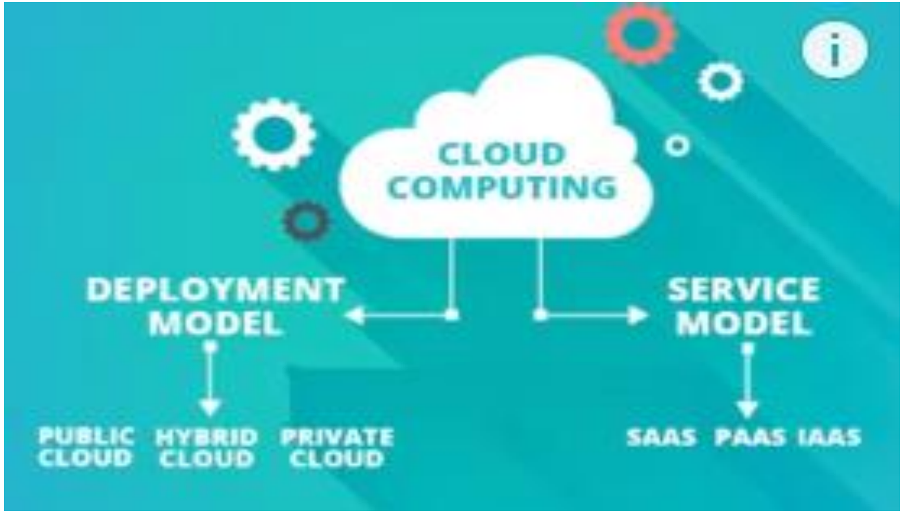
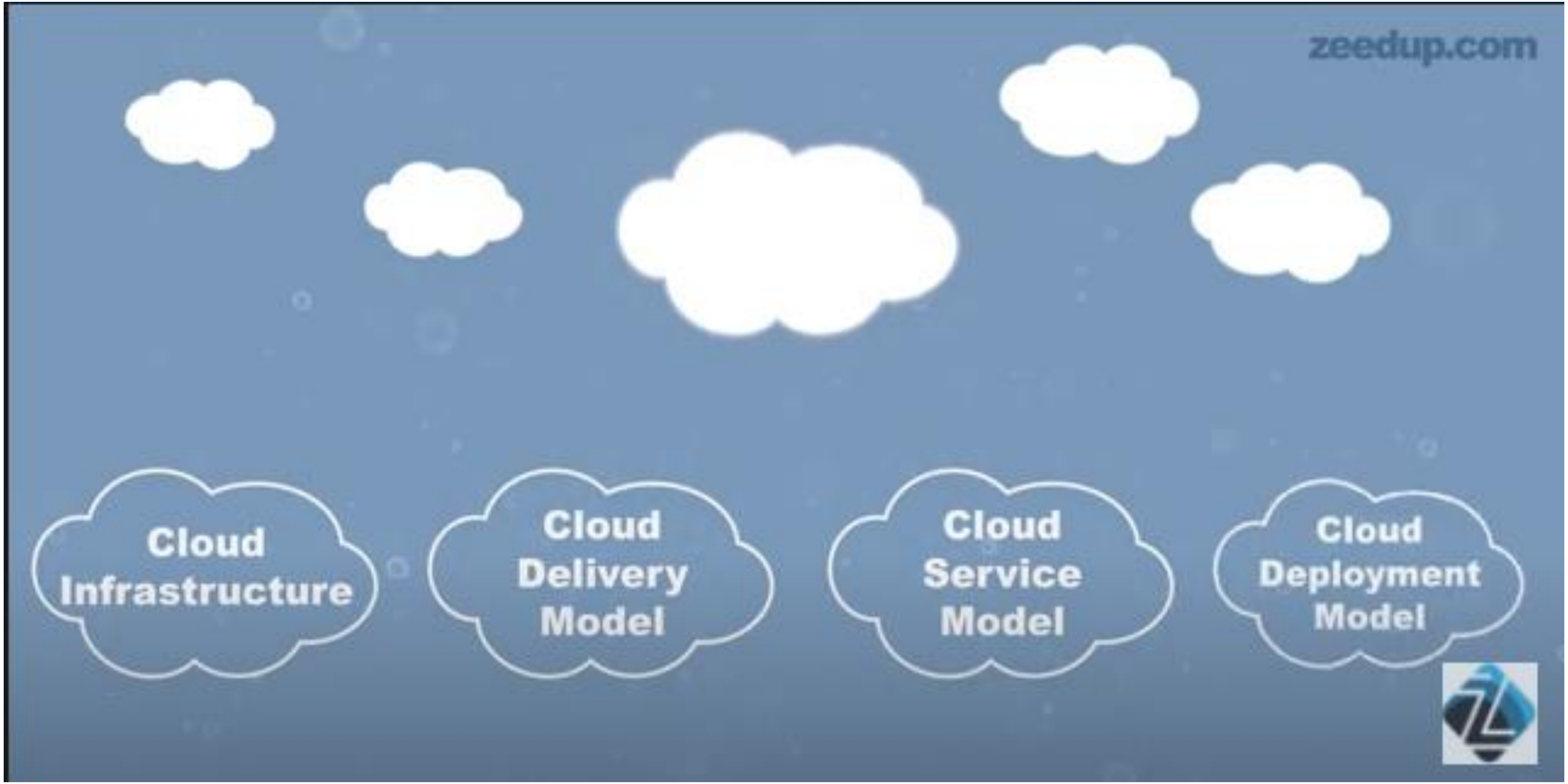
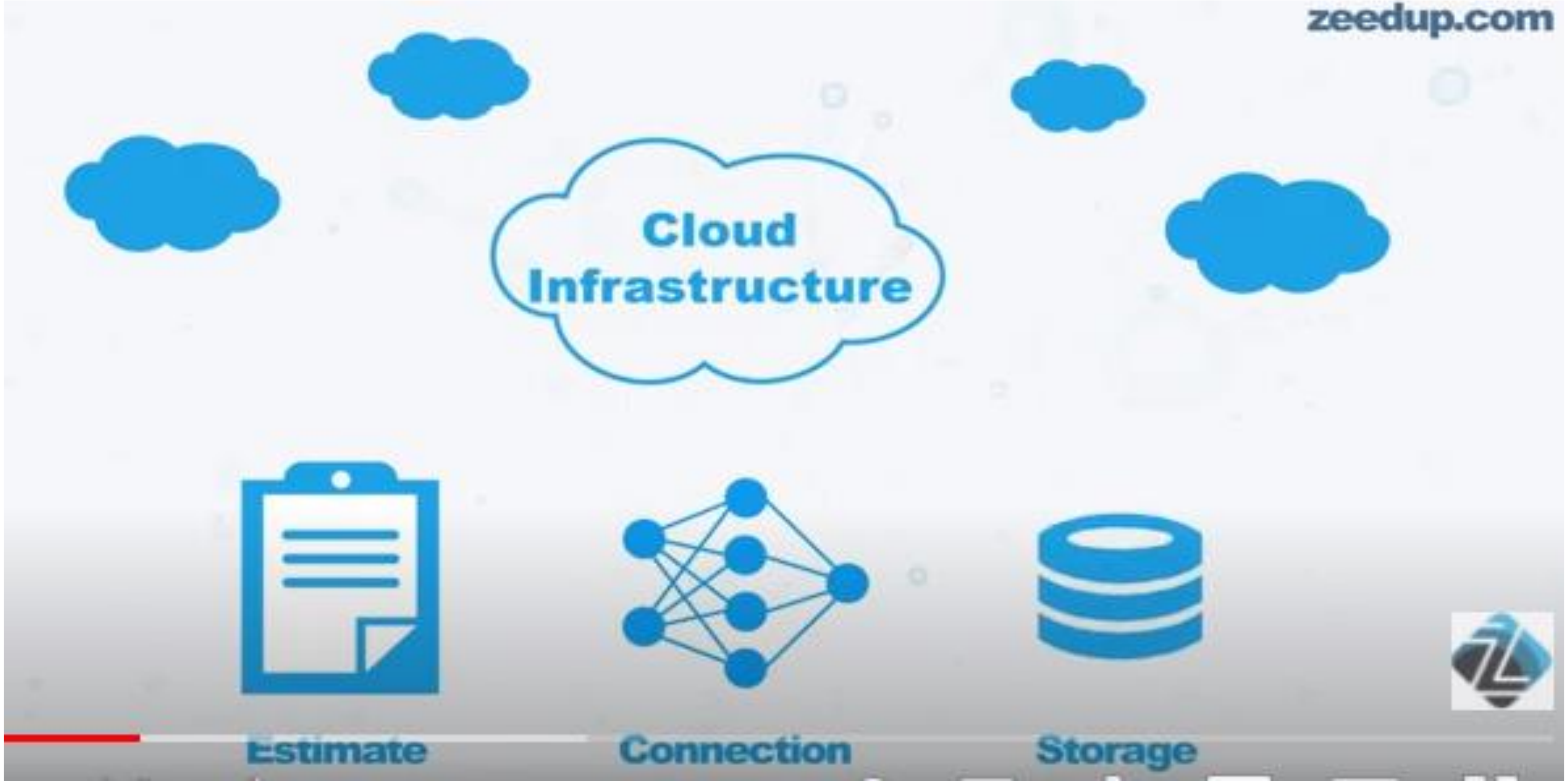
Types of Cloud Computing and Cloud Services



Types of Cloud Computing



Cloud Infrastructure



Cloud Infrastructure

- Cloud infrastructure is a term used to describe the components needed for cloud computing, which includes hardware, abstracted resources, storage, and network resources.
- An abstraction technology or process—like virtualization—is used to separate resources from physical hardware and pool them into clouds; automation software and management tools allocate these resources and provision new environments so users can access what they need—when they need it.

Components of Cloud Infrastructure

Hardware

- Although you probably think of clouds as being virtual, they require hardware as part of the infrastructure.
- A cloud network is made up of a variety of physical hardware that can be located at multiple geographical locations.
- The hardware includes networking equipment, like switches, routers, firewalls, and load balancers, storage arrays, backup devices, and servers.
- Virtualization connects the servers together, dividing and abstracting resources to make them accessible to users.

Virtualization

- Virtualization is technology that separates IT services and functions from hardware.
- Software called a hypervisor sits on top of physical hardware and abstracts the machine's resources, such as memory, computing power, and storage.
- Once these virtual resources are allocated into centralized pools they’re considered clouds.
- With clouds, you get the benefits of self-service access, automated infrastructure scaling, and dynamic resource pools

Components of Cloud Infrastructure

Storage

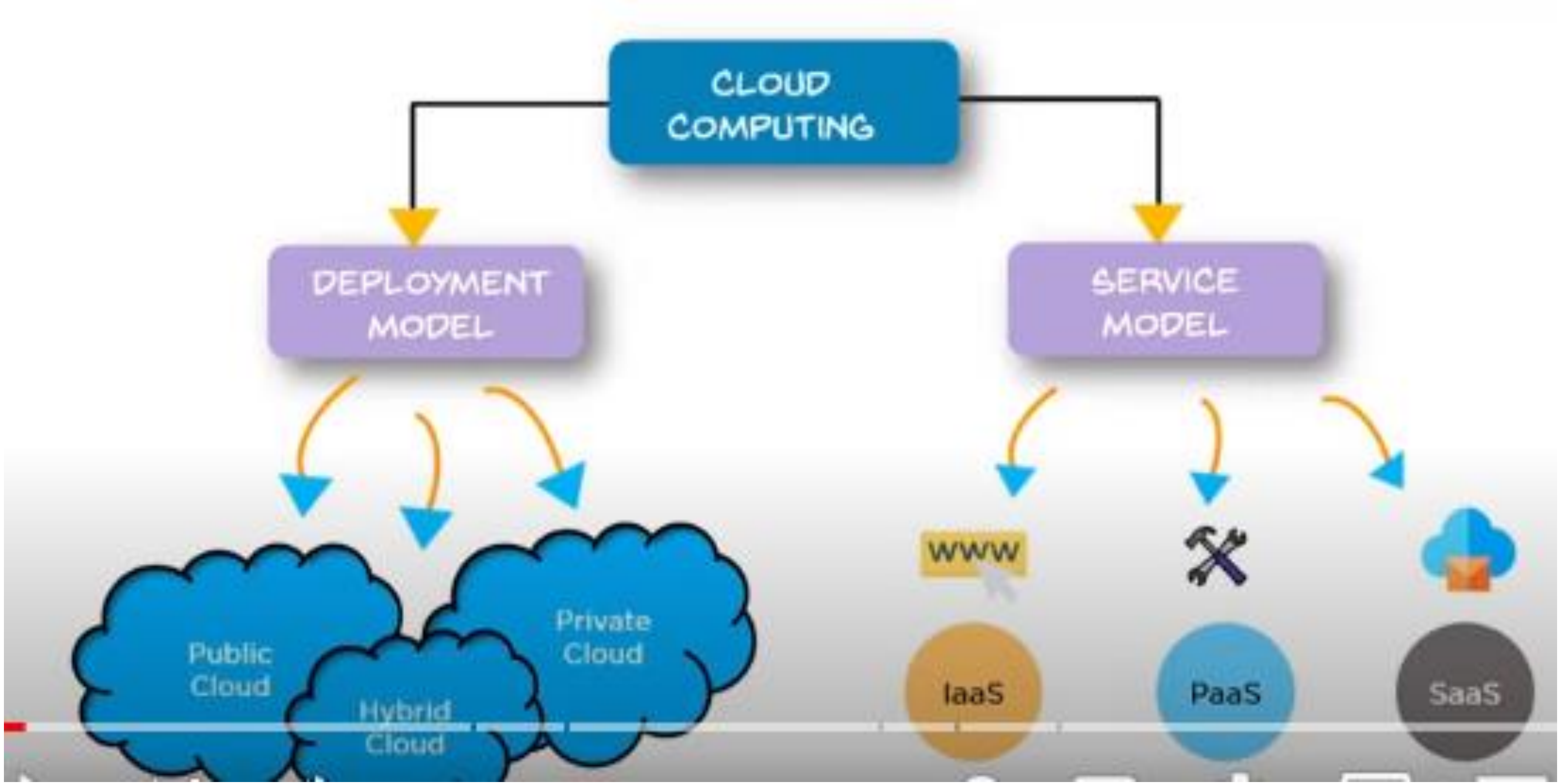
- Within a single datacenter, data may be stored across many disks in a single storage array. Storage management ensures data is correctly being backed up, that outdated backups are removed regularly, and that data is indexed for retrieval in case any storage component fails.
- Virtualization abstracts storage space from hardware systems so that it can be accessed by users as cloud storage.
- When storage is turned into a cloud resource, you can add or remove drives, repurpose hardware, and respond to change without manually provisioning separate storage servers for every new initiative.

Network

- The network is composed of physical wires, switches, routers, and other equipment. Virtual networks are created on top of these physical resources.
- A typical cloud network configuration is composed of multiple subnetworks, each with varying levels of visibility. The cloud permits the creation of virtual local area networks (VLANs) and assigns static and/or dynamic addresses as needed for all network resources.
- The cloud resources are delivered to users over a network, such as the internet or an intranet, so you can access cloud services or apps remotely on demand.

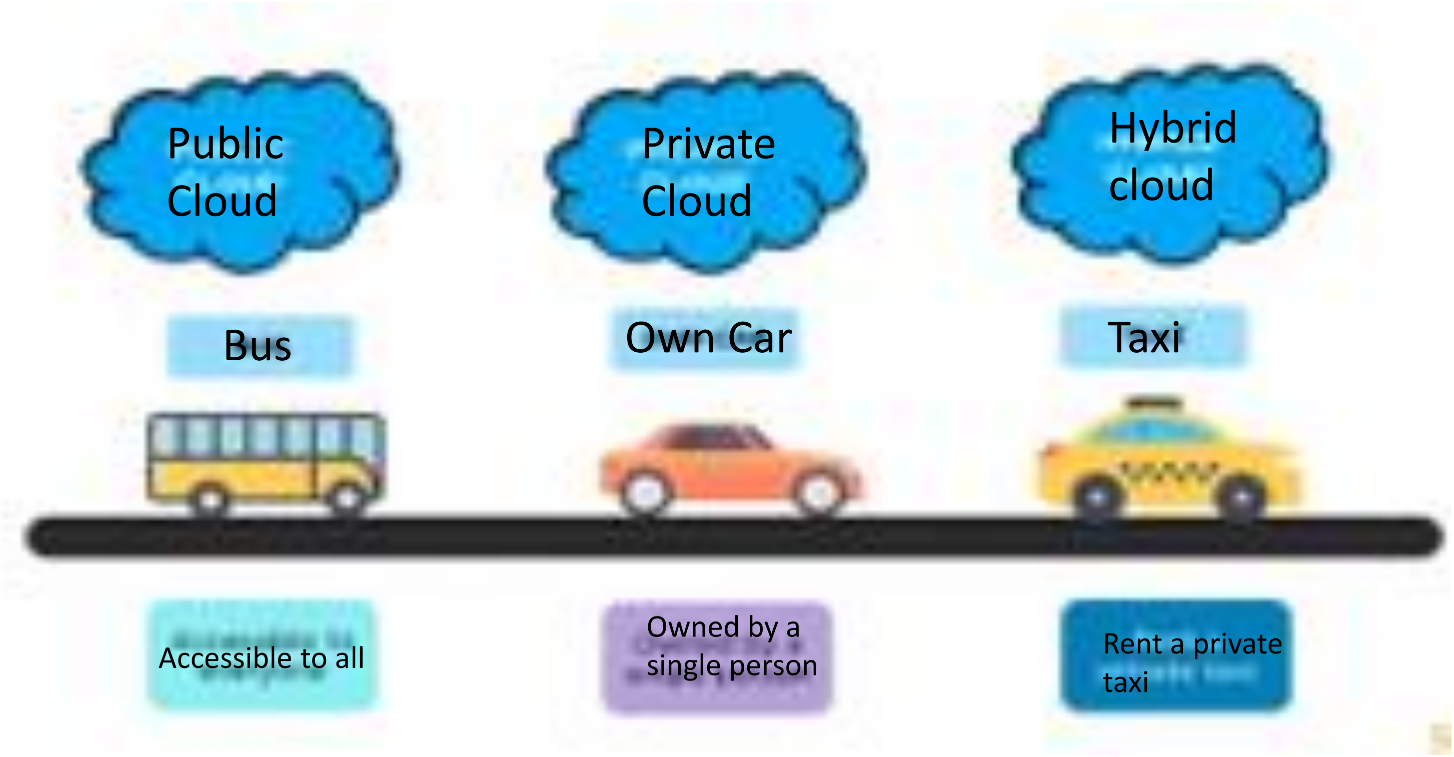
Cloud Delivery Model

Cloud Computing



Vishwakarma Institute of Technology

Deployment Model



Public Cloud	Private Cloud	Hybrid cloud
Bus	Own Car	Taxi
Accessible to all	Owned by a single person	Rent a private taxi

Cloud Computing- Types

There are 4 main types of cloud computing:

- Public clouds,
- Private clouds,
- Hybrid clouds,
- Multiclouds

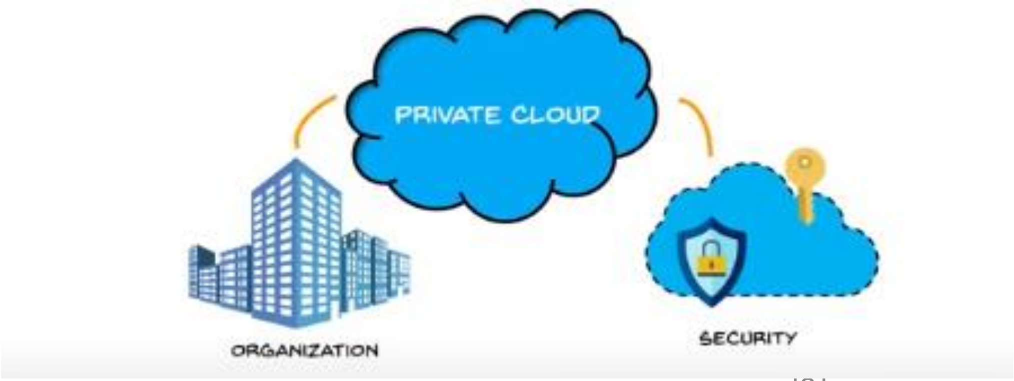
- Choosing a cloud type or cloud service is a unique decision.
- No 2 clouds are the same (even if they're the same type), and no 2 cloud services are used to solve the same problem.
- But by understanding the similarities, you can be more informed about how the caveats of each cloud computing type and cloud service might impact your business.

Public Clouds

- The cloud infrastructure is made available to the general public over the internet and is owned by a cloud provider.
  Public clouds are cloud environments typically created from IT infrastructure not owned by the end user. Some of the largest public cloud providers include Alibaba Cloud, Amazon Web Services (AWS), Google Cloud, IBM Cloud, and Microsoft Azure.
- Traditional public clouds always ran off-premises, but today's public cloud providers have started offering cloud services on clients' on-premise data centers. This has made location and ownership distinctions obsolete.
- All clouds become public clouds when the environments are partitioned and redistributed to multiple tenants. Fee structures aren't necessary characteristics of public clouds anymore, since some cloud providers (like the Massachusettes Open Cloud) allow tenants to use their clouds for free. The bare-metal IT infrastructure used by public cloud providers can also be abstracted and sold as IaaS, or it can be developed into a cloud platform sold as PaaS.

Private Clouds

- Private clouds are loosely defined as cloud environments solely dedicated to a single end user or group, where the environment usually runs behind that user or group's firewall. All clouds become private clouds when the underlying IT infrastructure is dedicated to a single customer with completely isolated access.
- But private clouds no longer have to be sourced from on-prem IT infrastructure. Organizations are now building private clouds on rented, vendor-owned data centers located off-premises, which makes any location and ownership rules obsolete. This has also led to a number of private cloud subtypes, including:



The cloud infrastructure is exclusively operated by a single organisation. It can be managed by the organisation or a third party and may exist on or off premise. Ex. AWS,VMware

Private Clouds

Managed private clouds

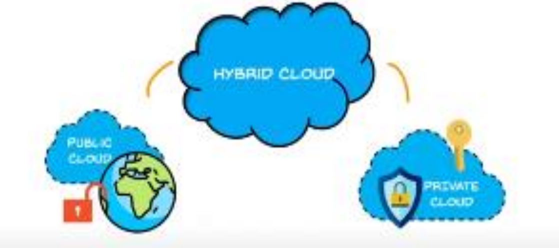
Customers create and use a private cloud that's deployed, configured, and managed by a third-party vendor. Managed private clouds are a cloud delivery option that helps enterprises with understaffed or underskilled IT teams provide better private cloud services and infrastructure.

Dedicated clouds

A cloud within another cloud. You can have a dedicated cloud on a public cloud (e.g. Red Hat OpenShift® Dedicated) or on a private cloud. For example, an accounting department could have its own dedicated cloud within the organization's private cloud.

Hybrid Clouds

- A hybrid cloud is a seemingly single IT environment created from multiple environments connected through local area networks (LANs), wide area networks (WANs), virtual private networks (VPNs), and/or APIs.
- The characteristics of hybrid clouds are complex and the requirements can differ, depending on whom you ask. For example, a hybrid cloud may need to include:
- At least 1 private cloud and at least 1 public cloud
- 2 or more private clouds
- 2 or more public clouds
- A bare-metal or virtual environment connected to at least 1 public cloud or private cloud
- But every IT system becomes a hybrid cloud when apps can move in and out of multiple separate—yet connected—environments. At least a few of those environments need to be sourced from consolidated IT resources that can scale on demand. And all those environments need to be managed as a single environment using an integrated management and orchestration platform.



Multiclouds

- Multiclouds are a cloud approach made up of more than 1 cloud service, from more than 1 cloud vendor—public or private. All hybrid clouds are multiclouds, but not all multiclouds are hybrid clouds. Multiclouds become hybrid clouds when multiple clouds are connected by some form of integration or orchestration.
- A multicloud environment might exist on purpose (to better control sensitive data or as redundant storage space for improved disaster recovery) or by accident (usually the result of shadow IT). Either way, having multiple clouds is becoming more common across enterprises that seek to improve security and performance through an expanded portfolio of environments.

Which Cloud should be used?

Based on the Application

- Workloads with high volume or fluctuating demands might be better suited for a public cloud.
- Workloads with predictable use patterns might be better off in a private cloud.
- Hybrid clouds are the catch-all, because any workload can be hosted anywhere.

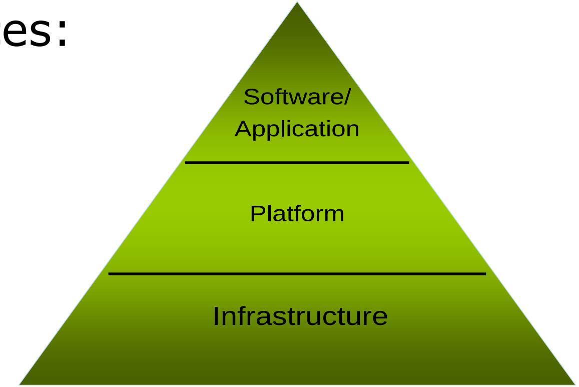
Cloud Safety

- Public clouds tend to have a wider variety of security threats due to multi-tenancy and numerous access points. Public clouds often split security responsibilities. For instance, infrastructural security can be the provider’s responsibility while workload security can be the tenant's responsibility.
- Private clouds are thought to be more secure because workloads usually run behind the user's firewall, but that all depends on how strong your own security is.
- Hybrid cloud security is made up of the best features of every environment, where users and admins can minimize data exposure by moving workloads and data across environments based on compliance, audit, policy, or security requirements.

Service Models

There are 3 main types of cloud computing services:

- Infrastructure-as-a-Service (IaaS),
- Platforms-as-a-Service (PaaS),
- Software-as-a-Service (SaaS).



Which cloud service is suitable for you?

- **IAAS-** If your business needs a virtual machine , opt for infrastructure as a service.
- **PAAS-** If your company requires a platform for building software products, pick platform as a service.
- **SAAS-** If your business doesn't want to maintain any IT equipment, then choose software as a service

IAAS

Infrastructure-as-a-Service (IaaS)

- IAAS is a cloud service that provides basic computing infrastructure
- Services are available on Pay-for-what-you-use model
- IAAS providers include Amazon Web Services, Microsoft Azure and Google compute Engine.
- **Users :** IT administrators

PRO's and CON's

- **Pros-**
- The cloud provides the infrastructure
- Enhanced Scalability- Dynamic workloads are supported
- IaaS is flexible
- **Cons-**
- Security issues
- Network and service
- **Ex. Companies** that use cloud computing- Amazon Web Services.
- **Users-**IaaS is mainly for Sys. Administrators

PAAS

Platform-as-a-Service (PaaS)

- PaaS provides cloud platforms and runtime environment for developing, testing and managing applications
- It allows software developers to display applications without requiring all the related infrastructure
- A service model that involves outsourcing the basic infrastructure and platform (Windows, Unix)
- PaaS facilitates deploying applications without the cost and complexity of buying and managing the underlying hardware and software where the applications are hosted.

- **The customer uses their own applications**

PRO’s and CON’s

- **Pros-**
- Cost effective rapid development
- Faster market for developers
- Easy deployment of Web Applications
- Private or public deployment is possible
- **Cons-**
- Developers are limited to the providers languages and tools
- Migration Issues- such as the risk vendor lock-in
- **Products and services** -AWS elastic beanstalk , heroku,windows Azure
- **Users-** software Developers

SAAS

Software-as-a-Service (SaaS)

- Also referred to as “software on demand,” this service model involves outsourcing the infrastructure, platform, and software/applications.

- Typically, these services are available to the customer for a fee, pay-as-you-go, or a no charge model.

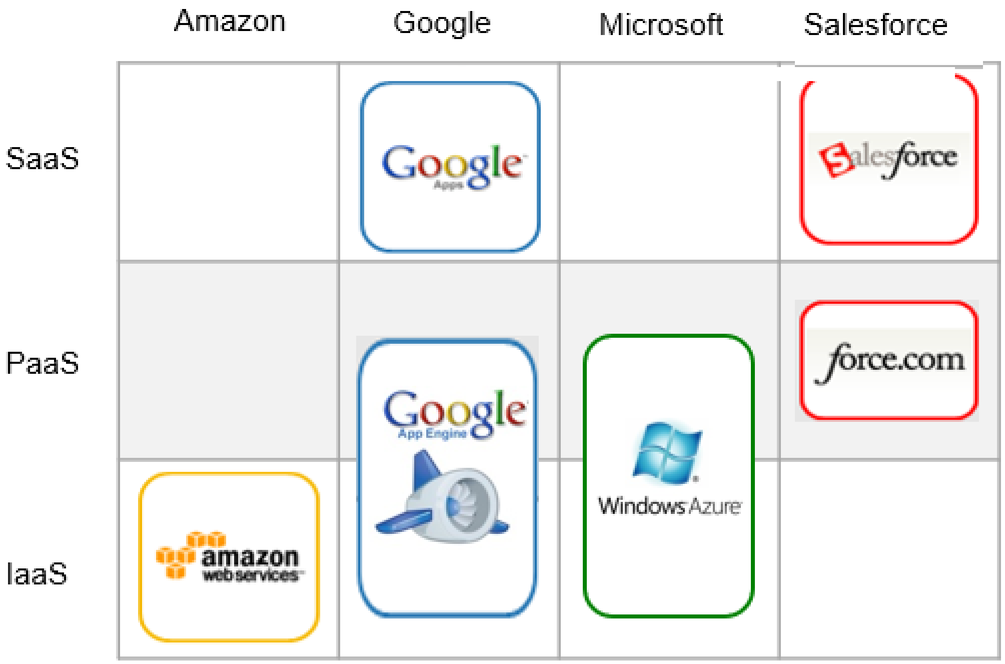
- The customer accesses the applications over the internet.

- All software and hardware are provided and managed by a vendor so you don’t have to maintain anything

Pros and Cons

- **Pros-**
- Universally accessible from any platform
- No need to commute, you can work from any place
- Excellent for collaborative working
- Vendor provides modest software tools
- Allows for Multi-Tenancy
- **Cons-**
- Portability and browser issues
- Internet performance may dictate overall performance
- Compliance restrictions
- **Users-** End customers
- Gmail, Microsoft Office 365

Service Delivery Model Examples



	Amazon	Google	Microsoft	Salesforce
SaaS		Google Apps		Salesforce
PaaS		Google App Engine	Windows Azure	force.com
IaaS	amazon web services			

Products and companies shown for illustrative purposes only and should not be construed as an endorsement