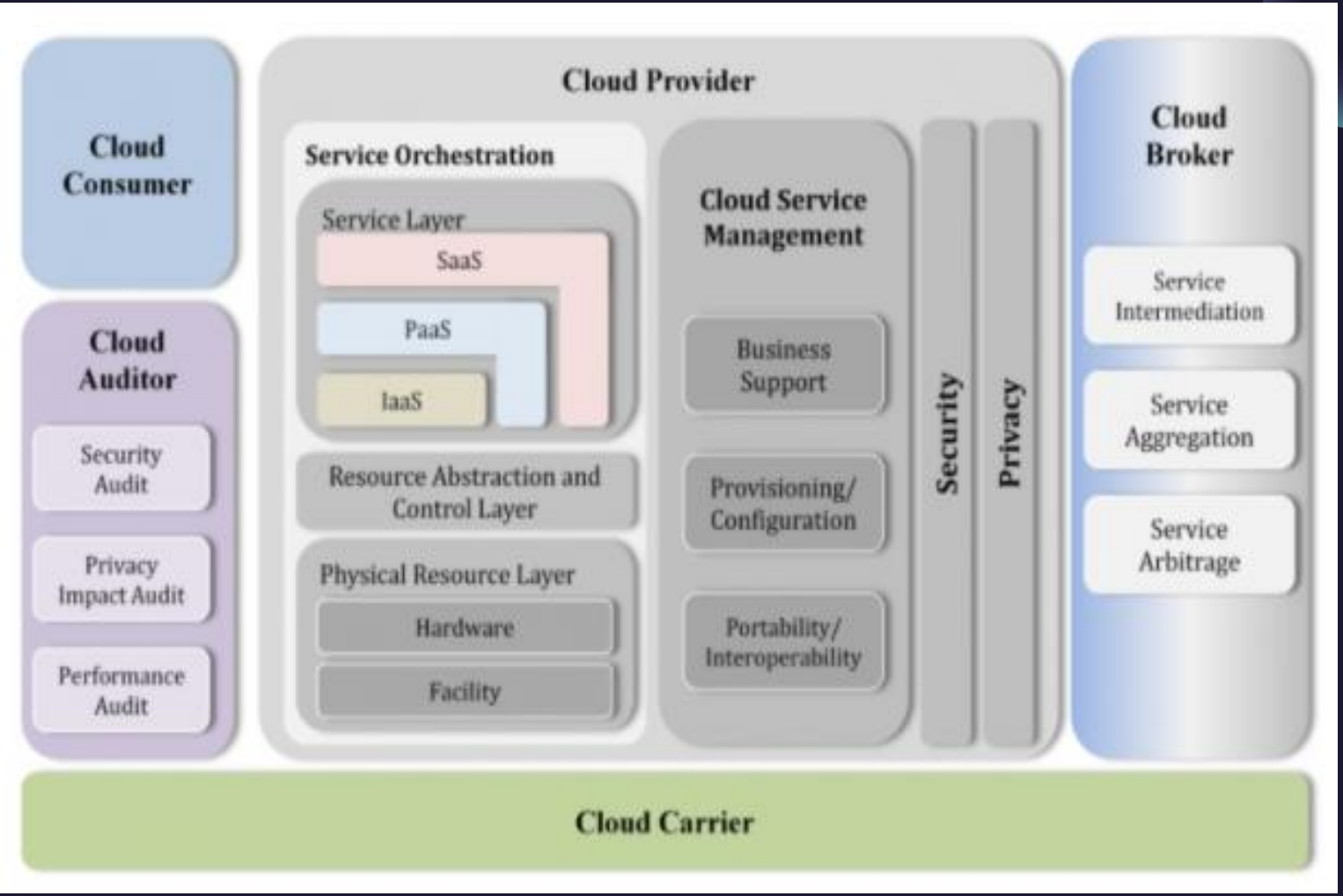
# UNIT II – CLOUD COMPUTING ARCHITECTURE




The Conceptual Reference Model

## CLOUD COMPUTING

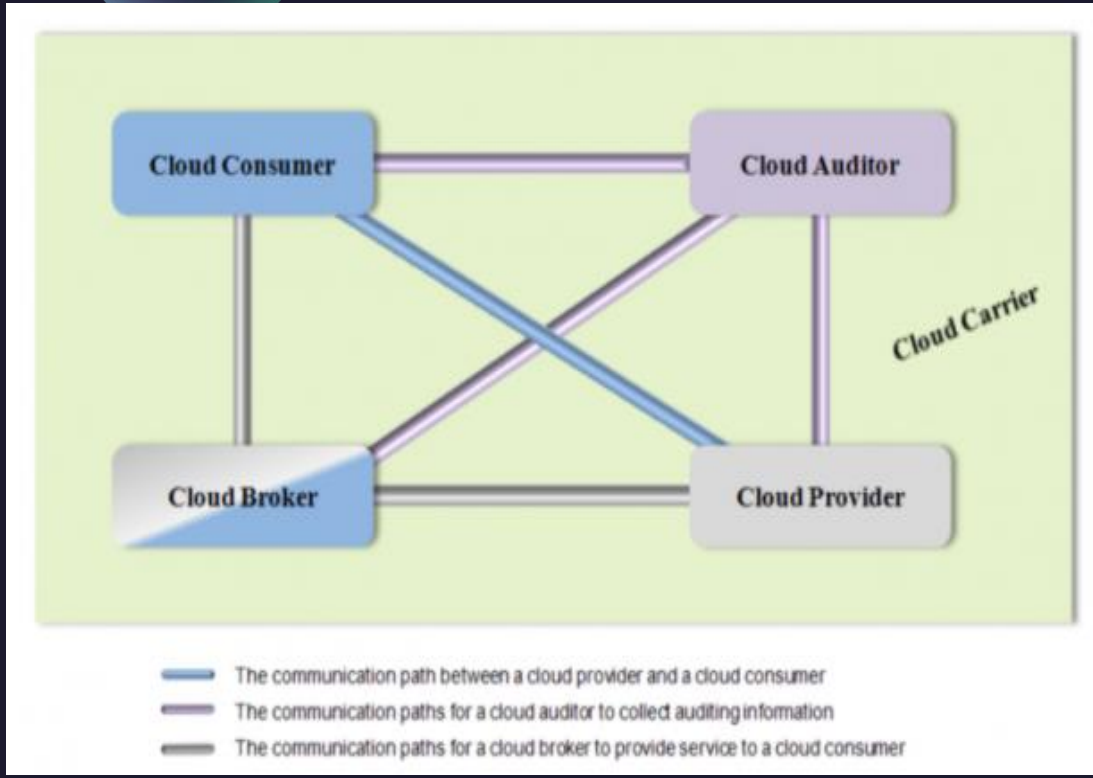
MR. VIJAY KOLTE

# UNIT II – CLOUD COMPUTING ARCHITECTURE

MSPM's Let us Rise Above The Rest DIEMS

**Actors in Cloud Computing**

| SNO | Actor | Definition |
|---|---|---|
| 1 | Cloud Consumer | A person or organization that maintains a business relationship with, and uses service from, Cloud Providers. |
| 2 | Cloud Provider | A person, organization, or entity responsible for making a service available to interested parties. |
| 3 | Cloud Auditor | A party that can conduct independent assessment of cloud services, information system operations, performance and security of the cloud implementation. |
| 4 | Cloud Broker | An entity that manages the use, performance and delivery of cloud services, and negotiates relationships between Cloud Providers and Cloud Consumers. |
| 5 | Cloud Carrier | An intermediary that provides connectivity and transport of cloud services from Cloud Providers to Cloud Consumers. |

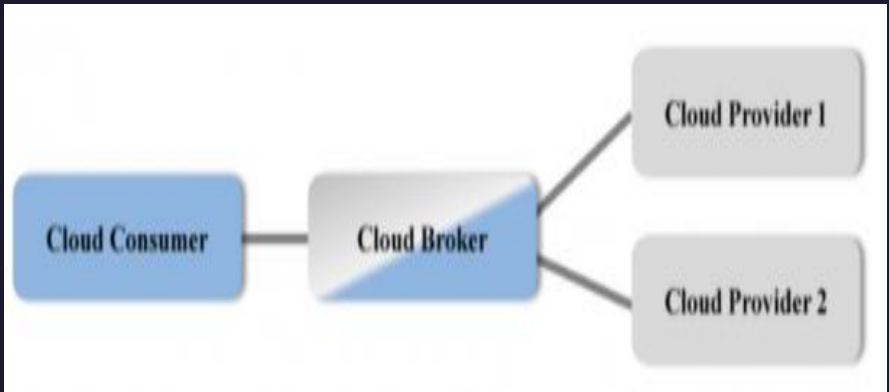



Interactions between the Actors in Cloud Computing

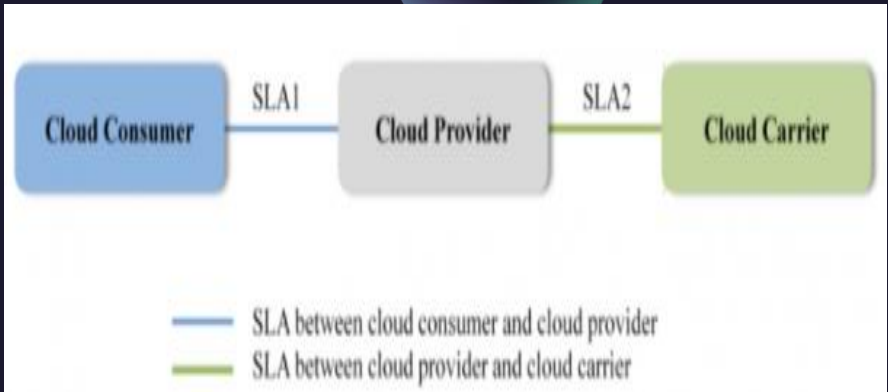
# UNIT II – CLOUD COMPUTING ARCHITECTURE



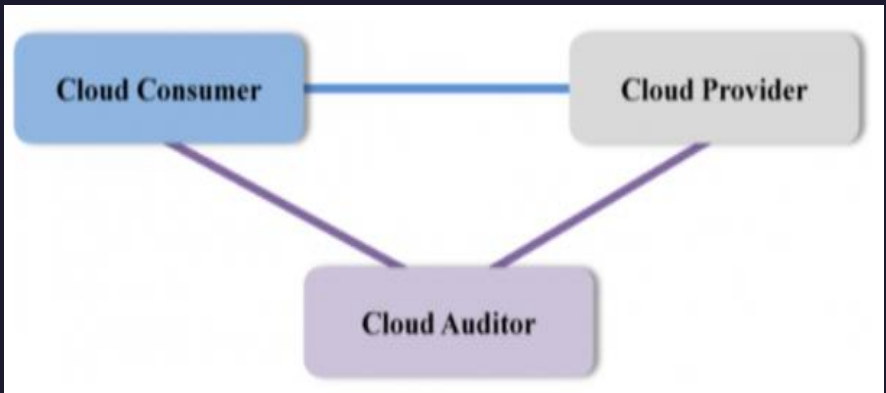
**Scenario 1** Usage Scenario for Cloud Brokers



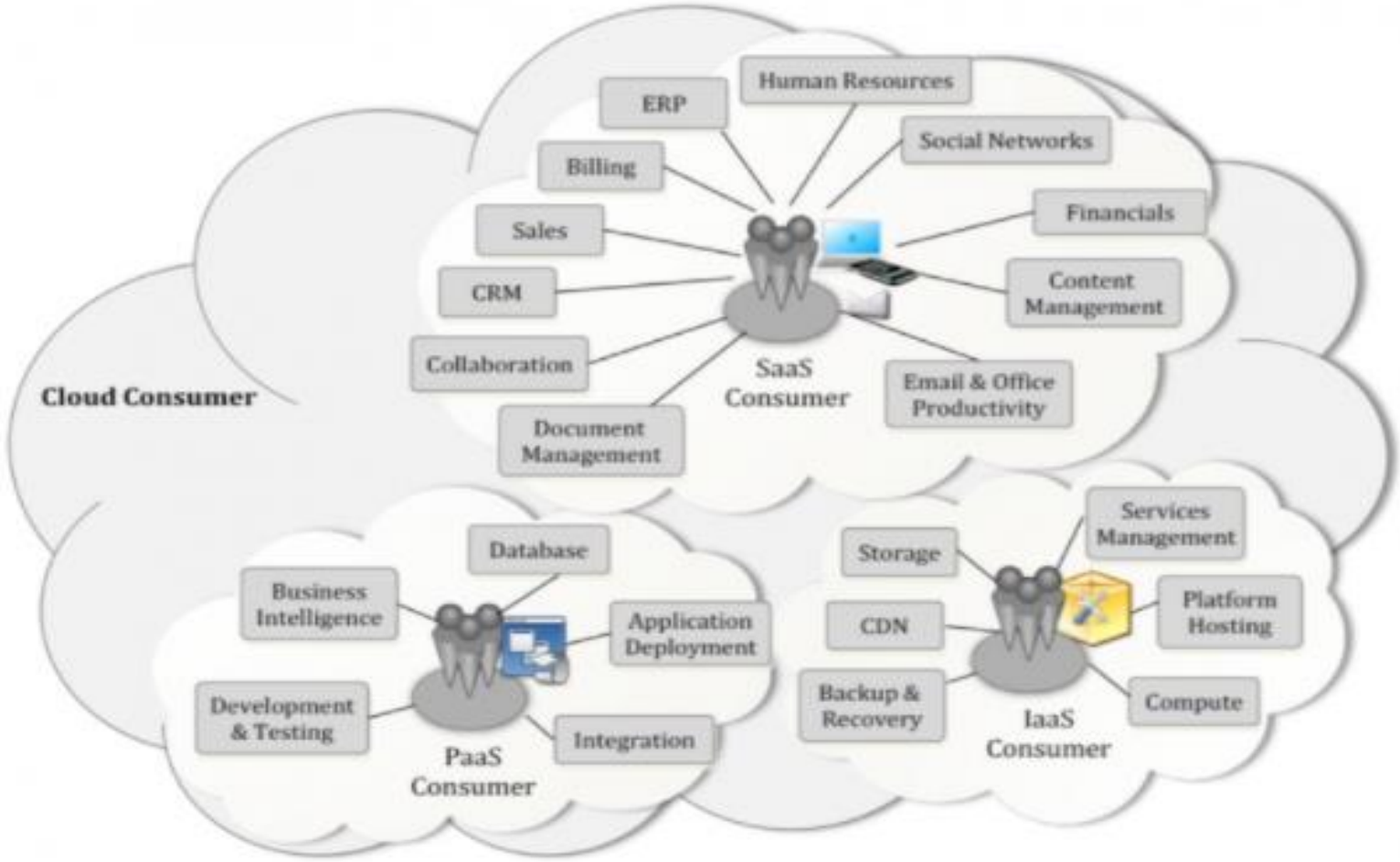

**Scenario 2** Usage Scenario for Cloud Carriers




**Scenario 3** Usage Scenario for Cloud Auditors

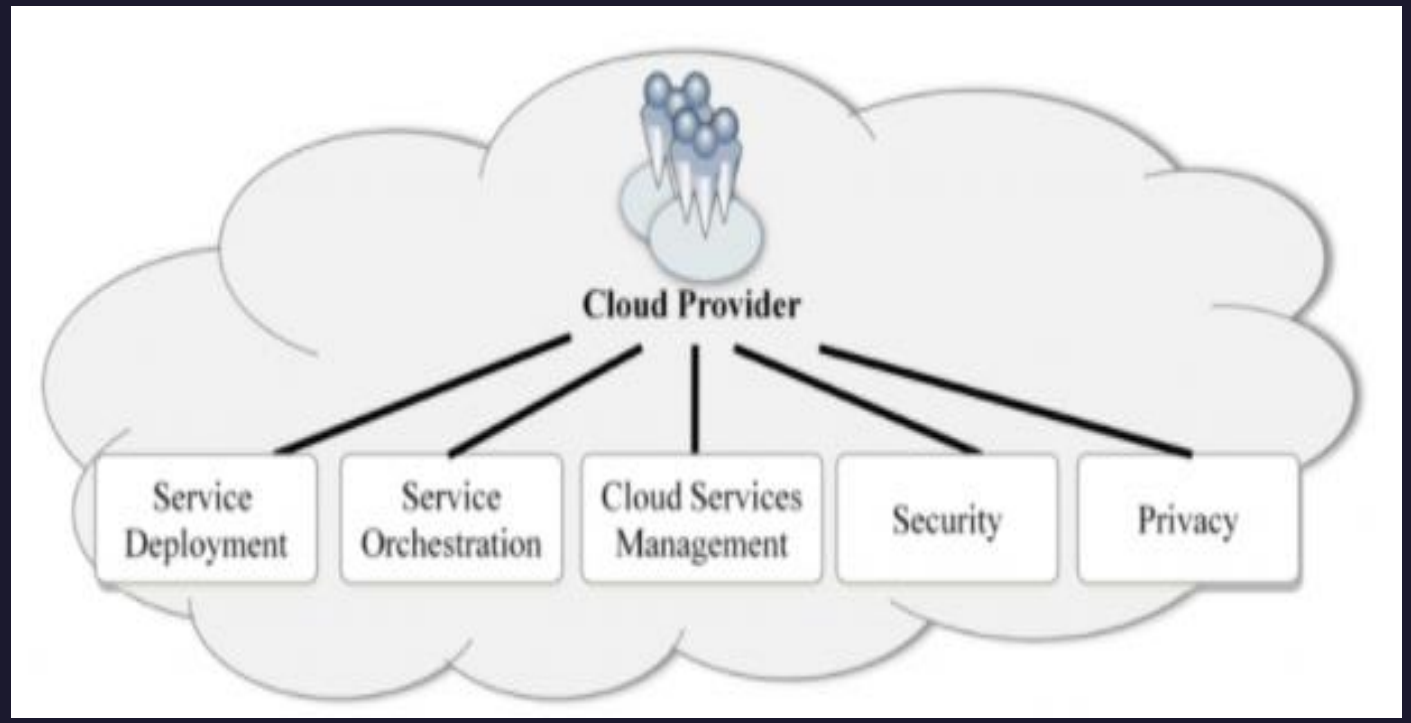


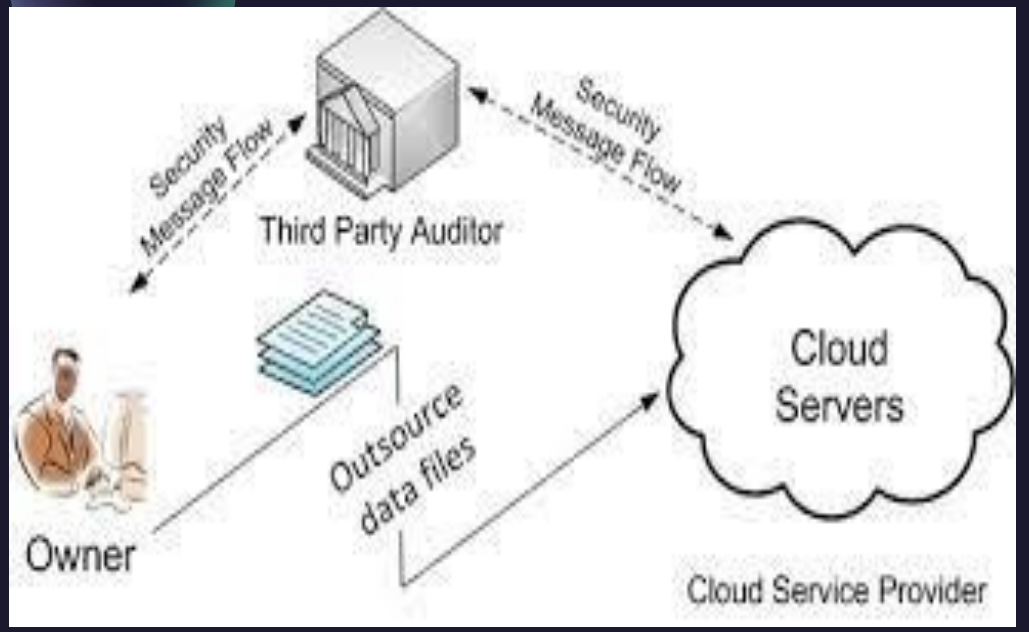
# UNIT II – CLOUD COMPUTING ARCHITECTURE




Cloud consumers

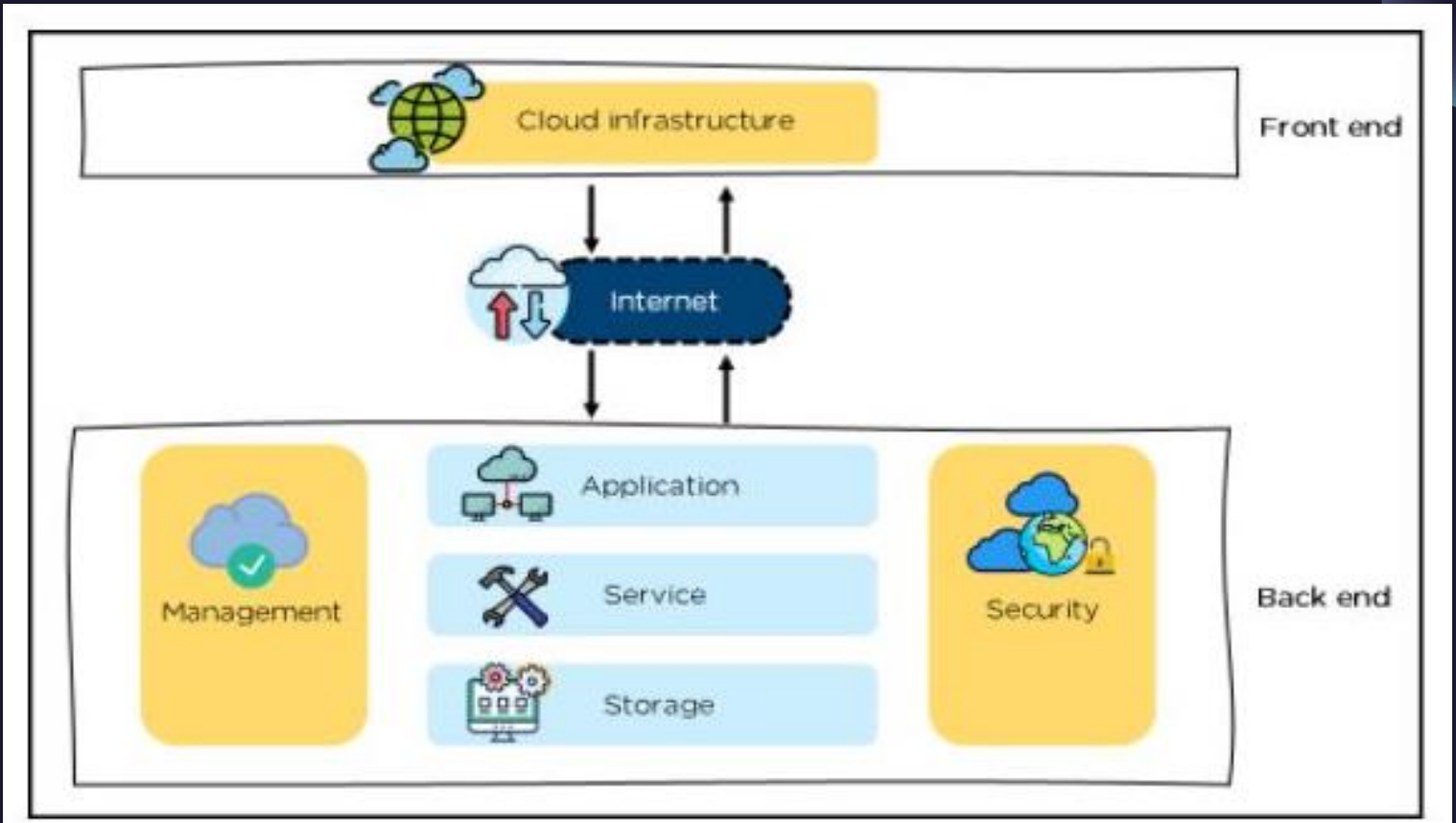
# UNIT II – CLOUD COMPUTING ARCHITECTURE



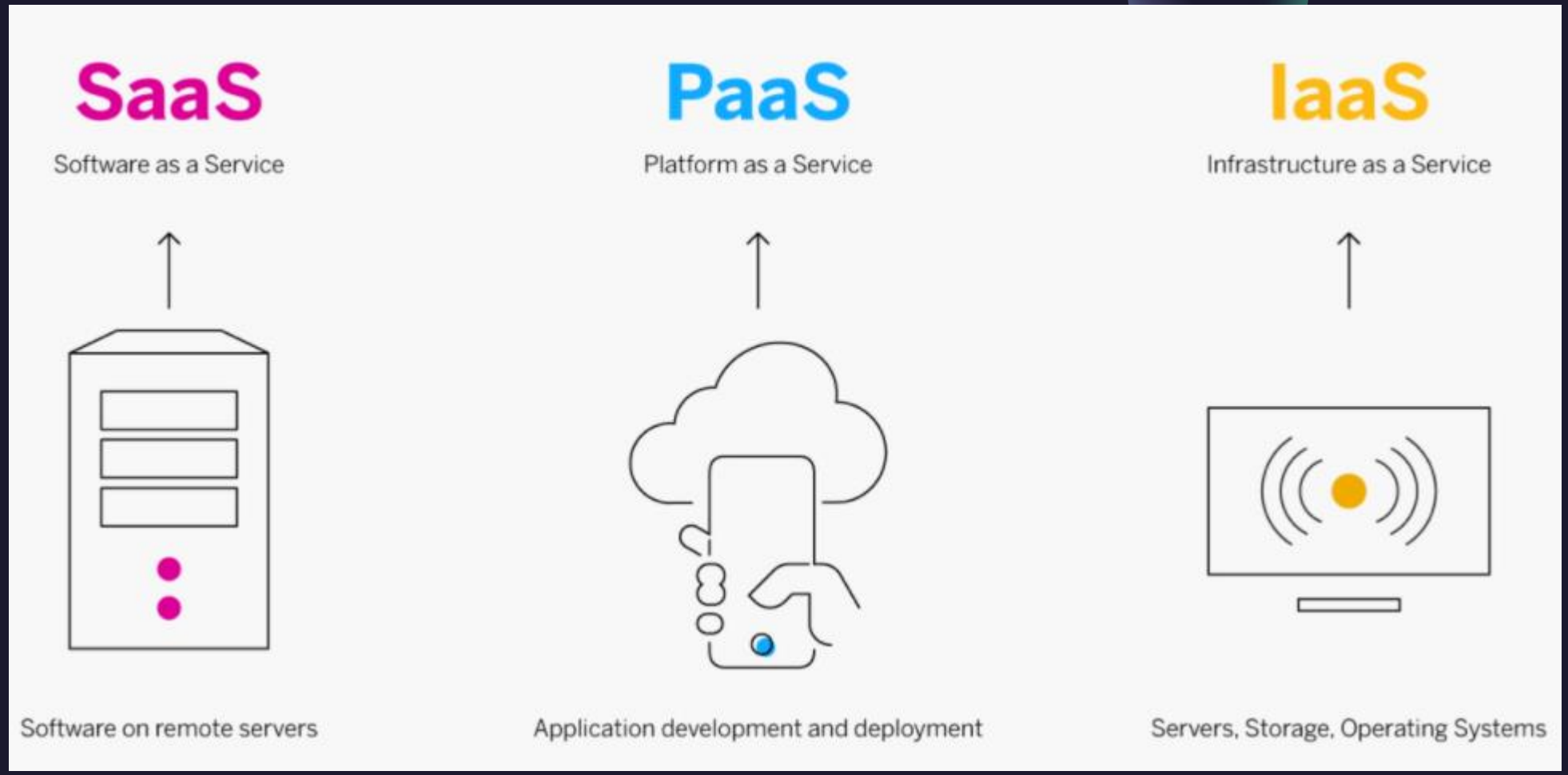

- Cloud Provider – Major Activities

# UNIT II – CLOUD COMPUTING ARCHITECTURE

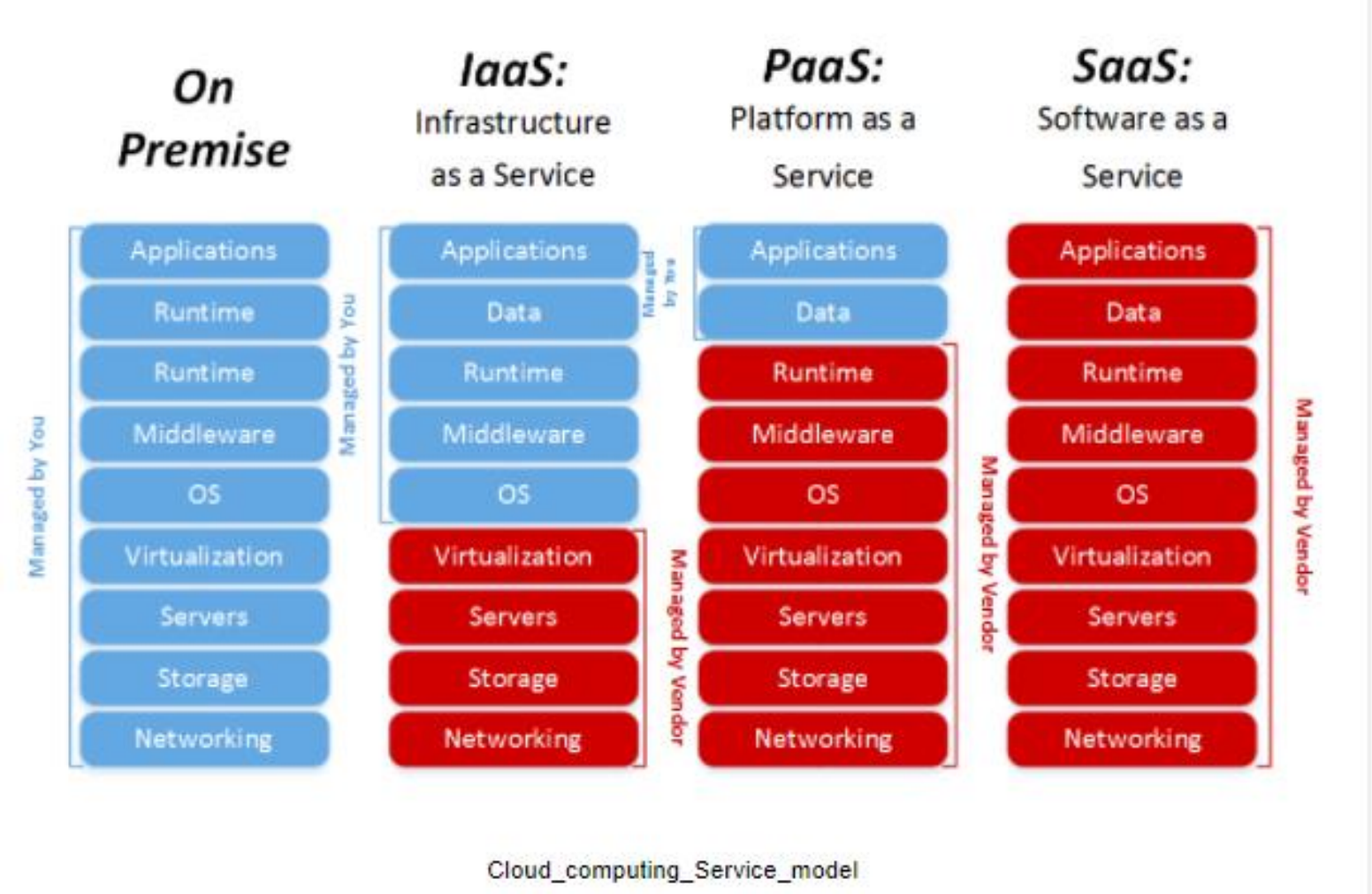



Cloud Computing Architecture

# UNIT II – CLOUD COMPUTING ARCHITECTURE

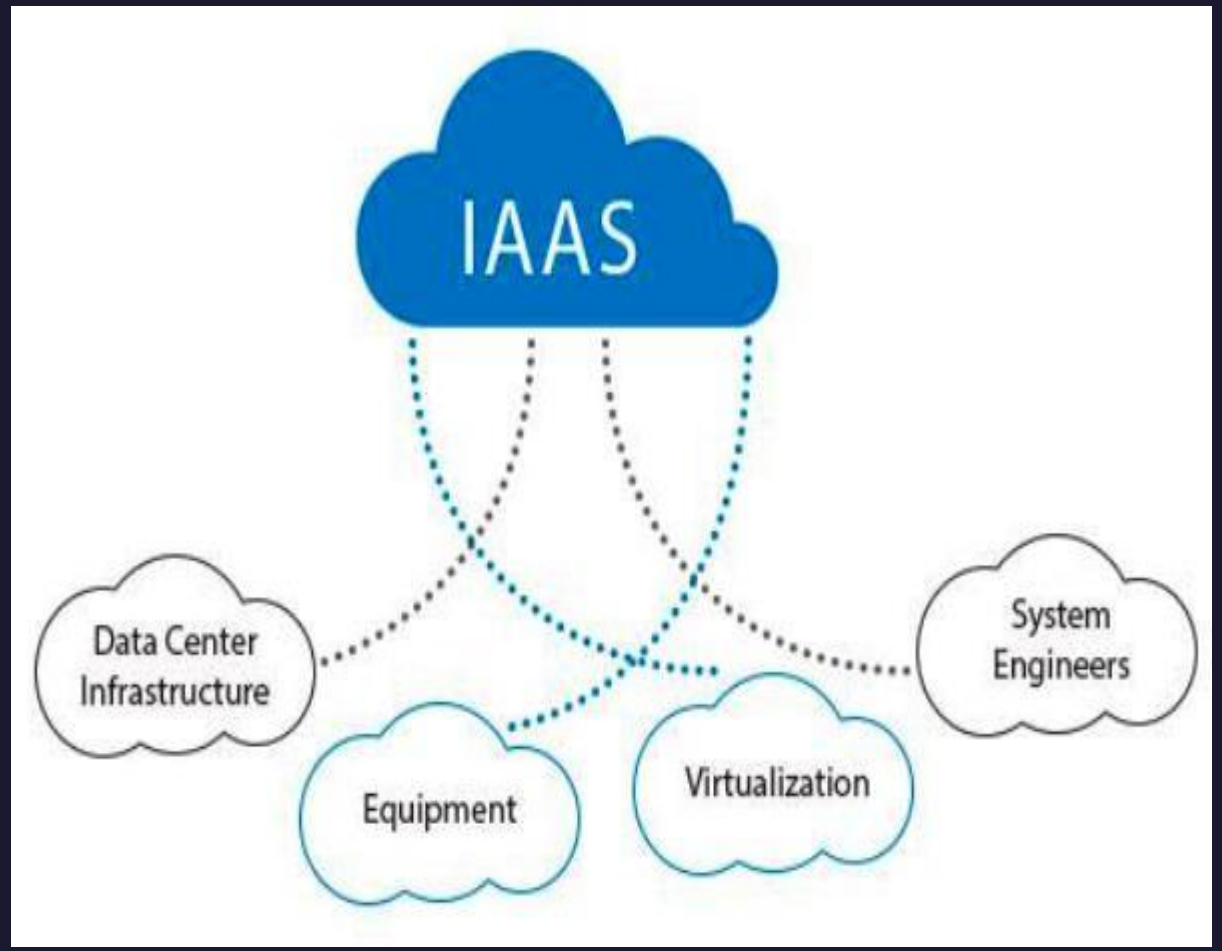


# UNIT II – CLOUD COMPUTING ARCHITECTURE




Cloud_computing_Service_model

# UNIT II – CLOUD COMPUTING ARCHITECTURE



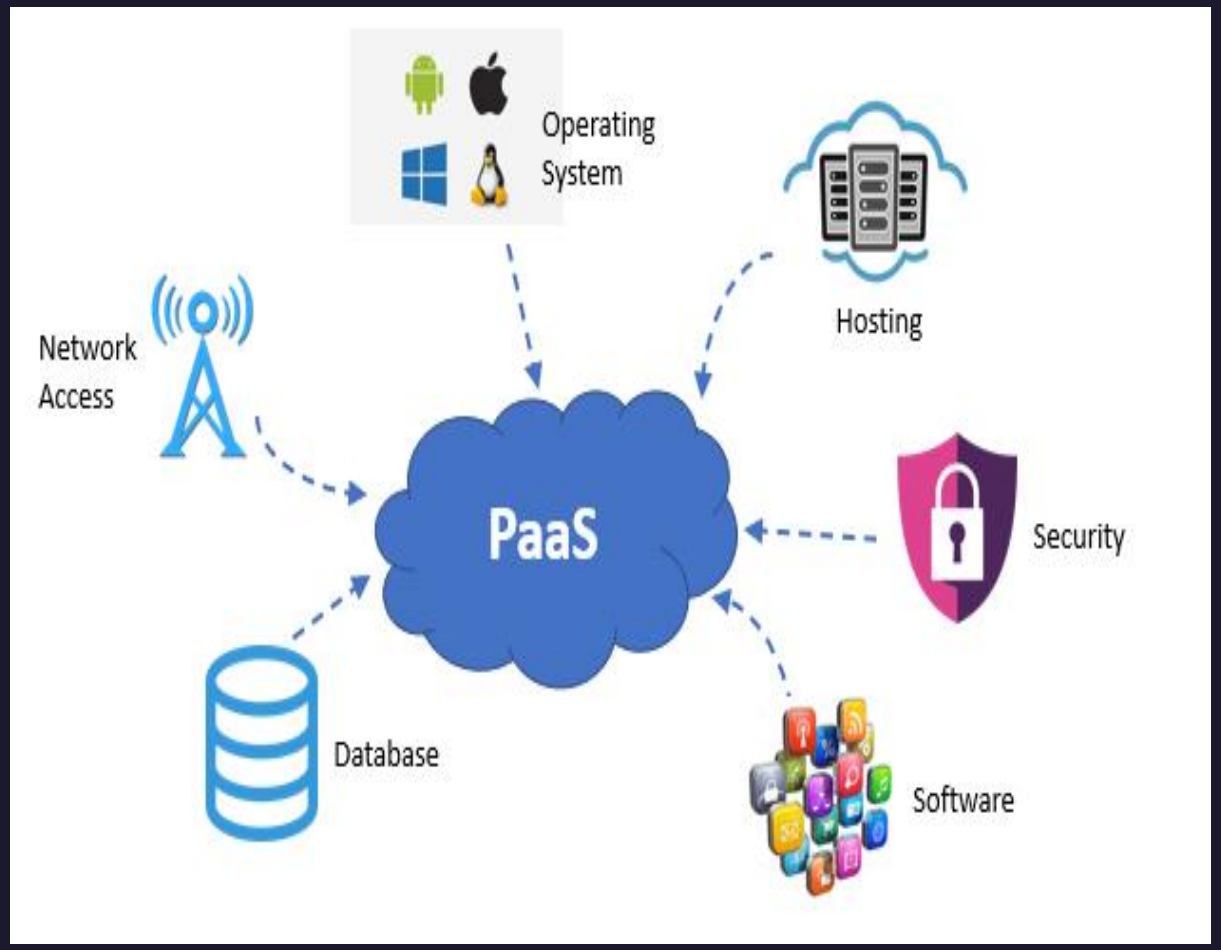

Below are some important features of IaaS:

- Dynamically Scalable
- Rented / licensed / pay as you go
- Several Levels of Services
- 100% Resource Availability
- GUI or CLI based easy access

Ex – Vultr, Kamatera, AWS, GCP

| IAAS PROS | IAAS CONS |
|---|---|
| Lower infrastructure costs | Legal limitations |
| Secure physical infrastructure | Potential security flaws |
| On-demand scalability | Doesn't work without an internet connection |

# UNIT II – CLOUD COMPUTING ARCHITECTURE

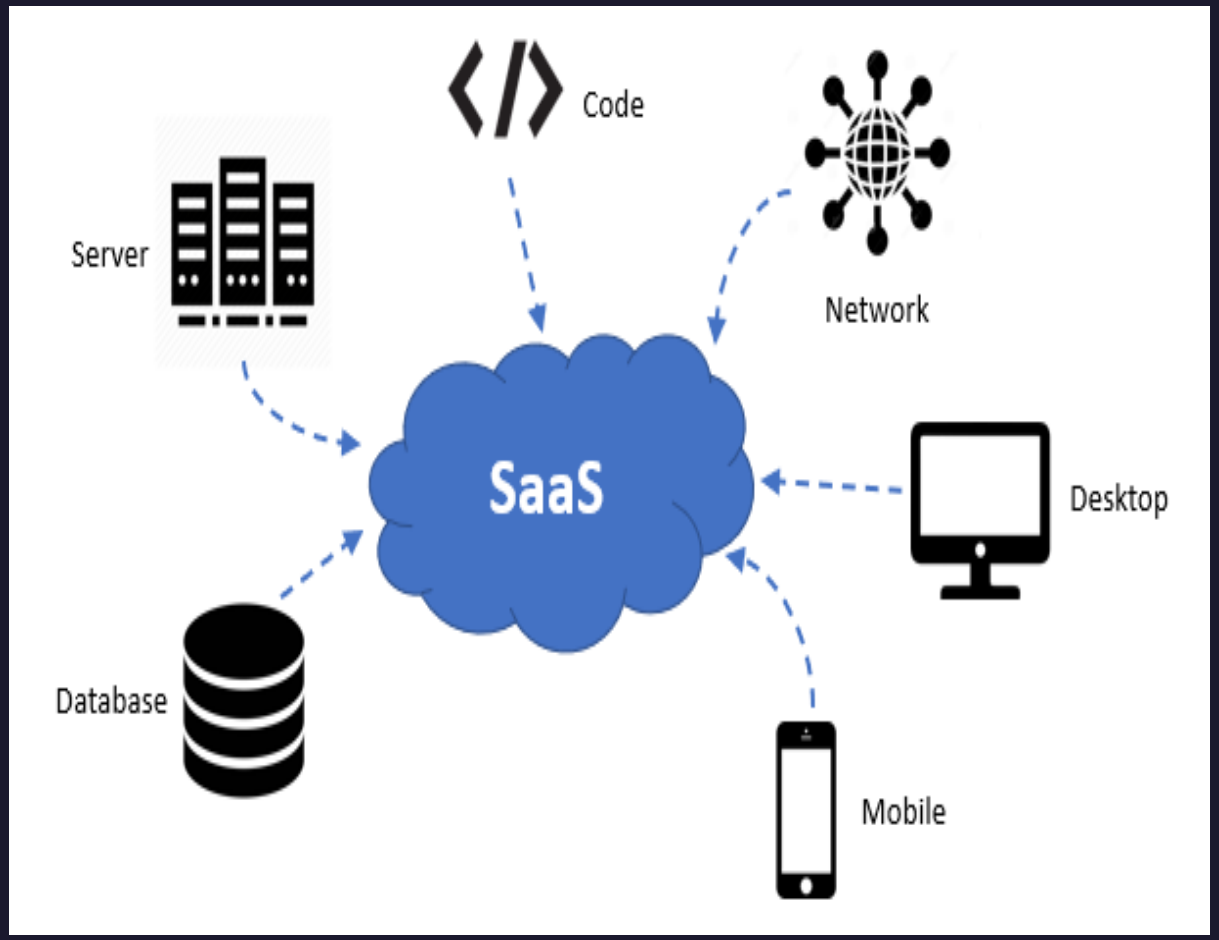



Some of the benefits of using PaaS are the following.

- Faster development and delivery
- Create/Deploy applications on the fly
- Easily Upgradable
- Provides backup, recovery and data security
- Easily accessible from multiple locations (by multiple teams)

Ex – App Engine from Google Cloud.

# UNIT II – CLOUD COMPUTING ARCHITECTURE




Some benefits:

- On-demand service
- Independent platform
- No need to install anything
- Resource managed by the Vendor
- Available 24×7

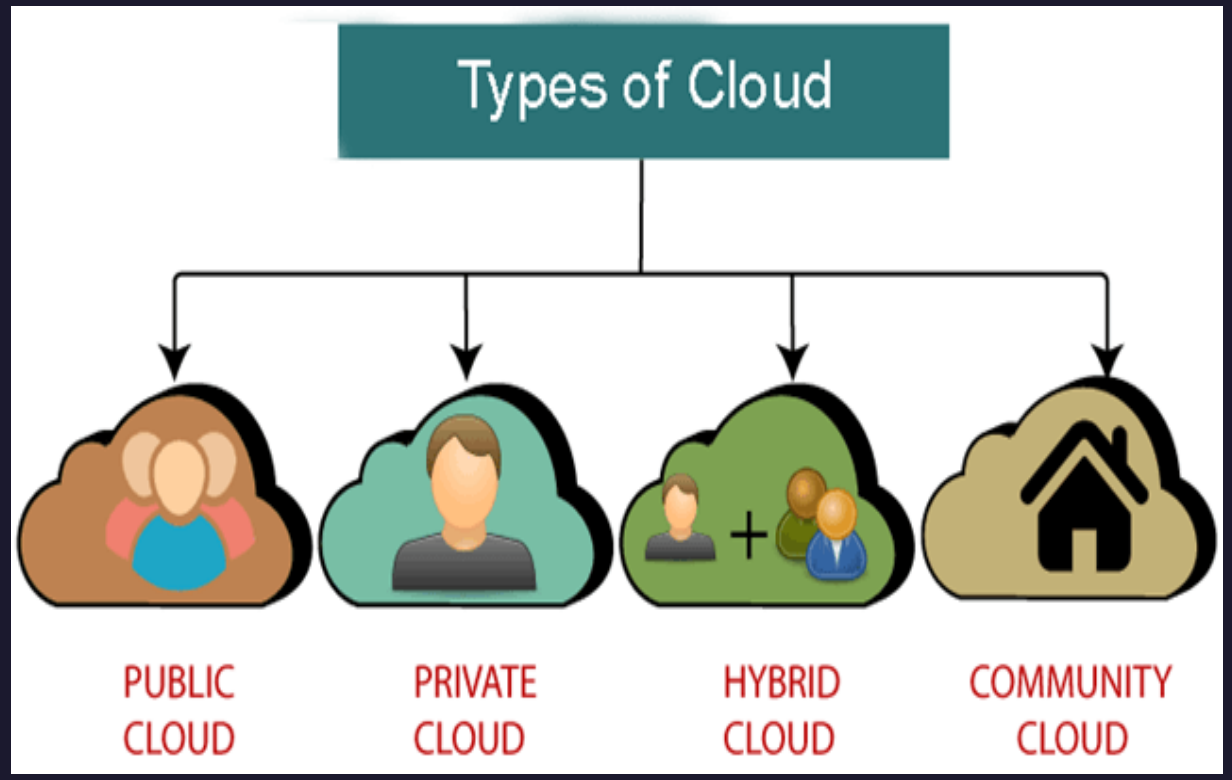
Ex – Freshdesk as a helpdesk and self-service solution.

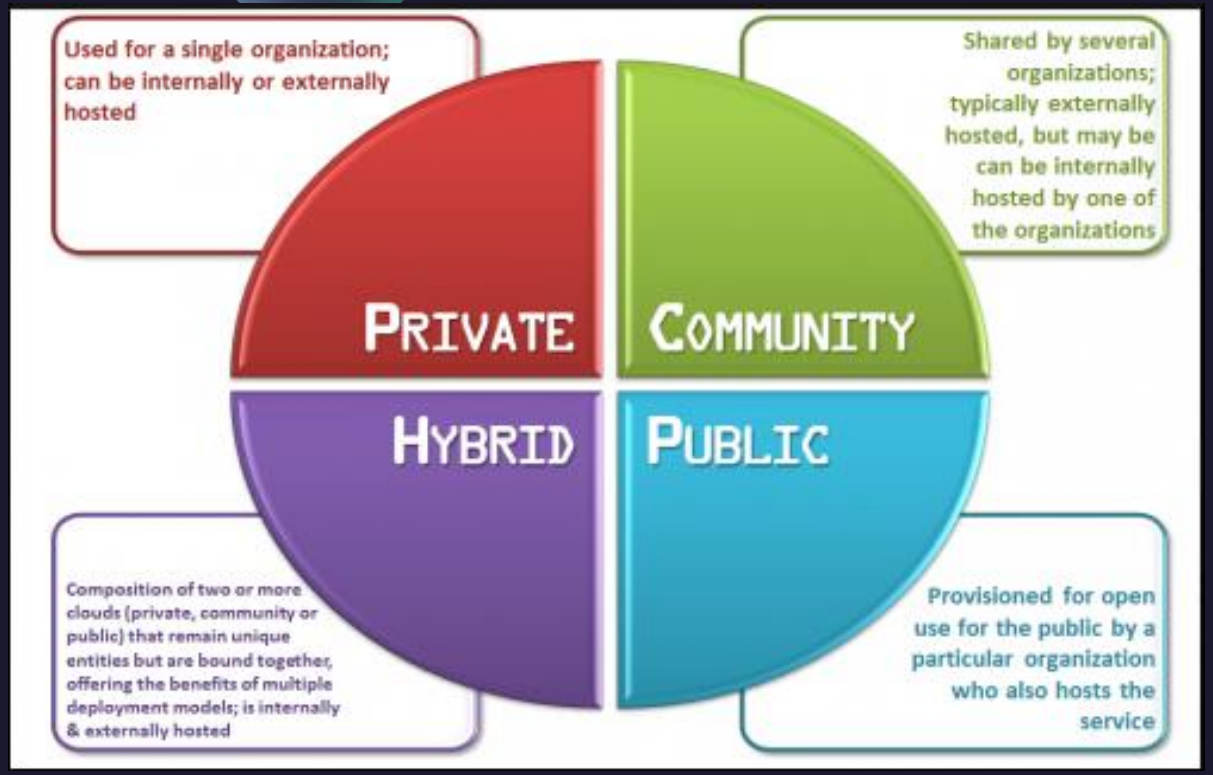
# UNIT II – CLOUD COMPUTING ARCHITECTURE



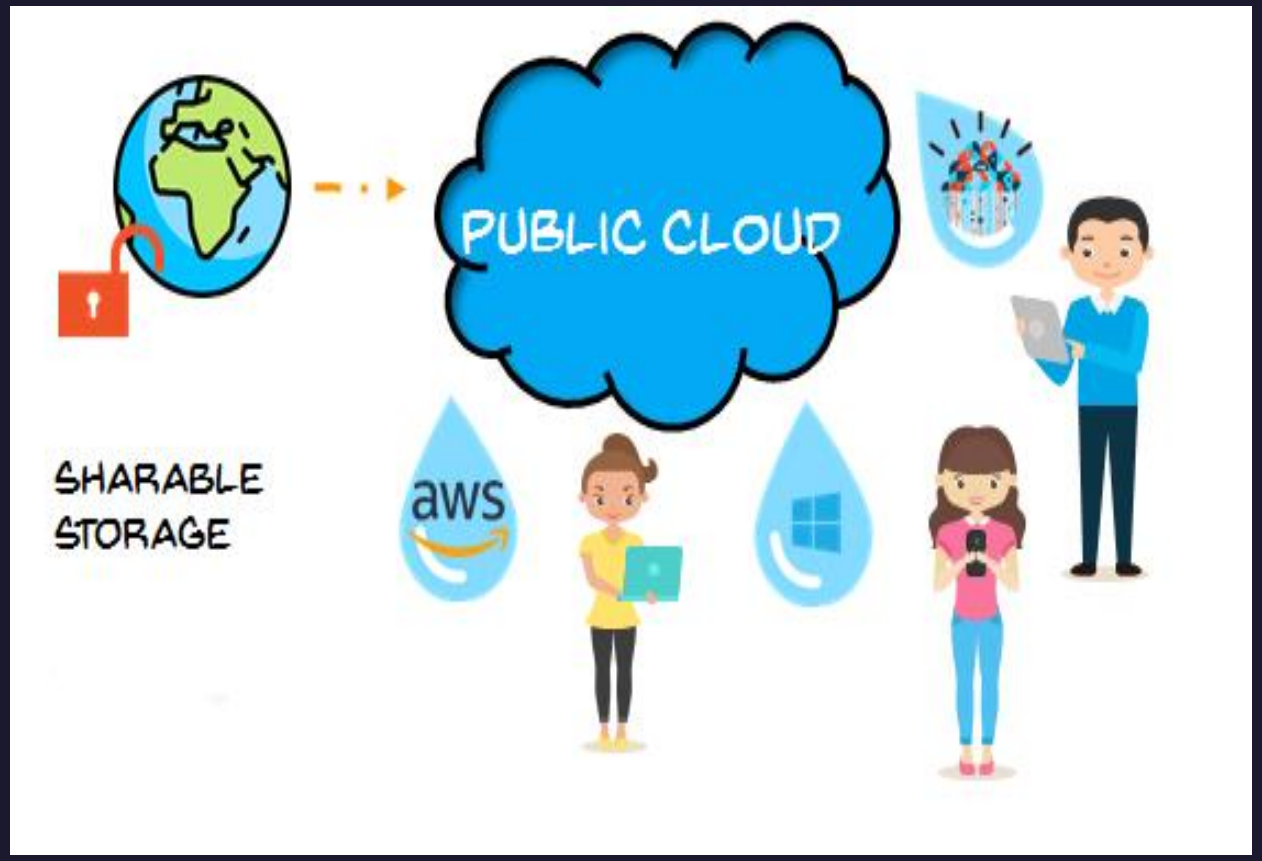
| | SaaS | PaaS | IaaS |
|---|---|---|---|
| Who Uses It | Business users | Developers | System admins |
| What You Get | Software applications | Development platform | Computing resources |
| Purpose | To complete business tasks | To build and deploy applications | To access storage, networking, servers, and other infrastructure online |
| Provider Controls | Apps, data, runtime, middleware, O/S, virtualization, servers, storage, networking | Runtime, middleware, O/S, virtualization, servers, storage, networking | Virtualization, servers, storage, networking |
| Customer Controls | N/A – everything is managed by the provider | Apps, data | Apps, data, runtime, middleware, O/S |

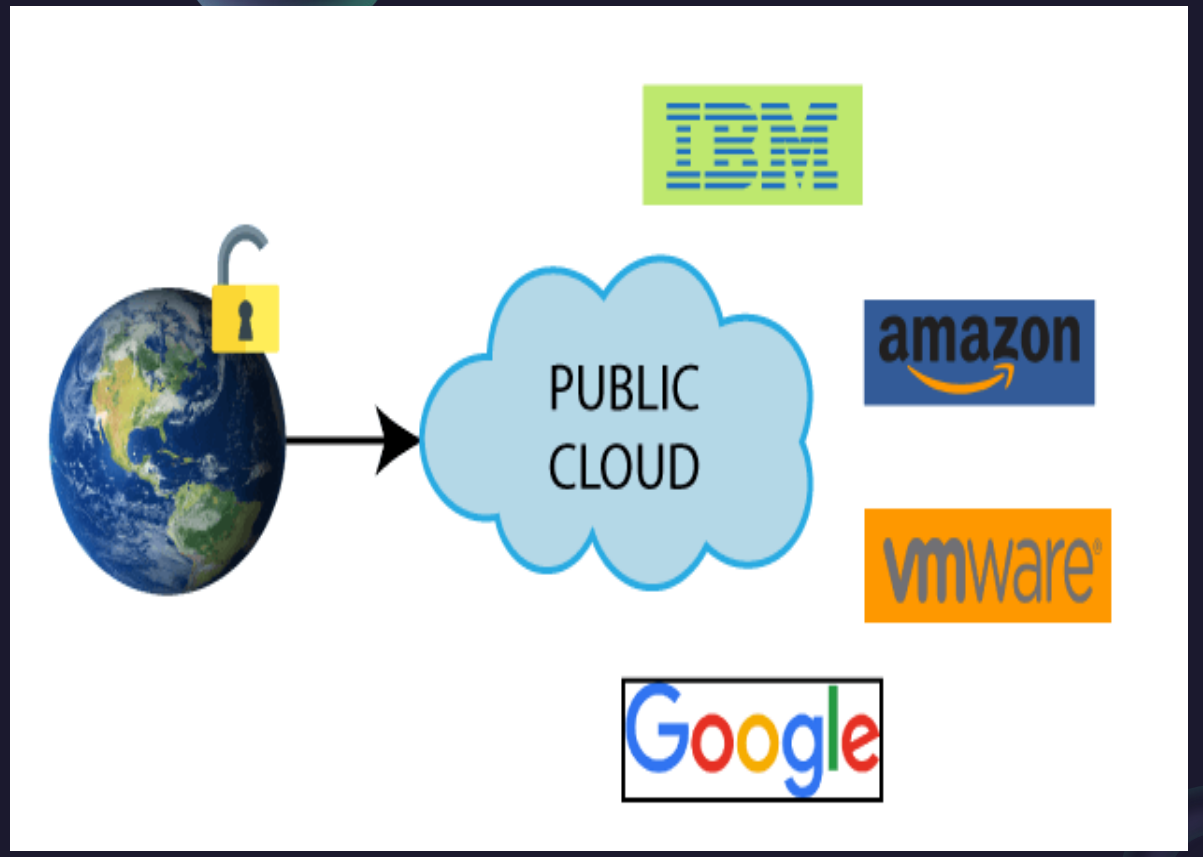
# UNIT II – CLOUD COMPUTING ARCHITECTURE



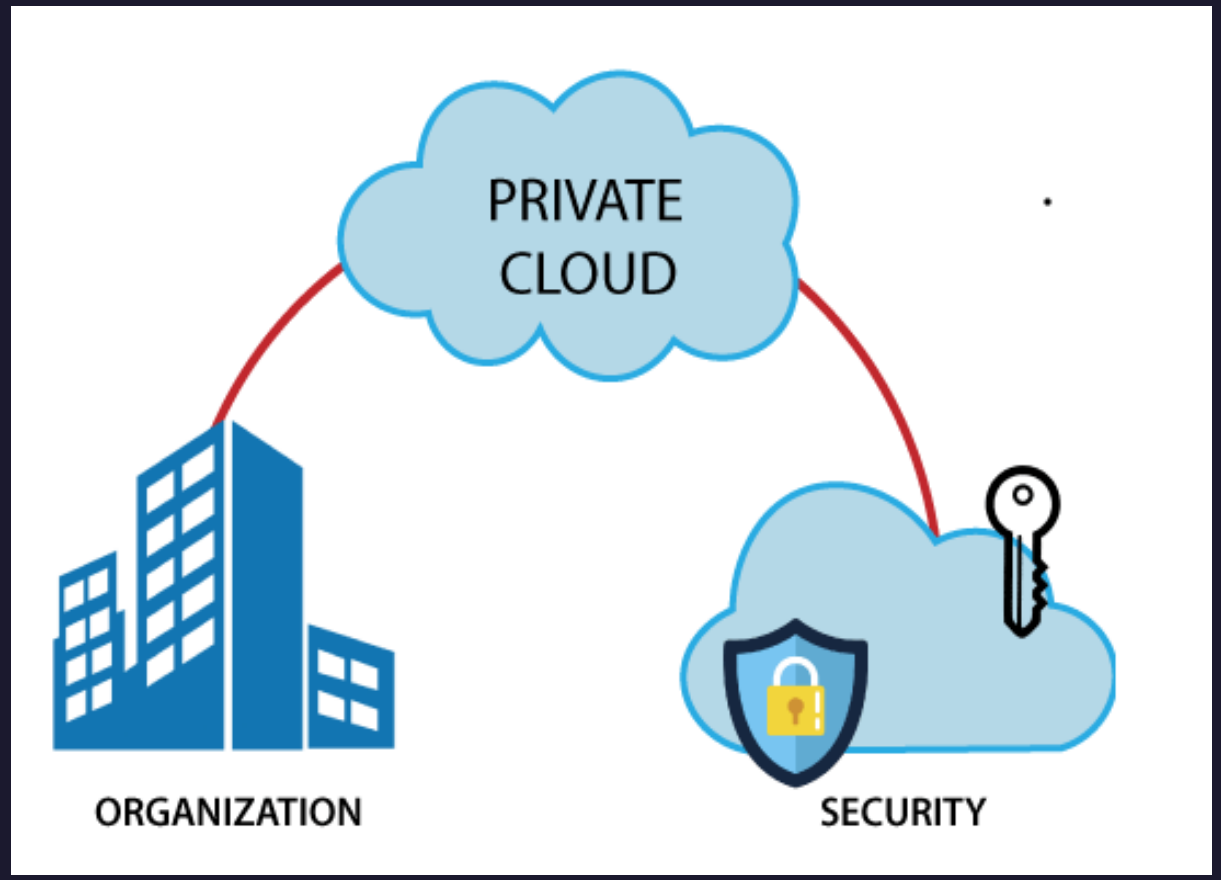



# UNIT II – CLOUD COMPUTING ARCHITECTURE



# UNIT II – CLOUD COMPUTING ARCHITECTURE



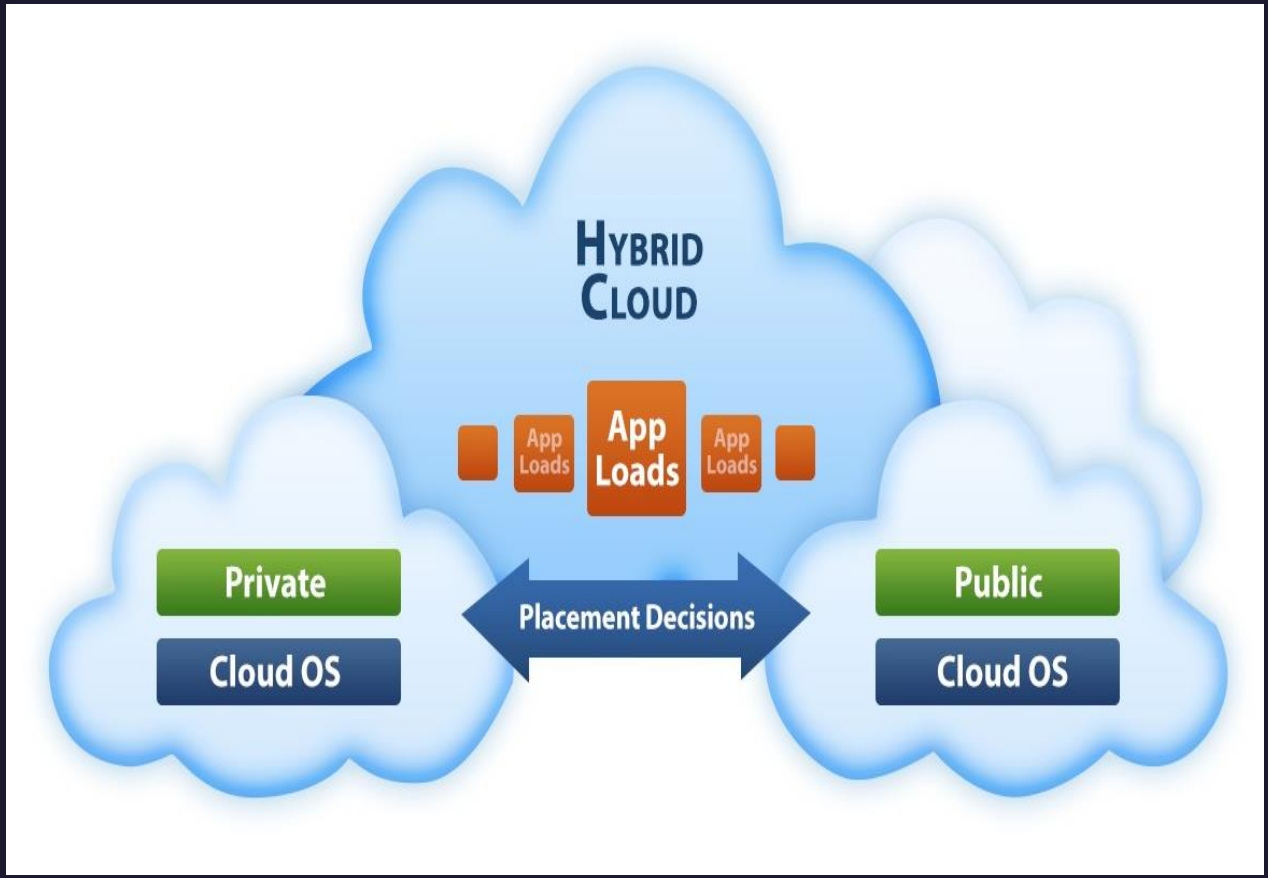

**Public Cloud**

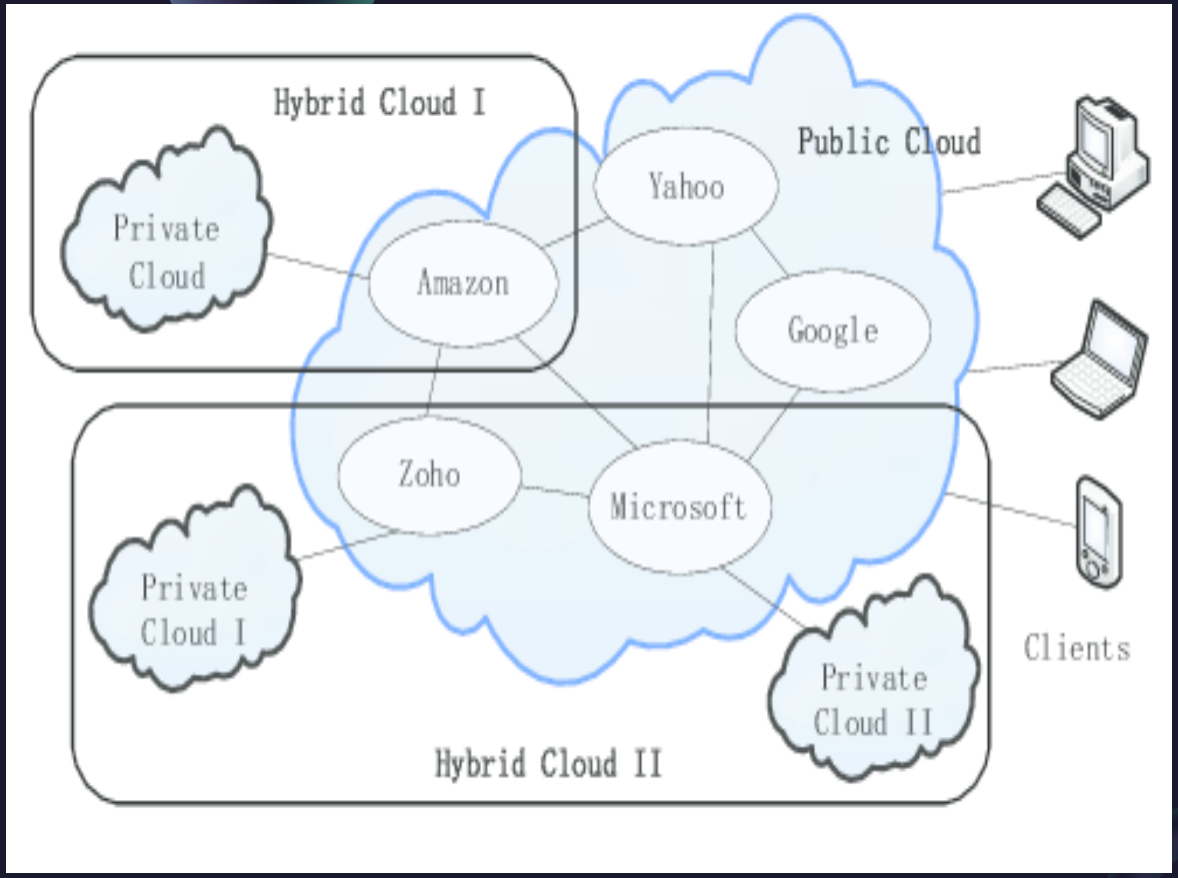
- Multiple Clients
- Hosted at Providers Location
- Shared Infrastructure
- Access over Internet
- Low-cost

**Private Cloud**

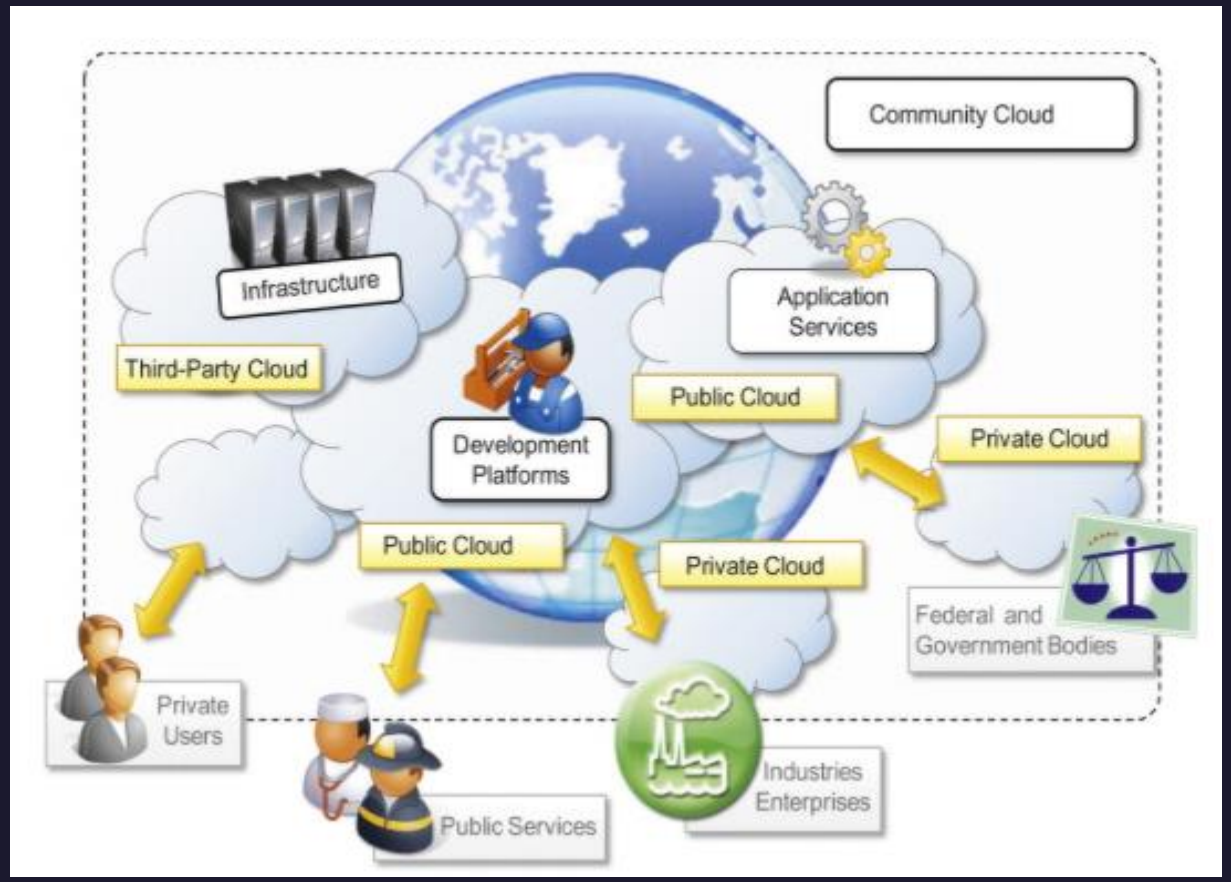
- Single Client
- Hosted at Providers / Orgs Location
- Access over Internet / Private Network
- High-security

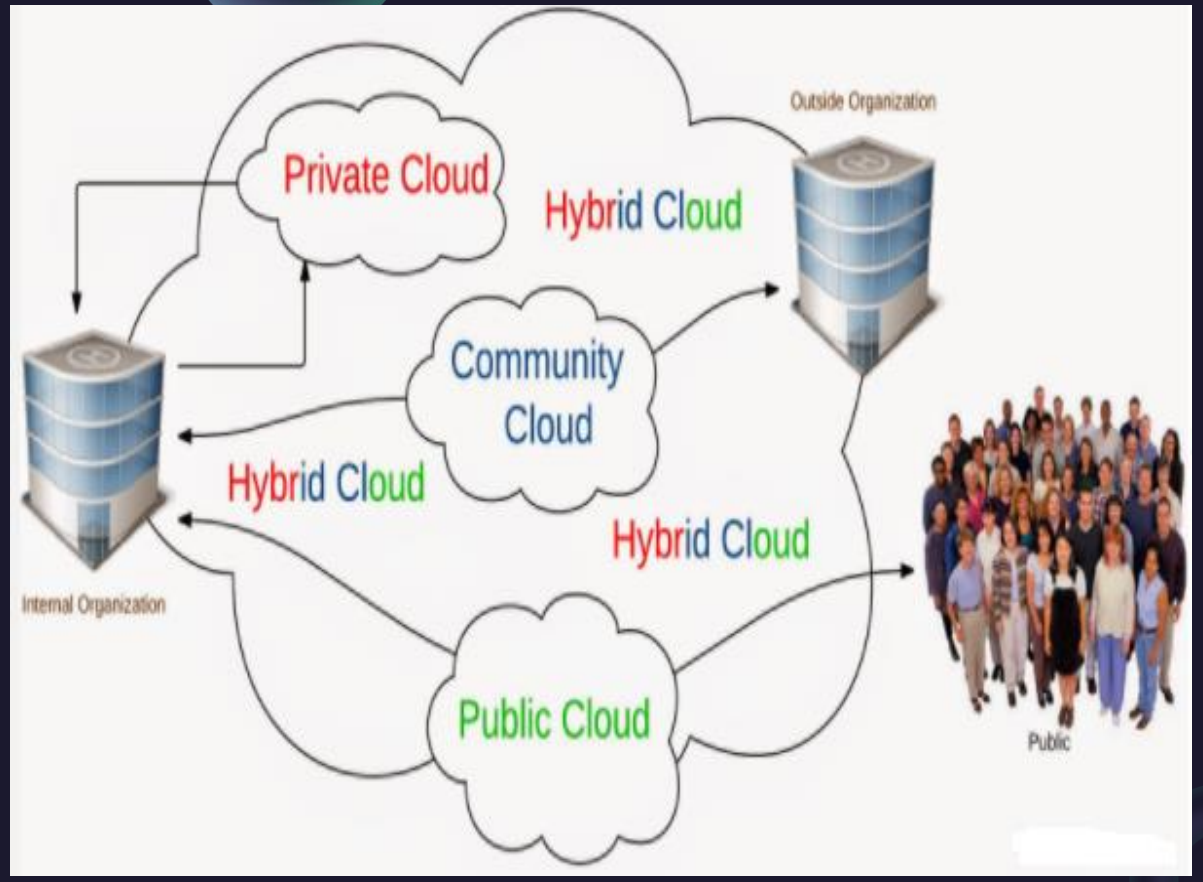
# UNIT II – CLOUD COMPUTING ARCHITECTURE



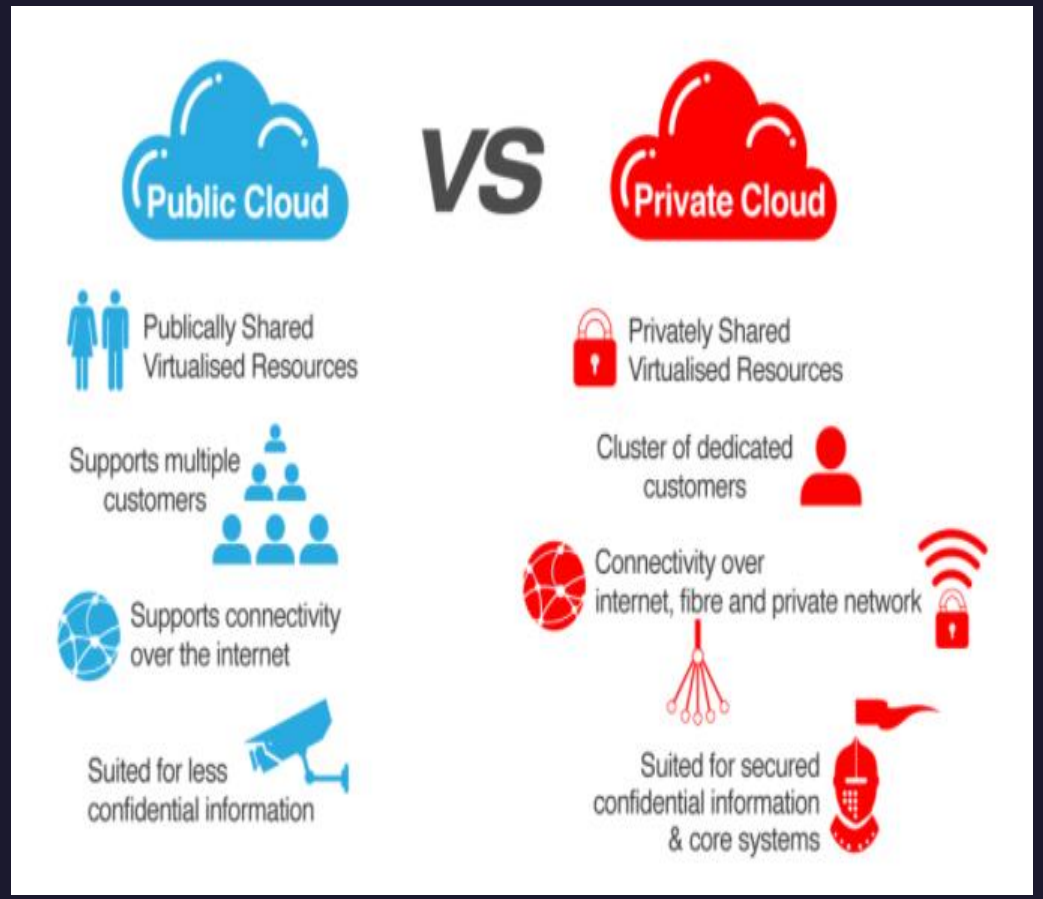



# UNIT II – CLOUD COMPUTING ARCHITECTURE



# UNIT II – CLOUD COMPUTING ARCHITECTURE




| Parameters\Type | Public Cloud | Private Cloud | Hybrid Cloud | Community Cloud |
|---|---|---|---|---|
| Description | In public cloud, services are available for public users. | Private cloud is build up with existing private infrastructure. This type of cloud has some authentic users who can dynamically provision the resources. | Hybrid cloud is a heterogeneous distributed system, resulting from a private cloud, which incorporates different types of services and resources from public clouds. | Different types of cloud are integrated together to meet a common or particular need for some organizations. |
| Scalability | Very High | Limited | Very High | Limited |
| Reliability | Moderate | Very High | Medium to High | Very High |
| Security | Totally Depends on service provider | High class security | Secure | Secure |
| Performance | Low to medium | Good | Good | Very Good |
| Cost | Cheaper | High Cost | Costly | Costly |
| Examples | Amazon EC2, Google AppEngine | VMWare, Microsoft, KVM, Xen | IBM, HP, VMWare vCloud, Eucalyptus | SolaS Community Cloud, VMWare |

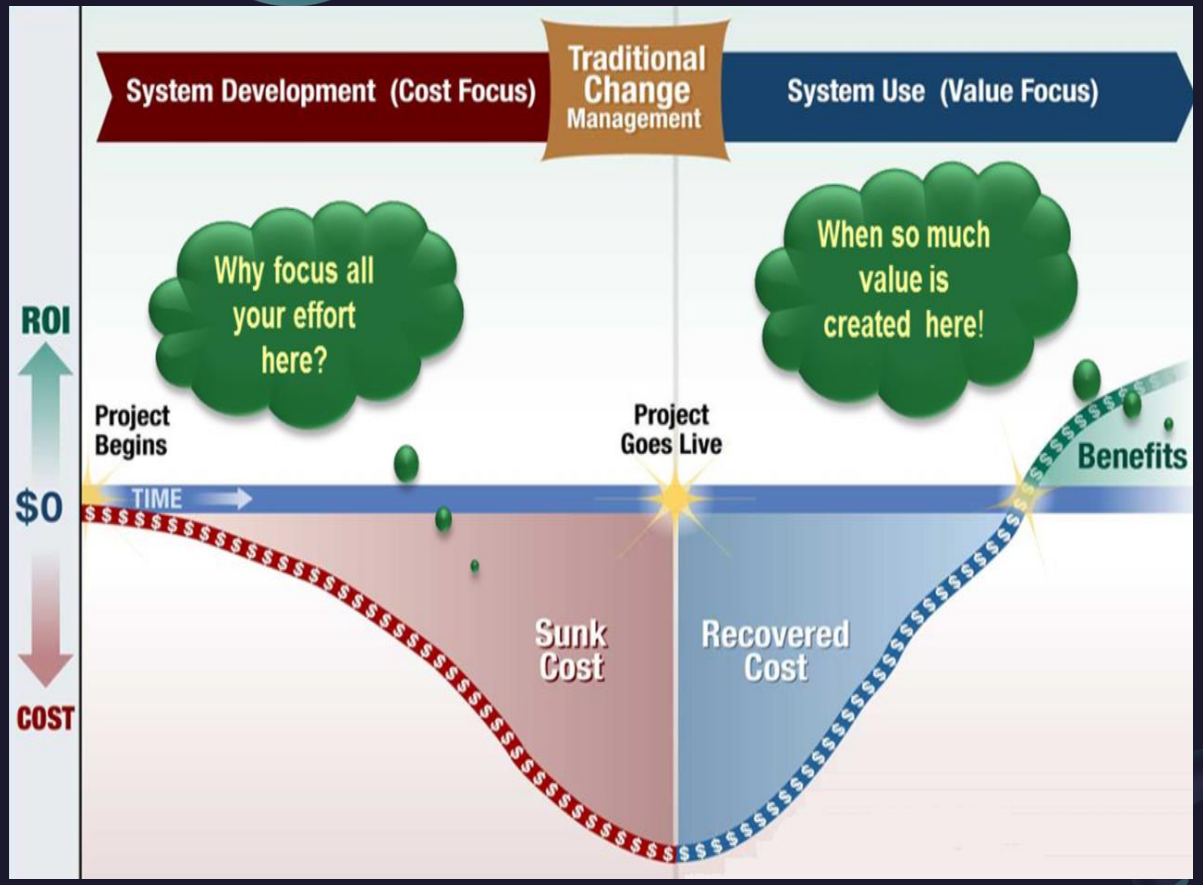
# UNIT II – CLOUD COMPUTING ARCHITECTURE

MSPM's Let us Rise Above The Rest DIEMS

## Economics of Cloud

Cloud economics is the study of cloud computing's costs and benefits and the economic principles that underpin them.

As a Business Owner need to calculate ROI of Business




## How to calculate the cost of moving to the cloud?

1. **Total cost of ownership**
2. **Cost of your current data center**
3. **Cost of estimated cloud infrastructure**
4. **Cost of cloud migration execution**

# UNIT II – CLOUD COMPUTING ARCHITECTURE



With SaaS tools for HCM you will reduce your Total Cost of Ownership (TCO) because:

- You won't need in-house infrastructure anymore
- Implementation is rather easy and faster than ERP systems.
- You can use business processes and form templates
- Tool upgrades are transparent: all clients will access to newest versions when made available by the provider.

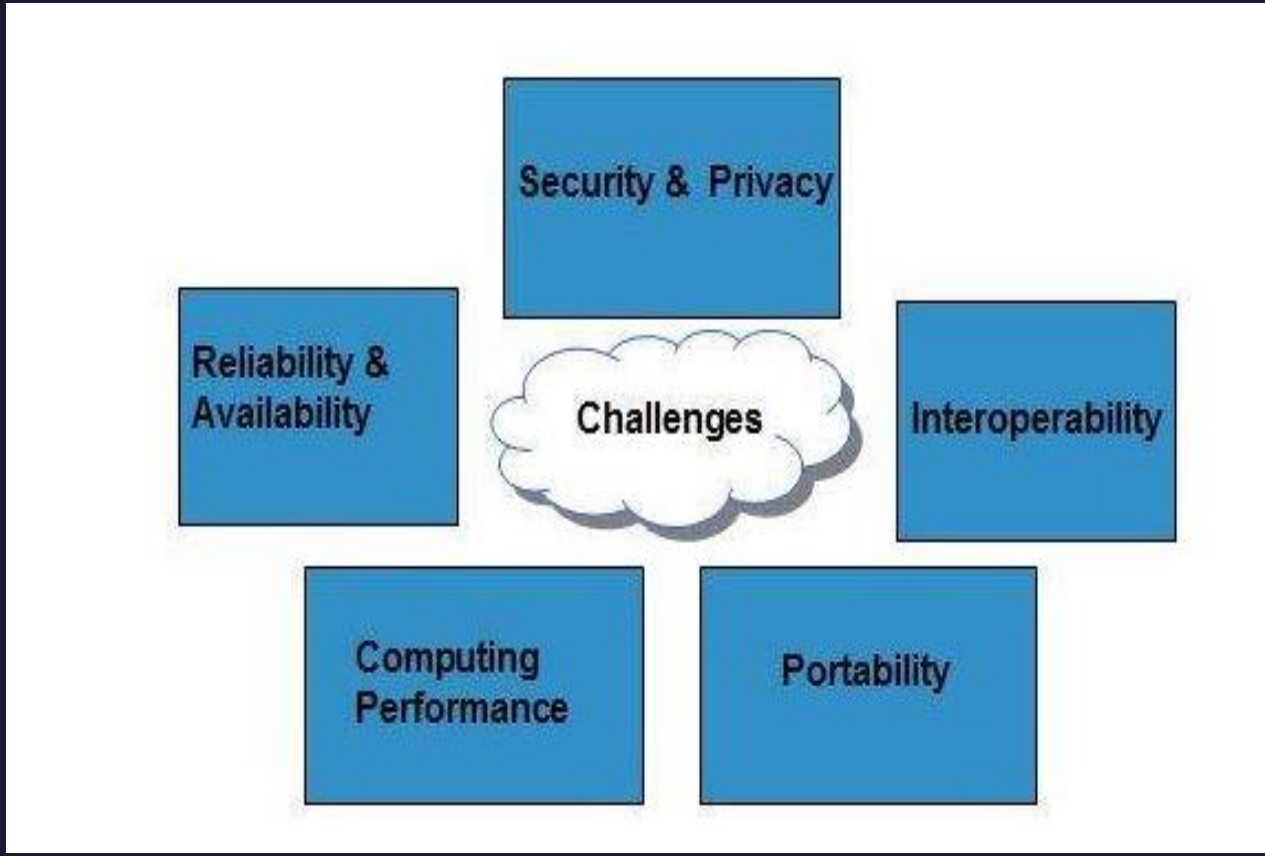
FIGURE 1

**Total Cost of Ownership Differences**

Sample implementation of Performance Management Software (5000 seats)

| | TOTAL COST OF OWNERSHIP, $ THOUSAND | | |
|---|---|---|---|
| | ON-PREMISE | SAAS | SOURCES OF SAVINGS |
| **IMPLEMENTATION, DEPLOYMENT** | | | |
| **Implementation Fees**<br>• Professional Services<br>• Basic infrastructure testing, deployment<br>• Application infrastructure testing, deployment | 150 | 20 | Reduced deployment time, limited customization, no application or infrastructure testing required |
| **SOFTWARE** | | | |
| **User licenses, subscriptions** | 500 | 105 | On-Premise requires significant up front costs plus 20-30% annual maintenance. SaaS is a flat fee. |
| **Maintenance (Year 1)** | | | |
| **Annual License Fee (Years 2-5)** | N/A | 105 | |
| **Annual Maintenance Fee (Years 2-5)** | 110 | N/A | |
| **UPGRADE** | | | |
| **Upgrade Expenses (est. every 4 years)** | 250 | 0 | SaaS upgrades are included in the annual fee. |
| **5 year total ($ thousand)** | **1340** | **545** | |

# UNIT II – CLOUD COMPUTING ARCHITECTURE



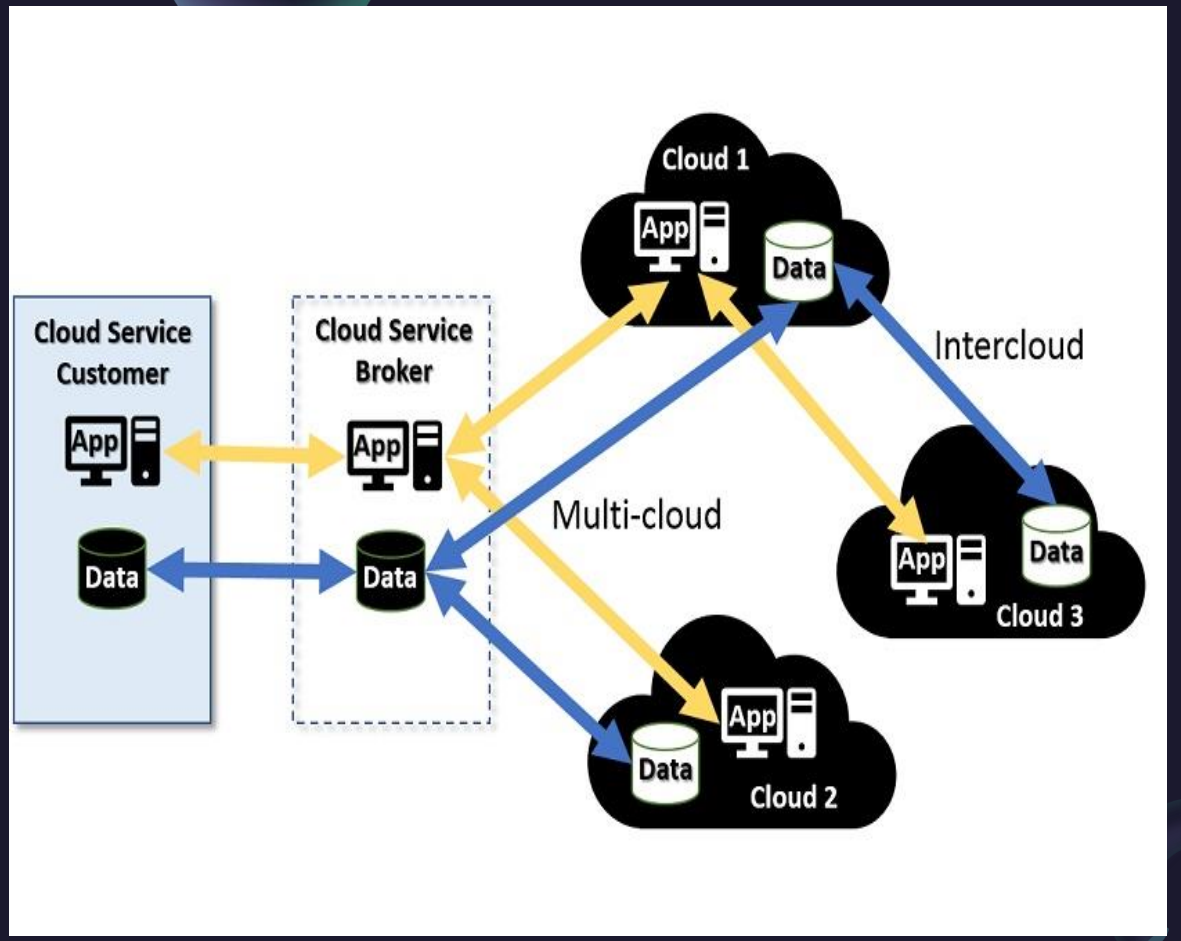

# UNIT II – CLOUD COMPUTING ARCHITECTURE

MSPM's Let us Rise Above The Rest DIEMS

## What is interoperability in cloud?

Cloud interoperability is the ability of a customer's system to interact with a cloud service or the ability for one cloud service to interact with other cloud services by exchanging information according to a prescribed method to obtain predictable results.

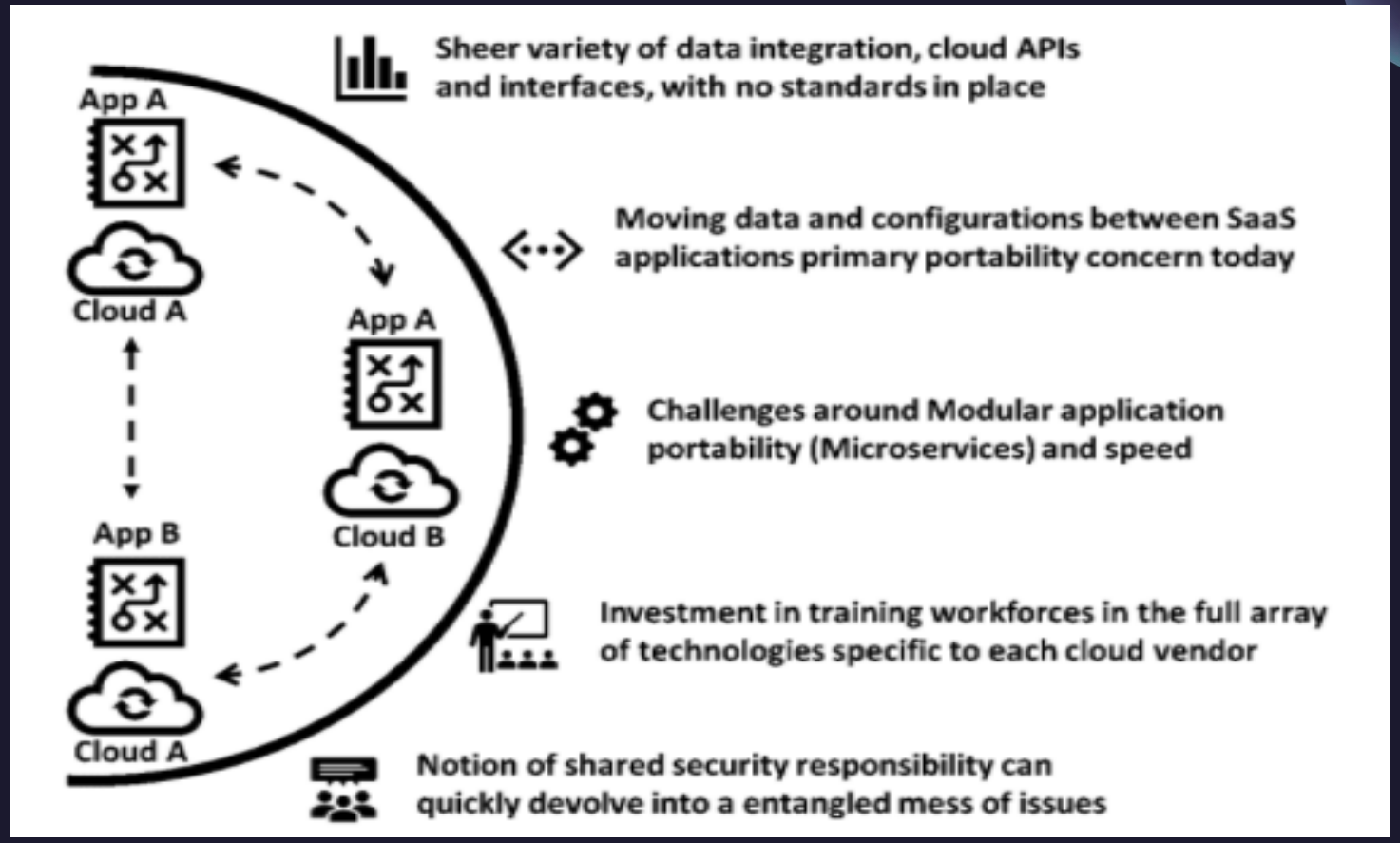
Cloud interoperability refers to the ability of the systems to work efficiently and collaborate effectively across different cloud platforms.




## Example of Interoperability in Health Care

Interoperability ensures that patient data is shared accurately among providers and organizations, improving efficiency, decreasing unnecessary diagnostic testing, and improving communication between referring doctors and specialists.

# UNIT II – CLOUD COMPUTING ARCHITECTURE

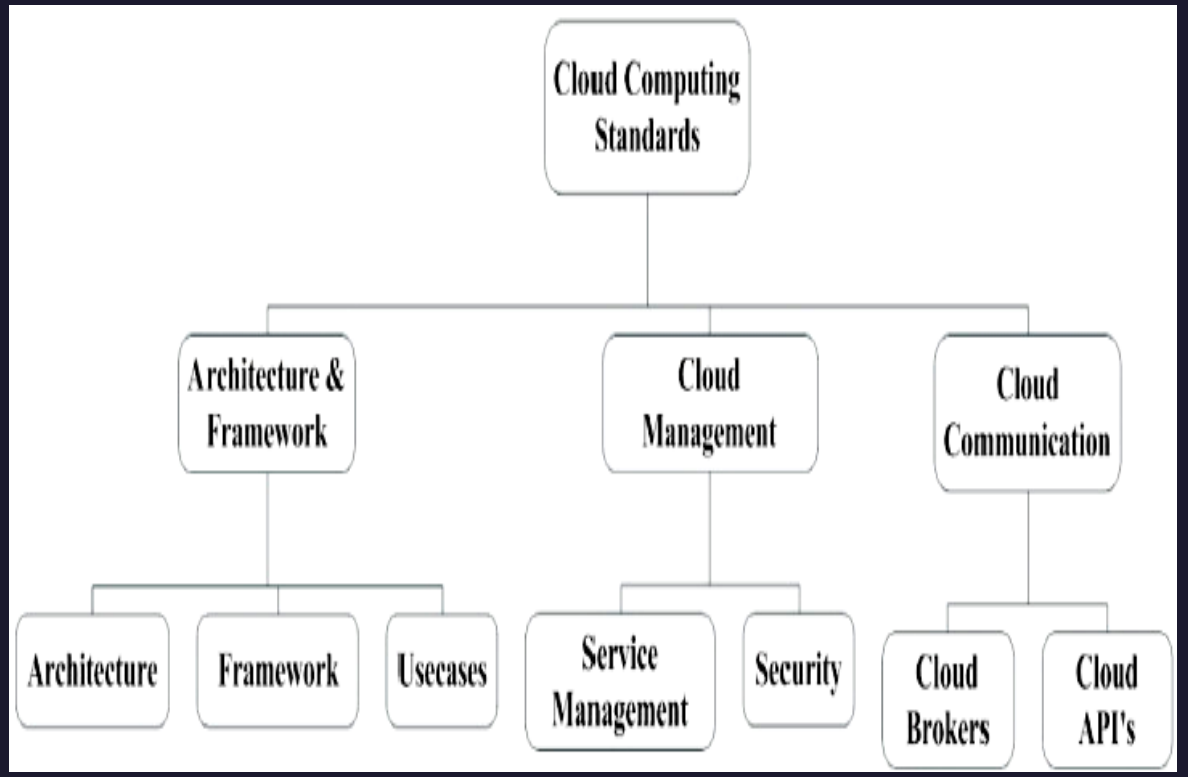


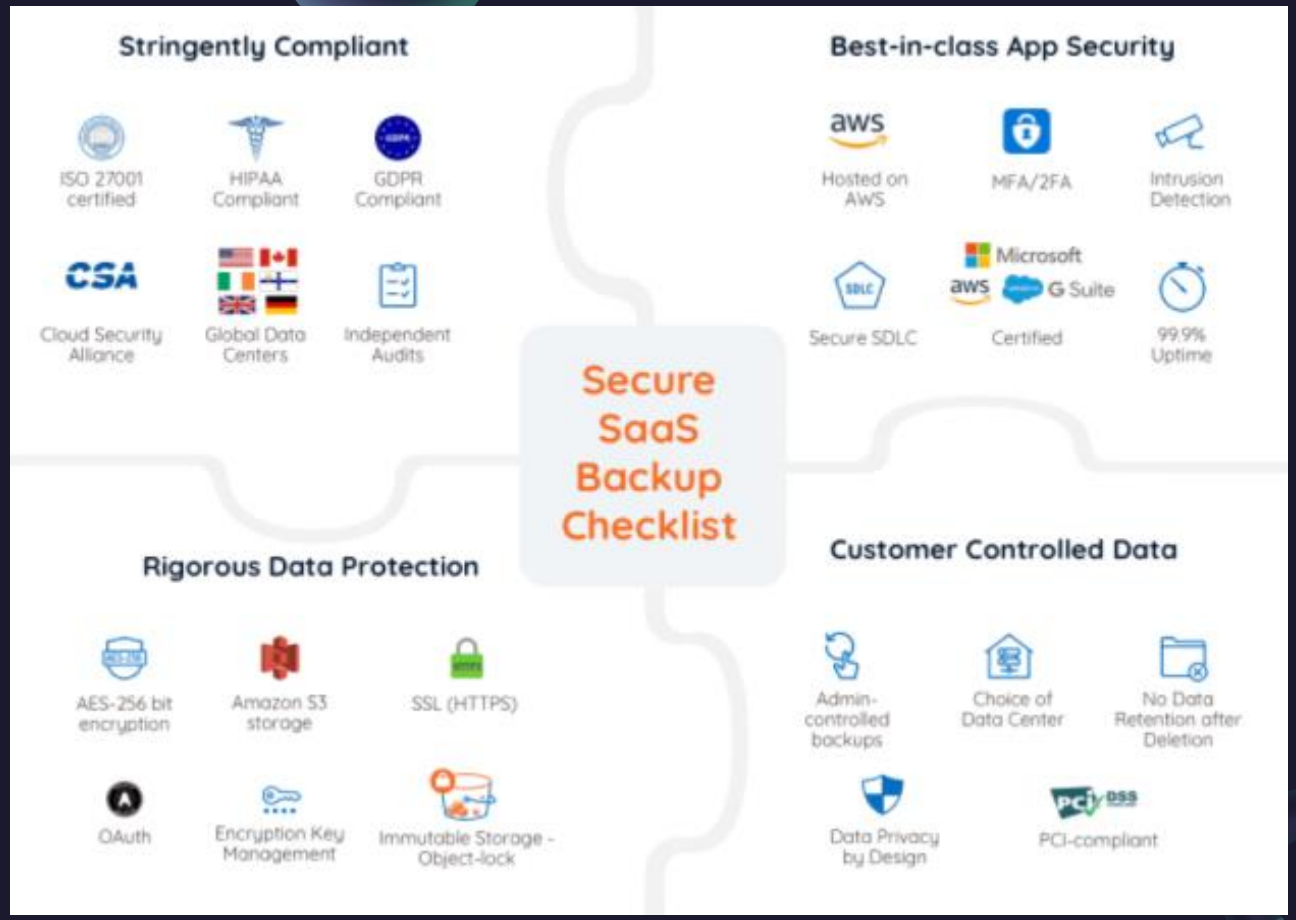

CHALLENGES WITH CLOUD INTEROPERABILITY TODAY

## Interoperability Challenges

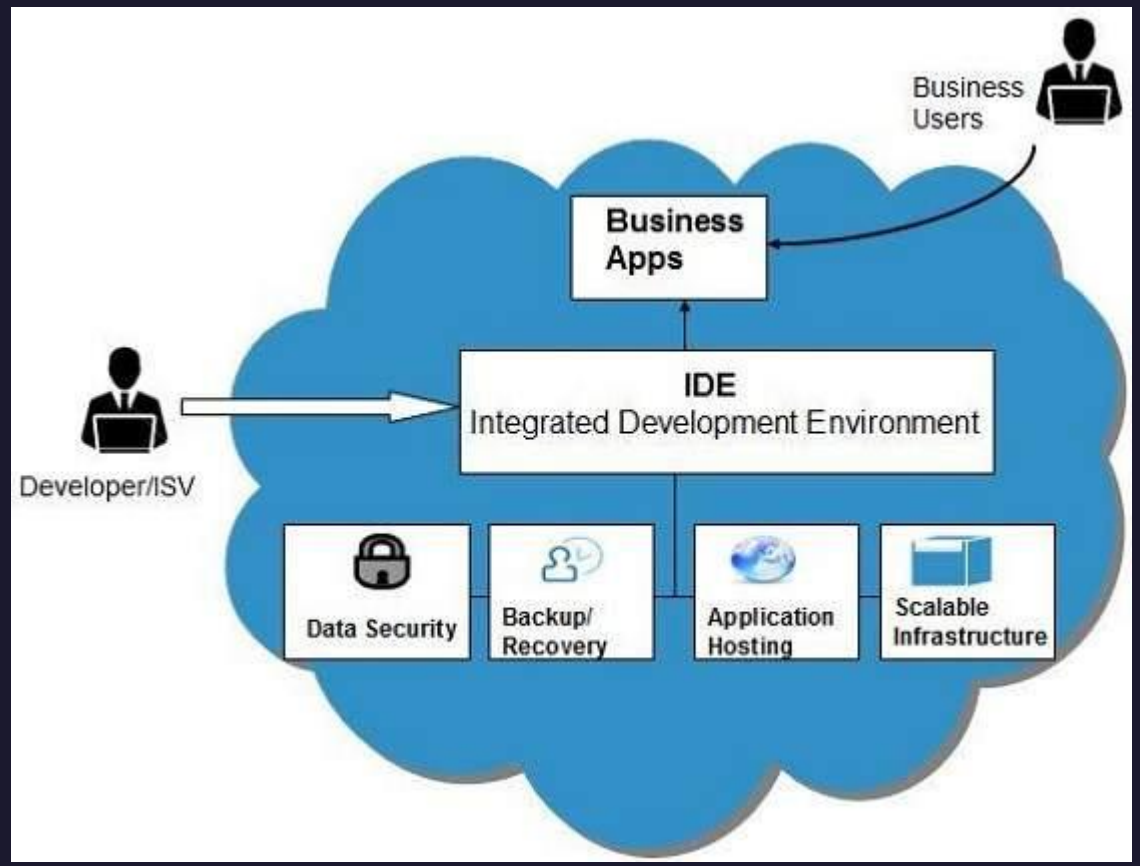
- Multiple interfaces & APIs across several dimensions
- Non-standardized interfaces & APIs
- IaaS has highest level of interoperability
- PaaS has lower level of interoperability
- SaaS has lowest level of interoperability
- Potential solutions:
  - ESBs can help address interoperability challenges
  - Inter-cloud providers (i.e. brokers) are an option

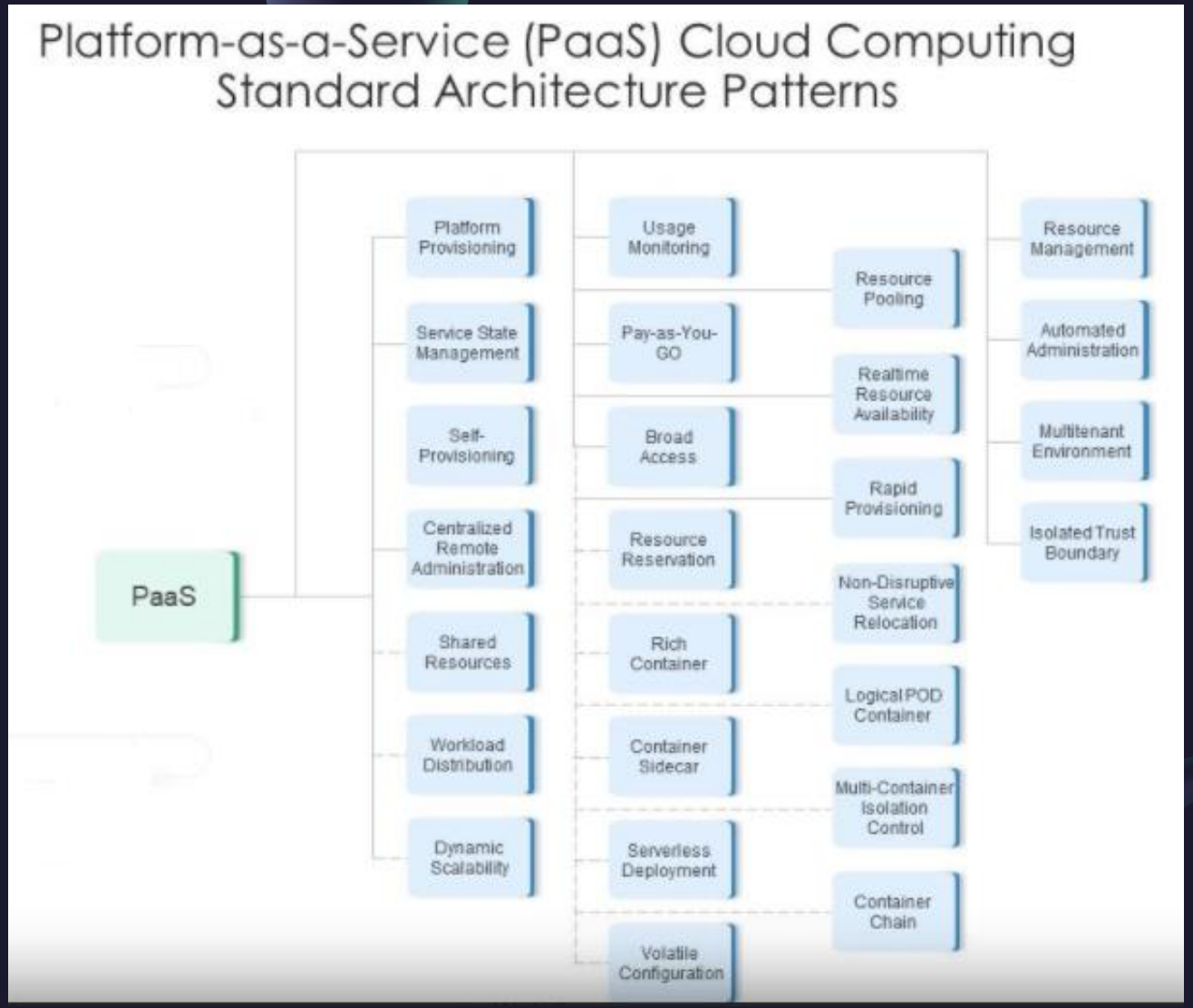
# UNIT II – CLOUD COMPUTING ARCHITECTURE



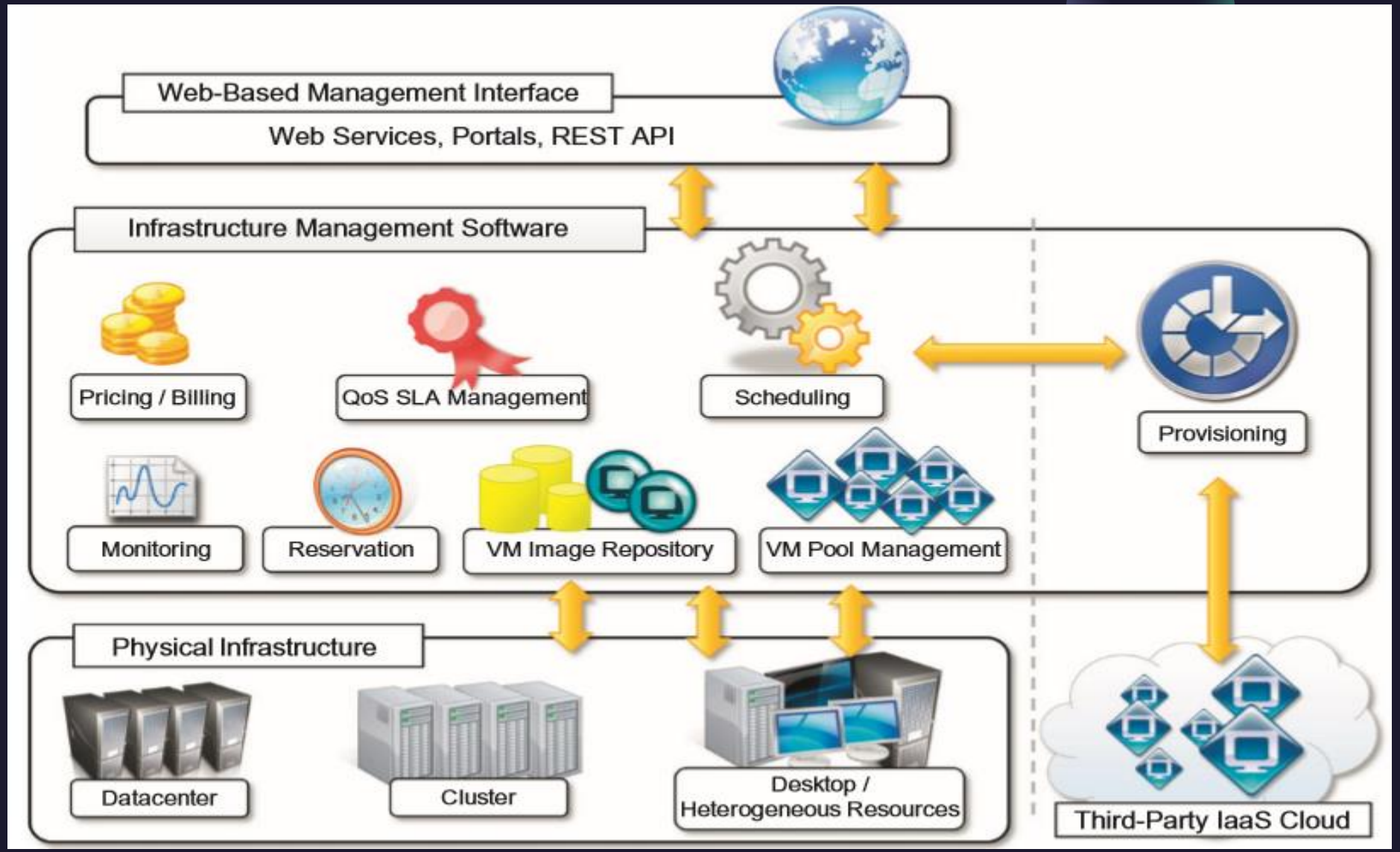



# UNIT II – CLOUD COMPUTING ARCHITECTURE

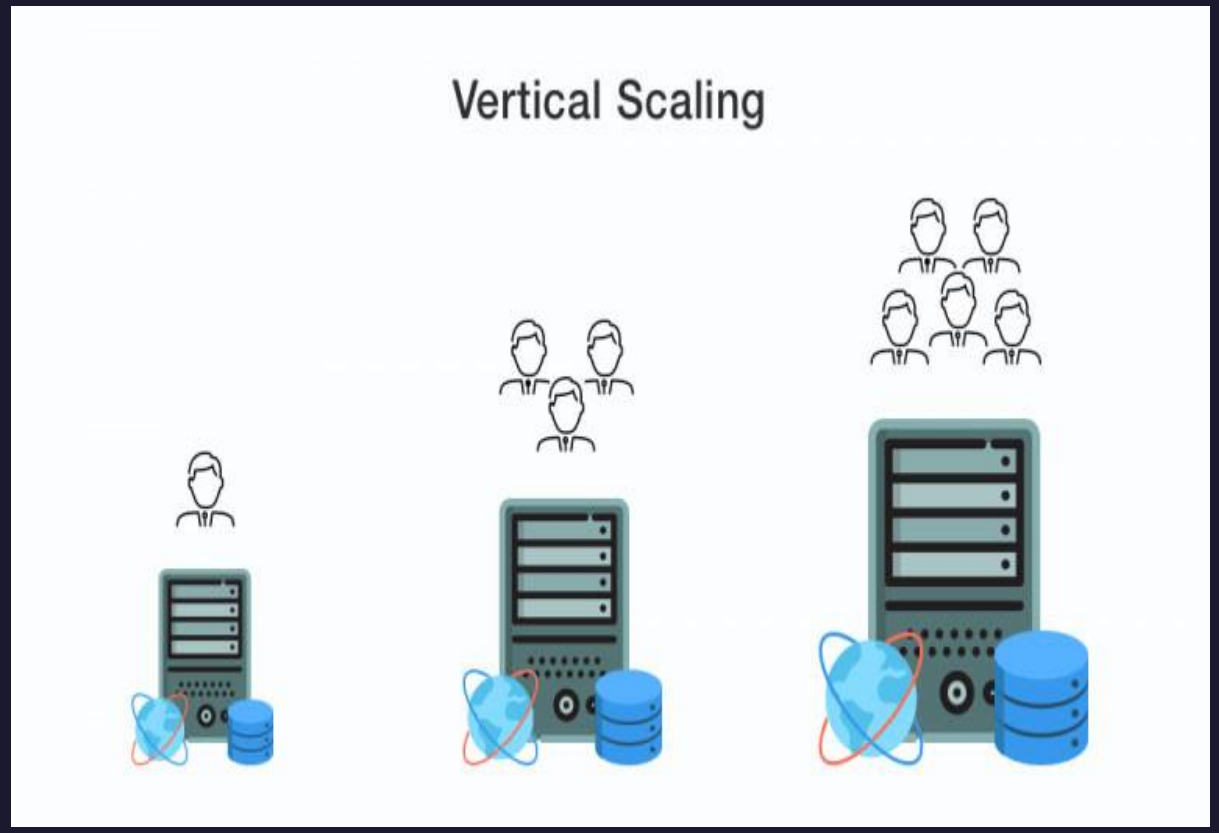


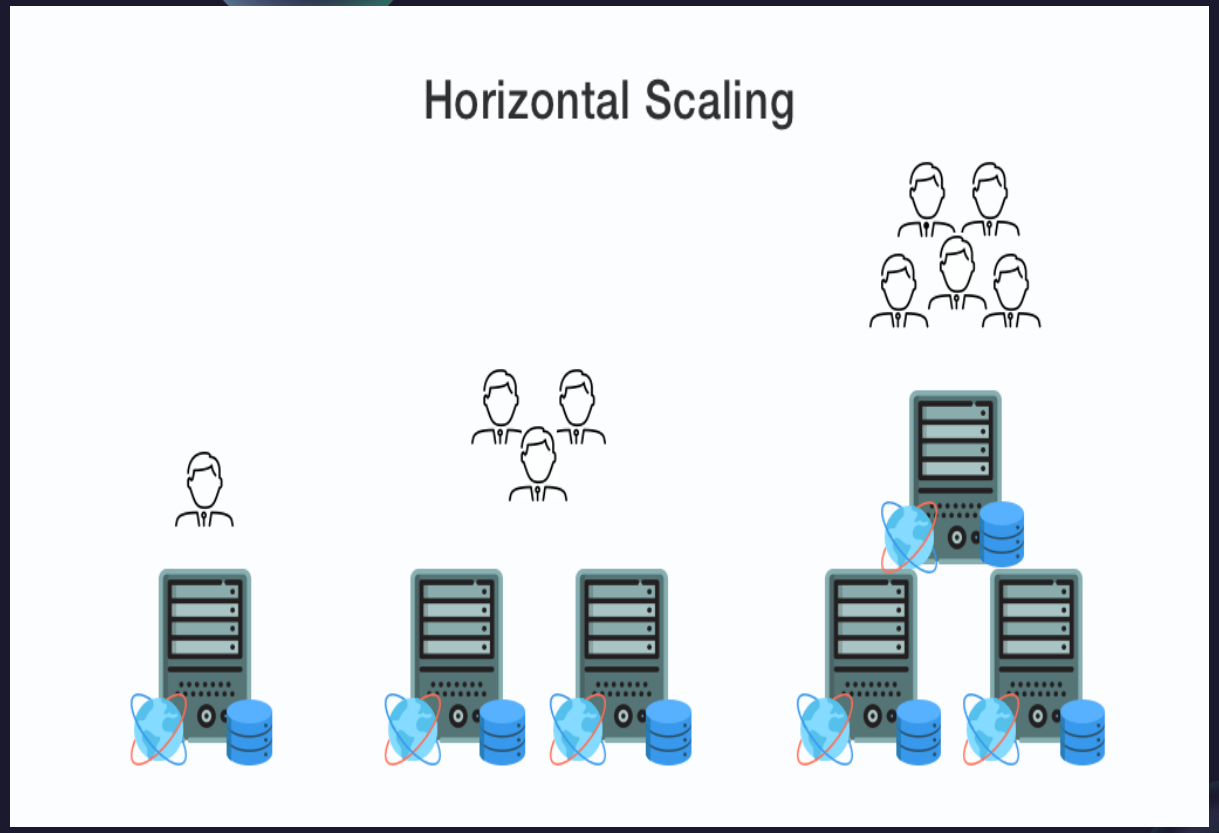



# UNIT II – CLOUD COMPUTING ARCHITECTURE

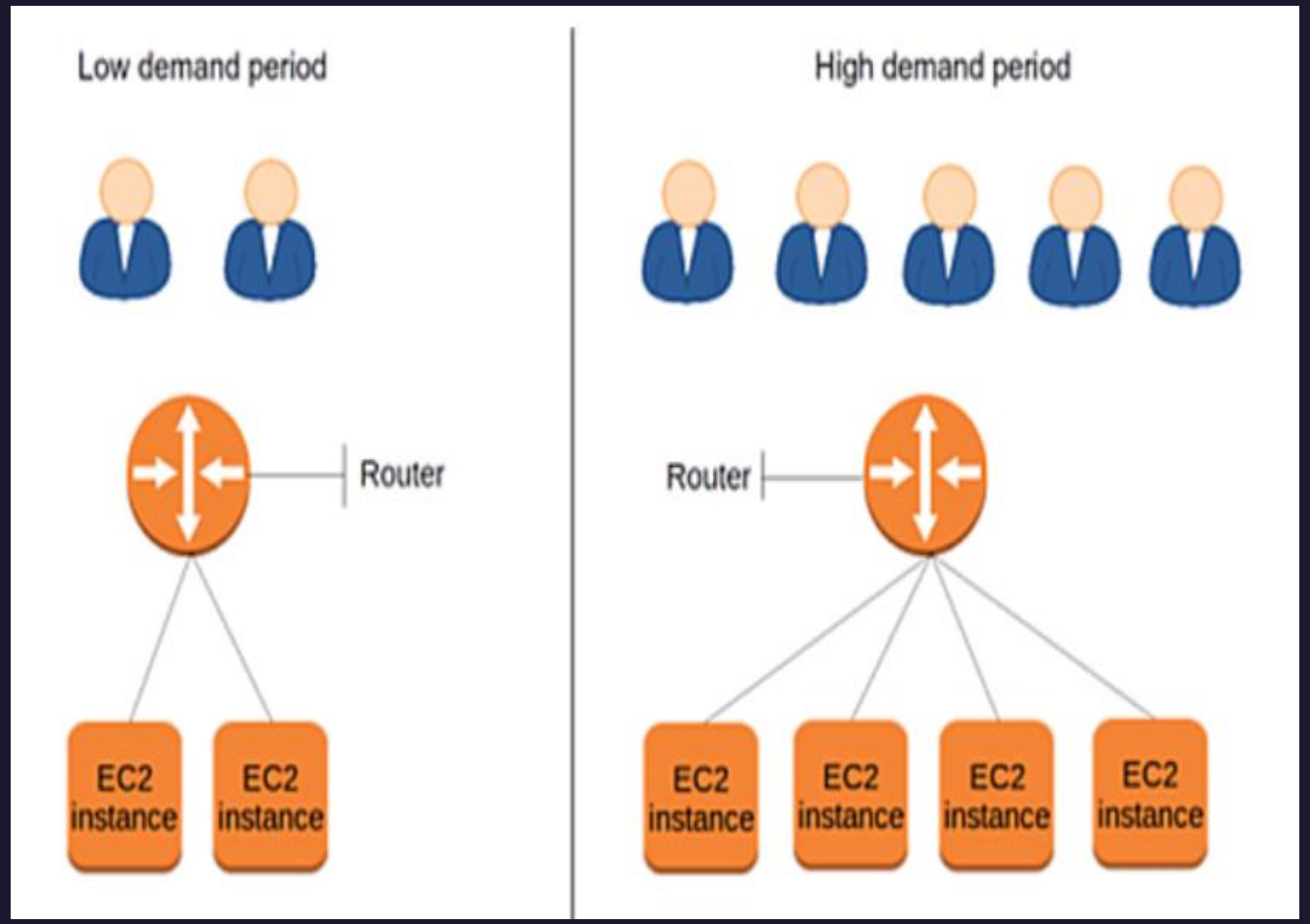


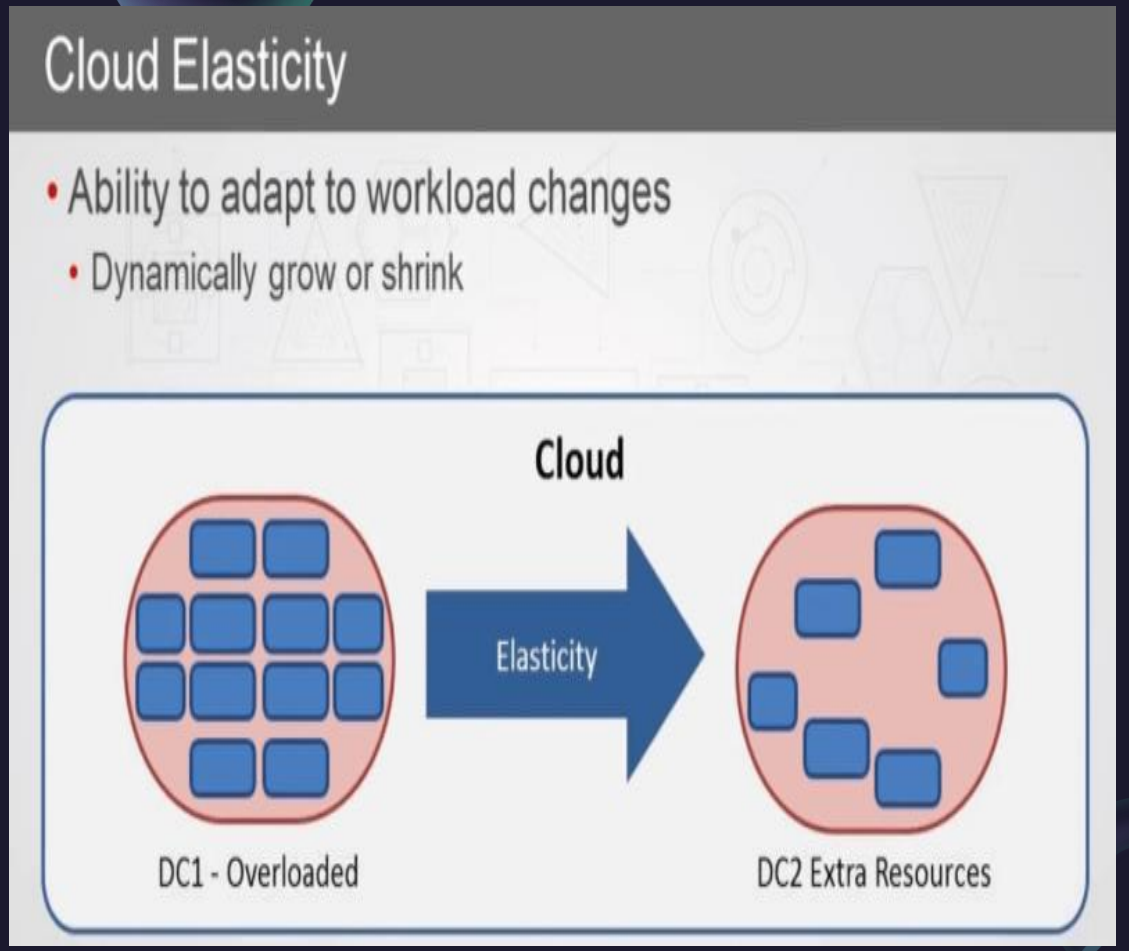
# UNIT II – CLOUD COMPUTING ARCHITECTURE



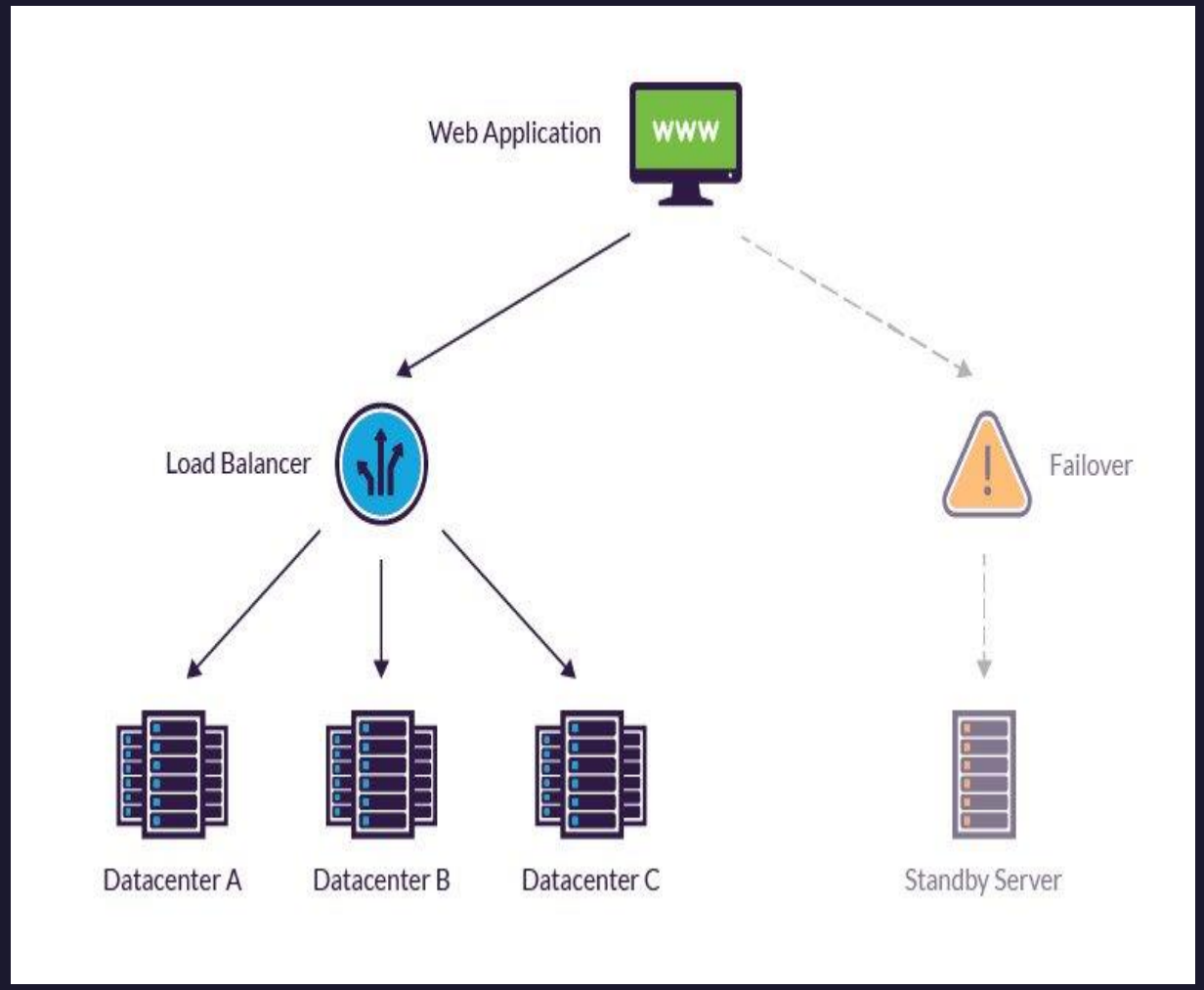



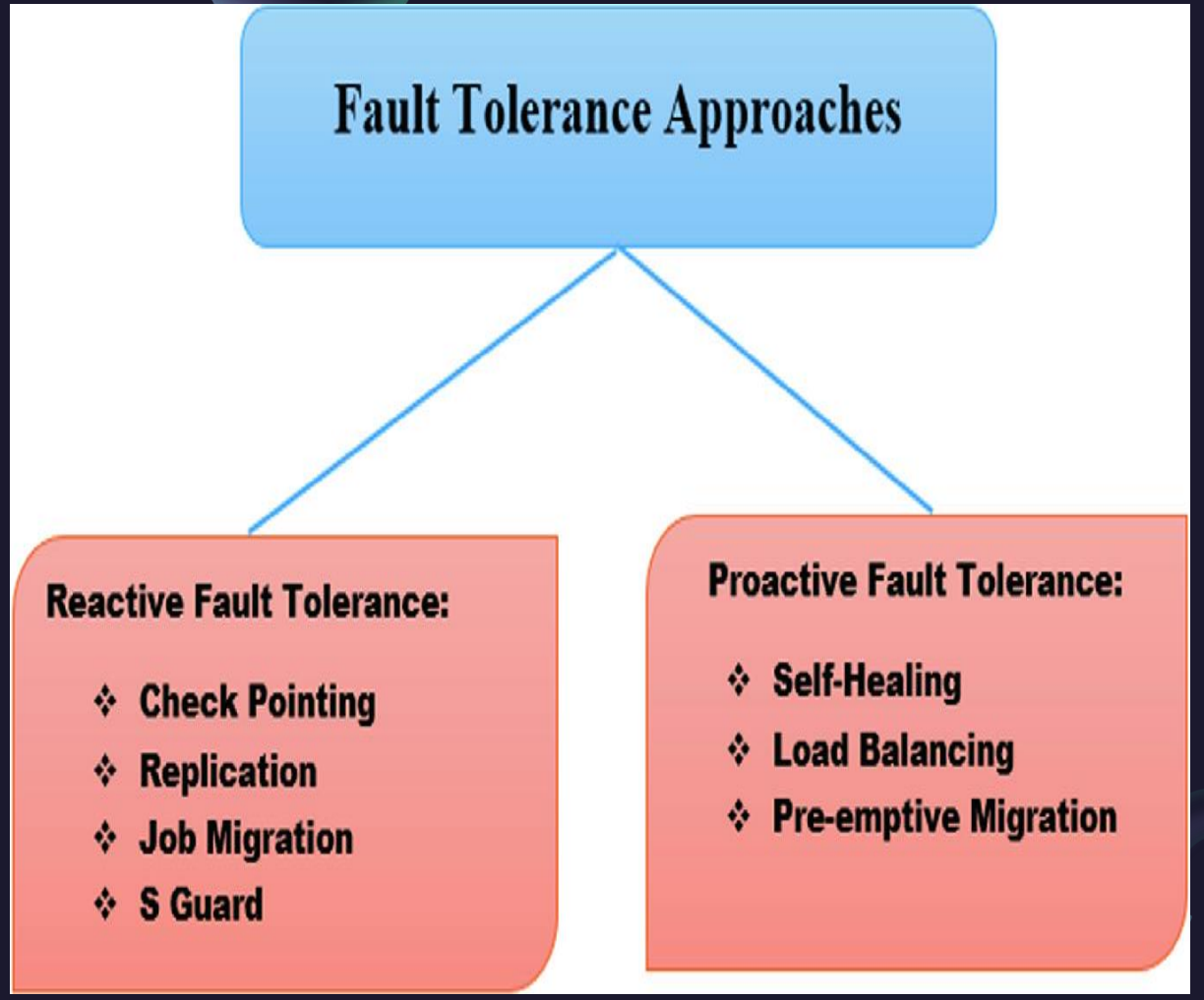
# UNIT II – CLOUD COMPUTING ARCHITECTURE



# UNIT II – CLOUD COMPUTING ARCHITECTURE



# UNIT II – CLOUD COMPUTING ARCHITECTURE

## Ready for the Cloud

### Web Application Design

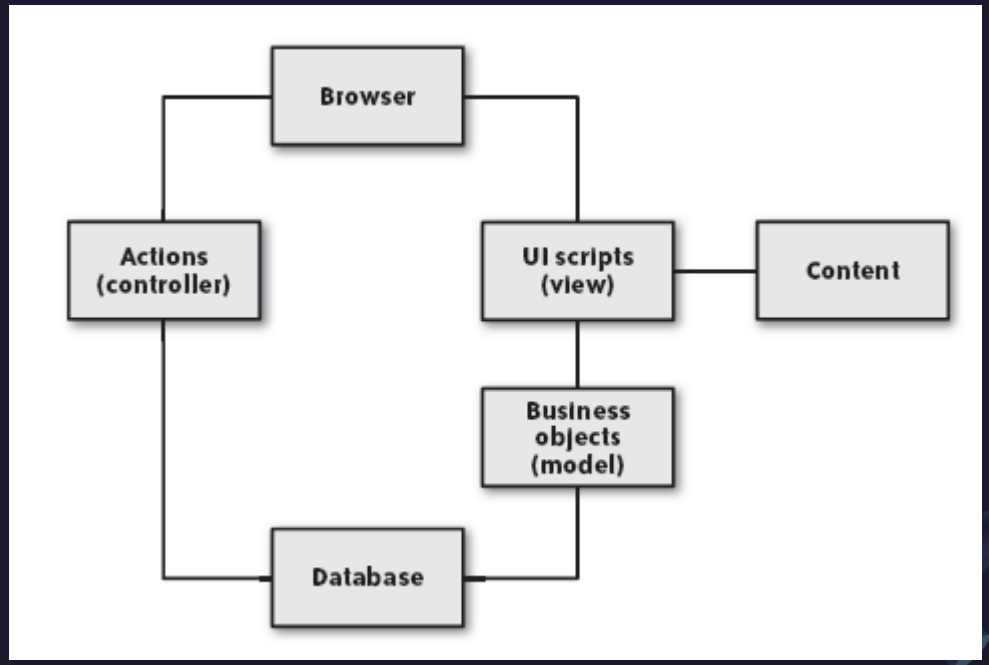
Many developers are used different platforms for developing their web application.

Examples: .NET, Ruby, Java, PHP, or anything else.

**System State and Protecting Transactions**

- How your application manages its state on cloud?

**Transactional integrity through stored procedures**



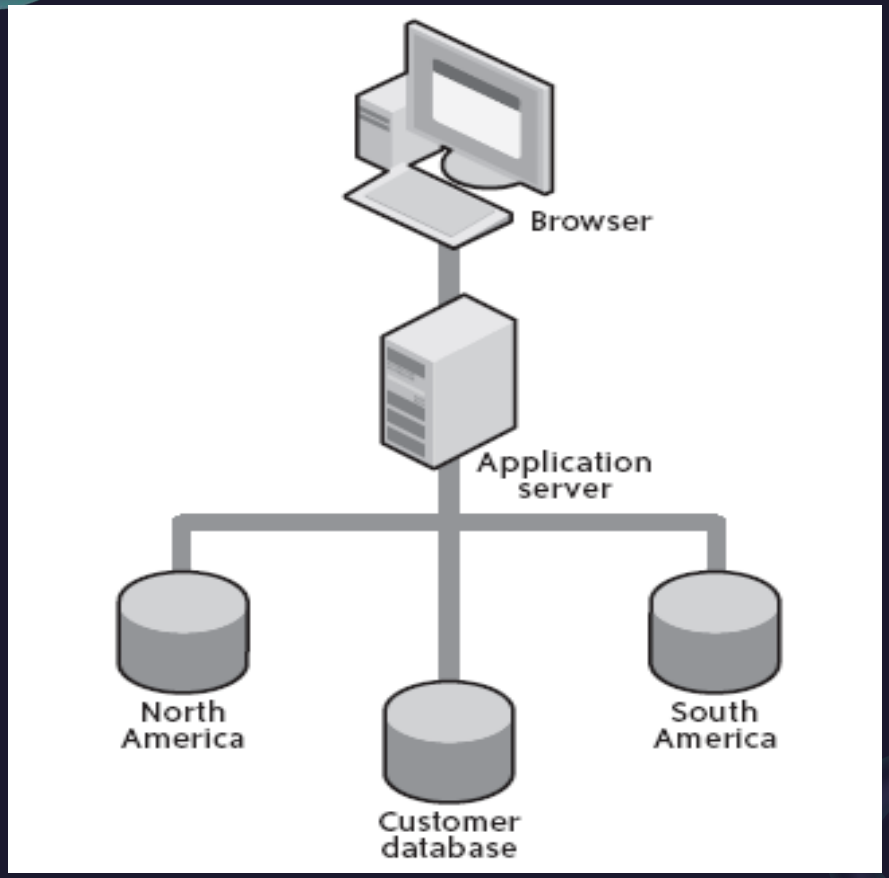

Common MVC model for web application

# UNIT II – CLOUD COMPUTING ARCHITECTURE

## Ready for the Cloud

### Web Application Design

**When Servers Fail**




*Supporting different hotels on different servers guarantees no double bookings*

# Ready for the Cloud

## Machine Image Design

Two indirect benefits of the cloud are:

- **It forces discipline in deployment planning**
- **It forces discipline in disaster recovery**

Thanks to the way virtualized servers launch from machine images.

The machine image (in Amazon, the AMI) is a raw copy of your operating system and core software for a particular environment on a specific platform. When you start a virtual server, it copies its operating environment from the machine image and boots up. If your machine image contains your installed application; deployment is nothing more than the process of starting up a new virtual instance.

# Ready for the Cloud

**Amazon Machine Image Data Security**

**What Belongs in a Machine Image?**

The full process of establishing a machine image consists of the following steps:

1. Create a component model that identifies what components and versions are required to run the service that the new machine image will support.
2. Separate out stateful data in the component model. You will need to keep it out of your machine image.
3. Identify the operating system on which you will deploy.
4. Search for an existing, trusted baseline public machine image for that operating system.
5. Harden your system using a tool such as Bastille.
6. Install all of the components in your component model.
7. Verify the functioning of a virtual instance using the machine image.
8. Build and save the machine image.

# Ready for the Cloud

## Database Management

### Clustering or Replication?

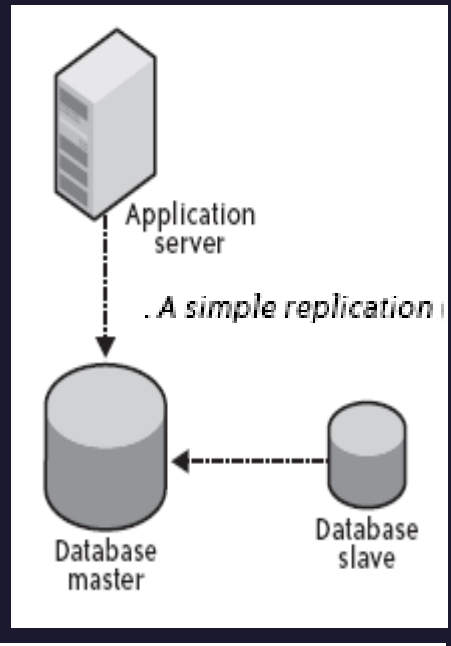
The most effective mechanism for avoiding corruption is leveraging the capabilities of a database engine that supports true clustering.

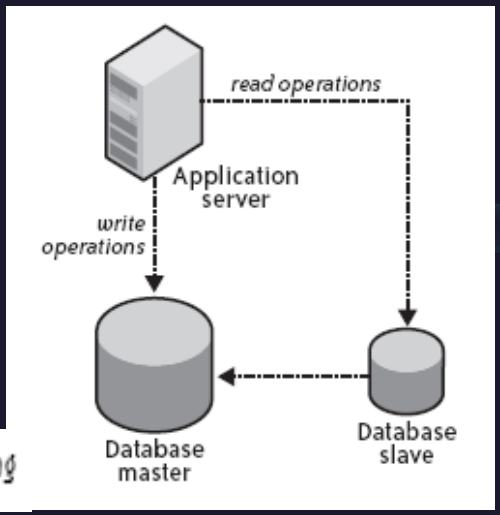
Unfortunately, database clustering is very complicated and generally quite expensive.

The alternative to clustering is replication. A replication-based database infrastructure generally, has a main server, referred to as the database master. Client applications execute write transactions against the database master. Successful transactions are then replicated to database slaves.

Replication has two key advantages over clustering:

- It is generally much simpler to implement.
- It does not require an excessive number of servers or expensive licenses.




By separating read operations to execute against slaves, your applications can scale without clustering

# Ready for the Cloud

## Database Management

### Primary Key Management

How to generate globally unique primary keys?

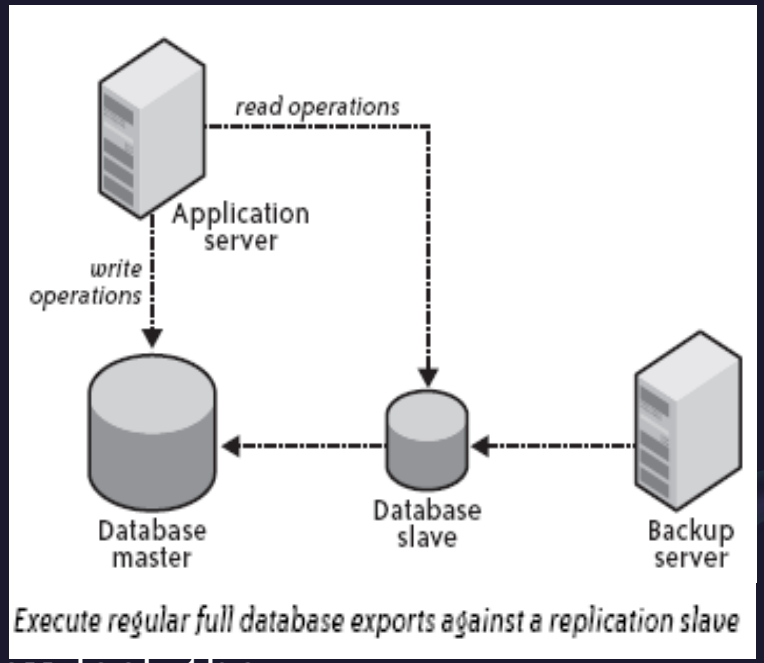
First, you could use standard UUIDs to serve as your primary key mechanism.

### Database Backups

Types of database backups

Typically, your database engine will offer at least these backup options.

- Database export/dump backup
- Filesystem backup
- Transaction log backup



Execute regular full database exports against a replication slave

### Applying a backup strategy for the cloud

The best backup strategy for the cloud is a file-based backup solution. You lock the database against writes, take a snapshot, and unlock it.

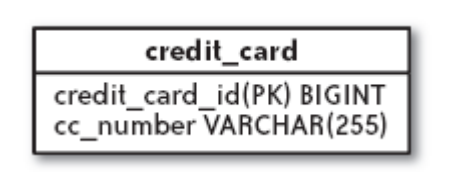
# Ready for the Cloud

## Privacy in Cloud

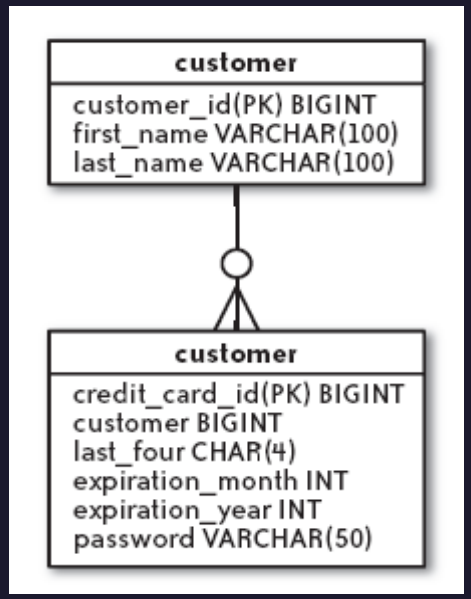
The key to privacy in the cloud - is the strict separation of sensitive data from non sensitive data followed by the encryption of sensitive elements.

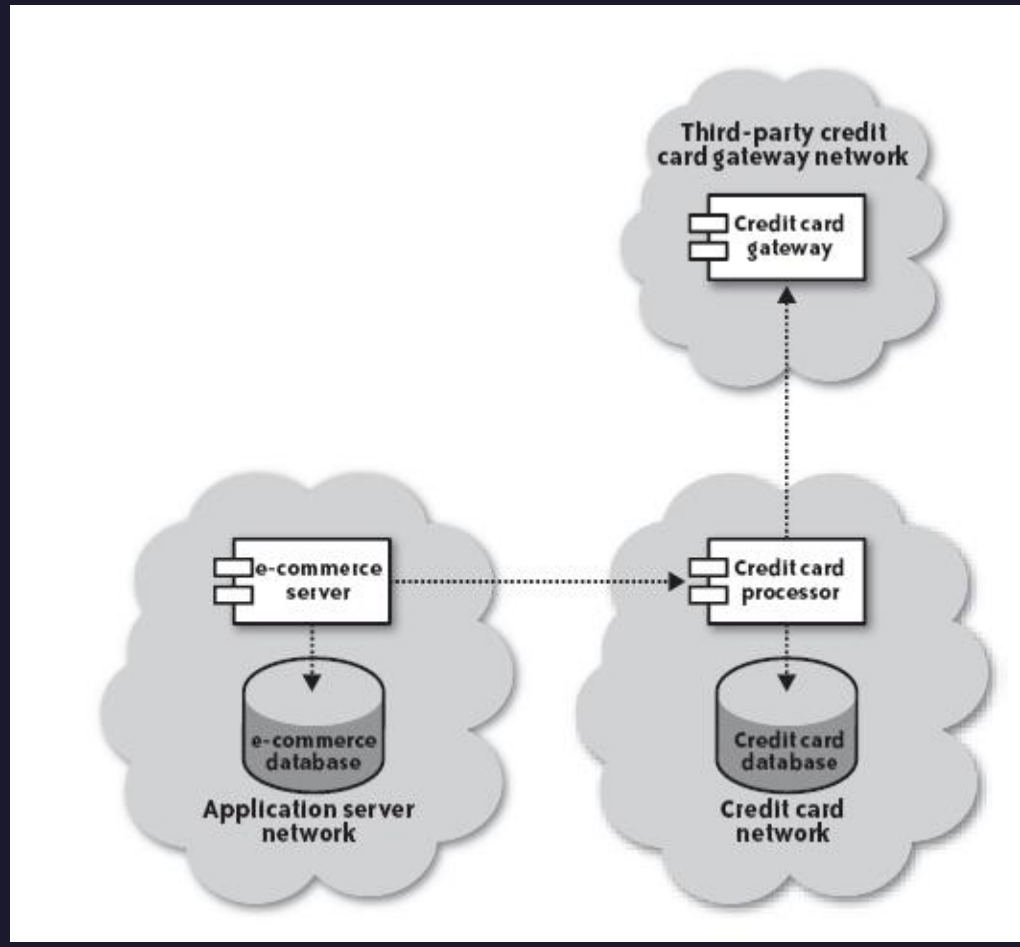
Example is storing credit cards. You may have a complex e-commerce application storing many data relationships.

**Managing the credit card encryption**




*The credit card processor stores the encrypted credit card number and associates it with the e-commerce credit card ID*

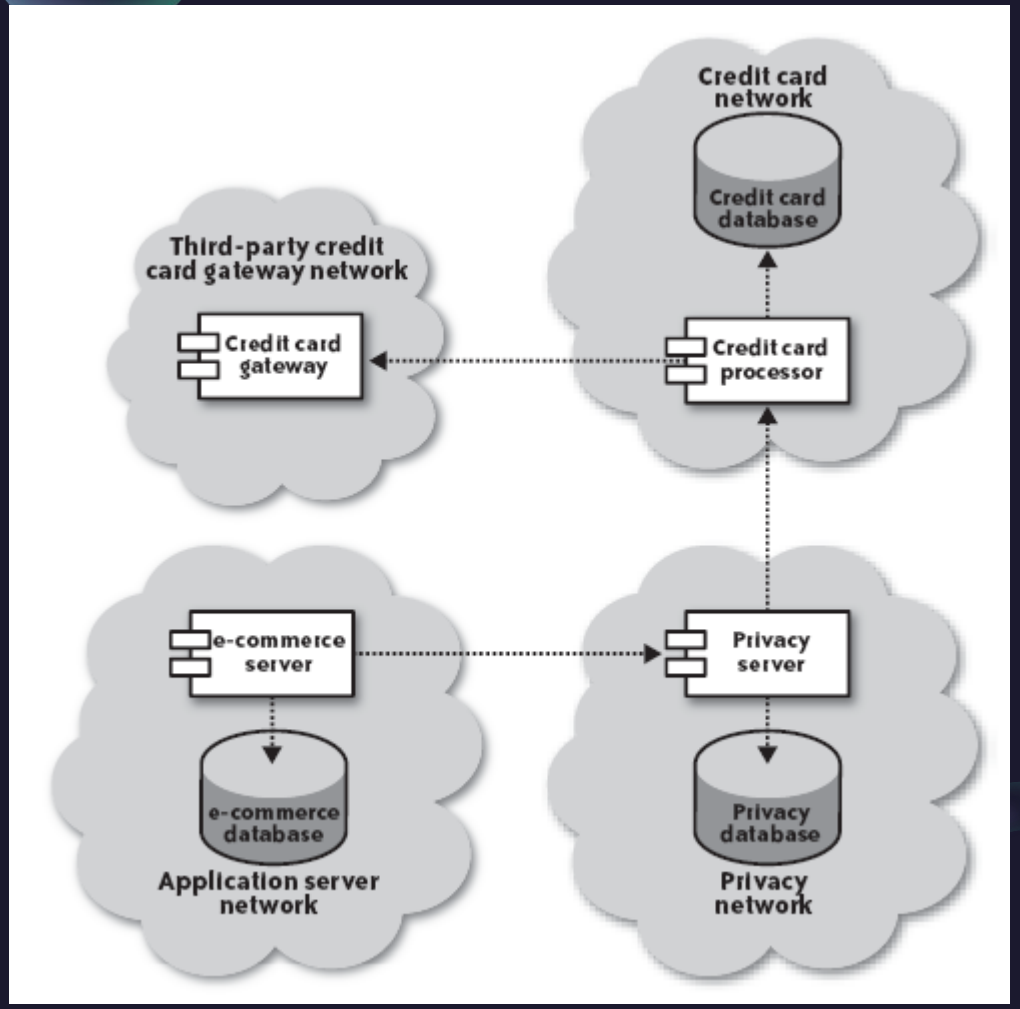


# Ready for the Cloud

## Privacy in Cloud

### When the Amazon Cloud Fails to Meet Your Needs




*Pulling private data out of the cloud creates three different application components*

MSPM's Let us Rise Above The Rest DIEMS

# Ready for the Cloud

## Data Security in Cloud

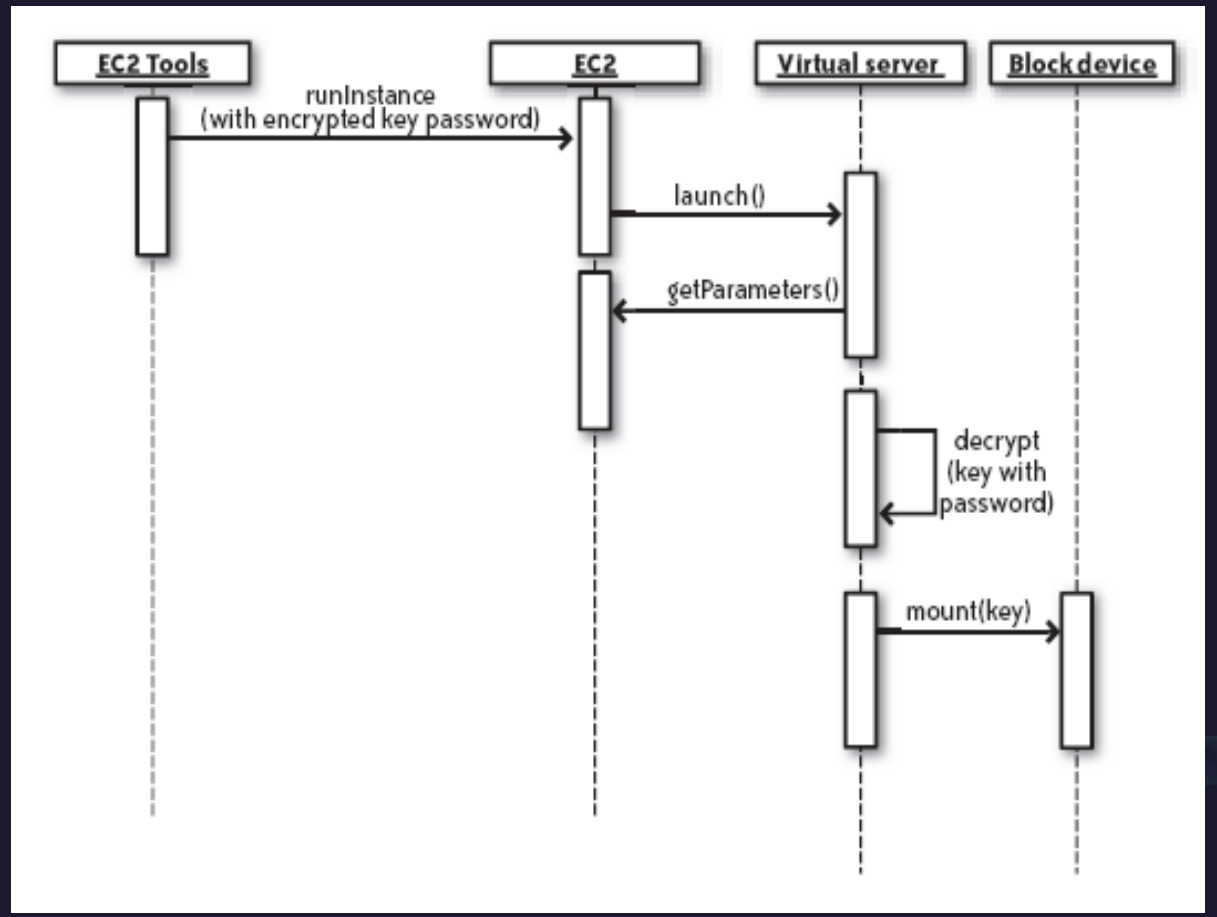
**Data Control**

**When the cloud provider goes down?**

**When your cloud provider fails to adequately protect their network ?**

**Solution:**

**Encrypt Everything, Encrypt your network traffic, Encrypt your backups, Encrypt your filesystems**



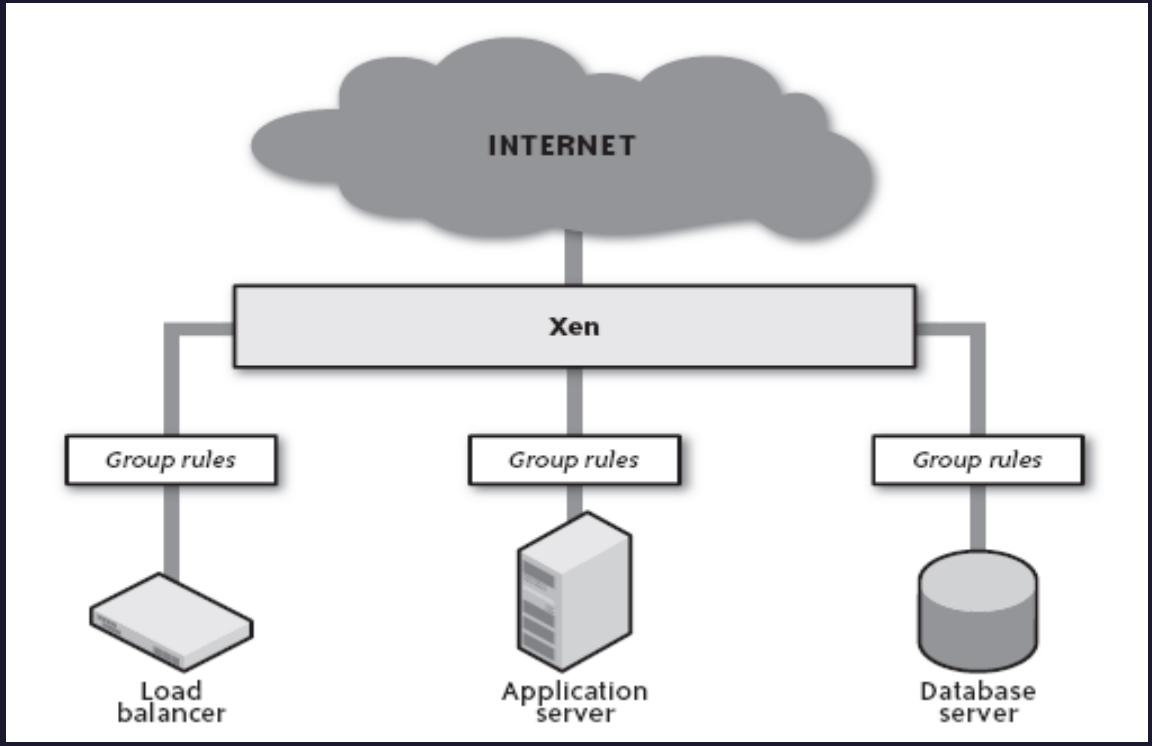

*The process of starting a virtual server with encrypted filesystems*

# UNIT II – CLOUD COMPUTING ARCHITECTURE

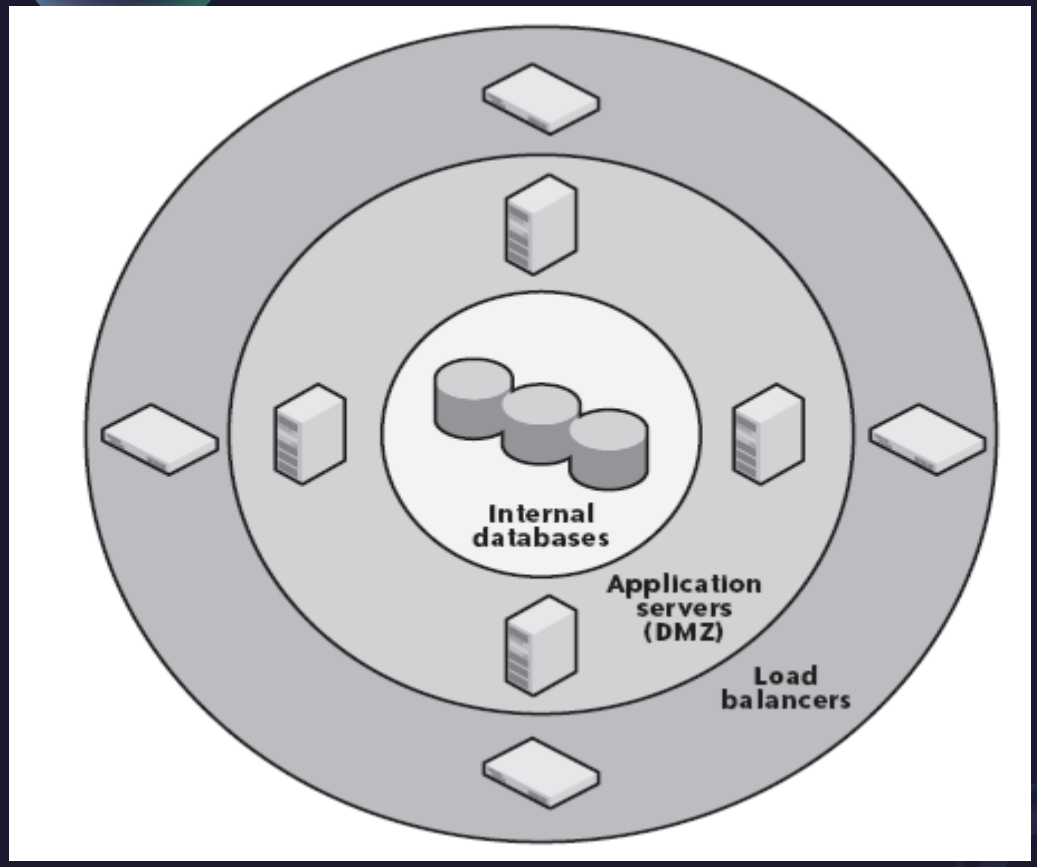
## Ready for the Cloud

### Network Security in Cloud

**Firewall Rules**




*There are no network segments or perimeters in the cloud*




*Firewalls are the primary tool in perimeter security*

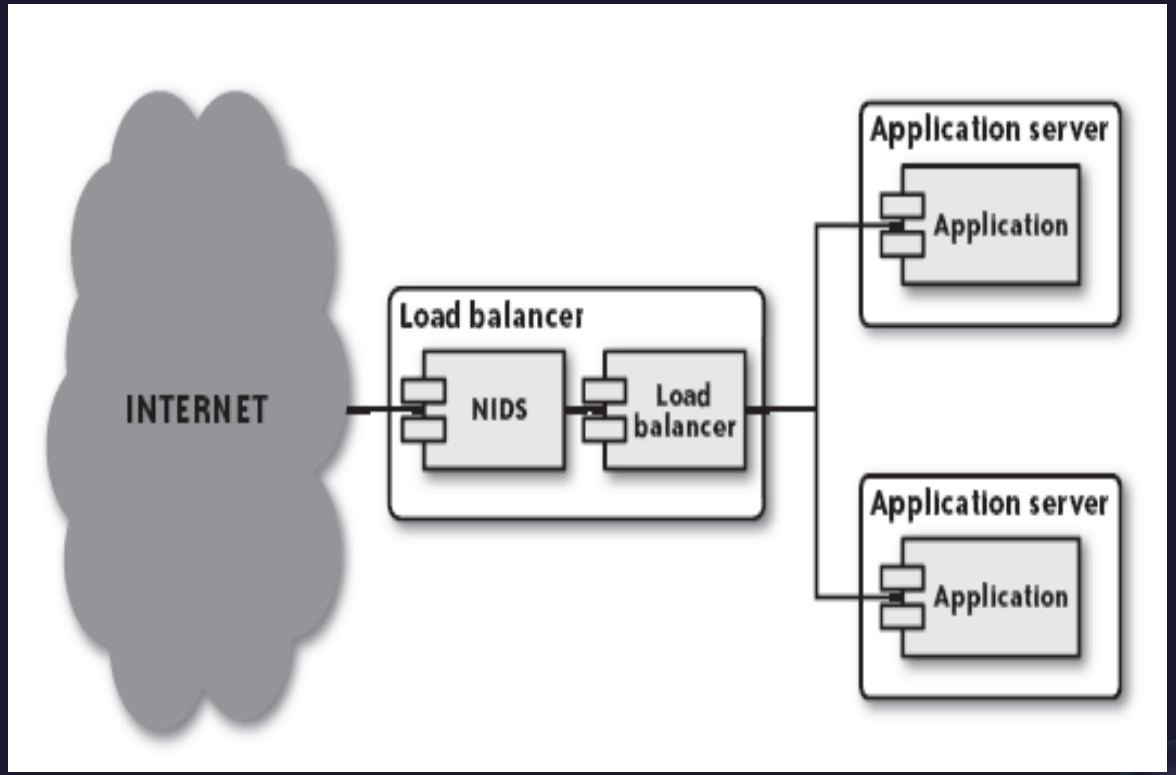
# Ready for the Cloud

## Network Security in Cloud

### Network Intrusion Detection

Perimeter security often involves network intrusion detection systems (NIDS), such as Snort, which monitor local traffic for anything that looks irregular. Examples of irregular traffic include:

- Port scans
- Denial-of-service attacks
- Known vulnerability exploit attempts




*A network intrusion detection system listening on a load balancer*

# Ready for the Cloud

## Host Security in Cloud

Host security describes how your server is set up for the following tasks:

- Preventing attacks.
- Minimizing the impact of a successful attack on the overall system.
- Responding to attacks when they occur.

In the cloud, rolling out a patch across the infrastructure takes three simple steps:

1. Patch your AMI with the new security fixes.
2. Test the results.
3. Relaunch your virtual servers.

### System Hardening

- Prevention begins when you set up your machine image. As you get going, you will experiment with different configurations and constantly rebuild images. Once you have found a configuration that works for a particular service profile, you should harden the system before creating your image.
- Server hardening is the process of disabling or removing unnecessary services and eliminating unimportant user accounts.

# Ready for the Cloud

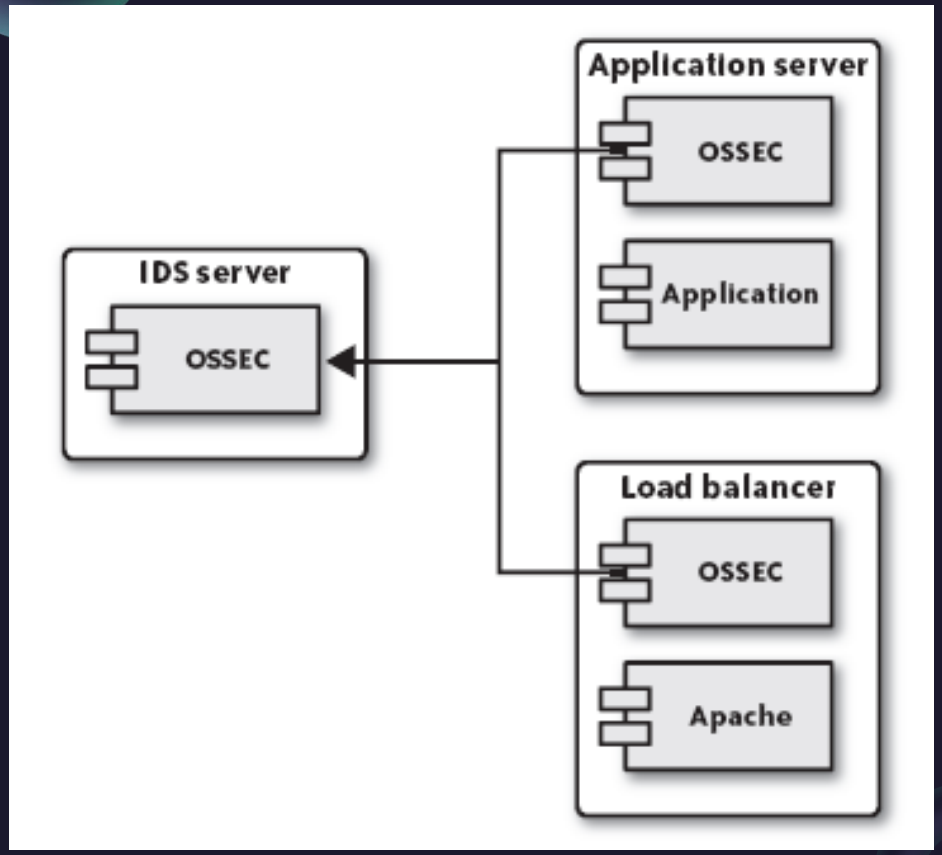
## Host Security in Cloud

### Antivirus Protection

Some regulations and standards require the implementation of an antivirus (AV) system on your servers.

### Host Intrusion Detection

Whereas a network intrusion detection system monitors network traffic for suspicious activity, a host intrusion detection system (HIDS) such as OSSEC monitors the state of your server for anything unusual. An HIDS is in some ways similar to an AV system, except it examines the system for all signs of compromise and notifies you when any core operating system or service file changes.




*A HIDS infrastructure reporting to a centralized server*