# 6.1t:transcript

What is Cloud computing?

Cloud computing can be described as a model for ubiquitous and on-demand access to a shared pool of network or configurable computing resources (for example, networks, servers, storage, applications, and services). It can be rapidly provisioned and removed with little management effort or interaction from the service provider. This cloud model promotes availability and is composed of five essential characteristics, three service models, and four deployment models.

Cloud computing provides an economically scalable and professional network management platform, and professional security management. These features can be attractive to large and small businesses, government agencies, and also the end user. The individual or company is required only to pay for the storage capacity and services required. The end user does not have to be concerned with the setup process of a database system, acquiring hardware or require to perform system maintenance, the backup of data us all part of the cloud service.

Theoretically, another advantages of using cloud computing for data storage and sharing is that the cloud service provider is responsible for security. However, this not necessarily mean the customer is fully protected. There have been a number of security failures among cloud providers. A prime example of this is of Dropbox, who made headlines in 2012 where a considerable number of passwords from user accounts were stolen.

Types of cloud services available

In this section, we will look the common definition of cloud, cloud services. First, we must analyse the three service models, commonly defined by NIST as:

* Software as a Service (SaaS)
* Platform as a Service (PaaS)
* Infrastructure as a Service (IaaS)

These can be viewed as nested service alternatives, as shown in the diagram. These models are the universally accepted basic service models that we see in cloud computing today. Lets cover some of the fundaments of each of these deployment models:

Software as a Service

A SaaS cloud provides a software platform to deliver a service, specifically software that is required to be accessed within the cloud. SaaS follows the web services model, whoever this concept is then applied to cloud resources. SaaS enables the customer to utilise applications of the provider in the cloud infrastructure. A web client is usually used for clients to interact with the application. Licensing for software is the responsibility of the cloud provider and not the enterprising subscribing to that service.

SaaS avoids complexity of software installation, maintenance, upgrades, and patches. Typical examples of SaaS services are Google Gmail, Office 365, etc.

Common use cases for SaaS are employees’ access to office software suites, such as document management and e-mail services. Individuals also commonly use the SaaS model to acquire cloud resources using specific applications on demand. A cloud provider usually offers data-related features such as data backup and sharing of data between the end users.

Platform as a Service

PaaS provides an infrastructure to which a customer can run their own applications and enables them to deploy their own or acquired applications. The PaaS cloud provides the building blocks and development tools like programming language tools, runtime environments, and other tools to help deploy new applications. In essence, PaaS is an operating system that runs within the cloud. PaaS is useful for an organisation that requires computing resources needed for running applications tailored to requirements. Google App Engine and Microsoft Azure, are typical examples of PaaS providers.

Infrastructure as a Service

IaaS provides customer access to the underlying cloud infrastructure resources. IaaS provisions virtual machines and abstraction of hardware and operating systems. IaaS provides processing, storage, networks, and other crucial computing resources so that arbitrary software can be run by the customer, this include operating systems and applications.

IaaS combines basic computing services for the customer, and offers capabilities such as number crunching and storage of data, to build highly scalable computer systems.

It is typical for the customer to self-provision an infrastructure, by the use of a web-based interface that serves as a management interface for the infrastructure. Customers can also opt to access the platform via API as an alternative. Typical examples of IaaS are Amazon EC2, Microsoft Windows Azure, Google Compute Engine (GCE).

Looking at the diagram a side by side comparison of each type of service can be seen. As we move further to the right, the responsibility shifts further away from the customer on to the cloud provider. The type of service use provides a trade-off between both elements, and the customer should choose a service that is appropriate to resource availability and reliance on skillsets to manage the chosen service.

Cloud Deployment models

It is commonplace to see many organisations now moving their IT infrastructures to the cloud. Given this choice, there lies many other options that determine ownership and management of cloud services. In this section we look at the four most common deployment models seen in cloud computing infrastructures today.

Public Clouds

Public cloud infrastructures provide services to the general public or large industry groups from a cloud services provider. Cloud infrastructure and data control operations are the prime responsibilities of a public cloud provider. Ownership, management and operations of public clouds vary from academic, government or business organisations, or potentially a combination, and resides on the cloud service provider premises.

The major components in a public cloud are often located within a multi-tenant infrastructure and availability of applications and storage are made across the Internet through a secured IP based environment, whereby the services can be offered for free or on a pay-per-usage basis. Amazon and Google web applications, Facebook or Instagram social media provide free storage of data such as photos, documents etc. Public clouds are usually inexpensive and are designed to scale towards the needs of the end user. It is typical to provide low scale or no service level agreements (SLA) and therefore not offer any guarantee against loss of data or corruption that is commonly found through private or hybrid cloud solutions.

 Public cloud services are appropriate for end consumers and entities that do not require the same level of service expected within a firewall. It is also important to note that public IaaS clouds don’t necessarily accommodate restrictions or are compliant with privacy laws, these aspects are the subscriber or corporate end user responsibility.

The majority of public clouds place focus on the consumer market or small to medium-size businesses, where it is common to see pay-per-use pricing, often equating to low costs per gigabyte of storage. An example of such services might involve image or audio sharing, backup of laptops or mobile phone data, or for file sharing files amongst users.

One of the primary advantage public cloud services is the costs involved. An organisation will only pay for the services and resources that it requires and can adjust these as and when is needed. Furthermore, the subscriber does not have the responsibility of management overheads, further cutting costs. The primary concern with public cloud servers, however, is security. Public cloud providers have now focused their efforts to security their systems, and in many cases have focused their efforts and resources in this area more than those in private clouds to ensure customer data security.

Private Clouds

Private clouds are implemented within an internal IT environment of the organisation. This type of cloud may be managed in house or the management function can be outsourcing to a third-party entity. Additionally, cloud servers and storage can be deployed on or off premises.

Private clouds services can deliver an IaaS platform on an internal basis to employees or branch networks through via an intranet or through the Internet using a virtual private network (VPN). Software applications or storage services can also be provided to branch offices as and when required. Private clouds utilise existing infrastructures to deliver services, offering privacy of using the organisational network. There are several examples of private cloud services, these include on-demand derivatives of services such as database, e-mail, and storage.

The prime use case for private clouds is emphasis on security. Private cloud infrastructures enforce greater control over geographic location of data storage and other aspects of security. Another benefit of private clouds is that they can pool resources and can be rapidly deployed to organisational entities.

Community Clouds

Community clouds share attributes with both private and public clouds. As with private clouds, community clouds hold restricted access. Similar to public clouds, resources are shared across independent organisations. These organisations are likely to have similar requirements and therefore are likely to share data from within the cloud. The community cloud concept is particularly popular in the healthcare industry, particularly because they can be implemented with emphasis on government privacy regulations, as well as other regulations, with data exchanged done so in a controlled environment. Community clouds can be managed by the participating organisation or it may also be managed by a third party that exists on or offsite. This deployment model is likely to be more expensive than the likes of public clouds, primarily due to the spread of cost over less users, however it is not as costly as private clouds, where administration of such services may only be managed and funded by a single or few organisations. On this basis, only some of the cost benefits are realised over public cloud services.

Hybrid Clouds

Hybrid clouds are a mixture of a multitude of cloud types such as private, public or community. They are unique entities in themselves but are bound by proprietary technology which enables portability of applications and data. Hybrid clouds allow sensitive data to be placed in the private cloud, whilst less sensitive data can be placed without the public area of the cloud. This kind of setup can be more attractive to smaller companies, where applications with less emphasis on security can be transferred with a considerably cheaper outlay on price. This means a business does not need to commit to moving potentially sensitive data to a public cloud, thus reducing the potential of data breaches of sensitive customer data.

SDN and NFV

In this section we are going to look at how SDN and NFV are relevant to Cloud Computing. Cloud computing actually pre-dates other network paradigms we have discussed earlier in this module such as SDN and NFV, so it has been deployed and managed without these services in mind, however it is now becoming apparently that the use of both of these services is advantageous and compelling for both public and private cloud operators.

The centralised nature of SDN means that network resources and traffic usage patterns can be managed from an SDN controller, resulting in tight integration that can be highly beneficial to Cloud Computing, particularly resource management. This means a single or distributed controller can configure and manage virtual networks and deploy Quality of Service, which is paramount for a decent user experience, ultimately this reduces the burden of network management and reduce the amount of time it takes to manage individual network devices.

In terms of NFV and cloud computing, the deployment of NFV automates and virtualises the provisioning of network-based hardware such as firewalls and switches, as well as storage devices. It also enables scaling out of devices on an as needed basis. What this means is that for each cloud customer, it does not require a separate piece of equipment to provide services, all devices are deployed in a centralised environment through a hypervisor platform and enforced with rules and policies based upon organisational requirements.