“The Cloud”

Canberra Tech Talks
Wednesday, 1st August 2012

Jessica Smith
Twitter: @itgrrl
Blog: www.itgrrl.com

What is the cloud?

Cloud computing is 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. This cloud model is composed of five essential characteristics, three service models, and four deployment models.

The NIST Definition of Cloud Computing

See? Easy! Let’s hit the bar... :-)

In more user-friendly terms...

- The cloud is a 'black box'
- The cloud is a cloud (network diagram)
- The cloud is where cloud computing takes place
    - …and cloud computing is computing that takes place in the cloud ;-)
- Initially a very nebulous descriptor not widely agreed upon
- Has gradually coalesced into a broadly-agreed-upon term for 'various components of computing delivered as a service'
    - Now usually broken down into
        - Software as a Service (SaaS) e.g. Salesforce.com - CRM
        - Infrastructure as a Service (IaaS) e.g. Amazon Web Services (AWS) - cloud-based servers, data storage/backup, HPC clusters, etc.
        - Platform as a Service (SaaS) e.g. Amazon Web Services (AWS) - used for app development
- In a sense, the cloud is what the Internet is evolving into.

How does it work?

- It's essentially outsourcing of most aspects of computing
- A specialist company purchases/builds a huge volume of servers, storage, network infrastructure, data connectivity, and/or applications and rents to organisations who need it
    - Enabled largely by virtualisation technology (...which is a topic for another night)
    - Provides the ability to rapidly scale up to meet unexpected (or planned) demand
    - Some cloud providers have ‘shipping container data centres’ that can be redeployed based on need
- Saves users from up-front hardware, operating system (OS), and/or software costs
- Reduces the need for in-house IT expertise - although sometimes it just changes the mix of IT expertise required
- Support services may be part of the deal

Key benefits of moving to the cloud

- Elasticity - the ability to quickly scale up to meet unexpected peaks in demand
    - Also the ability to scale up and down as needed for businesses where demand is 'lumpy'
- Reliability - cloud providers are specialists, and create infrastructure that is generally much more fault-tolerant than traditional in-house IT resources
    - Redundancy is a key aspect of this - workloads can be automatically moved to different servers in the event of a problem in any one server, cluster, or data centre
    - Geographical redundancy is provided by replication of resources at multiple data centres across the planet - this is usually well beyond the resources of small-to-medium IT departments for cost reasons
- Cost-effectiveness
    - Massively reduced up-front costs
    - Usually significantly reduced ongoing costs
    - Reduced need for certain IT specialists in-house, especially hardware specialists

Examples of cloud services

- Web-based email: Gmail, Hotmail, Yahoo! mail
- On-demand IT infrastructure & data storage: Amazon Web Services (AWS), Google Cloud, Windows Azure
- 'Big Data': Amazon EC2, Google Cloud, Windows Azure
- Scalable web hosting: Rackspace Cloud, Amazon AWS, Google Cloud
- Online storage: DropBox, iCloud, Amazon S3
- Productivity & collaboration tools: Microsoft Office 365, Google Apps for domains, Evernote
- Application hosting: Windows Azure, Microsoft Office 365 (SharePoint),
- CRM: Salesforce.com, Sage CRM, SugarCRM
- Entertainment: last.fm, Spotify, Netflix

What are the privacy implications of storing data in the cloud?

- Traditional model of IT keeps all data 'inside the perimeter' of an organisation's network
    - Risks are well-understood, risk-management is handled in-house
- Cloud model of IT moves some or all data outside the network perimeter
    - Moves risk-management to the cloud provider, but legal responsibility usually remains with the customer
    - Forces the organisation to place their trust in the cloud vendor
        - This trust is not always well-founded
        - Most service providers have an 'all care, no responsibility' legal agreement
        - Who gets the blame in the case of a data breach?
          Hint: the PR disaster usually lands squarely at the feet of the company who 'owns' the data. (If the cloud provider specialises in data security, it will 'splash back' on them too...)
- Legal jurisdiction becomes an issue - the physical location of the data centre(s), as well as the place of incorporation of the cloud provider can affect a range of operational considerations
    - Regulatory compliance issues for governments and corporations
    - What data can or can't legally be stored in the service
    - What the legal obligations are for notifying LEOs (law-enforcement officers) about potential illegal data or activities? It's often unclear - that's why we have lawyers. ;-)

What about the implications for security?

- Security is definitely a major issue in cloud computing
- For small companies, security is actually likely to be enhanced by migrating to the cloud
    - Cloud providers are specialists, and bring a level of expertise that small organisations can usually only dream of
    - Reliability is also usually much higher than
- For larger organisations with existing in-house security expertise and well-established security processes, the cost benefits of migrating to the cloud need to be balanced against a potential reduction in security
- What cloud are you in? This decision can impact the level of security
    - Public cloud - who are you sharing the public swimming pool with?
    - Private clouds - much more controlled, but more expensive
    - Community clouds - a 'gated community' of like-minded tenants
    - Hybrid clouds - mixtures of any of the above
- From a legal perspective, you should operate on the basis that 'you can't outsource blame' - and you certainly can't outsource the negative publicity that can arise from security breaches that become public knowledge
- Organisations who deal with sensitive data - government departments, security agencies, and businesses with very high security requirements - can (and should!) implement data encryption on top of whatever services their cloud provider(s) offer
- Certain risks simply move location - e.g. risk of cloud provider's employees having access to data rather than in-house employees having access to data

For ownership?

- My data is my own, right? Well, maybe...
    - The contract you sign could determine whether your cloud provider has any rights over your data
    - Legal issues in different jurisdictions may also come into play
        - e.g. What happens if a LEA (law-enforcement agency) or other TLA (FBI, CIA, NSA, ASIO, ASIS) executes a search warrant on your cloud provider's equipment? Will your data be included? Will your services remain running?
- It's a complex and evolving area of international law
- Vendor collapse - what happens if your cloud provider goes belly-up?
- Termination of contract - what happens if you decide to terminate your contract (for breach, etc.) or if your provider decides to terminate the contract?
    - How long before you get your data back?
    - Can you be 'held to ransom'?
- Data portability
    - Built-in tools to download/migrate data
    - Vendor lock-in - may be difficult or costly to migrate to another provider

For innovative products and services?

- Massively-improved affordability is a huge issue and one of the dominant drivers of cloud computing - the entry barrier is lowered (or smashed) for a whole raft of compute-intensive tasks
    - e.g. 30,000-core cluster built for pharma company cost ~$10,000 to run a 7-hour job rather than costing $millions in hardware and a full week to run
- Makes simple redundancy for small infrastructure affordable
    - Have multiple servers in multiple data centres for failover redundancy, geographic redundancy easily achievable
    - Web hosting, data backup and archiving, virtual infrastructure for disaster recovery
- We're still in the early days of 'the cloud' - expect new products and services to emerge as innovators explore the boundaries of what's now possible

For you?

- Eh. As an ‘end-user’, in most cases you won't have any idea whether the websites and services you use are hosted in-house or in the cloud.
- Cost reductions in IT infrastructure flow down to customers, making services affordable for small businesses and individuals that were previously prohibitively expensive.
- Makes entirely new services possible
    - e.g. that new thing that gal thought up and is about to launch... :-)

Is the cloud any different to what came before?

- Initially, not so much. Now, yes, Very much.

Further reading

So, what is the cloud? (SMH, 31/7/12)
http://www.smh.com.au/it-pro/cloud/so-what-is-cloud-20120731-23bns.html

Is cloud computing secure?
http://www.smh.com.au/it-pro/security-it/is-cloud-computing-secure-20120725-22pti.html?rand=1343696076395

References

The NIST Definition of Cloud Computing
http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf

$1,279-per-hour, 30,000-core cluster built on Amazon EC2 cloud
http://arstechnica.com/business/2011/09/30000-core-cluster-built-on-amazon-ec2-cloud/