Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction."

5 NIST Characteristics of Cloud Computing

On-Demand Self-Service: A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service provider.
Broad Network Access: Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, tablets, laptops, and workstations).
Resource Pooling: The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand.
Rapid Elasticity: Capabilities can be elastically provisioned and released, in some cases automatically, to scale rapidly outward and inward commensurate with demand. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be appropriated in any quantity at any time.
Measured Service: Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled, and reported, providing transparency for both the provider and consumer of the utilized service

IaaS - This gives the consumer the capability to provision their own storage, net-works, and any other fundamental computing resources that are required by the consumer.
PaaS - This gives the consumer a platform on which they can launch their application onto a cloud infrastructure.
Saas- This is where the consumer can utilise a provider's application that is running on a cloud infrastructure.

Private Cloud

This is where the cloud infrastructure is designed for exclusive use by a single organisation with multiple consumers. It may be owned, managed and operated by the organisation themselves, a third party or a combination of both.
It can exist either on or off premises.

Hybrid Cloud

This cloud infrastructure is a combination of two or more definitive cloud infrastructures. They remain unique entities but are bound together by standardised or branded technology that enables data and application portability.

Community Cloud

This cloud infrastructure is designed for exclusive use by a specific community of users from organisations that have shared interests. It may be owned, managed and operated by either one or more of the organisations involved, by a third party or a combination of both. It can also exist on or off premises.

Public Cloud

This is a cloud infrastructure that is designed for use by the public. It can be managed, owned and operated by a business, academic or government organisation or any combination of them. It can also exist on or off premises.

Virtualization is using computer resources to imitate other computer resources or whole computers. It is the process of using a single physical machine to run multiple unique virtual machines. It separates resources and services from the underlying physical delivery environment.

Host server - This is the host machine which provides the underlying environment that the client virtual machines run on. It is the role of the host server to provide the interaction between the physical hardware and then simulate a hardware environment for the client's virtual machines.
Client virtual machines - The aim of the host machine is to run multiple client virtual machines. Each of these virtual machines will be allocated specific resources (such as disc space, Memory/RAM and CPU time) for their usage. Client machine should remain independent and have separation from one another.

Virtual memory: Disks have a lot more space than computer memory. Therefore, with virtual memory, the computer frees valuable memory space by placing information it doesn't use often into disk space.
Software: Companies have built software that can emulate a whole computer. That way, one computer can perform as though it were actually 20 computers.

Partitioning: In virtualization, many applications and operating systems (OSes) are supported in a single physical system by partitioning (separating) the available resources.
Isolation: Each virtual machine is isolated from its host physical system and other virtualized machines. Because of this isolation, if one virtual-instance crashes, it doesn't affect the other virtual machines. In addition, data isn't shared between one virtual container and another.
Encapsulation: A virtual machine can be represented (and even stored) as a single file, so you can identify it easily based on the service it provides. In essence, the encapsulated process could be a business service. This encapsulated virtual machine can be presented to an application as a complete entity. Therefore, encapsulation can protect each application so that it doesn't interfere with another application.

What makes virtualization so important for the cloud is that it decouples the software from the hardware. Decoupling means that software is put in a separate container so that it's isolated from operating systems.

Layers of Virtualisation

- **Access Virtualization** — hardware and software technology that allows nearly any device to access any application without either having to know too much about the other.
- **Application Virtualization** — software technology allowing applications to run on many different operating systems and hardware platforms.
- **Processing Virtualization** — hardware and software technology that hides physical hardware configuration from system services, operating systems or applications.
- **Storage Virtualization** — hardware and software technology that hides where storage systems are and what type of device is actually storing applications and data.
- **Network Virtualization** — hardware and software technology that presents a view of the network that differs from the physical view.
- **Management of virtualized environments** — software technology that makes it possible for multiple systems to be provisioned and managed as if they were a single computing resource.

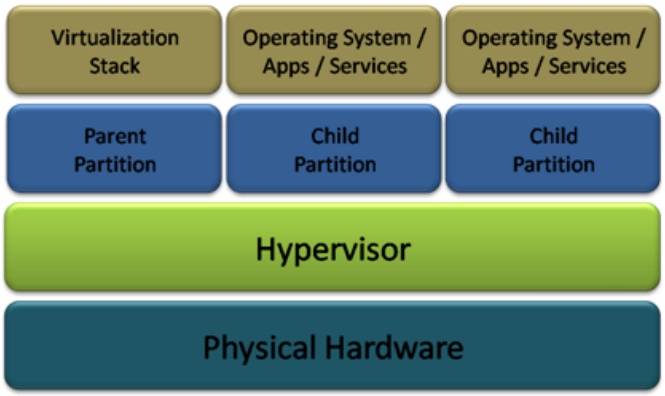


Figure 1 (Hyper-V Stack)

Benefits

- Resource Pooling, High Redundancy, Highly Available , Rapidly Deploy New Servers, Easy to Deploy, Reconfigurable while services are running, Optimizes Physical Resources by doing more with less, Decreases Power Output of Company
- Simplifies Disaster Recovery, Faster deployment of information technology resources, Lower Operational costs associated with reduced resource management and admin, Standardised hardware configuration, Smooth migration paths, Power Efficiency, Rapid Scalability

Disadvantages

- Harder to conceptualise, More Costly , Licensing Costs, Vulnerable to Server failure, Compromise of virtualized hosts will affect guest machines, Additional Guest Servers will require their own admin measures, Initial Cost can be high - renewal of associated infrastructure must be added

Multi Tenancy

Multitenancy is a reference to the mode of operation of software where multiple independent instances of one or multiple applications operate in a shared environment. The instances (tenants) are logically isolated, but physically integrated. Multi tenancy enables separation between tenants running applications in a shared environment. In a multi-tenant environment, the resources controlled by one tenant are physically or logically separated and secured from other tenants.

Is it essential for the cloud as it enables rapid and elastic scaling or resources and cost efficiency.

One of the key decision parameters in selecting the cloud model is the amount of ownership the consumer is willing to retain within their control. PaaS provides productivity, IaaS offers flexibility.

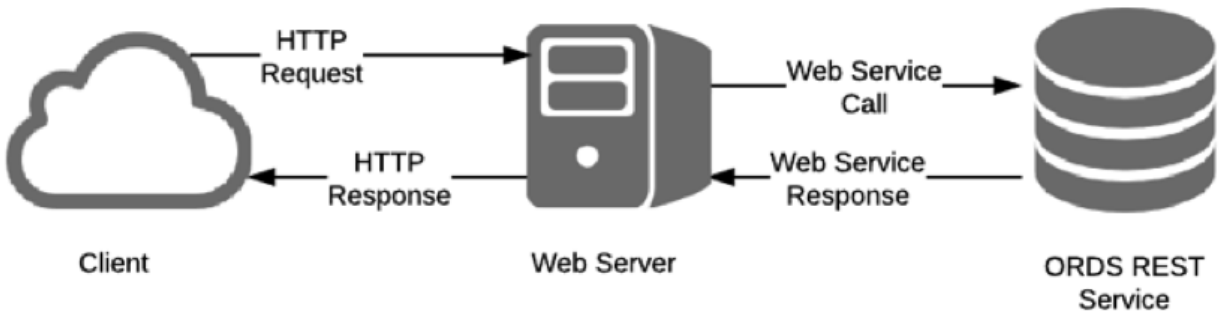
- IaaS (Infrastructure as a Service)
    - Multiple Guest OS on one host OS
    - Encryption between tenants both in transit and at rest
- PaaS (Platform as a Service)
    - Consolidation implies that multiple PaaS instances will reside on the same servers and there must exist a way to isolate Tenants from each other. At a minimum, a PaaS solution must isolate
        - Tenant sessions, Tenant processes, Tenant data
    - Physical Isolation
        - Dedicate resources for each component (server, DB) running entirely within virtualised containers on the hypervisor.
        - Not common
    - Virtual Isolation
        - Multiple virtualised containers execute on shared hardware. Containers may be a fully realised guest OS or specialised JVM
        - Decoupling enables containers to be moved to other servers without modification.
    - Logical isolation
        - Components are directly configured on target physical server. Each component must support isolation. Segmented databases using tenant specific identities.
        - Required more management work that virtual
        - Needs consideration when application is being developed.

REST

Representational State Transfer (REST)

Rest is a client server architecture which operates on the transfer of representations (usually in JSON or XML) of resources and is a popular was of providing interoperability between web services and systems.

HTTP is the main and the best example of a REST style implementation, but should not be confused with REST.



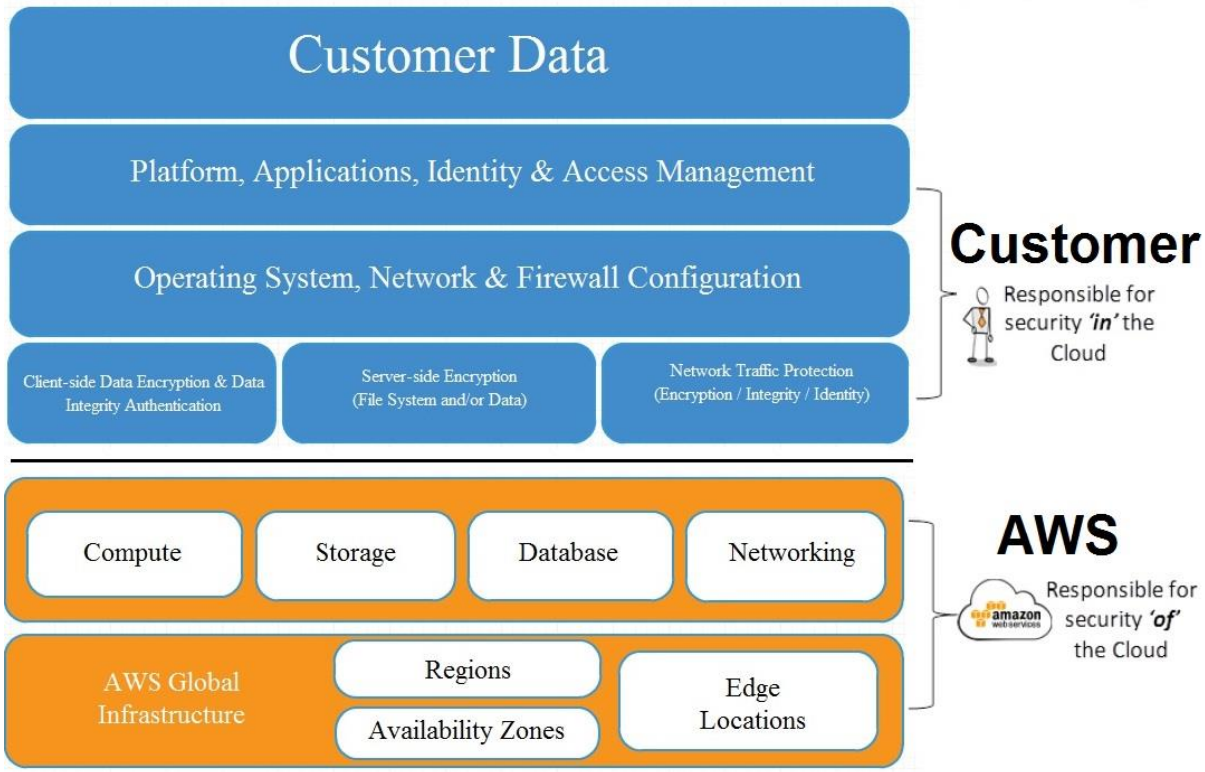
Cloudburst

Cloud burst can be either a positive and negative phenomenon that defines a cloud infrastructure's ability to handle traffic and computing surges. A positive cloud burst refers to a cloud-based application or infrastructure platform that efficiently and capably manages cloud-hosted application scalability. A negative cloud burst refers to a cloud-based application or infrastructure's inability to efficiently manage resource requirements.

The term can also refer to a situation in a hybrid cloud where there is a burst of data and the application scales from the private to the public cloud. Cloud bursting in this sense has the same result -- the app performs -- it's just that the public cloud resources were used to accomplish the scalability.

Memory Ballooning

Virtual memory ballooning is a computer memory reclamation technique used by a hypervisor to allow the physical host system to retrieve unused memory from certain guest virtual machines (VMs) and share it with others. Memory ballooning allows the total amount of RAM required by guest VMs to exceed the amount of physical RAM available on the host. When the host system runs low on physical RAM resources, memory ballooning allocates it selectively to VMs.



Security Layers

1. Perimeter (Physical)
2. Remote Access Control (VPN)
3. Network Security (Firewall, DMZ)
4. Compute Security (Hardening, Anti Virus)
5. Storage Security (Encryption, Zoning)

Role of the Cloud Architect

Reference: Luis Praxmarer (Experton-Group) - Cloud Architect Role
4 main roles of the cloud Architect:

- The Business Analyst Architect:
- The Technology Enabler Architect:
- The Process Re-Engineer Architect:
- Cloud Application Architect:

Business Reasons for moving to the cloud and the decision of public or private

Financial Reasons for moving to the cloud:

1. Fully utilized hardware. Cloud computing brings natural economies of scale.
2. Lower power costs. Cloud computing uses less electricity.
3. Lower people costs.
4. Zero capital costs.
5. Resilience without redundancy

Public Cloud

- Shared computing storage and networking. Limited supply but scalable on demand.
- Shared resources can be accessed from anywhere
- Limited control
- High availability
- Shared physical resources present security risks

A PUBLIC CLOUD SOLUTION MAY BE RIGHT FOR YOU IF:

- Business growth is dynamic and computing demand fluctuates over time
- Security is an imperative, but workloads can be appropriately segmented to reduce any risk that might be associated with industry or government compliance mandates
- Keeping costs low by taking advantage of economies of scale is appealing

Private Cloud

- Limited supply of resources matched to demand
- Predictable operating expense predictable over time
- Single organisation retains ability to configure resources
- High availability
- Combination of physical and logical separation adds more security.

A PRIVATE CLOUD SOLUTION MAY BE RIGHT FOR YOU IF:

- Business growth is predictable and computing demand is stable over time
- Industry or government compliance mandates limit the feasibility of shared resources
- Accepting higher, but predictable costs to ensure dedicated resources is strongly desired

EU DATA PROTECTION ACT

The EU data protection act is an important regulation for operations in the cloud. Even if the cloud provider is based in the US or elsewhere, to provide services to EU customers or store any relevant data in EU governed states they need to be compliant.

HIPAA

The Health Insurance Portability and Accountability Act (HIPAA) is a regulation which applied to health information [14]. This act applies stringent rules to the storage and transfer of health information and with many health and insurance companies migrating their services to the cloud it is very important.

USA PATRIOT ACT

This act states that the US government can access data stored outside of the US by US based cloud service providers or subsidiaries. This also has implications for private data as, under the guise of national security the US can bring this act to bear to gain access to private data.