# Cloud Deployment Models

# Introduction

- Models include:
  - Private cloud (deployed within organisation's firewall)
  - Public cloud (deployed outside organisation's firewall), hosted by third party
- Datacenter
  - Houses computer systems and related components such as for communications and storage systems
  - Has redundant or backup power supplies, data communication connections, environment controls like AC, fire suppression, and also security
- Clouds are locations dependent
- Reliability and redundancy supported by multiple data centers.
- Clouds certainly span One or many datacenters.

# Cloud characteristics

- On-demand service
- Ubiquitous n/w access
- Location independent resource pooling
- Rapid elasticity

# Cloud characteristics

- On-demand service
  - Provisions computing capabilities such as server time and n/w storage
  - Automatically without requiring human interaction

- Ubiquitous n/w access
  - Services available over the n/w accessed through standard mechanisms
  - Can be used on heterogeneous client platforms( mobiles, laptops , PCs)

- Location independent resource pooling
  - Multitenant
  - Resources pooled to serve multiple customers
  - Physical and virtual servers dynamically assigned based on demand
  - Location independence, customer has no control of the locations of services located
  - Example of resources storage, processing, memory, n/w bandwidth.

- Rapid elasticity
  - Services can be rapidly and elastically provisioned
  - Can scale out automatically and rapidly, and
  - Can be quickly released
  - Customer have unlimited services that can be purchased in any quantity at any time

# Measured service

- Cloud systems automatically control and optimise resources
- Leverages metering at some level of abstraction suitable for a service
- Resource usage can be monitored, controlled and reported providing transparency for the utilized service
- More the standardization, and virtualization, more the reduction in infrastructure costs

# Why organizations migrating to cloud?

- Greater flexibility
- Cost reduction
- Avoid problems and delays arising from apps that have varying loads

# How can cloud vendor's address clients challenges?

- Prioritising cloud apps based on business impact and risk
- Identifying apps that are suitable and have high business impact
- Addressing problems of workloads to improve the client experience
- Mitigating risk of costly implementation delays
- Avoiding apps with complex and integrated workloads
- Leveraging expertise to help successfully migrate apps to cloud environment
- Help accelerate cloud initiatives

# Cost factor

- Virtualization and standardization allows to deliver services with fewer resources and drive up utilization
- Automation reduces labour cost to give cost benefit
- Frees up budget to be diverted to core services and to innovation and development of new services
- Enables smarter way to deliver services because of self service portals
- Cost also matters when high security requirement leads to high level SLA's
- increases productivity by providing dynamic infrastructure, and
- Providing resources to team wherever and whenever required

- Virtualization driving up utilisation lowers current and future capital investments
- Self service portals enables clients to help themselves with less support people
- Automation reduces IT operation costs
- Test and development environments are different and complex, so
- Multiple skills such as for OS, DB, apps , middleware skills are required to deliver to customers
- Cloud that allows to define environments and reuse it, drives down the labour cost

# Cloud Deployment Models

- Cloud delivery models classified into 3 types:
  - **Public**:
    - capabilities are rented and paid by use
    - Drives efficiency
    - Retains more control and customization
  - **Private:**
    - business convert their IT environment into cloud to deliver services
    - Standardised and low security risk
  - **Hybrid:** combine elements of public and private

# Public clouds

- the services and infrastructure are provided off-site over the Internet
- offer the greatest level of efficiency in shared resources
- are also more vulnerable than private clouds
- Need not buy, service or maintain any infrastructure

It is a good choice when:

- Standardized applications is used by lots of people, such as e-mail
- There are SaaS (Software as a Service) applications from a vendor who has a well-implemented security strategy
- need incremental capacity (the ability to add computer capacity for peak times)
- doing an ad-hoc software development project using a Platform as a Service (PaaS) offered by cloud
- Wiki's, blogs, social networking websites
- Batch processing with limited security requirements
- Looking for online storage solutions
- In applications where latency is not an issue

Public clouds are NOT suitable when:

- Apps composed on multiple co-dependent services
- Online transaction processing systems
- That require high level of auditability and accountability
- Apps that are based on third party software that does not have virtualization or *cloud aware licensing strategy*.
- Data is sensitive information like employee info and health care records

# Private clouds

- Are deployment inside the company's firewall
- Have onsite data centers
- services and infrastructure are maintained on a private network
- Has greater control over infrastructure
- Improved security
- Enterprises have to still purchase and maintain all the software and infrastructure, which increases the costs

Is suitable when:

- Data is business hence, control and security are critical
- Business enforces strict security and data privacy issues
- Enterprise is large enough to run a cloud data centre efficiently and effectively on its own
- Vendor lock-in problems are to be avoided
  - It can be *data or tools or platform* lock-in due specific vendors having rights or license over some tools or platforms and makes migrating difficult on public cloud

# High cost of privacy

- Ownership of hardware or software eliminates the pay per use feature
- There is huge upfront cost
- Hardware is sized for peal loads hence there will be inefficient excess capacity.
- Involves complex procurement cycles
- Complete ownership of implementation and hence complete control

# Comparison

| | Public cloud | Private cloud |
|---|---|---|
| Initial cost | zero | high |
| Running cost | Predictable | Unpredictable |
| Customization | Impossible | Possible |
| Privacy | No (provider has access to the data) | Yes |
| Single sign-on | difficult | Possible |
| Scaling up | Easy | Difficult |

# Hybrid cloud

- Combination of private and public cloud
- Can outsource non business critical info processing to public cloud and keep business critical services and data in private
- It is usually used in evolution process of outsourcing to public clouds.
- Try to keep different aspects of business in suitable clouds
- Can address different security and control requirements

# Security in public clouds

- Private clouds tend to use older technology than public clouds
- Public clouds are hardened through continual hacking attempts
- Public clouds attract the best security people available
- As they seek out the top security experts and treat them as the most important part of their businesses
- So Private cloud staff competence is less

- Multi tenancy
  - As long as the provider provides security to highest-risk client, all the lower risk clients get better security
- Security assessment
  - Assessment can be done regularly by the provider and each client can given the assessment to know the current state of security
- Shared risk
  - A cloud provider may not be the cloud operator
  - A provider of SaaS may be using the IaaS service provided by another provider
  - Multi-tier service provider arrangement shares the risk of security issues among many layers
- Staff security screening
- Distributed data centers

- Physical Security
- Coding
- Data Leakage