**Module 3 Architecture & Design**

**3.7 Cloud**

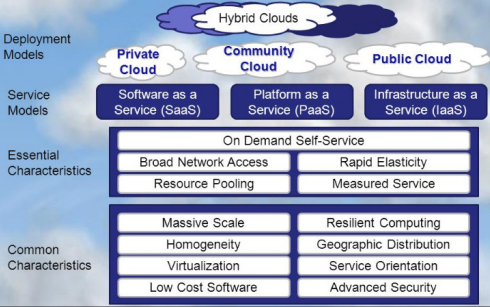
**Cloud Computing Definition**

* NIST SP800-145 – cloud computing is model for enabling ubiquitous, convenient, on-demand network access to shared pool of configurable computing resources (Eg. Networks, servers, storage, apps & services) that can be rapidly provisioned & released with minimal management effort/service provider interaction

**On-Premise vs. Hosted vs. Cloud**

* On-Premise – servers at organisation’s location
* Hosted – servers outsourced to external provider
* Cloud – using shared servers

**NIST Cloud Framework**



**Essential Characteristics of Cloud Computing**

* On-demand self-service
* Broad network access
* Resource pooling
* Rapid elasticity/expansion
* Measured service

**Cloud Computing Service Models – Software as a Service (SaaS)**

* According to NIST

1. Capability provided to consumer is to use provider’s apps running on cloud infrastructure
2. Apps accessible from various client devices through either thin client interface (Eg. Web browser – web-based email) or program interface
3. Consumer does not manage/control underlying cloud infrastructure including network, servers, OS, storage or individual app capabilities with possible exception of limited user-specific app configuration settings

**Cloud Computing Models – Platform as a Service (PaaS)**

* According to NIST

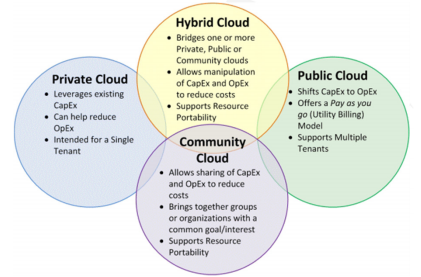
1. Capability provided to consumer is to deploy onto cloud infrastructure consumer-created/acquired apps created using programming languages, libraries, services & tools supported by provider
2. Consumer does not manage/control underlying cloud infrastructure including network, servers, OS or storage but has control over deployed aps & possibly configuration settings for the app-hosting environment

**Cloud Computing Models – Infrastructure as a Service (IaaS)**

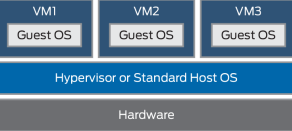
* According to NIST

1. Capability provided to consumer is to provision processing, storage, networks & other fundamental computing resources where consumer is able to deploy & run arbitrary software, which can include OS & apps
2. Consumer does not manage/control underlying cloud infrastructure but has control over OS, storage & deployed apps & possibly limited control of select networking components (Eg. Host firewalls)

**Cloud Deployment Models**



**Virtualisation**

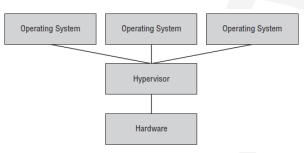


**Hypervisors**

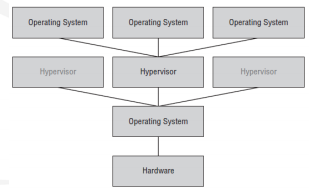
* Underlying technology that creates & runs virtual machines
* Presents guest OS with virtual operating platform & manages execution of guest OS
* 2 implementation methods

1. Type 1 – native/bare-metal
2. Type 2 – hosted

* Type 1 Hypervisor



* Type 2 Hypervisor



**Containers**

* Replacing/used with hypervisors
* Lightweight, stand-alone, executable package of software that includes everything needed to run it – code, runtime, system tools, system libraries, settings

**VDI (Virtual Desktop Infrastructure)/VDE (Virtual Desktop Environment)**

* VDE (Virtual Desktop Environment) – desktop virtualisation
* VDI (Virtual Desktop Infrastructure)

1. User’s desktop running inside virtual machine that resides on server in datacentre
2. Form of VDE that enables fully personalised desktops for each user

**Cloud Storage – Network Storage**

* DAS (Direct Attached Storage)
* NAS (Network Area Storage)
* SANs (Storage Area Network)
* Data Security – encryption on storage device

**Virtualisation Security**

* VM Escape Protection – leaving assigned VM
* VM Sprawl Avoidance – overusing shared resources
* Cloud Access Security Token (CASB) – security policy enforcement points
* Security as a Service – subscription-based business model for acquiring & managing security functions (virtual SOC (System On a Chip))