advantage of a much more efficient delivery mechanism provided. Cloud Computing is capable of offering organisations reduced costs in several sections freeing up capital for other investments. Regarding further development of Cloud Computing, Gartner estimate that Cloud Computing will bring in revenue of approximately €140 Billion in 2014. Gartner estimates that by 2014, enterprises will spend €100 Billion on software as a service (SaaS), platform as a service (PaaS), and infrastructure as a service (IaaS), combined (Marston, 2011). There are still many issues surrounding the security of cloud computing especially in the wake of the Snowden NSA leaks where it seems more important than ever to encrypt data before uploading to public cloud services. We expect however this aspect to be addressed and for more of the world's data to be moved towards the cloud services belonging to Amazon, Microsoft, Dropbox and many of the other giants in this fast growing industry.

REFERENCES

- Carlin, S., & Curran, K. (2011). Cloud Computing Security. *International Journal of Ambient Computing and Intelligence*, 3(1), 14-19. January-March 2011, DOI: 10.4018/jaci.2011010102, ISSN: 1941-6237, IGI Publishing.
- Carlin, S., & Curran, K. (2012). Cloud Computing Technology. *International Journal of Cloud Computing and Services Science*, 1(2), 59-65.
- Chowdhary, S. K., Yadav, A., & Garg, N. (2011) Cloud computing: Future prospect for e-health, *Electronics Computer Technology (ICECT), 2011 3rd International Conference on*, vol.3, no., pp.297,299, 8-10 April 2011
- Cox, P. (2011). Mobile Cloud Computing: Devices, Trends, Issues, and the Enabling Technologies. *IBM developerWorks*.
- Marston, S. (2011). Cloud Computing – The Business Perspective. In *Proceedings of the 44th, Hawaii International Conference on System Sciences* (pp. 32-40).
- Mather, T., Kumaraswamy, S., & Latif, S. (2009). *Cloud Security and Privacy*. O'Reilly.
- McKelvey, N., & Curran, K. (2012). Maintaining Payment Card Industry (PCI) Compliance in a vulnerable Cloud International. *Journal of Engineering and Technology*, 2(5), 863-867.
- McFedries, P. (2008). The Cloud Is The Computer. *IEEE Spectrum*, 42-50.
- Mikkilineni, R., & Sarathy, V. (2009). Cloud Computing and the Lessons from the Past. In *Proceedings of The 18th IEEE International Workshops on Enabling Technologies: Infrastructures for Collaborative Enterprises*. Groningen, The Netherlands.
- Ohlman, B., Eriksson, A., & Rembarz, R. (2009) What Networking of Information Can Do for Cloud Computing. In *Proceedings of The 18th IEEE International Workshops on Enabling Technologies: Infrastructures for Collaborative Enterprises*. Groningen, The Netherlands.
- Qureshi, S. S., Ahmad, T., & Rafique, K. Shuja-ul-islam. (2011). Mobile cloud computing as future for mobile applications - Implementation methods and challenging issues. In *Proceedings of the Cloud Computing and Intelligence Systems (CCIS), 2011 IEEE International Conference* (pp.467,471), doi: 10.1109/CCIS.2011.6045111.
- Satyanarayanan, M., & Bahl, P. (2009). The case for VM-based cloudlets in mobile computing. *IEEE Pervasive Computing / IEEE Computer Society [and] IEEE Communications Society*, 8(4), 14-23. doi:10.1109/MPRV.2009.82
- Sullivan, D. (2010). *The Definitive Guide to Cloud Computing*. USA: IBM.

Weiss, A. (2007). Computing in the Clouds. *Networker*, 11(4), 16–25. doi:10.1145/1327512.1327513

ADDITIONAL READING

Jamsa, K. (2013). *Cloud Computing*. UK: Jones and Barlett Learning.

KEY TERMS AND DEFINITIONS

Cloud Computing: A new supplement, consumption, and delivery model for IT services based on Internet protocols, and it typically involves provisioning of dynamically scalable and often virtualized resources.

Cloud Service Providers: Offer an opportunity for organisations to make resources available online. These resources can range from extensive customer relationship management (CRM) software to the relatively widespread online email access.

Hybrid Clouds: Incorporate both public and private clouds (see figure 2) within the same network. It allows the organisations to benefit from both deployment models. For example, an organisation could hold sensitive information on their private cloud and use the public cloud for handling large traffic and demanding situations.

Public Clouds: Typically pay a yearly subscription to an external company toward storing data and the providing and facilitating the running of application programs.

Private Clouds: Allow users to have the benefits of cloud computing without some of the pitfalls. Private clouds grant complete control over how data is managed and what security measures are in place. This can lead to users having more confidence and control. The major issue with this deployment model

is that the users have large expenditures as they have to buy the infrastructure to run the cloud and also have to manage the cloud themselves.

Multitenant Architectures: Many companies share the same infrastructure within the Public Cloud, and the term given to this is Multitenant Architectures.

Quality of Service: A measure of network performance that reflects the network's transmission quality and service availability. QoS can come in the form of traffic policy in which the transmission rates are limited which guarantees a certain amount of bandwidth will be available to applications.

Router: A device or setup that finds the best route between any two networks, even if there are several networks to traverse. Like bridges, remote sites can be connected using routers over dedicated or switched lines to create WANs.

Switch: A network device that selects a path or circuit for sending a unit of data to its next destination. A switch may also include the function of a router (see above). In general, a switch is a simpler and faster mechanism than a router, which requires knowledge about the network and how to determine the route.