ISSN:2229-712X

Available online at www.elixirjournal.org

Network Engineering

Elixir Network Engg. 38 (2011) 4069-4072

# Security issues in cloud computing

Kevin Curran, Sean Carlin and Mervyn Adams

Faculty of Computing and Engineering, University of Ulster, Northern Ireland, UK.

**ARTICLE INFO**

**Article history:**

Received: 22 June 2011;

Received in revised form:

20 August 2011;

Accepted: 26 August 2011;

**Keywords**

Customer relationship management (CRM),

Elastic Compute Cloud.

**ABSTRACT**

Cloud Computing is a distributed architecture that centralizes server resources on a scalable platform so as to provide on demand computing resources and services. Cloud computing has become a variable platform for companies to build their infrastructures upon. If companies are to consider taking advantage of cloud based systems, they will be faced with the task of seriously re-assessing their current security strategy, as well as the cloud-specific aspects that need to be assessed. We outline here what cloud computing is, the various cloud deployment models and the main security risks and issues that are currently present within the cloud computing industry.



## Introduction

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. Cloud computing allows these companies to benefit from porting their existing systems to an online environment where they can be accessed by anyone with the required privileges. The most appealing advantage of this is that the cloud service provider takes care of the required hardware, software and networking including the associated costs. The cloud service provider will then be able to 'rent out' what the company requires; this means that the company will only ever use the resources necessary. The service provider will have the hardware and software setup to enable them to scale far and beyond what any company will require, this means that they can offer a 'pay-as-you-go' type service. The service provider will be able to offer similar resources to multiple companies, meaning that they can offer this at a reduced price (Sheriff, 2011).

Cloud computing is not a new technology but rather a new delivery model for information and services using existing technologies. It uses the internet infrastructure to allow communication between client side and server side services/applications (Weiss, 2007). Cloud service providers (CSP's) offer cloud platforms for their customers to use and create their web services, much like internet service providers offer costumers high speed broadband to access the internet. CSPs and ISPs both offer services. The cloud provides a layer of abstraction between the computing resources and the low level architecture involved. The customers do not own the actual physical infrastructure but merely pay a subscription fee and the cloud service provider grants them access to the clouds resources and infrastructure. A key concept is that the customers can reduce expenditure on resources like software licenses, hardware and other services (e.g. email) as they can obtain all these things from one source, the cloud services provider. Recent studies have found that disciplined companies achieved on average an 18% reduction in their IT budget from cloud computing and a 16% reduction in data centre power costs (McFedries, 2008).

There are two initial forms of cloud computing, Public Cloud and Private Cloud. Within Public Cloud computing companies pay a yearly subscription to an external company such as Amazon's Elastic Compute Cloud (EC2) toward storing data and the providing and facilitating the running of application programs. Many companies share the same infrastructure within the Public Cloud, and the term given to this is Multitenant Architectures. This term is significant because a server is split up into virtual servers software controlled slices allocated to customers, in essence one server becomes many with many customers. The Private Cloud would be the next progression for many companies as the Private Cloud is in-part managed in-house and is considered Hosted or Corporate cloud. The cloud is managed within the company's domain and data storage is centralized replacing the company's previous infrastructure as the network becomes virtualized. Most data storage is handled in-house because of its sensitivity which must be protected. This is the most secure option and the most expensive but still cost effective compared to their older structures in-which the companies maintained themselves.

As Public Cloud is considered a multitenant architecture the Private Cloud is considered a Proprietary Architecture which provides hosted services to a limited number of people behind a firewall. This firewall is located at the network gateway server. Physical hardware resources such as Servers are only allocated to one customer. The fire wall allows public internet access also accommodating VPN Virtual Private Networks allowing company employees to connect to the company intranet safely and securely from their homes. The added feature of a VPN is the ability to use public networks like the Internet and rely on private leased lines. These restricted access networks utilize the same cabling and routers as a public network, and is categorized within a wide area network. Virtualization toward this extent is a relatively new concept within the IT industry, which has really taken off since 2005, the three main areas where virtualization is showing greatest significance is within Virtual Networks, Storage Virtualization and Server Virtualization. The combination of these three important elements provides autonomic computing within the IT environment and is practically self managing saving cost an incentive. Within

Tele:

E-mail addresses: kj.curran@ulster.ac.uk

Network Virtualization a methodology is used to combine the availability of resources into a network by splitting up the available bandwidth into channels, and each is independent from one another. This helps toward performance as each one can be assign and reassigned to a different device or server in real-time.

Virtualization disguises the true complexity of a network as it breaks it up into manageable parts.

Storage Virtualization is the pooling of physical storage from multiple network storage devices into what could be considered as one singular storage device. This pooling storage device is managed by a central console.

Server Virtualization is the masking of server resources including the number and identity of individual physical servers, processors, and operating systems from server users. Designed and implemented in a way that the user does not have manage the complexity of server settings, while increasing resource sharing and maintaining the capacity to expand later.

The combination of these three important elements provides autonomic computing in which the IT environment would manage itself. Within a private cloud there would be an administrator who would oversee the running of the Virtual Network.

We provides here an overview of the key aspects of Cloud Computing.

**The Cloud**

Cloud computing has five key attributes which grant it some advantages over similar technologies and these attributes include:

• **Multitenancy (shared resources):** Unlike previous computing models, which assumed dedicated resources dedicated to a single user or owner, cloud computing is based on a business model in which resources are shared at the network, host and application level.

• **Massive scalability:** Cloud computing provides the ability to scale to tens of thousands of systems, as well as the ability to massively scale bandwidth and storage space.

• **Elasticity:** Users can rapidly increase and decrease their computing resources as needed, as well as release resources for other uses when they are no longer required.

• **Pay as you go:** Users pay for only the resources they actually use and for only the time they require them.

• **Self-provisioning of resources:** Users self-provision resources, such as additional systems (processing capability, software & storage) and network resources (Mather et al., 2009).

There is a buzz around cloud computing, as users of the cloud services only have to pay for what they use and the resources that they need to cope with demanding situations can be adjusted depending on the demand. This is recognized as the cloud delivery model (SPI – see figure 1) which consists of three services known as Software-as-a-service (SaaS), Platform-as-a-service (PaaS) and Infrastructure-as-a-service (IaaS).

Software-as-a-service allows the users to utilize various applications from the cloud rather than using applications on their own computer. The cloud service provider would usually provide some sort of software development environment to allow applications to be developed for use within the cloud.

The application programming interface (API) which the users use to access and interact with the software allows the user to use the software without having to worry about how or where the data is being stored or how much disk space is available as the cloud service provider will manage this for them.

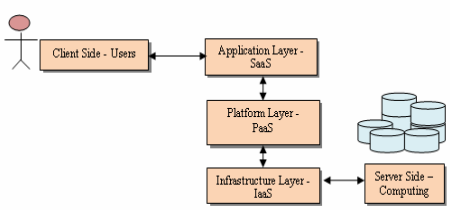


**Figure 1: Showing layers of the cloud delivery model**

Platform-as-a-service operates at a lower level than the SaaS. It is responsible for the management of the storage space, bandwidth allocation and computing resources available for the applications. It retrieves the resources needed to run the software and dynamically scales up these resources when more is needed. This service holds a key attribute of the cloud mentioned above as self-provisioning of resources. Infrastructure-as-a-service dynamically scales bandwidth allocation and server resources for the cloud. This service allows the cloud to operate during high traffic/demanding situations as resources are dynamically increased as they are needed. The pay as you go attribute plays a large role in this service as the user is charged for how much bandwidth or server resources are needed.

There are three main types of cloud deployment models - public, private and hybrid clouds.

**Public Clouds** – are the most common type of cloud. This is where multiple customers can access web applications and services over the internet. Each individual customer has their own resources which are dynamically provisioned by a third party vendor. This third party vendor hosts the cloud for multiple customers from multiple data centers, manages all the security and provides the hardware and infrastructure for the cloud to operate. The customer has no control or insight into how the cloud is managed or what infrastructure is available.

**Private Clouds** – emulate the concept of cloud computing on a private network. They 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.

**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.

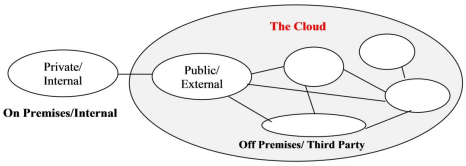


**Figure 2: Showing Hybrid Cloud Deployment Model**

**Security in the Cloud**

One of the risks that people perceive concerning the cloud is that cloud service providers may not be able to cope with the large scale of or that the infrastructure will not be able to scale properly with large amounts of usage (Ohlman et al., 2009). Privacy is important for organisations, especially when individual's personal information or sensitive information is

being stored but it is not yet completely understood whether the cloud computing infrastructure will be able support the storing of sensitive information without making organisations liable from breaking privacy regulations. Many believe that cloud authorisation systems are not robust enough with as little as a password and username to gain access to the system, In many private clouds, usernames can be very similar, degrading the authorisation measures further. If there was private/sensitive information being stored on a private cloud then there is a high chance that someone could view the information easier than many might believe. The customer is advised to only give their data or use the cloud providers system if they trust them.

As companies move onto Cloud Computing with the incentive of low cost by the aggregation of servers and data into a centralized location which intern can translate to severity toward aggregation of risk. There have been significant incidents of successful disruption on Cloud Networks due to hackers. Google were the target of attacks aimed at stealing intellectual property and identifying that human-rights activists were targeted seeking reforms in China. The incident prompted the Internet search giant to re-evaluate whether it will continue doing business in the country (MarketWatch, 2010). Google's infrastructure is mainly on the Cloud and companies with high profiles become bigger targets. The resources such companies have toward security investment is considerable and Google supply software security also more so to business. Attacks to date have not just been on Google but companies from a wide range of businesses–including the Internet, finance, technology, media and chemical sectors–have been similarly targeted (Everiss, 2010).

Cloud service providers believe encryption is the key and can help with a lot of the security issues but what comes along with the benefits of encryption are the pitfalls as encryption can be processor intensive. Encrypting is not always full proof for protecting data, there can be times when little glitches occur and the data cannot be decrypted leaving the data corrupt and unusable for customers and the cloud service provider. The clouds resources can also be abused as cloud providers reassign IP addresses when a customer no longer needs the IP address. Once an IP address is no longer needed by one customer after a period of time it then becomes available for another customer to use. Cloud providers save money and do not need as many IP addresses by reusing them, so it is in the cloud provider's interest to reuse them. Too many of these idle/used IP addresses can leave the cloud provider open to abuse of its resources. There is a period between an IP address being changed in DNS and the DNS caches holding the IP address getting cleared. If these old/used IP addresses are being held in the cache then they can be accessed which would grant a user access to the resources that are available at the IP address. Also another customer of the same cloud provider could potentially gain access to another customer's resources by navigating through the cloud provider's networks, if no/little security measures are put in place. Data and information is like a currency for cyber terrorists/crooks and clouds can hold enormous amounts of data so clouds are becoming an a attractive target for these crooks which is why cloud security must be top notch and should not be overlooked (Wayner, 2008).

Clouds API's and software-as-a-service are still evolving which means updates can be frequent but some clouds do not inform their customers that these changes have been made. Making changes to the API means changing the cloud configuration which affects all instances within the cloud (see figure 3). The changes could affect the security of the system as one change could fix one bug but create another. The customers of the cloud provider should enquire if any updates are made and should ask about what security implementations have been put into place to secure their data and what exactly has changed with the system. Some ways to verify if the company is right for your information is to ask is there a third party auditing their cloud or do they have any security certificates.

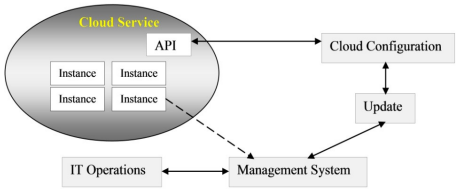


**Figure 3: Showing relationships of the cloud API and other key cloud components**

If a cyber criminal hacks into the cloud provider and data which belongs to the customer has been copied off the server then the customer may not know. The cloud provider will have access to the server logs and the customer will not. Multiple customers may be sharing the resources of the same servers and one customer could be using multiple hosts potentially every day. This would make tracking of the unauthorised access of the data to be nearly impossible for the cloud service provider as the data can been very widely spread throughout the cloud providers networks. Unless the cloud provider has developed some sort of monitoring software which can group/sort processes which have occurred for each user then this could be a large security risk and make attacking clouds even more attractive for cyber criminals.

Most customers will not know where their data is being stored by the cloud provider. This poses a number of issues especially if the information is important or valuable. Customers who are worried about security should ask their cloud provider where the physical servers are held, how often are they maintained and what sort of physical security measures have been taken (e.g. biometrics or PIN access) to restrict access to the server resources. There is a chance that the data will be held in another country which means the local law and jurisdiction would be different and could create a different security risk, as data that might be secure in one country may not be secure in another (Staten, 2009). By looking at the different views on data privacy between the US and the EU, this security risk becomes more evident as the US has a very open view on the privacy of data. The US Patriot Act grants government and other agencies with virtually limitless powers to access information including that belonging to companies whereas in the EU this type of data would be much more secure, so local laws and jurisdiction can have a large affect the security and privacy of data within a cloud (Mikkilineni and Sarathy, 2009).

**Conclusion**

One of the biggest security worries with the cloud computing model is the sharing of resources. Cloud service providers need to inform their existing customers on the level of security that they provide on their cloud. The cloud service providers need to educate potential customers about the cloud deployment models such as public, private and hybrids along with the pros and cons of each. They need to show their customers that they are providing appropriate security measure

that will protect their customer's data and build up confidence for their service. One way they can achieve this is through the use of third party auditors. New security techniques need to be developed and older security techniques needed to be radically tweaked to be able to work with the clouds architecture. Plugging in existing security technology will not work because this new delivery model introduces new changes to the way in which we access and use computer resources.

We must remember that when a corporation loses sensitive data, it is quite often an inside job therefore organisations must consider carefully who they are handing their sensitive data to. In the standard model of data remaining in-house, they can monitor closely the use of data and irregularities within staff. They can also set and unset the credentials required to access this data, enabling them to remain in control. However, in the cloud, they must place a lot of trust in the service provider, in their abilities to employ reliable members of staff and only offer the required security privileges to those who it deems necessary. A degree of trust will always remain, however there are external security standards (ISO27001), and if a cloud service provider conforms to this standard, they will be able to be audited to ensure the compliance. This will give considering companies an added boost of trust as they can ask to view any previous audits.

**References**

[1]Everiss, B. (2010). Google hacked by Chinese. Bruce on Games Blog. January 13th 2010 http://www.bruceongames.com/2010/01/13/google-hacked-by-chinese.

[2]Mather, T., Kumaraswamy, S. and Latif, S. (2009) Cloud Security and Privacy, O'Reilly, ISBN. 978-0-596-80276-9

[3]MarketWatch. (2010). US reportedly track down Google hacking-code writer. February 22nd 2010 http://www.marketwatch.com/story/us-reportedly-finds-google-hacking-code-writer-2010-02-22.

[4]McFedries, P. (2008) The Cloud Is The Computer, IEEE Spectrum, August 2008.

[5]Mikkilineni, R. and Sarathy, V. (2009) Cloud Computing and the Lessons from the Past. The 18th IEEE International Workshops on Enabling Technologies: Infrastructures for Collaborative Enterprises, Groningen, The Netherlands, June 29 - July 1, 2009

[6]Ohlman, B., Eriksson, A., Rembarz, R. (2009) What Networking of Information Can Do for Cloud Computing. The 18th IEEE International Workshops on Enabling Technologies: Infrastructures for Collaborative Enterprises, Groningen, The Netherlands, June 29 - July 1, 2009

[7]Sherriff, L. (2011) The risky business of assessing the public cloud. The Register. April 11th 2011 http://www.theregister.co.uk/2011/04/08/risk_assessment_cloud/

[8]Staten, J. (2009) Is Cloud Computing Ready for the Enterprise?, Forrester Report, March 7, 2009

[9]Wayner, P. (2008) Cloud versus cloud - A guided tour of Amazon, Google, AppNexus and GoGrid, InfoWorld, July 21st 2008

[10]Weiss, A. (2007) Computing in the Clouds. Networker, Vol. 11, No. 4, pp: 16-25, December 2007