॥ त्वं ज्ञानमयो विज्ञानमयोऽसि ॥
IIT Jodhpur

Excellence above all
SME

Technology • Innovation • Leadership

# Introduction to Cloud Computing

Dr. Deepak Saxena, SME IIT Jodhpur

# 1950-60s: Mainframe Computers

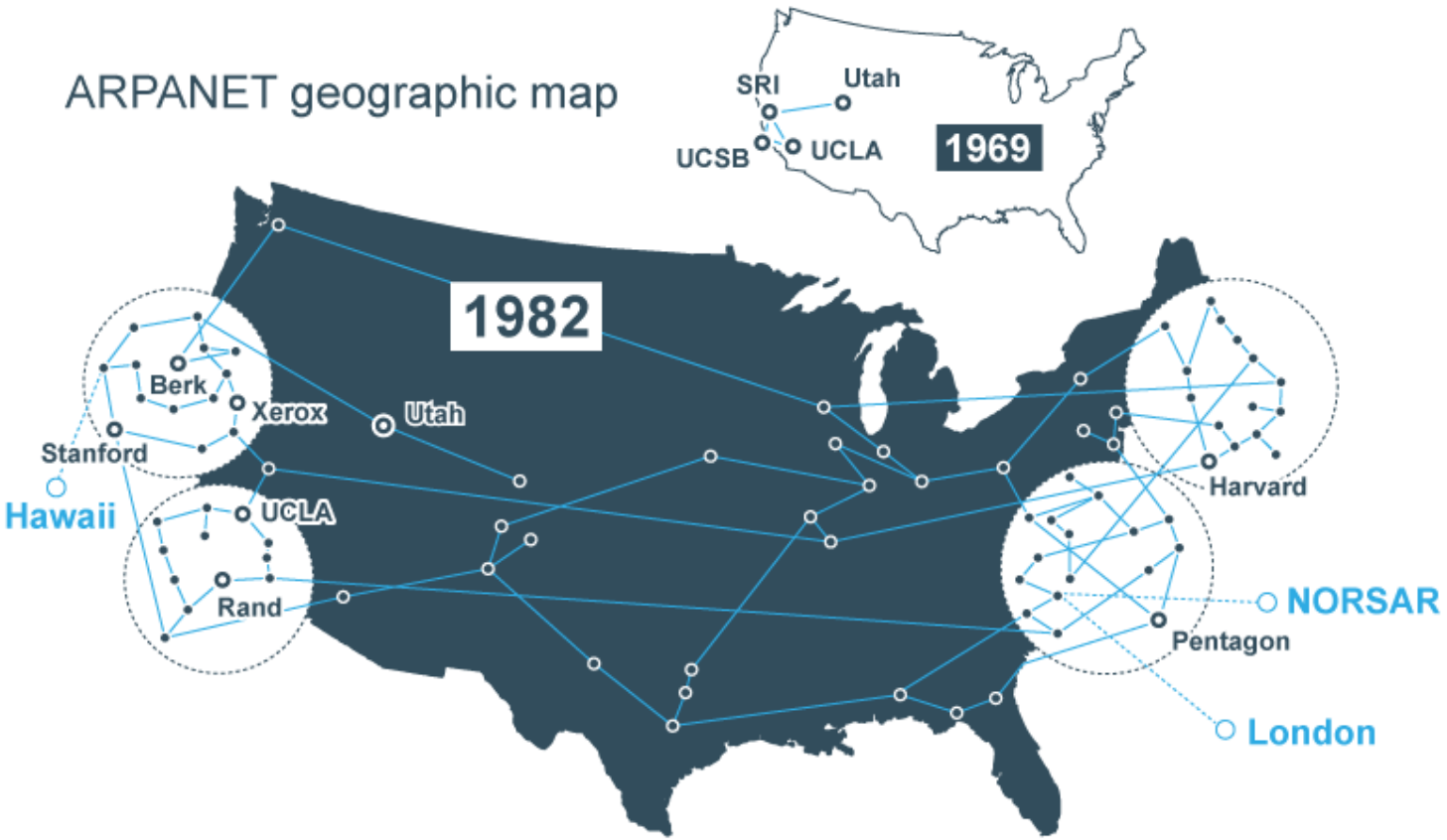
## Virtualization

Virtualization relies on software to simulate hardware functionality and create a virtual computer system. This enables IT organizations to run more than one virtual system – and multiple operating systems and applications – on a single server. The resulting benefits include economies of scale and greater efficiency.

## Virtual Machine

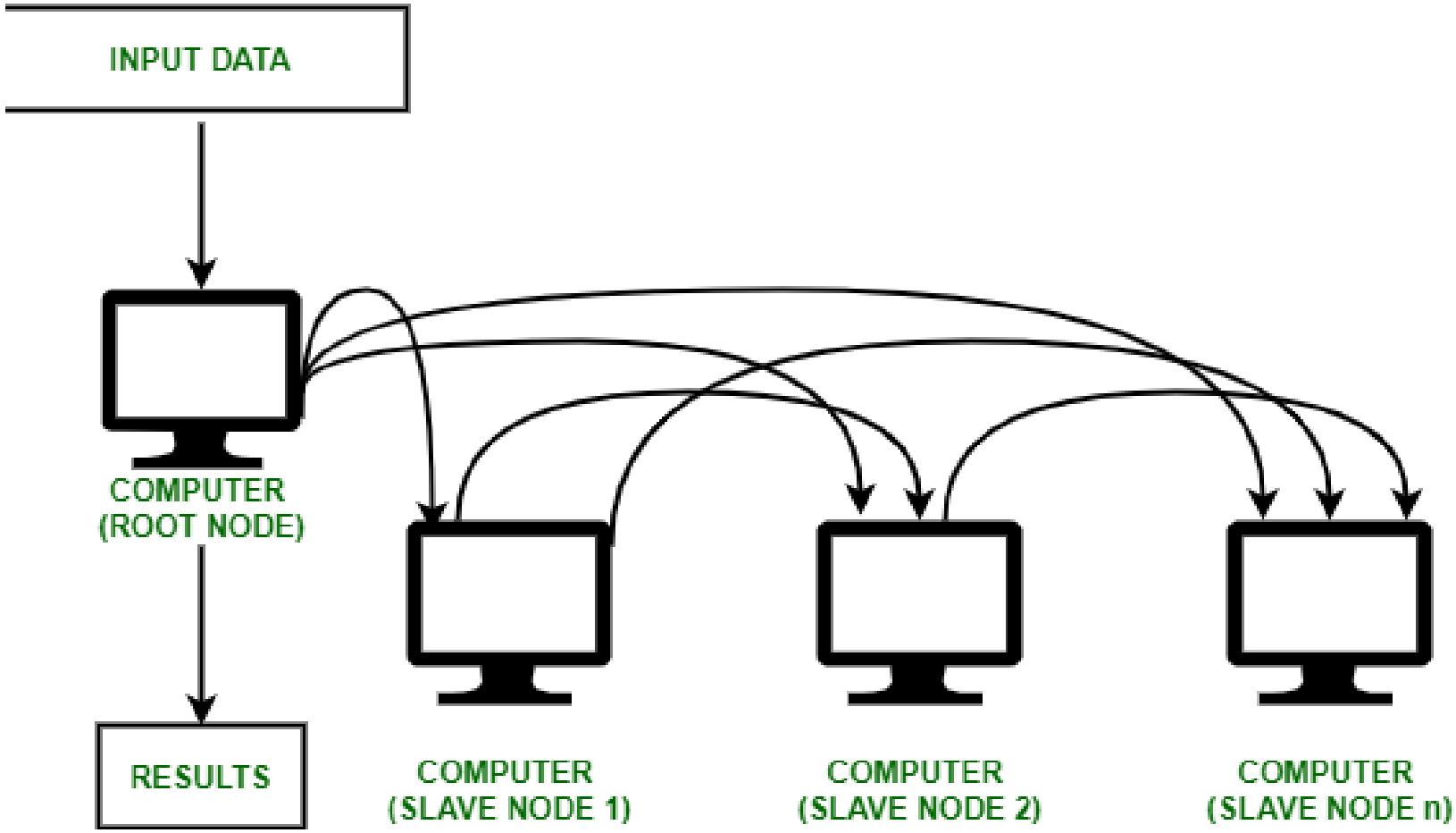
A tightly isolated software container with an operating system and application inside. Each self-contained VM is completely independent. Putting multiple VMs on a single computer enables several operating systems and applications to run on just one physical server, or “host.”

# 1970s: ARPANET

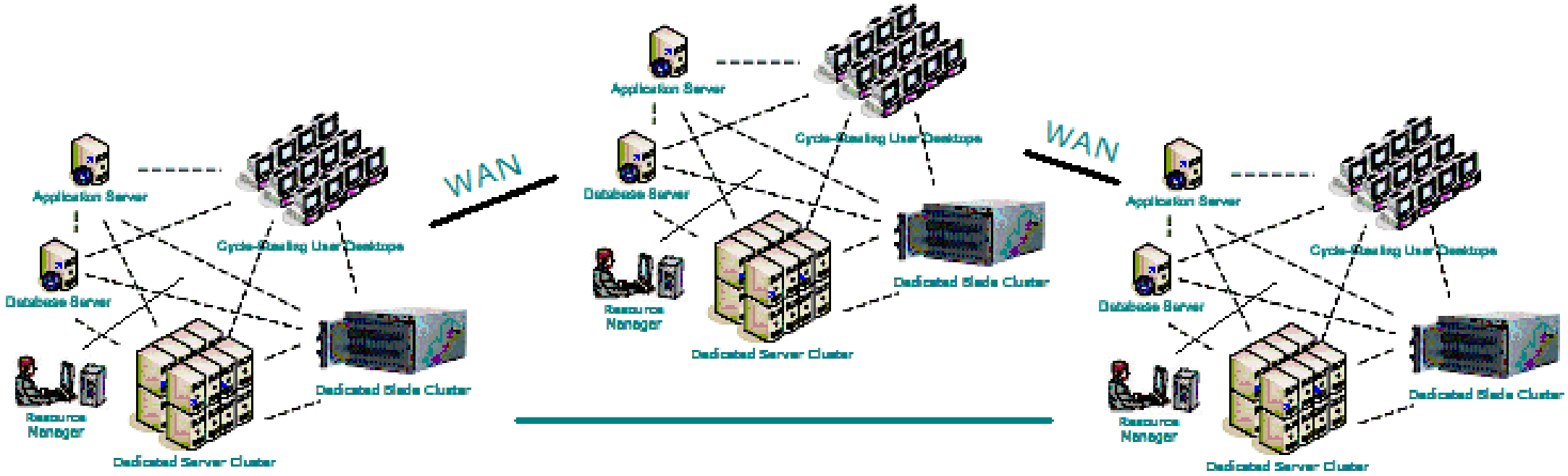



Gave birth to Internet

# 1980s: Cluster Computing



# 1990s: Grid Computing

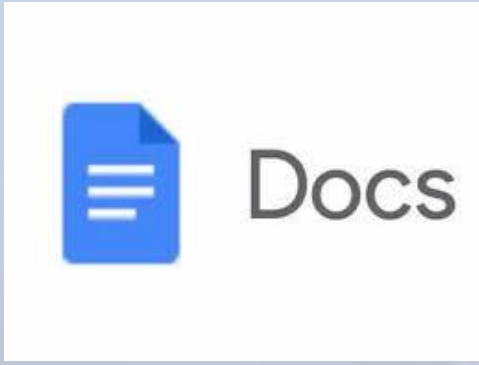


# Quick jumps

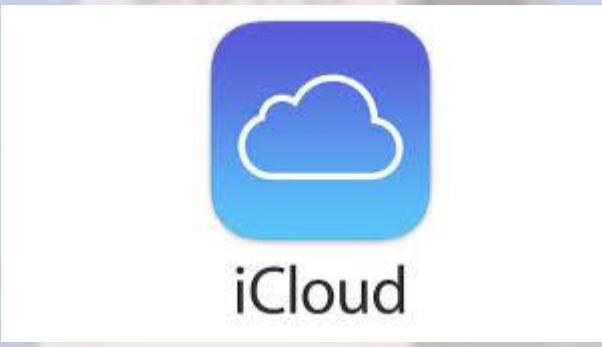
Prof. Ramnath K. Chellappa, PhD

- 1997: The term cloud computing used by Prof. Ramnath Cl
- 1999: In 1999, **Salesforce.com** started delivering of applications to users using a simple website
- 2006: Amazon launched Elastic Compute Cloud (EC2)
- 2006: Google Doc Services
- 2009: Google Apps also started to provide cloud computing enterprise applications.









# Cloud Computing

*"...a style of computing in which scalable and elastic IT-enabled capabilities are delivered as a service to external customers using Internet technologies."*

Gartner

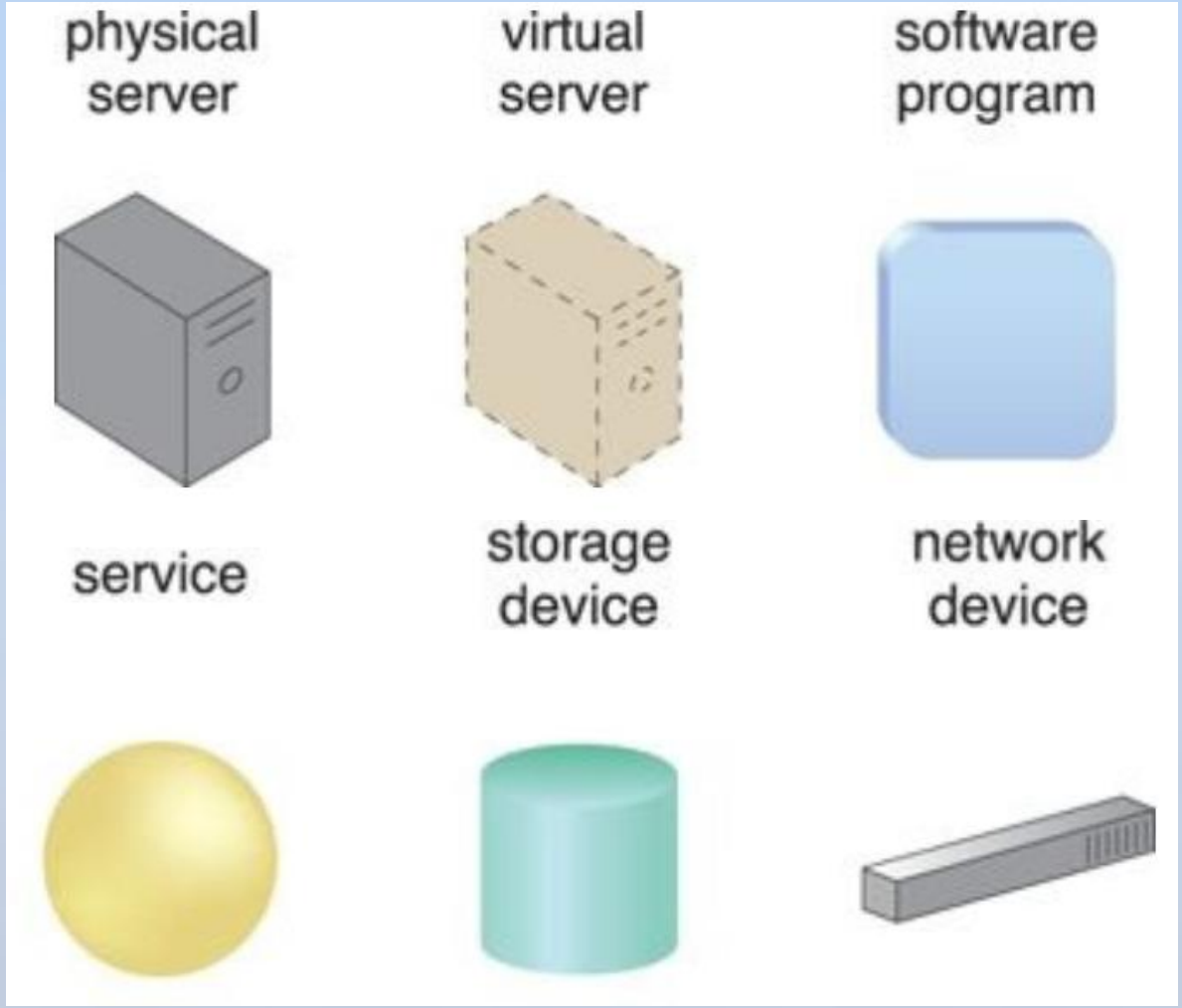
*"...a standardized IT capability (services, software, or infrastructure) delivered via Internet technologies in a pay-per-use, self-service way."*

Forrester Research

*"Cloud computing is a specialized form of distributed computing that introduces utilization models for remotely provisioning scalable and measured resources."*

National Institute of Standards and Technology

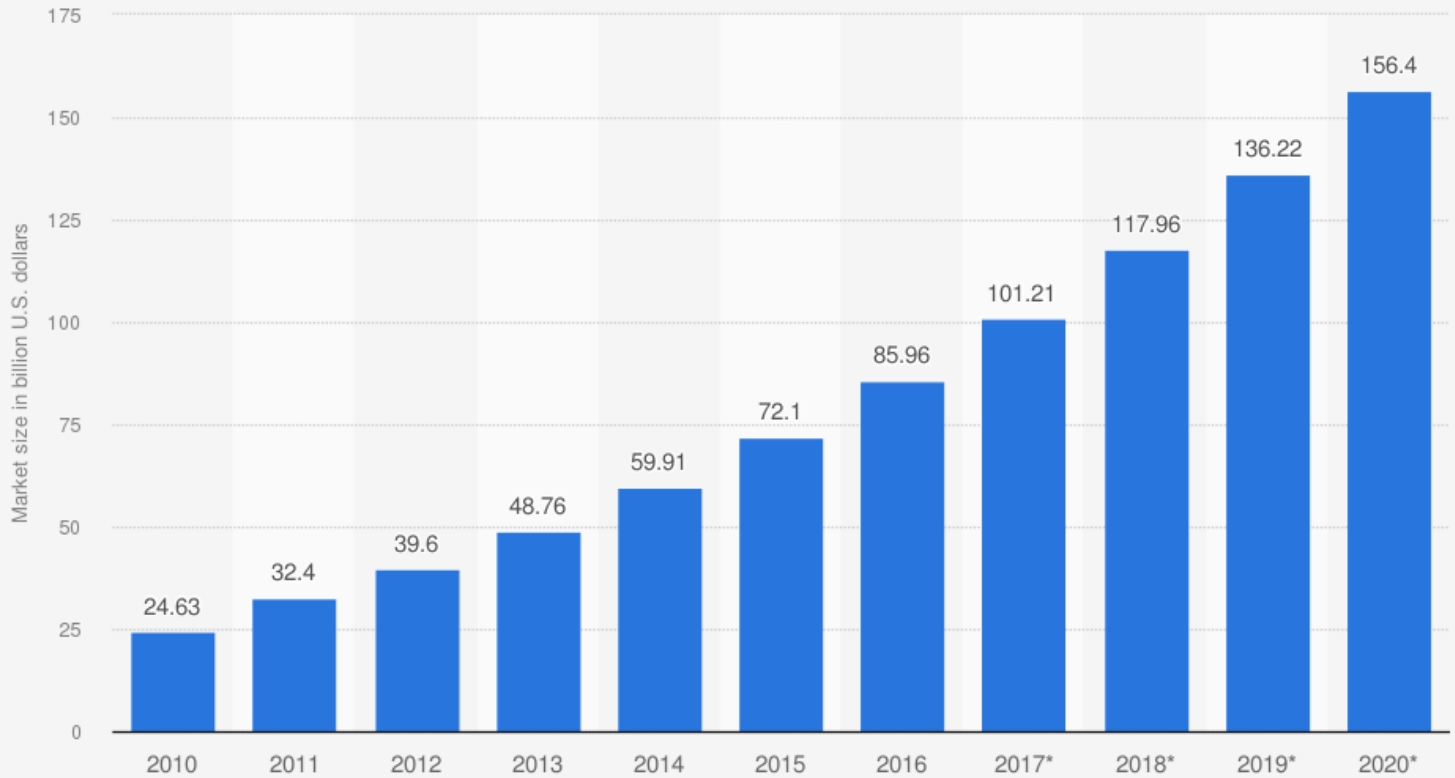
# IT Resources




# Provisioning

Cloud provisioning is the allocation of a cloud provider's resources and services to a customer.

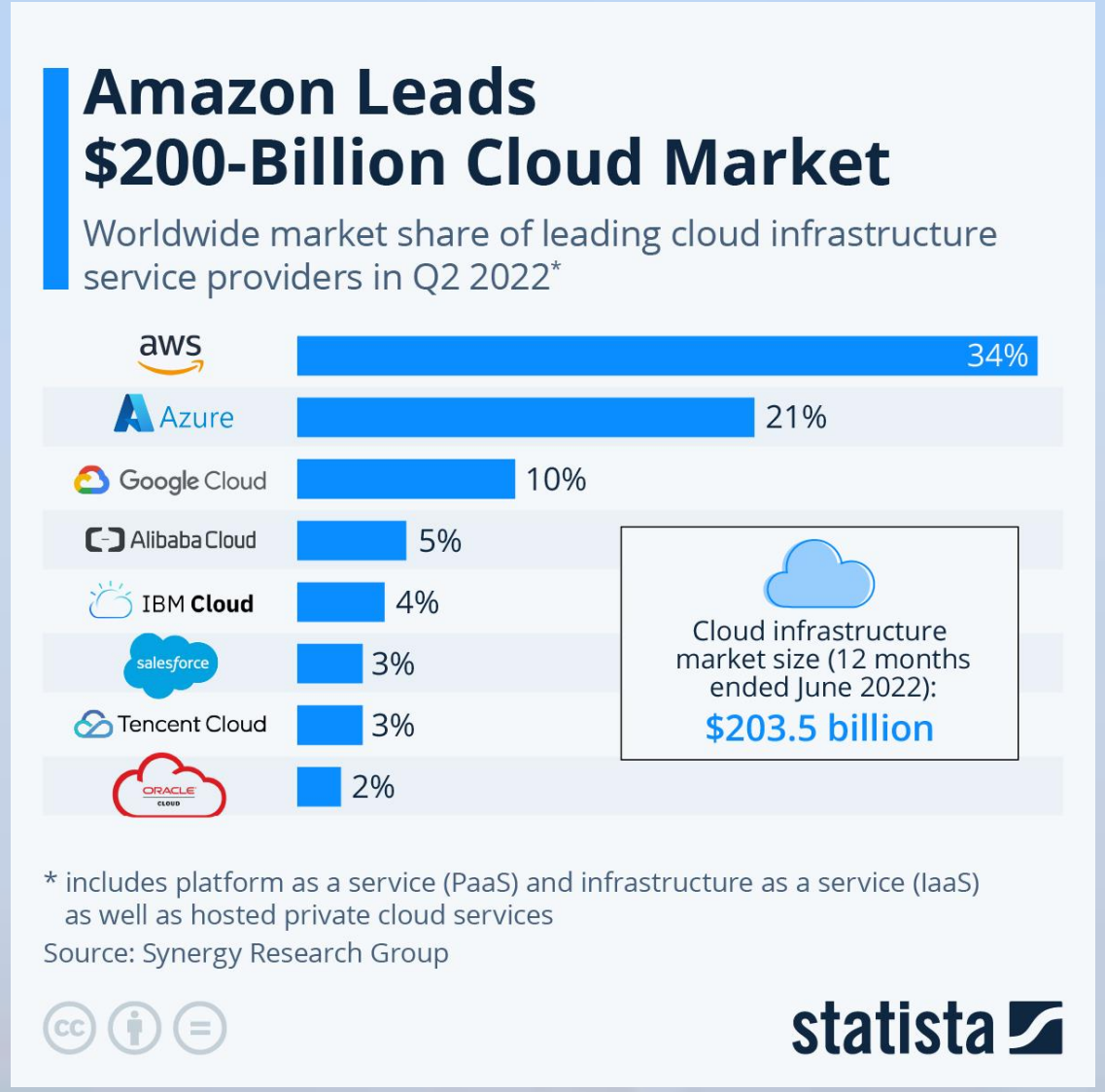
## Size of the cloud computing and hosting market market worldwide from 2010 to 2020 (in billion U.S. dollars)**




Source
451 Research


Additional Information:
Worldwide; 451 Research; 2010 to 2017

# Market Leaders



# Cloud Computing Fundamentals

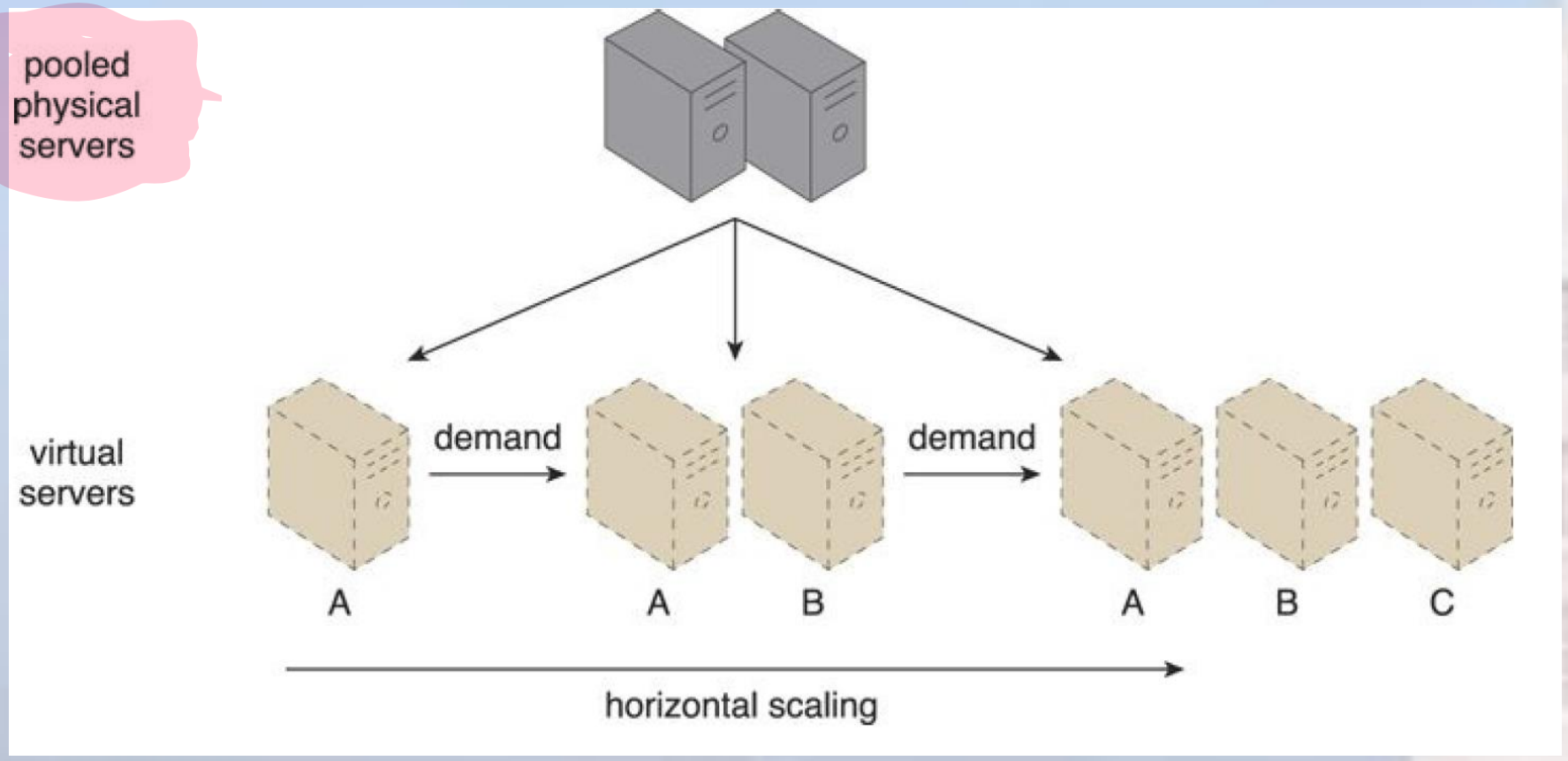
Dr. Deepak Saxena, SME IIT Jodhpur

# Basic Concepts and Terminology

- Cloud: refers to a distinct IT environment that is designed for the purpose of remotely provisioning scalable and measured IT resources.
- IT Resource: A physical or virtual IT-related artifact that can be either software-based, such as a virtual server or a custom software program, or hardware-based, such as a physical server or a network device.
- Scaling, from an IT resource perspective, represents the ability of the IT resource to handle increased or decreased usage demands.
  - Horizontal Scaling
  - Vertical Scaling

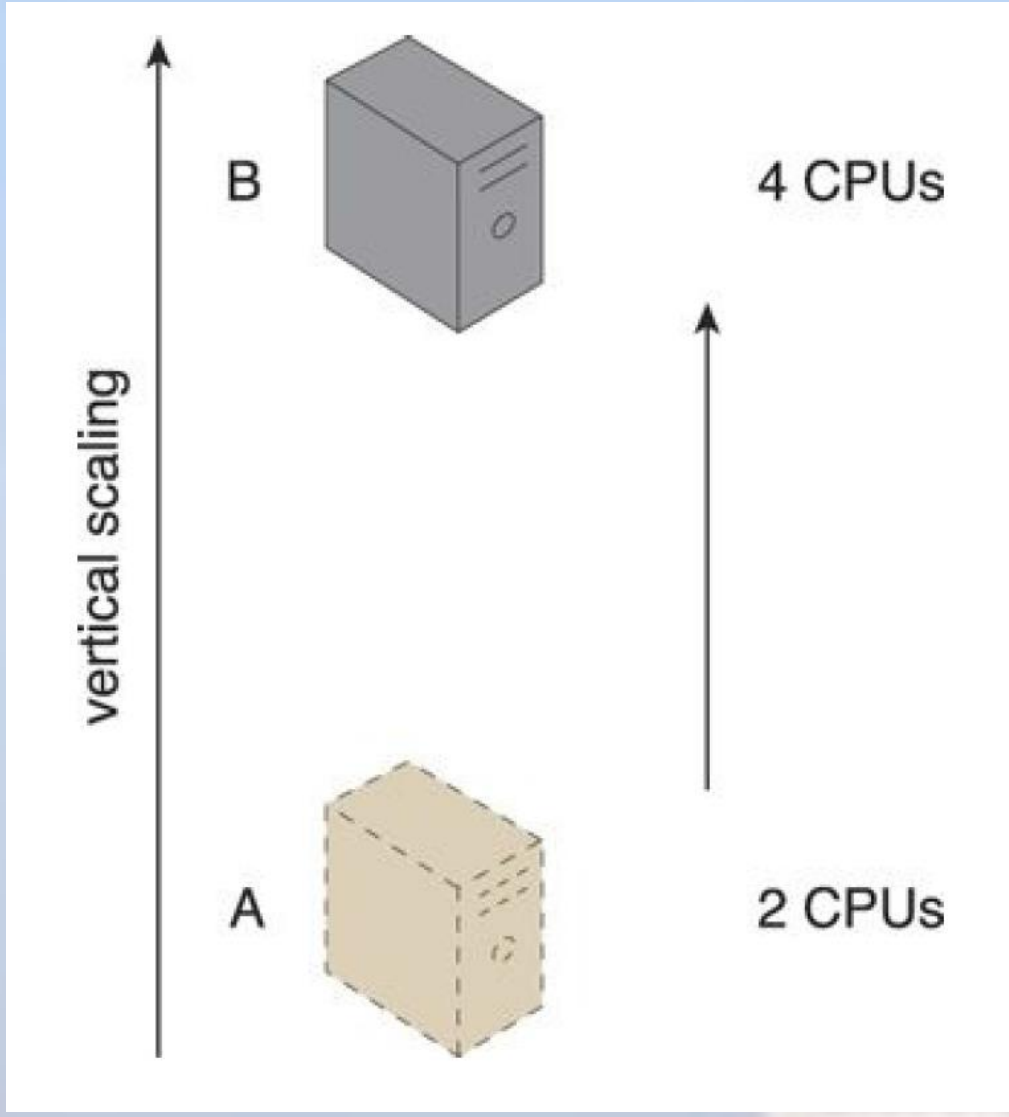
# Horizontal Scaling

- The allocating or releasing of IT resources that are of the same type.
- More common in cloud environments.



# Vertical Scaling

- When an existing IT resource is replaced by another with higher or lower capacity.
- Less common in cloud environments

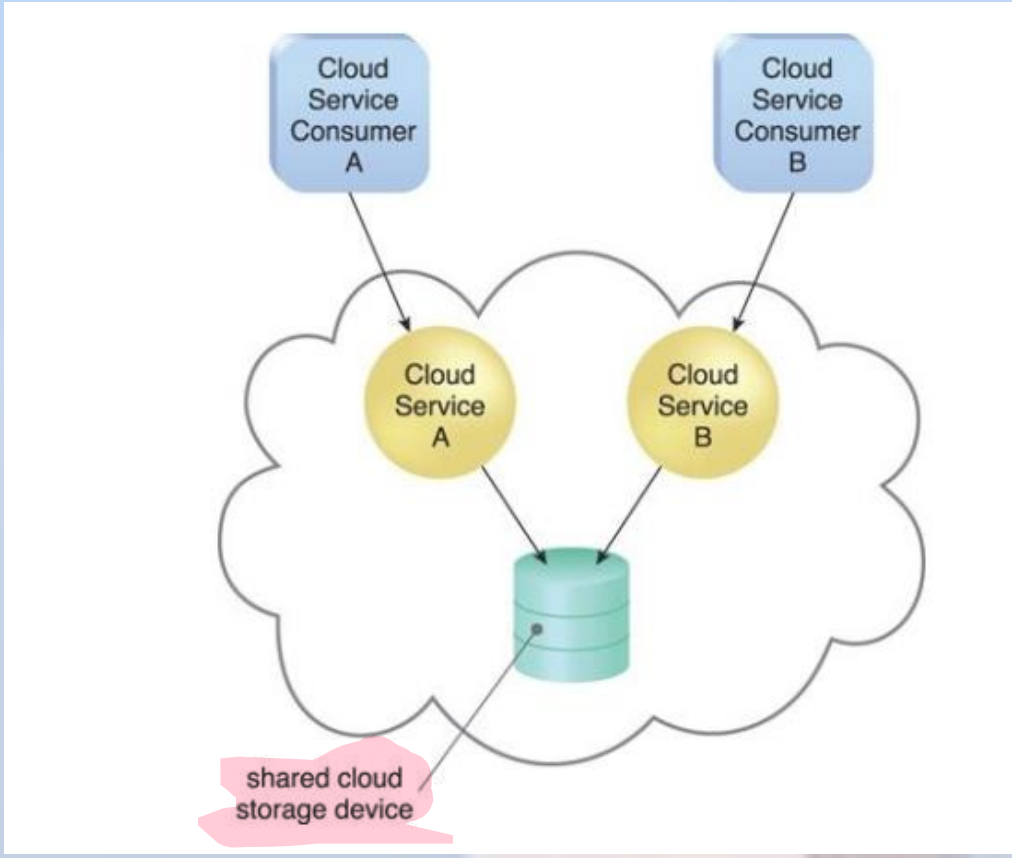


# Cloud Service

- A cloud service is any IT resource that is made remotely accessible via a cloud.
- Although a cloud is a remotely accessible environment, not all IT resources residing within a cloud can be made available for remote access.
- The driving motivation behind cloud computing is to provide IT resources as services that encapsulate other IT resources, while offering functions for client to use and leverage remotely.

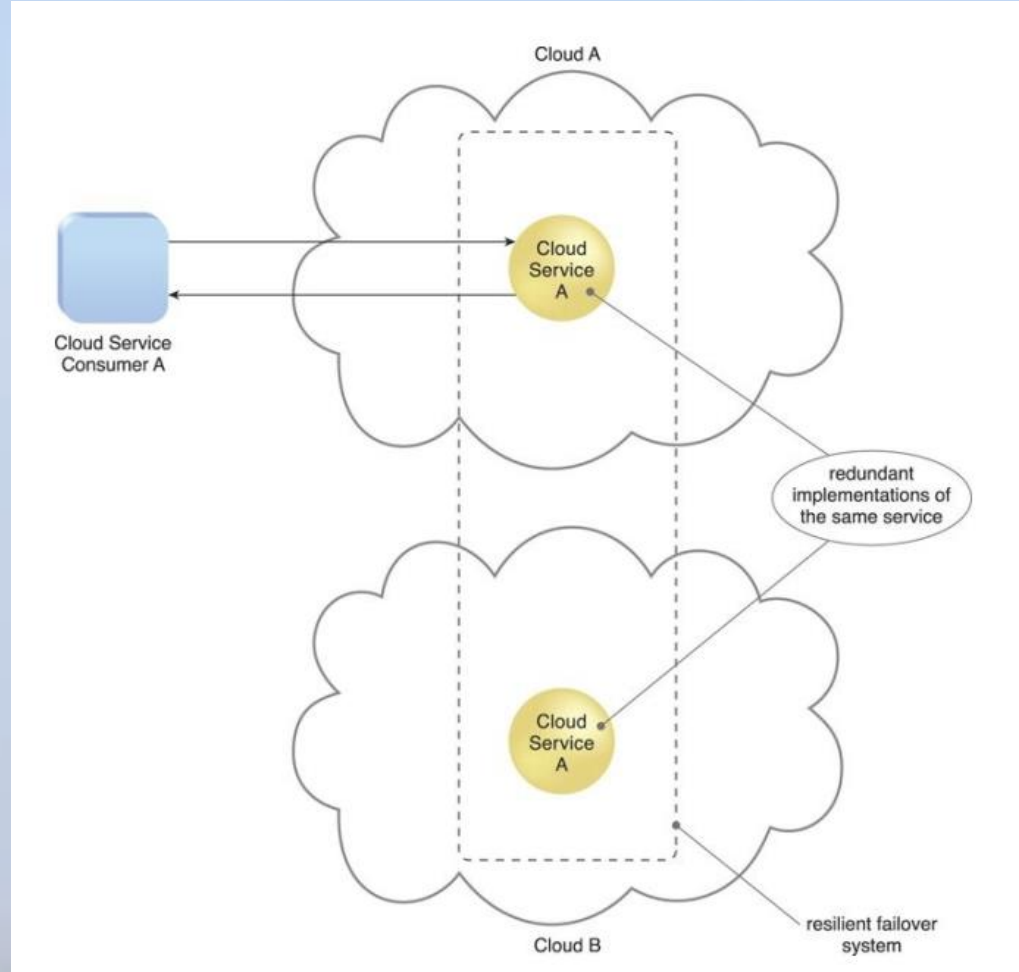
# Cloud Characteristics

- On-demand usage – self service provisioning
- Ubiquitous access – from anywhere
- Multitenancy (and resource pooling) – by cloud provider
- Elasticity – horizontal scaling
- Measured usage – keeping track of resource used
- Resiliency - redundant IT resources within the same cloud (but in different physical locations) or across multiple clouds



# Cloud Characteristics

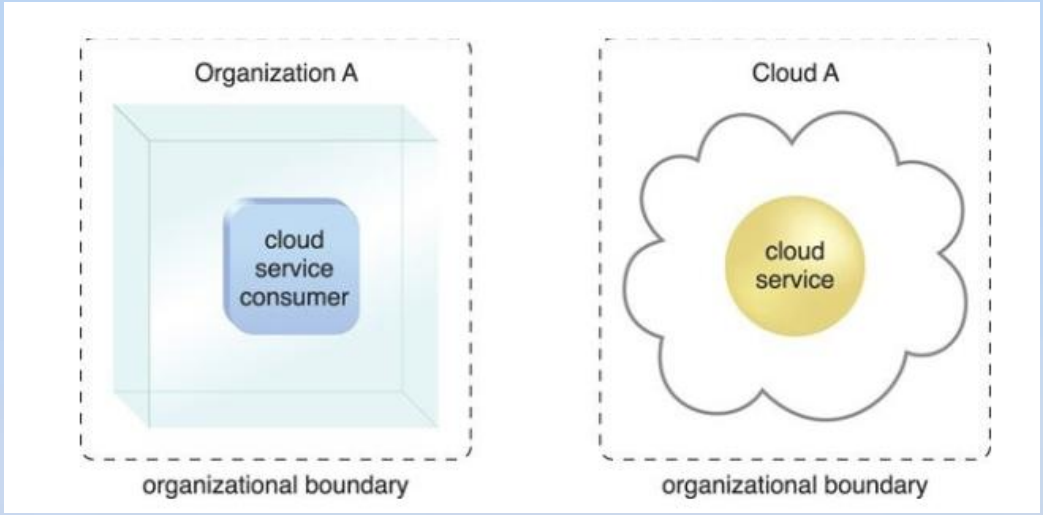
- On-demand usage – self service provisioning
- Ubiquitous access – from anywhere
- Multitenancy (and resource pooling) – by cloud provider
- Elasticity – horizontal scaling
- Measured usage – keeping track of resource used
- Resiliency - redundant IT resources within the same cloud (but in different physical locations) or across multiple clouds

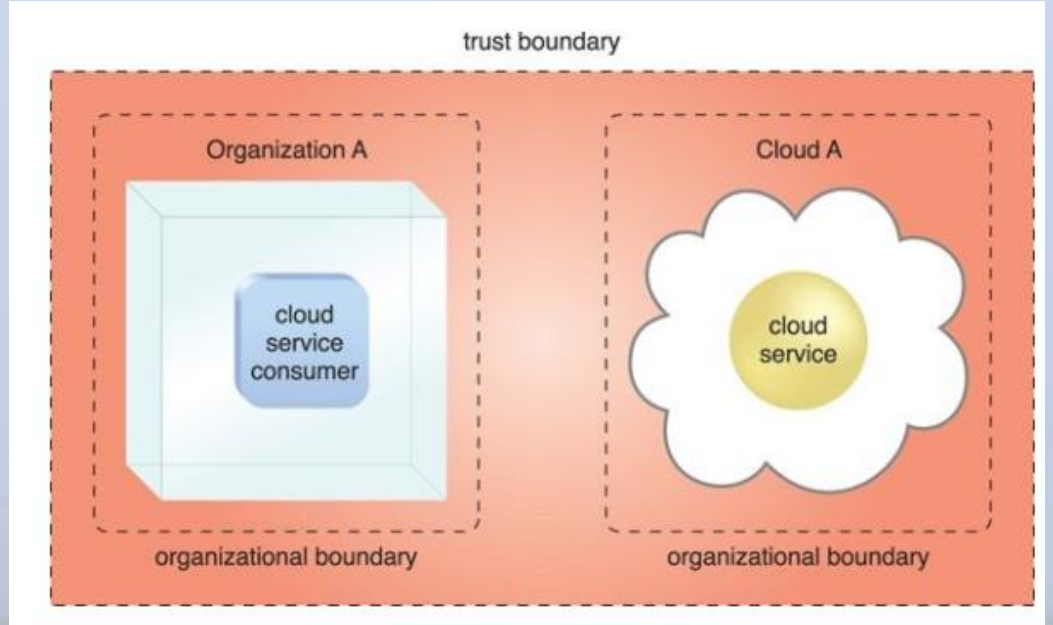


# Roles

- Cloud Provider: The organization that provides cloud-based IT resources
- Cloud consumer: an organization (or a human) that has a formal contract or arrangement with a cloud provider to use IT resources made available by the cloud provider
- Cloud resource administrator
  - The person or organization responsible for administering a cloud-based IT resource.
  - Can be (or belong to) the cloud consumer or cloud provider
  - Alternatively, it can be (or belong to) a third-party organization contracted to administer the cloud-based IT resource.

# Organisational Boundary vs Trust Boundary



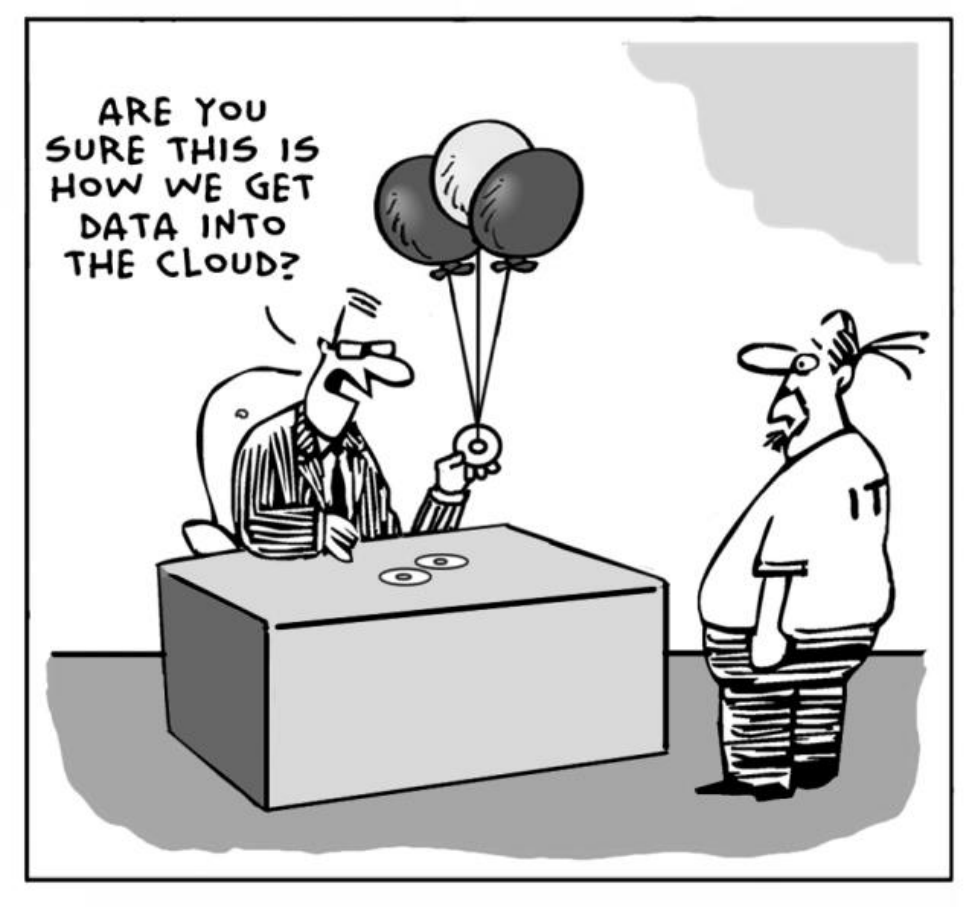
**Goals and Benefits**

- Reduced upfront Investments
- Proportional Costs
- Increased Scalability
- Increased Availability
- Increased Reliability

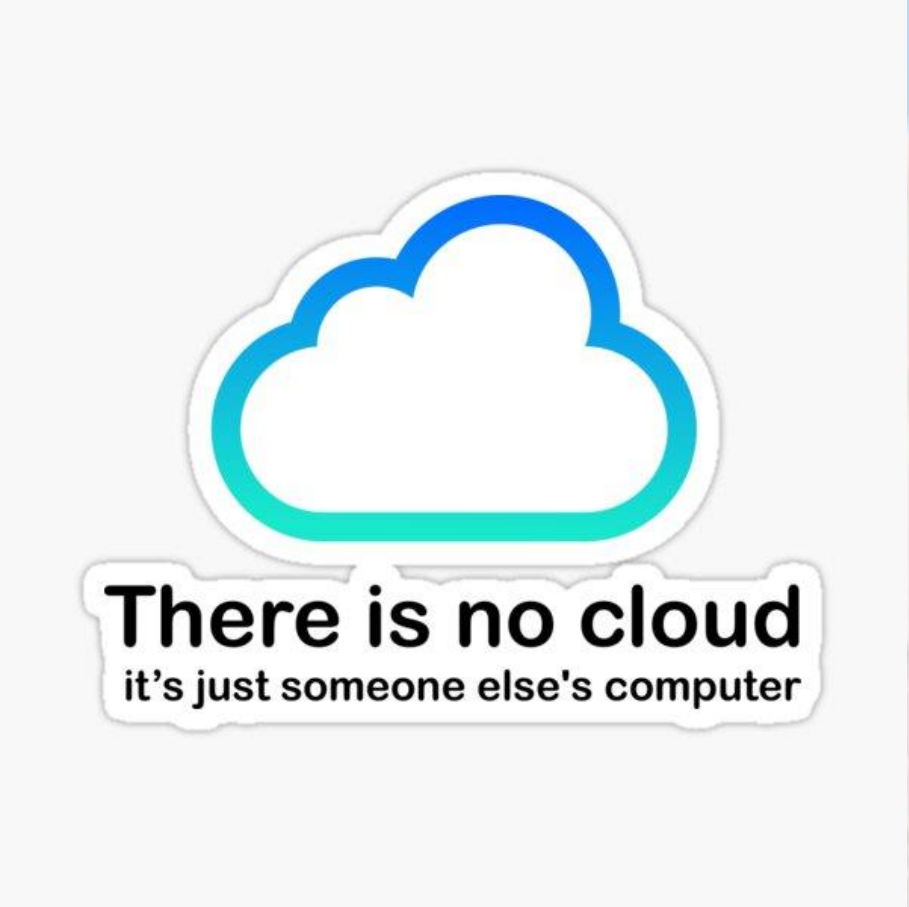
**Risks**

- Increased Security Vulnerabilities
- Reduced Operational Governance Control
- Limited Portability Between Cloud Providers
- Multi-Regional Compliance and Legal Issues

## What you don’t do…




## What you do but don’t say…



# Cloud Services Delivery Models

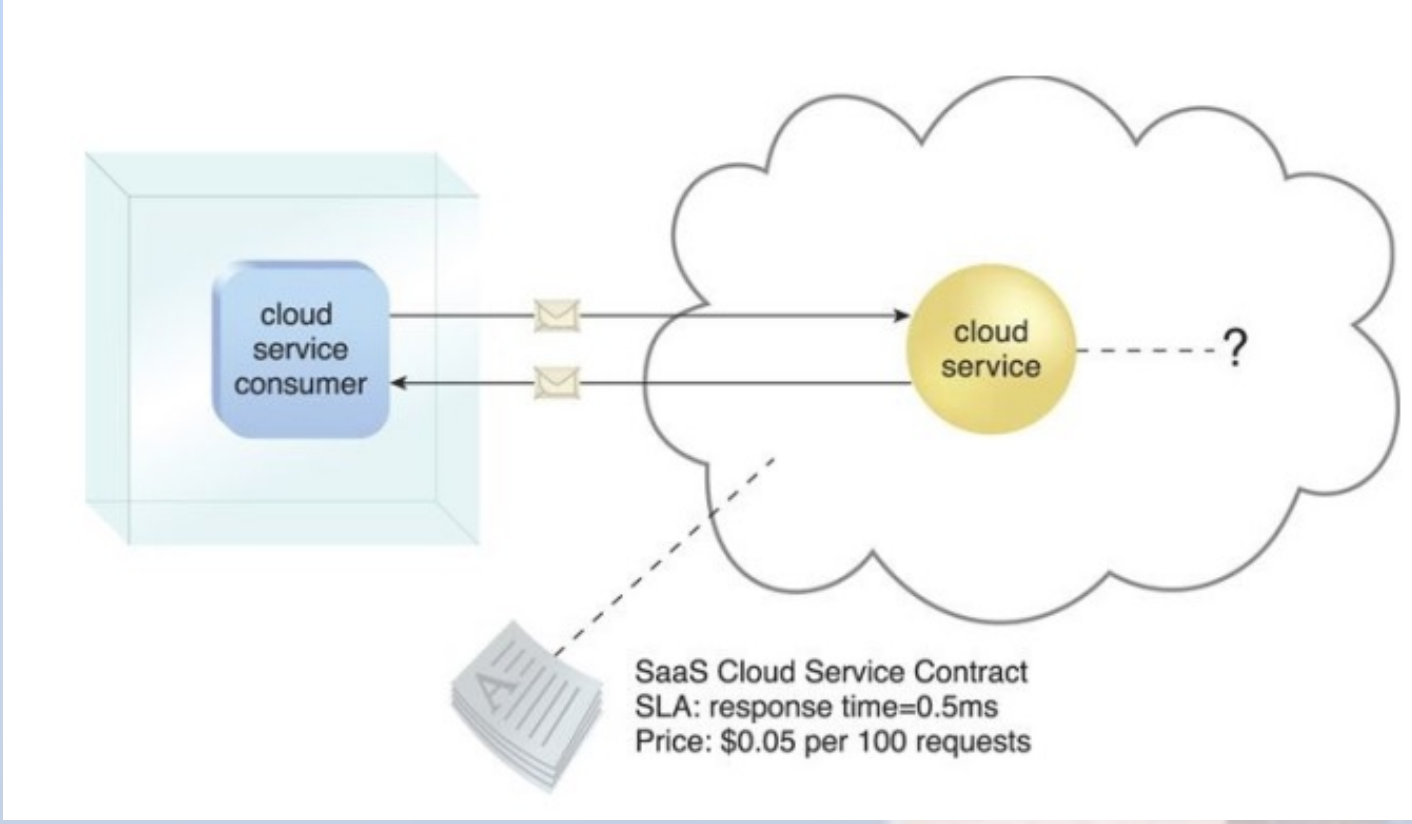
Dr. Deepak Saxena, SME IIT Jodhpur

# Cloud Delivery Models

- Software as a Service (SaaS)
- Platform as a Service (PaaS)
- Infrastructure as a Service (IaaS)

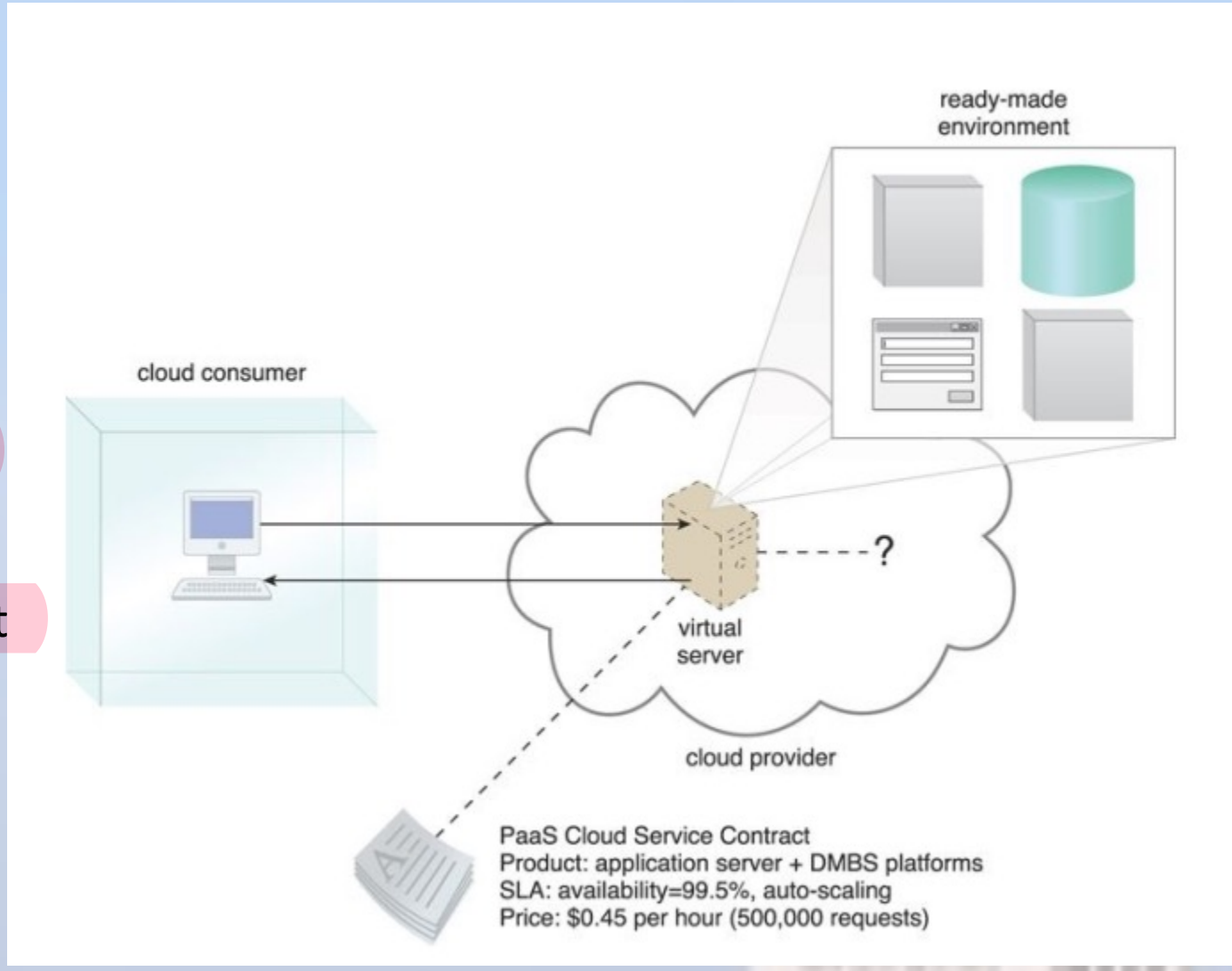
# SaaS

- A software program positioned as a shared cloud service and made available as a "product" or generic utility
- The SaaS delivery model is typically used to make a reusable cloud service widely available (often commercially) to a range of cloud consumers.
- Products: Google Workspace, Salesforce, Trello, Zoom, DocuSign, Slack.



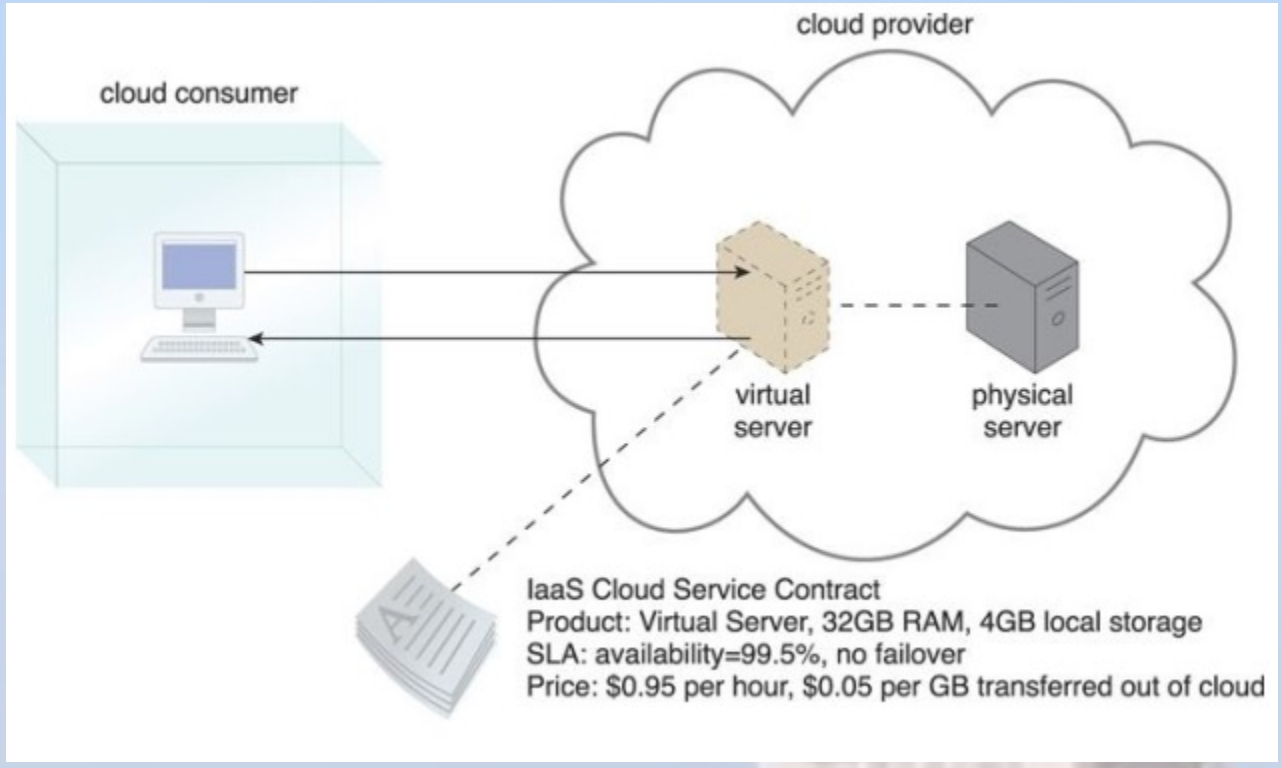
# PaaS

- A pre-defined “ready-to-use” environment typically comprised of already deployed and configured IT resources.
- PaaS relies on (and is primarily defined by) the usage of a readymade environment that establishes a set of pre-packaged products and tools used t support the entire delivery lifecycle of custom applications.
- Products: Google App Engine, AWS Elastic Beanstalk

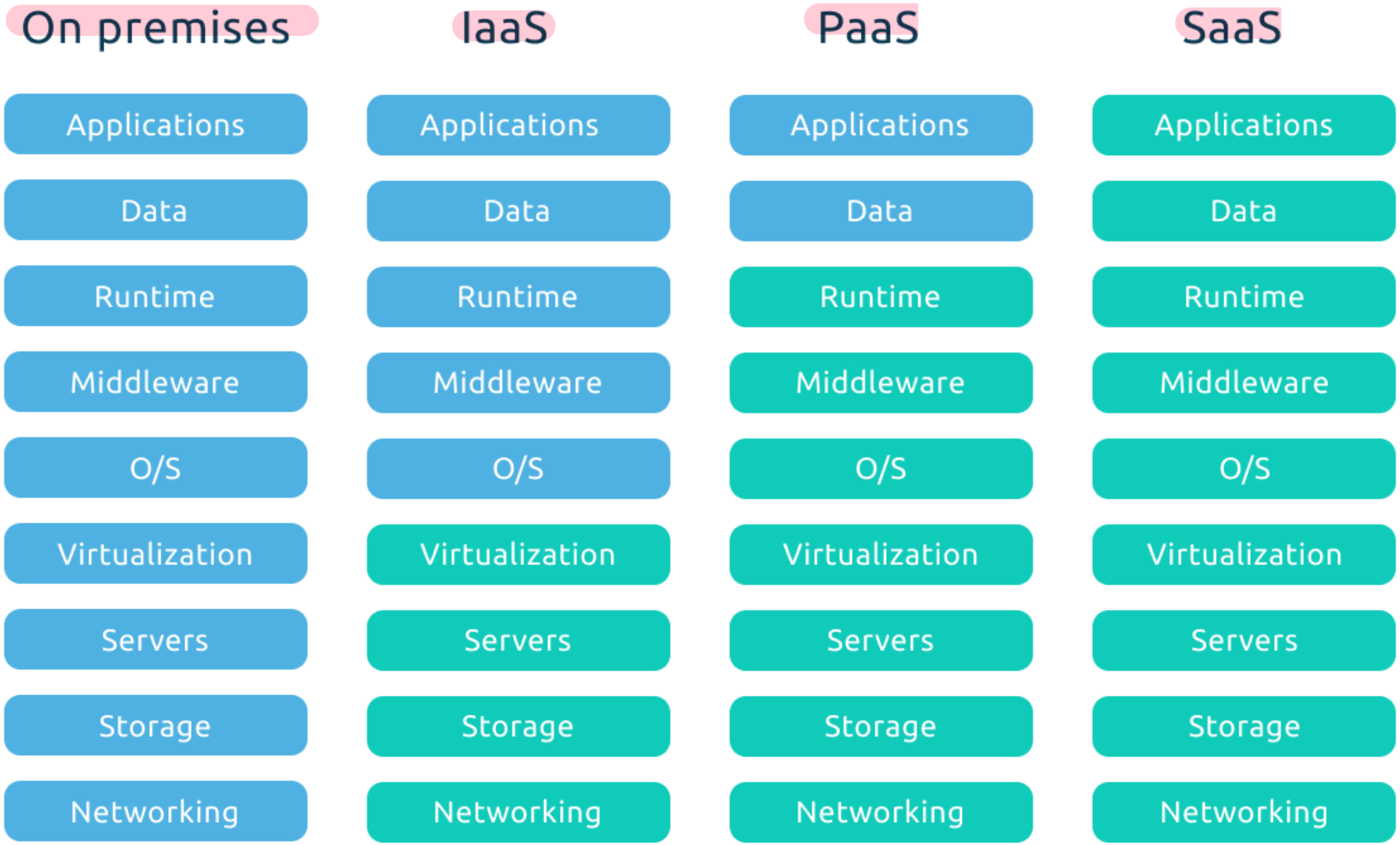


# IaaS

- A self-contained IT environment comprised of infrastructure-centric IT resources that can be accessed and managed via cloud service-based interfaces and tools.
- This environment can include hardware, network, connectivity, operating systems, and other “raw” IT resources.
- These IT resources are typically virtualized and packaged into bundles that simplify up-front runtime scaling and customization of the infrastructure.
- Products: Amazon EC2, Google Compute Engine, SAP Business Technology Platform



# Cloud Services Control Comparison




DigitalSkynet

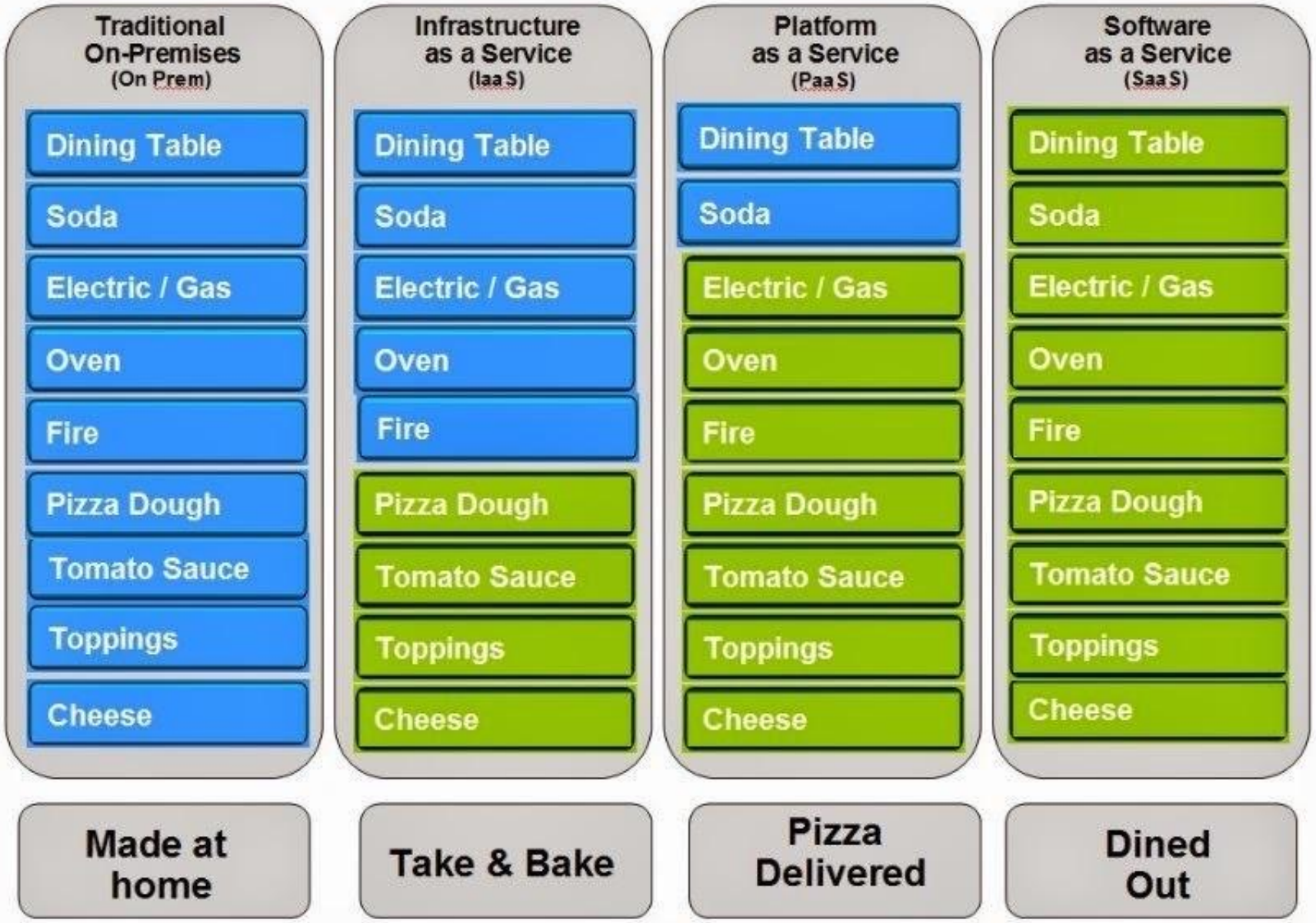
# A comparison of control levels in cloud delivery models

| Cloud Delivery Model | Typical Level of Control Granted to Cloud Consumer | Typical Functionality Made Available to Cloud Consumer |
|---|---|---|
| SaaS | usage and usage-related configuration | access to front-end user-interface |
| PaaS | limited administrative | moderate level of administrative control over IT resources relevant to cloud consumer's usage of platform |
| IaaS | full administrative | full access to virtualized infra-structure-related IT resources and, possibly, to underlying physical IT resources |

# Typical activities

| Cloud Delivery Model | Common Cloud Consumer Activities | Common Cloud Provider Activities |
|---|---|---|
| SaaS | uses and configures cloud service | implements, manages, and maintains cloud service<br><br>monitors usage by cloud consumers |
| PaaS | develops, tests, deploys, and manages cloud services and cloud-based solutions | pre-configures platform and provisions underlying infrastructure, middleware, and other needed IT resources, as necessary<br><br>monitors usage by cloud consumers |
| IaaS | sets up and configures bare infrastructure, and installs, manages, and monitors any needed software | provisions and manages the physical processing, storage, networking, and hosting required<br><br>monitors usage by cloud consumers |

# Pizza as a Service



॥ त्वं ज्ञानमयो विज्ञानमयोऽसि ॥
IIT Jodhpur

Excellence above all
SME

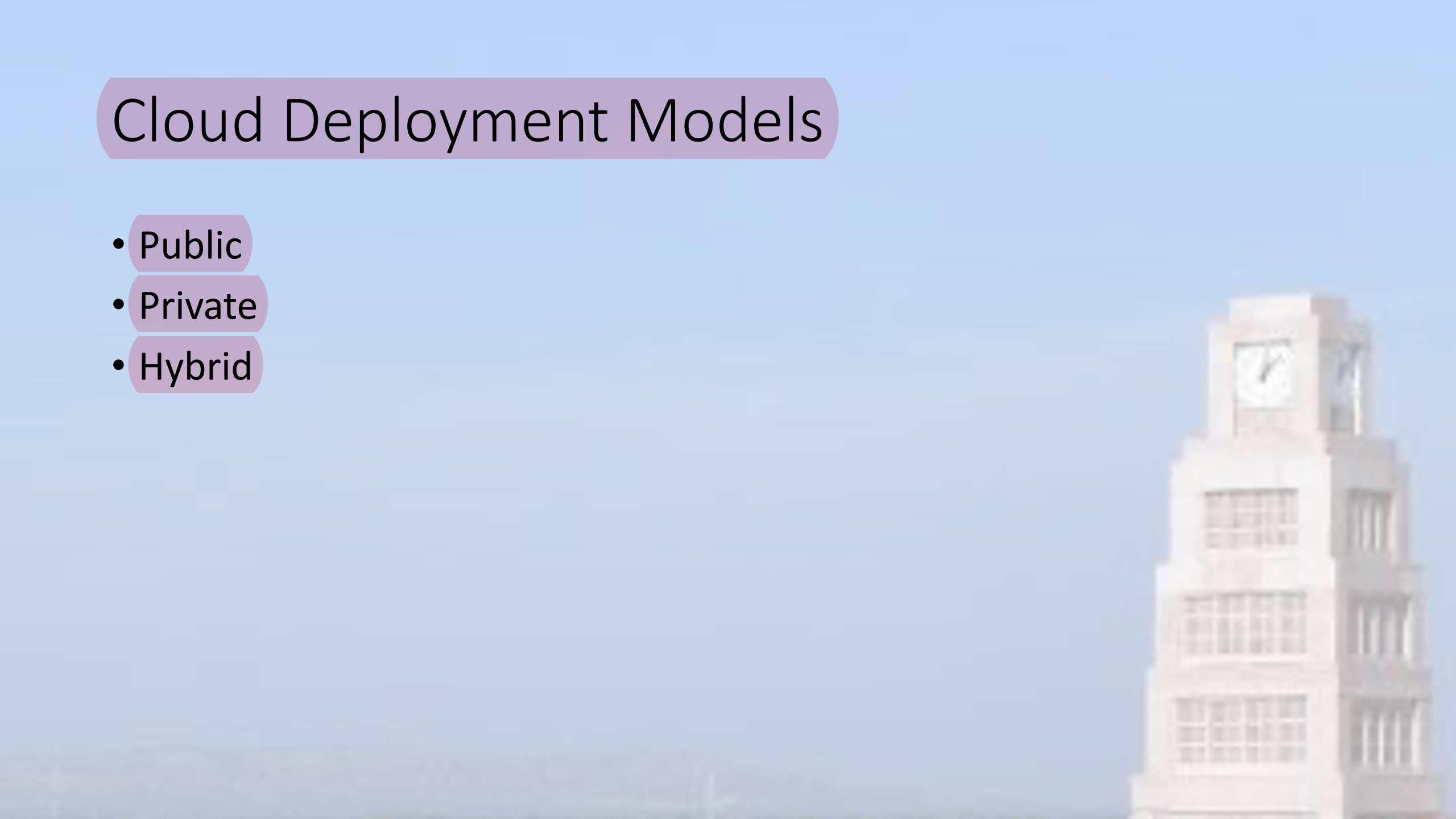
Technology • Innovation • Leadership

# Cloud Deployment Models

Dr. Deepak Saxena, SME IIT Jodhpur

# Cloud Deployment Models

- Public
- Private
- Hybrid



# Public Cloud

- Public clouds are the most common type of cloud computing deployment.
- The cloud resources (like servers and storage) are owned and operated by a third-party cloud service provider and delivered over the internet.
- With a public cloud, all hardware, software, and other supporting infrastructure are owned and managed by the cloud provider.
- Example: AWS, GCP, Microsoft Azure

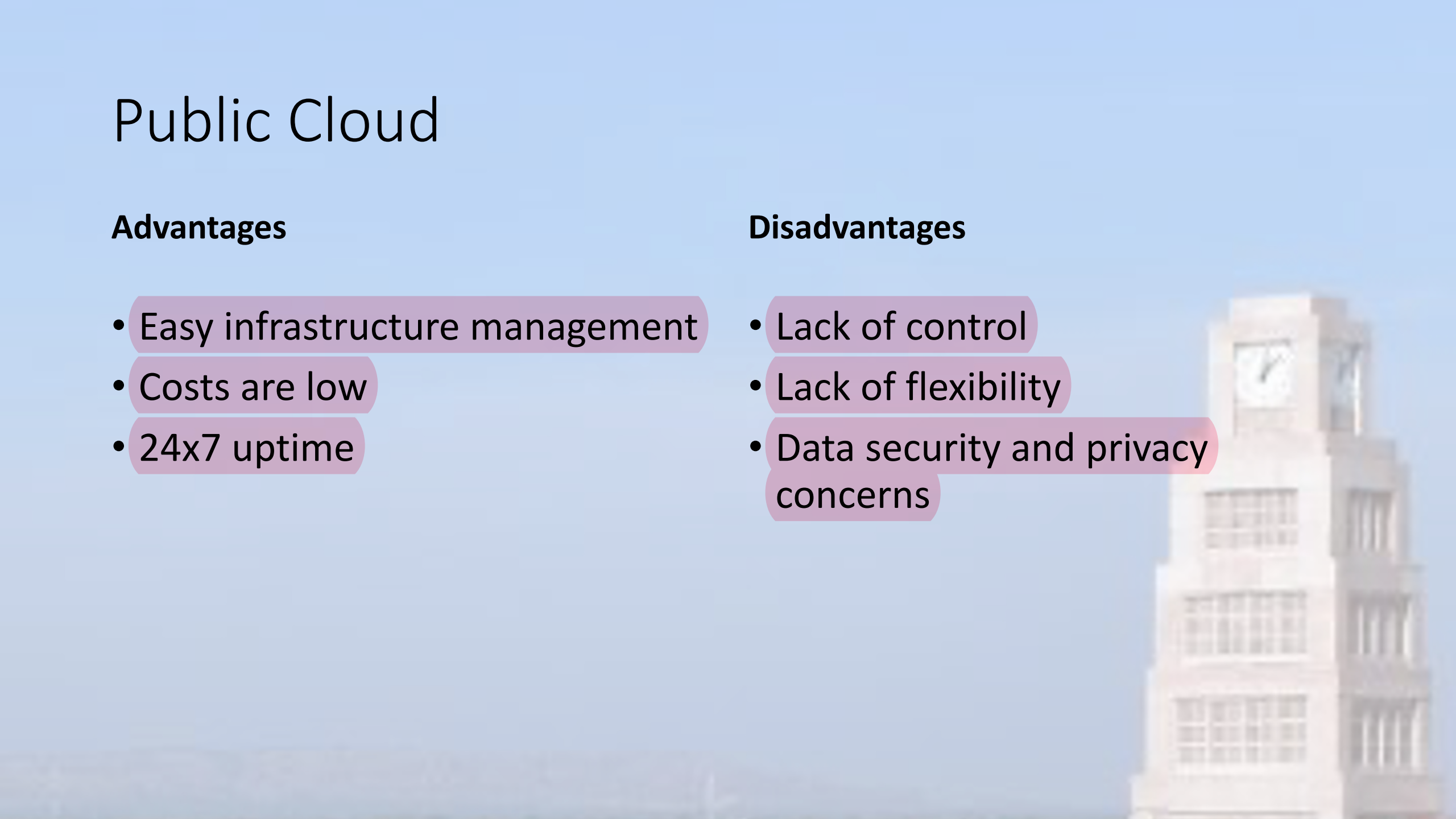
# Public Cloud

**Advantages**

- Easy infrastructure management
- Costs are low
- 24x7 uptime

**Disadvantages**

- Lack of control
- Lack of flexibility
- Data security and privacy concerns



# Private Cloud

- A private cloud consists of cloud computing resources used exclusively by one business or organization.
- The private cloud can be physically located at your organization's on-site data center, or it can be hosted by a third-party service provider.
- But in a private cloud, the services and infrastructure are always maintained on a private network and the hardware and software are dedicated solely to your organization.
- Example: IITJ Cloud (internal), Amazon VPC, VMware, OpenStack (external)

# Types of Private Cloud

- *Virtual Private Cloud* – simply a virtual network dedicated to one organization or user in a public cloud.
- *Managed Private Cloud* – the hardware and software are owned by the organization. It can be on-premises or off-premises. However, the entire management, operation, and maintenance tasks of the cloud are outsourced to external private cloud providers.
- *Hosted Private Cloud* – cloud providers provide isolated servers in their data centers. The cloud provider is responsible for the hardware, software, network, and security of the infrastructure.
- *On-premises private cloud* – allows users to host servers locally in data centers.

# Private Cloud

**Advantages**

- Greater isolation and control
- Greater data security and integrity
- Easy compliance
- Greater bandwidth
- Scope for customization

**Disadvantages**

- High upfront cost
- Less elasticity
- Higher requirements for personnel

# Sovereign Cloud

- Designed and built to provide data access in compliance with local laws and regulations.
- A sovereign cloud service provider will ensure that each subscriber's data — including their metadata — is protected from foreign access and stored in compliance with the originating country's privacy mandates.

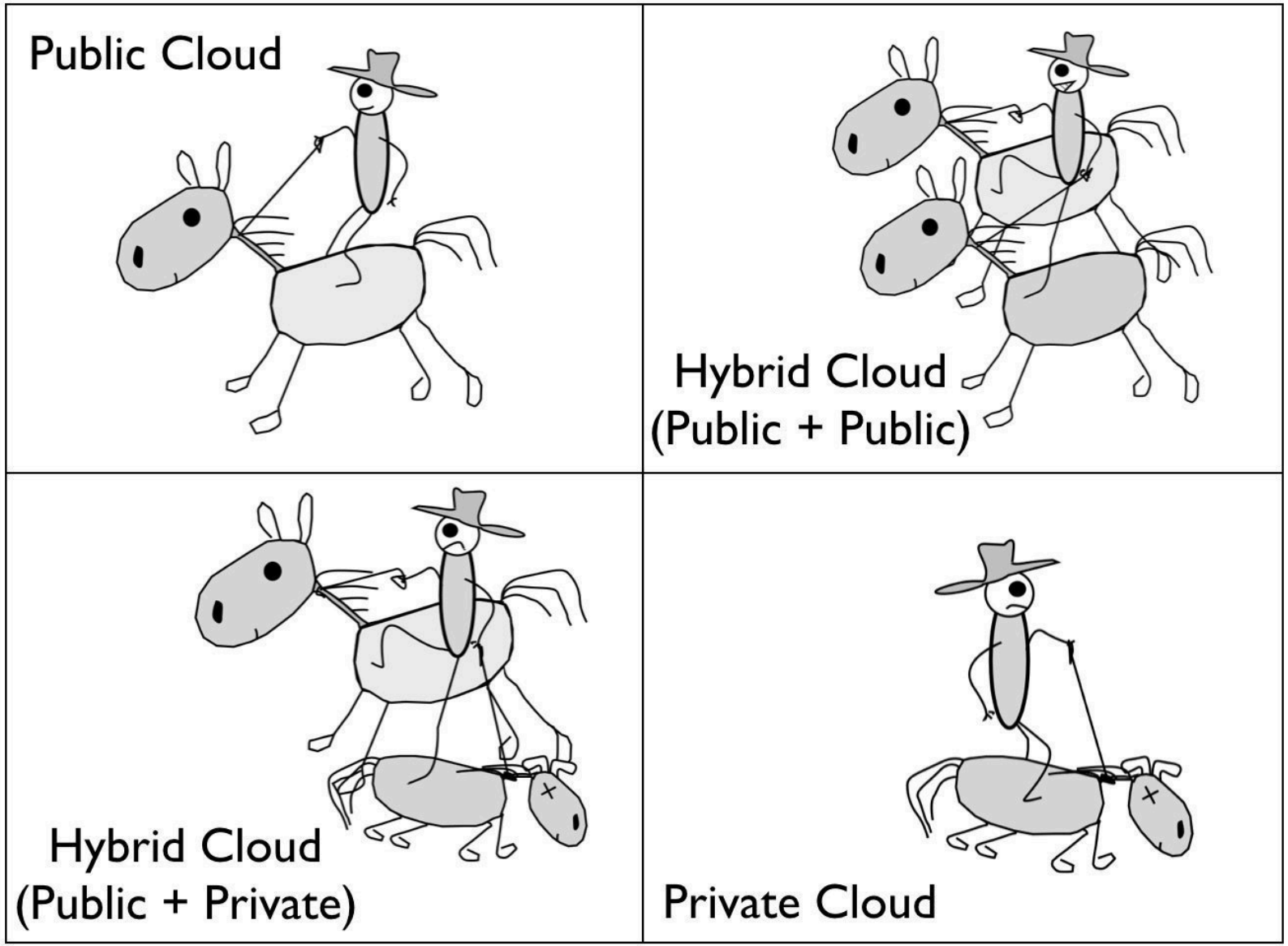
# Hybrid Cloud

- A hybrid cloud is a type of cloud computing that combines on-premises infrastructure—or a private cloud—with a public cloud.
- Hybrid clouds allow data and apps to move between the two environments.
- The hybrid cloud is evolving to include edge workloads as well. Edge computing brings the computing power of the cloud to IoT devices—closer to where the data resides.

# Advantages of Hybrid Cloud

- Control – the organization can maintain a private infrastructure for sensitive assets or workloads that require low latency.
- Flexibility – the organization can take advantage of additional resources in the public cloud when they need them.
- Cost-effectiveness – with the ability to scale to the public cloud, you pay for extra computing power only when needed.
- Ease – transitioning to the cloud doesn't have to be overwhelming because you can migrate gradually – phasing in workloads over time.

# Sometimes…


Public Cloud
Hybrid Cloud
(Public + Public)
Hybrid Cloud
(Public + Private)
Private Cloud
Simon Wardley CC3.0 BY-SA, extension of @adrianco "Roman Riding"

# The Business of Cloud

Dr. Deepak Saxena, SME IIT Jodhpur

# Cloud Provider Perspective

- Building cloud environment
  - OS, Memory, Processing, Backup capabilities
- Monitoring
  - Virtual server lifecycle, Data storage, Network traffic, Failure conditions, Event triggers
- Security
  - Encryption, hashing, digital signature, Identity and Access Management (IAM), SSO (Single sign on)
- Service
  - Service load balancing, Dynamic failure detection and recovery,  Storage maintenance, Elastic resource capability

# Cloud Consumer Perspective (IaaS)

- Controlling scalability features (automated scaling, load balancing)
- Controlling the lifecycle of virtual IT resources (shutting down, restarting, powering up of virtual devices)
- Controlling the virtual network environment and network access rules (firewalls, logical network perimeters)
- Establishing and displaying service provisioning agreements (account conditions, usage terms)
- Managing the pre-allocation of cloud-based IT resources (resource reservation)
- Managing credentials and passwords for cloud resource administrators
- Managing credentials for cloud-based security groups that access virtualized IT resources through an IAM
- Managing security-related configurations
- Managing customized virtual server image storage (importing, exporting, backup)
- Selecting high-availability options (failover, IT resource clustering)
- Selecting and monitoring SLA metrics
- Selecting basic software configurations (operating system, pre-installed software for new virtual servers)
- Selecting IaaS resource instances from a number of available hardware-related configurations and options (processing capabilities, RAM, storage)
- Selecting the geographical regions in which cloud-based IT resources should be hosted.
- Tracking and managing costs

# Cloud Consumer Perspective (PaaS)

- Establishing and displaying service provisioning agreements, such as account conditions and usage terms
- Selecting software platform and development frameworks for ready-made environments
- Selecting instance types, which are most commonly frontend or backend instances
- Selecting cloud storage devices for use in ready-made environments
- Controlling the lifecycle of PaaS-developed applications (deployment, starting, shutdown, restarting, and release)
- Controlling the versioning of deployed applications and modules
- Configuring availability and reliability-related mechanisms
- Managing credentials for developers and cloud resource administrators using IAM
- Managing general security settings, such as accessible network ports
- Selecting and monitoring PaaS-related SLA metrics
- Managing and monitoring usage and IT resource costs
- Controlling scalability features such as usage quotas, active instance thresholds, and the configuration and deployment of the automated scaling
- Listener and load balancer mechanisms

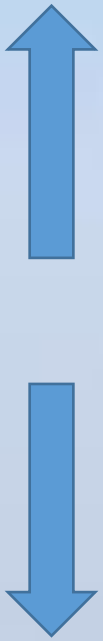
# Cloud Consumer Perspective (SaaS)

- Managing security-related configurations
- Managing select availability and reliability options
- Managing usage costs
- Managing user accounts, profiles, and access authorization
- Selecting and monitoring SLAs
- Setting manual and automated scalability options and limitations

# Business Cost Metrics

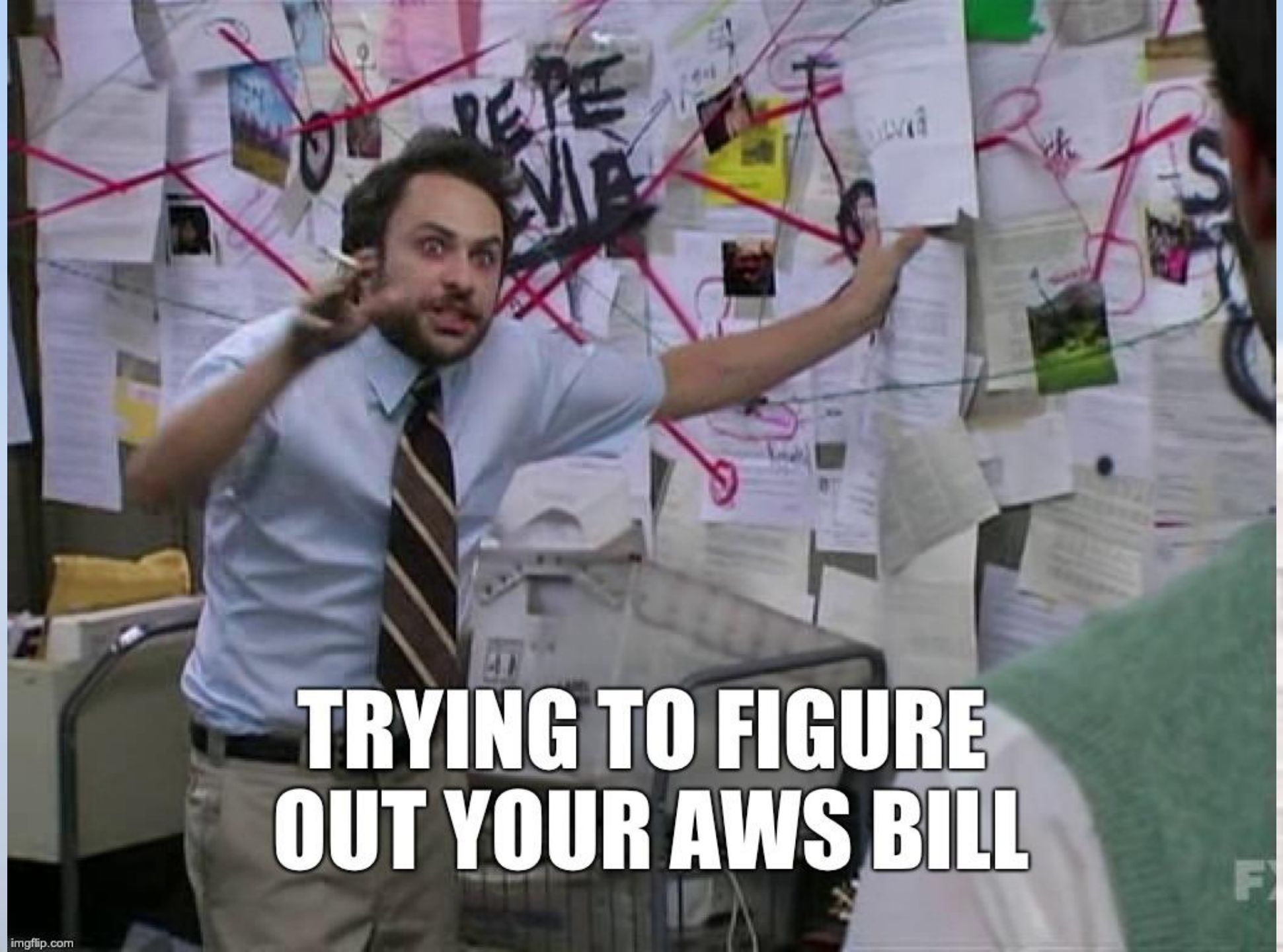
**On-Premise**

- Up-Front
  - Hardware
  - Software
  - Labor required for deployment.
- Ongoing
  - Licensing fees
  - Electricity
  - Insurance
  - Labor



**Cloud**

- Up-Front
  - labor costs required to assess and set up a cloud environment.
- Ongoing
  - Virtual hardware leasing fees,
  - Bandwidth usage fees
  - Licensing fees
  - Labor.


TRYING TO FIGURE
OUT YOUR AWS BILL
imgflip.com

# Some sample calculations

| Up-Front Costs | Cloud Environment | On-Premise Environment |
|---|---|---|
| Hardware | $0 | $15,000 |
| Licensing | $0 | $30,500 |
| Labor | $5,000 | $5,500 |
| **Total Up-Front Costs** | **$5,000** | **$51,000** |

| Monthly On-Going Costs | Cloud Environment | On-Premise Environment |
|---|---|---|
| Application Servers | $2,070 | $0 |
| Database Servers | $327 | $0 |
| WAN Network | $42 | $0 |
| Environment | $0 | $750 |
| Software Licensing | $0 | $520 |
| Hardware Maintenance | $0 | $100 |
| Administration | $800 | $2,600 |
| **Total On-Going Costs** | **$3,139** | **$3,970** |

In this case, company may decide moving to cloud.

Some sample calculations

| Up-Front Costs | Cloud Environment | On-Premise Environment |
|---|---|---|
| Hardware | $0 | $15,000 |
| Licensing | $0 | $15,200 |
| Labor | $45,000 | $5,500 |
| **Total Up-Front Costs** | **$45,000** | **$35,700** |

| Monthly On-Going Costs | Cloud Environment | On-Premise Environment |
|---|---|---|
| Application Servers | $3,420 | $0 |
| Database Servers | $1,635 | $0 |
| WAN Network | $80 | $0 |
| Environment | $0 | $1,050 |
| Software Licensing | $0 | $300 |
| Hardware Maintenance | $0 | $100 |
| Administration | $1,200 | $4,500 |
| **Total On-Going Costs** | **$6,335** | **$5,950** |

In this case, company may decide not moving to cloud.

# Cloud Usage Cost Metrics

- Network usage
- Server usage
- Cloud storage device
- Cloud service

# Network Usage

- Inbound
  - *Description* – inbound network traffic
  - *Measurement* – Σ, inbound network traffic in bytes
  - *Frequency* – continuous and cumulative over a predefined period
  - *Cloud Delivery Model* – IaaS, PaaS, SaaS
  - *Example* – up to 1 GB free, $0.001/GB up to 10 TB a month
- Outbound
  - *Description* – outbound network traffic
  - *Measurement* – Σ, outbound network traffic in bytes
  - *Frequency* – continuous and cumulative over a predefined period
  - *Cloud Delivery Model* – IaaS, PaaS, SaaS
  - *Example* – up to 1 GB free a month, $0.01/GB between 1 GB to 10 TB per month
- Intra-cloud

# Network Usage

- Intra-cloud
  - *Description* – network traffic between geographically diverse IT resources of the same cloud
  - *Measurement* – Σ, intra-cloud WAN traffic in bytes
  - *Frequency* – continuous and cumulative over a predefined period
  - *Cloud Delivery Model* – IaaS, PaaS, SaaS
  - *Example* – up to 500 MB free daily and $0.01/GB thereafter, $0.005/GB after 1 TB per month

# Server Usage

- On-demand Virtual Machine Instance Allocation
  - *Description* – uptime of a virtual server instance
  - *Measurement* – Σ, virtual server start date to stop date
  - *Frequency* – continuous and cumulative over a predefined period
  - *Cloud Delivery Model* – IaaS, PaaS
  - *Example* – $0.10/hour small instance, $0.20/hour medium instance, $0.90/hour large instance
- Reserved Virtual Machine Instance Allocation
  - *Description* – up-front cost for reserving a virtual server instance
  - *Measurement* – Σ, virtual server reservation start date to expiry date
  - *Frequency* – daily, monthly, yearly
  - *Cloud Delivery Model* – IaaS, PaaS
  - *Example* – $55.10/small instance, $99.90/medium instance, $249.90/large instance

# Cloud Storage device Usage

- On-demand storage space allocation
  - *Description* – duration and size of on-demand storage space allocation in bytes
  - *Measurement* – Σ, date of storage release / reallocation to date of storage allocation (resets upon change in storage size)
  - *Frequency* – continuous
  - *Cloud Delivery Model* – IaaS, PaaS, SaaS
- I/O Data Transferred Metric
  - *Description* – amount of transferred I/O data
  - *Measurement* – Σ, I/O data in bytes
  - *Frequency* – continuous
  - *Cloud Delivery Model* – IaaS, PaaS
  - *Example* – $0.10/TB

# Cloud Service Usage

- **Application Subscription Duration Metric**
  - *Description* – duration of cloud service usage subscription
  - *Measurement* – Σ, subscription start date to expiry date
  - *Frequency* – daily, monthly, yearly
  - *Cloud Delivery Model* – SaaS
  - *Example* – $69.90 per month
- **Number of Nominated Users Metric**
  - *Description* – number of registered users with legitimate access
  - *Measurement* – number of users
  - *Frequency* – monthly, yearly
  - *Cloud Delivery Model* – SaaS
  - *Example* – $0.90/additional user per month
- **Number of Transactions Users Metric**
  - *Description* – number of transactions served by the cloud service
  - *Measurement* – number of transactions (request-response message exchanges)
  - *Frequency* – continuous
  - *Cloud Delivery Model* – PaaS, SaaS
  - *Example* – $0.05 per 1,000 transactions

# Pricing as per model

- IaaS

  Pricing is usually based on IT resource allocation and usage, which includes the amount of transferred network data, number of virtual servers, and allocated storage capacity.

- PaaS

  Similar to IaaS, this model typically defines pricing for network data transferred, virtual servers, and storage. Prices are variable depending on factors such as software configurations, development tools, and licensing fees.

- SaaS

  Because this model is solely concerned with application software usage, pricing is determined by the number of application modules in the subscription, the number of nominated cloud service consumers, and the number of transactions.

# Exact pricing model depends upon many considerations

- Market competition and regulatory requirements
- Overhead incurred during the design, development, deployment, and operation of cloud services and other IT resources
- Opportunities to reduce expenses via IT resource sharing and data center optimization
- Negotiation

# Service Level Agreement (SLA)

- SLAs issued by cloud providers are human-readable documents that describe quality-of-service (QoS) features, guarantees, and limitations of one or more cloud-based IT resources.
- SLAs use service quality metrics (also called SLI – Service Level Indicators) to express measurable QoS characteristics.
  - *Availability* – up-time, outages, service duration
  - *Reliability* – minimum time between failures, guaranteed rate of successful responses
  - *Performance* – capacity, response time, and delivery time guarantees
  - *Scalability* – capacity fluctuation and responsiveness guarantees
  - *Resiliency* – mean-time to switchover and recovery

# Service Availability Metric

- Availability Rate Metric
  - *Description* – percentage of service up-time
  - *Measurement* – total up-time / total time
  - *Frequency* – weekly, monthly, yearly
  - *Cloud Delivery Model* – IaaS, PaaS, SaaS
  - *Example* – minimum 99.5% up-time
- Outage Duration Metric
  - *Description* – duration of a single outage
  - *Measurement* – date/time of outage end – date/time of outage start
  - *Frequency* – per event
  - *Cloud Delivery Model* – IaaS, PaaS, SaaS
  - *Example* – 1 hour maximum, 15 minute average

# Service Reliability Metric

- Mean-Time Between Failures (MTBF) Metric
  - *Description* – expected time between consecutive service failures
  - *Measurement* – Σ (start of downtime – start of uptime) / number of failures
  - *Frequency* – monthly, yearly
  - *Cloud Delivery Model* – IaaS, PaaS
  - *Example* – 90 day average
- Reliability Rate Metric
  - *Description* – percentage of successful service outcomes under pre-defined conditions
  - *Measurement* – total number of successful responses / total number of requests
  - *Frequency* – weekly, monthly, yearly
  - *Cloud Delivery Model* – SaaS
  - *Example* – minimum 99.5%

# Service Performance Metrics

| Metric | Definition | Applicable Models | Frequency | Example |
|---|---|---|---|---|
| Network Capacity | measurable characteristics of network capacity | IaaS, PaaS, SaaS | Continuous | 10 mbps |
| Storage Device Capacity | measurable characteristics of storage device capacity | IaaS, PaaS, SaaS | Continuous | 80 GB of storage |
| Server Capacity | measurable characteristics of server capacity | IaaS, PaaS | Continuous | 1 core at 1.7 GHz, 16 GB of RAM, 80 GB of storage |
| Web Application Capacity | measurable characteristics of Web application capacity | SaaS | Continuous | Maximum 100,000 requests per minute |
| Instance Starting Time | length of time required to initialize a new instance | IaaS, PaaS | Per event | 5 minute maximum, 3 minute average |
| Response Time | time required to perform synchronous operation | SaaS | daily, weekly, monthly | 5 millisecond average |
| Completion Time | time required to complete an asynchronous task | PaaS, SaaS | daily, weekly, monthly | 1 second average |

# Service Scalability Metrics

| Metric | Definition | Applicable Models | Frequency | Example |
|---|---|---|---|---|
| Storage Scalability (Horizontal) | permissible storage device capacity changes in response to increased workloads | IaaS, PaaS, SaaS | Continuous | 1,000 GB maximum (automated scaling) |
| Server Scalability (Horizontal) | permissible server capacity changes in response to increased workloads | IaaS, PaaS | Continuous | 1 virtual server minimum, 10 virtual server maximum (automated scaling) |
| Server Scalability (Vertical) | permissible server capacity fluctuations in response to workload fluctuations | IaaS, PaaS | Continuous | 512 core maximum, 512 GB of RAM |

# Service Resiliency Metrics

| Metric | Definition | Applicable Models | Frequency | Example |
|---|---|---|---|---|
| Mean-Time to Switchover (MTSO) | the time expected to complete a switchover from a severe failure to a replicated instance in a different geographical area | IaaS, PaaS, SaaS | monthly, yearly | 10 minutes average |
| Mean-Time System Recovery (MTSR) | time expected for a resilient system to perform a complete recovery from a severe failure | IaaS, PaaS, SaaS | monthly, yearly | 120 minutes average |

# Some Example SLAs

- AWS
- Google Cloud Platform
- Azure
- IBM

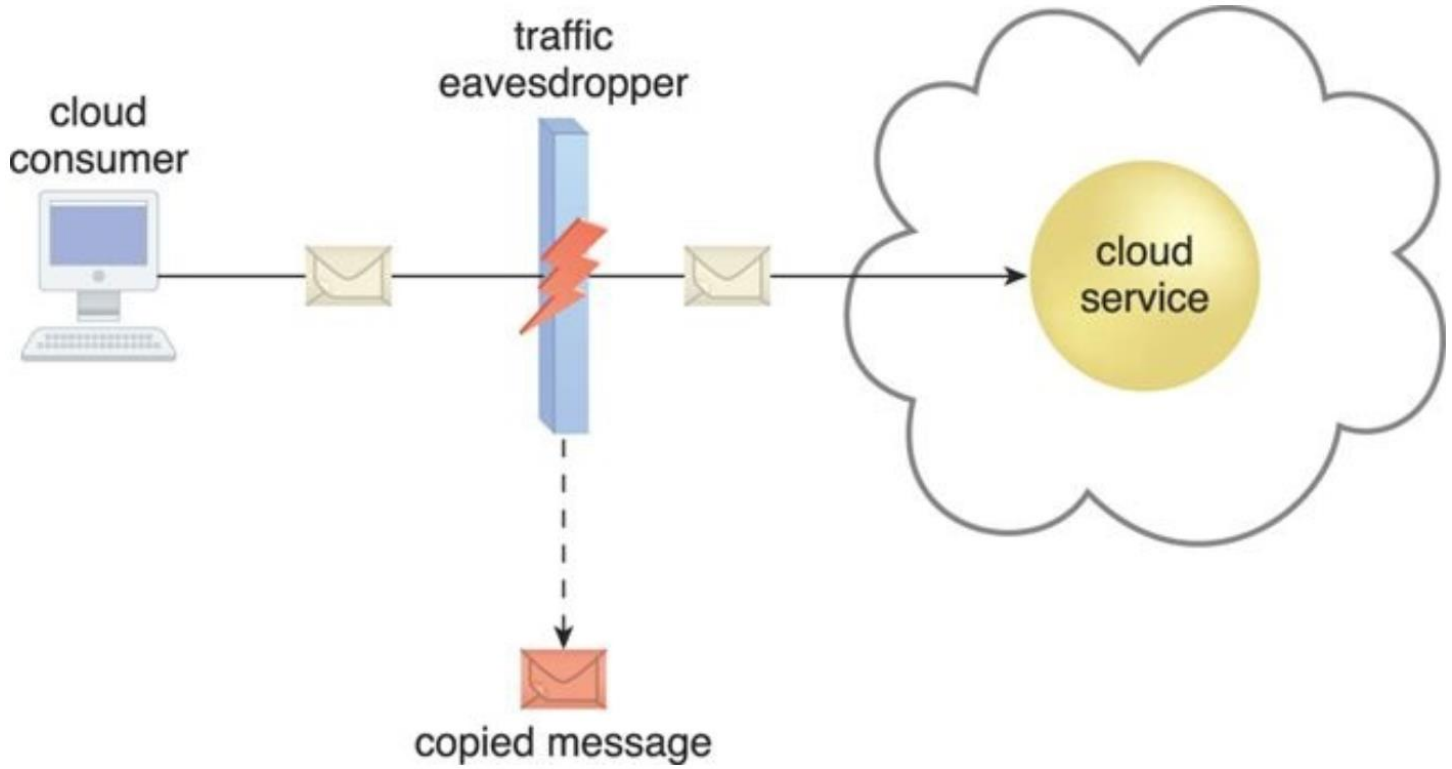
# Cloud Security

Dr. Deepak Saxena, SME IIT Jodhpur

# Cloud Security Threats

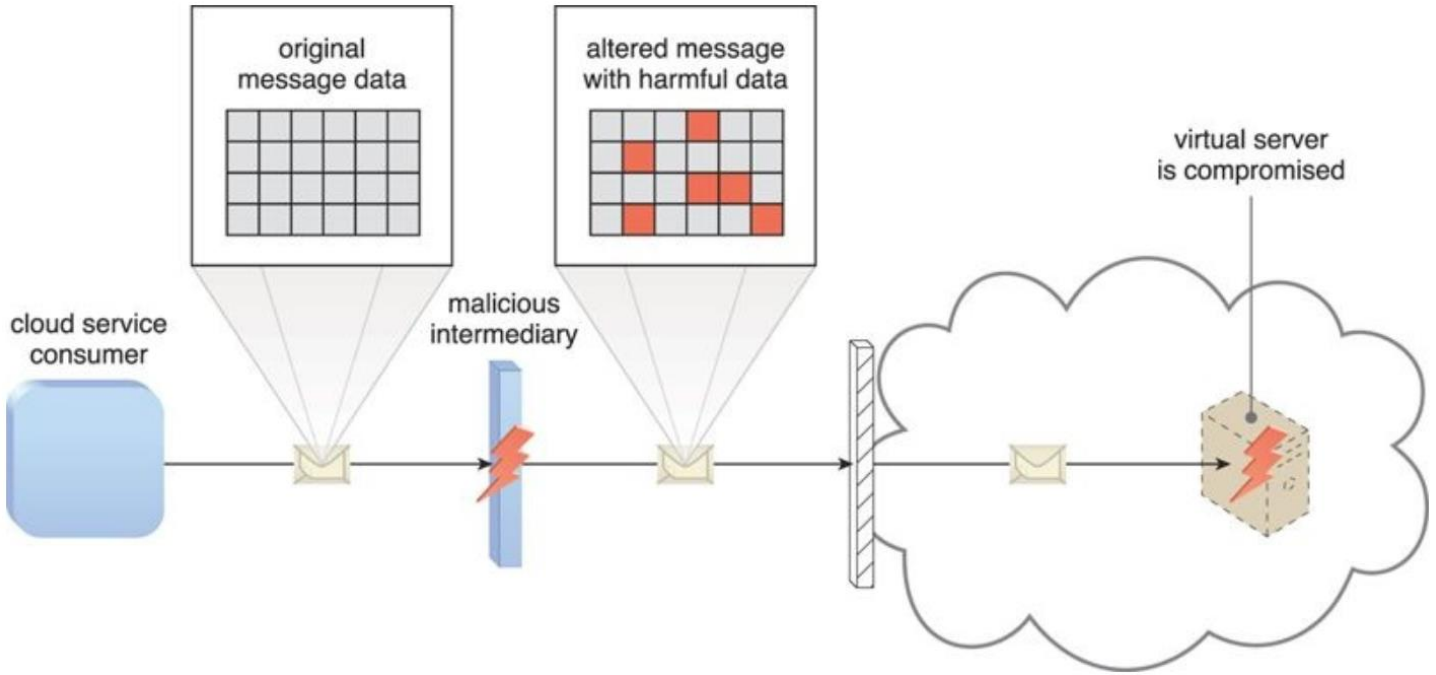
- Traffic Eavesdropping
- Malicious Intermediary
- Insufficient Authorization
- Denial of Service (DoS) Attack
- Virtualization Attack

# Traffic Eavesdropping



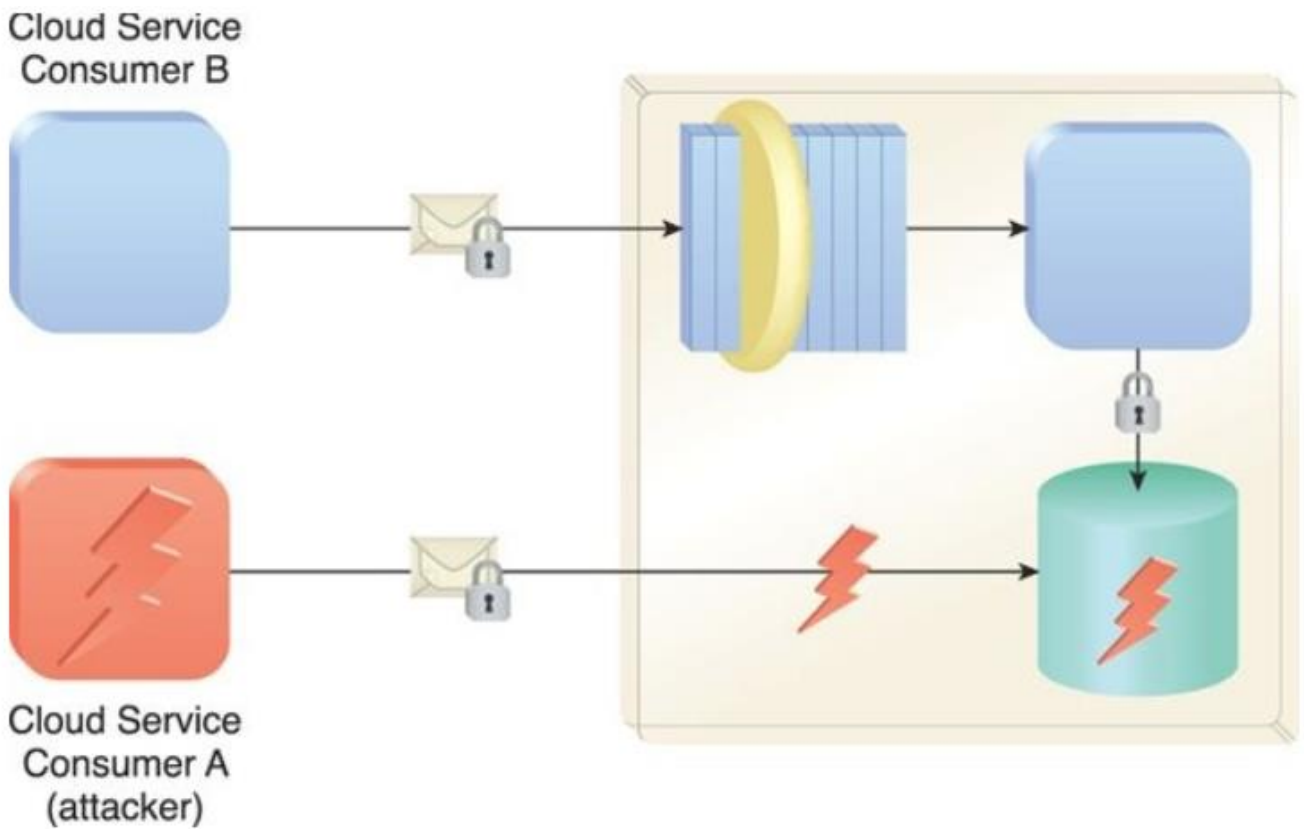

When data being transferred to or within a cloud (usually from the cloud consumer to the cloud provider) is passively intercepted by a malicious service agent for illegitimate information gathering purposes

# Malicious Intermediary



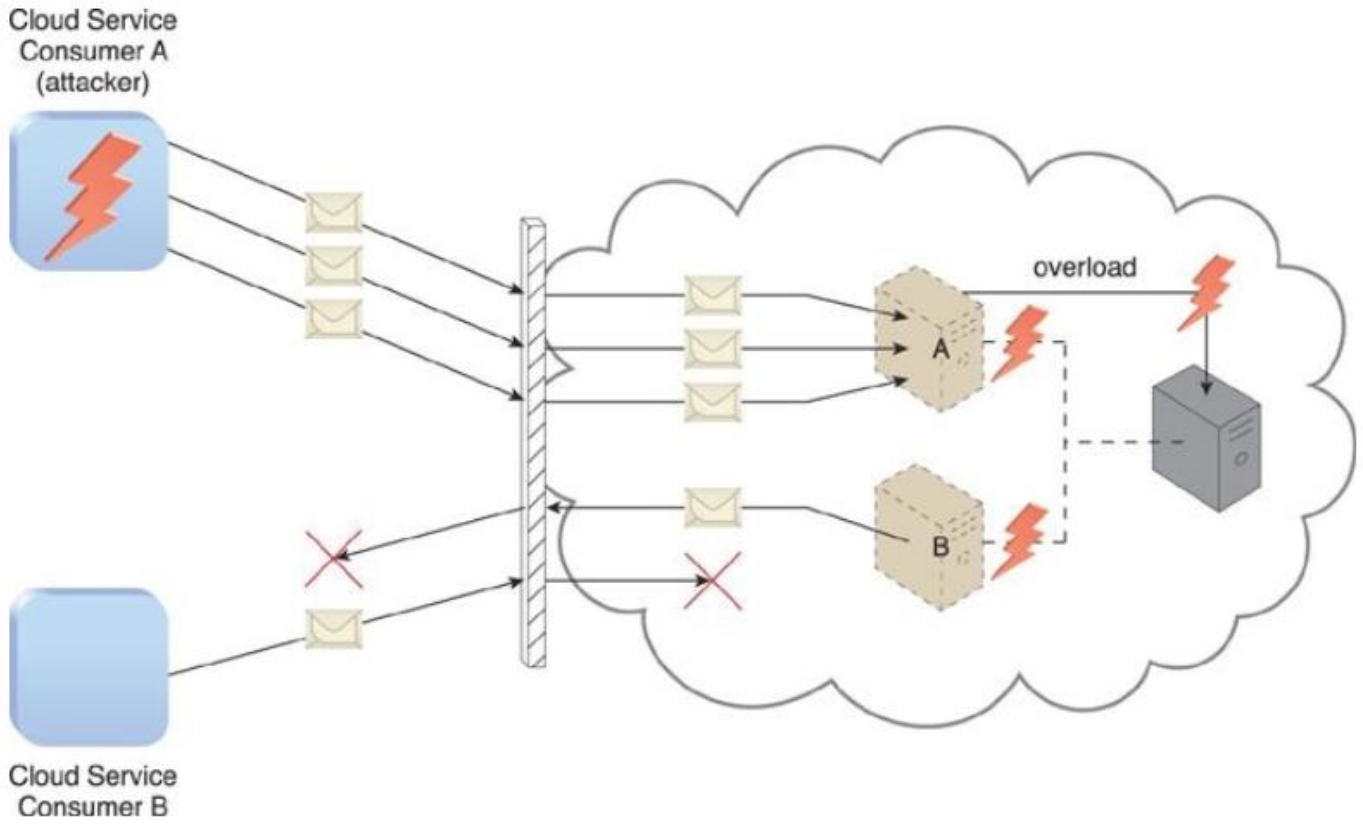

When messages are intercepted and altered by a malicious service agent, thereby potentially compromising the message's confidentiality and/or integrity.

# Insufficient Authorization



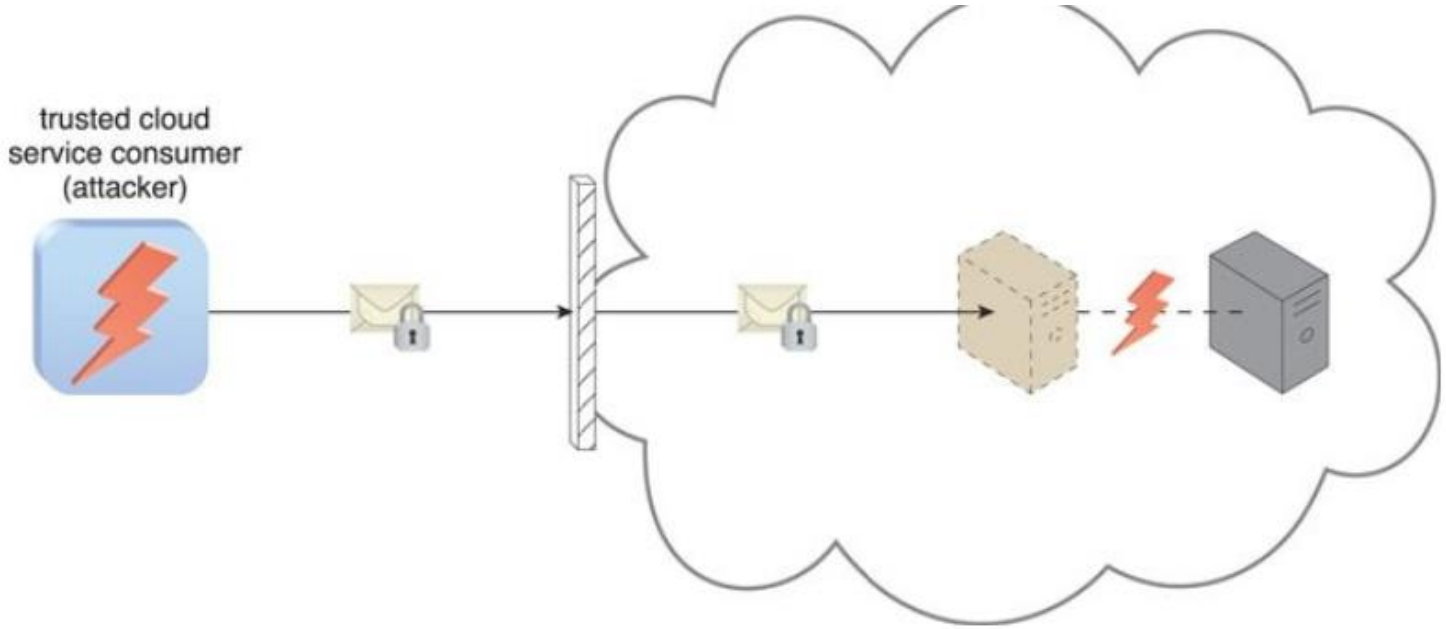

when access is granted to an attacker erroneously or too broadly, resulting in the attacker getting access to IT resources that are normally protected.

# Denial of Service (DoS) Attack




Overloads IT resources to the point where they cannot function properly.

# Virtualization Attack



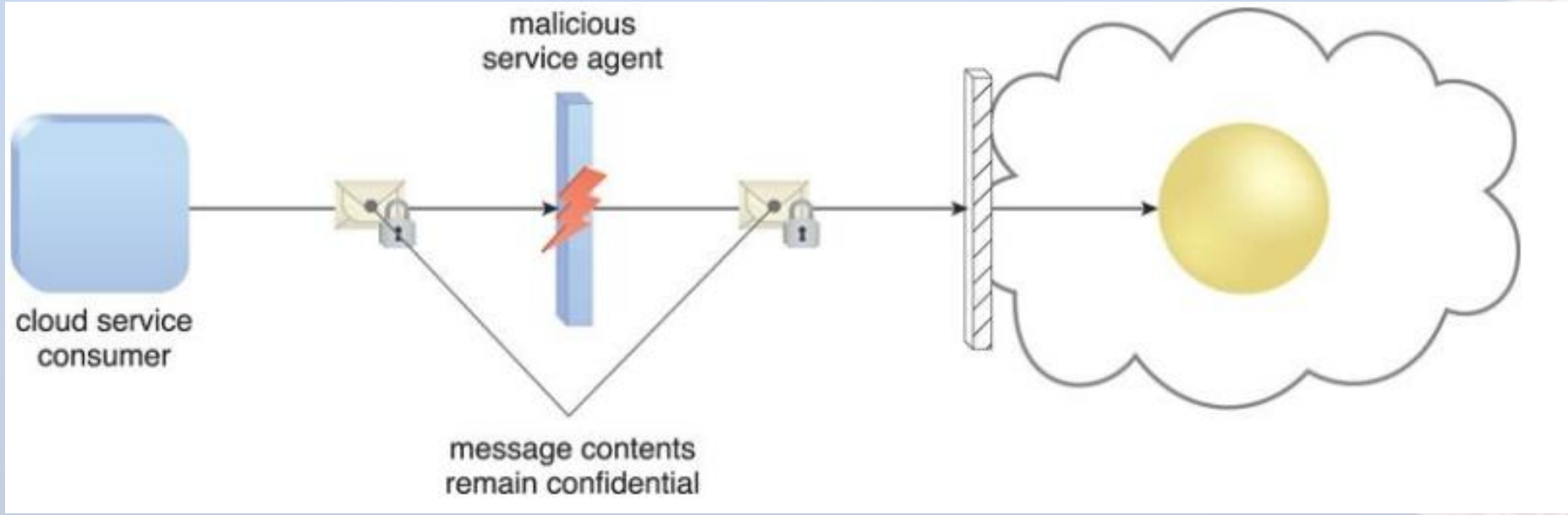

where a trusted attacker successfully accesses a virtual server to compromise its underlying physical server.

# Cloud Security Mechanisms

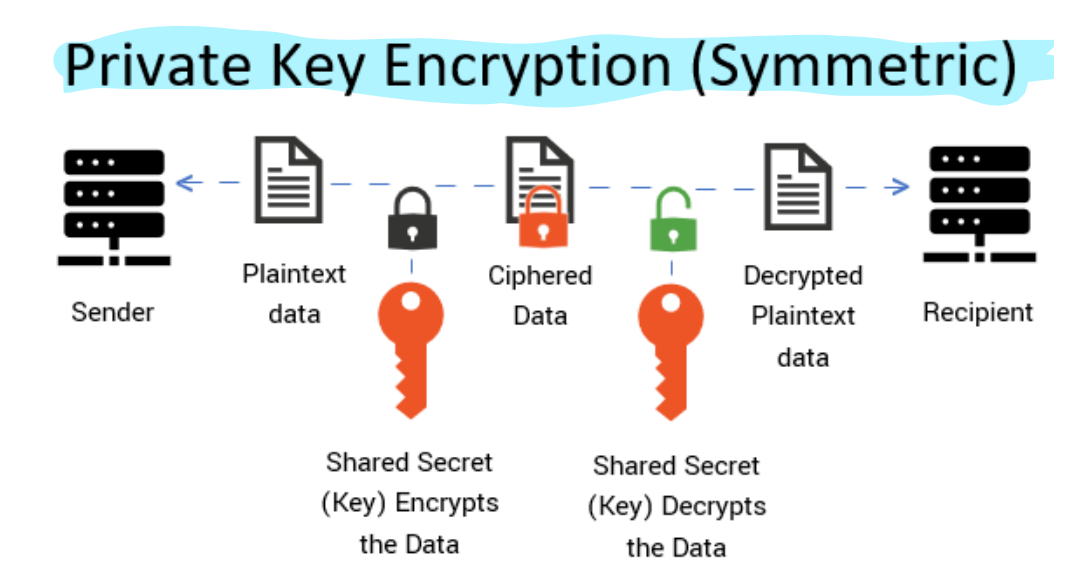
- (Public Key) Encryption
- Hashing
- Digital Signature
- Identity and Access Management (IAM)
- Single Sign-On (SSO)
- Cloud-Based Security Groups
- Hardened Virtual Server Images

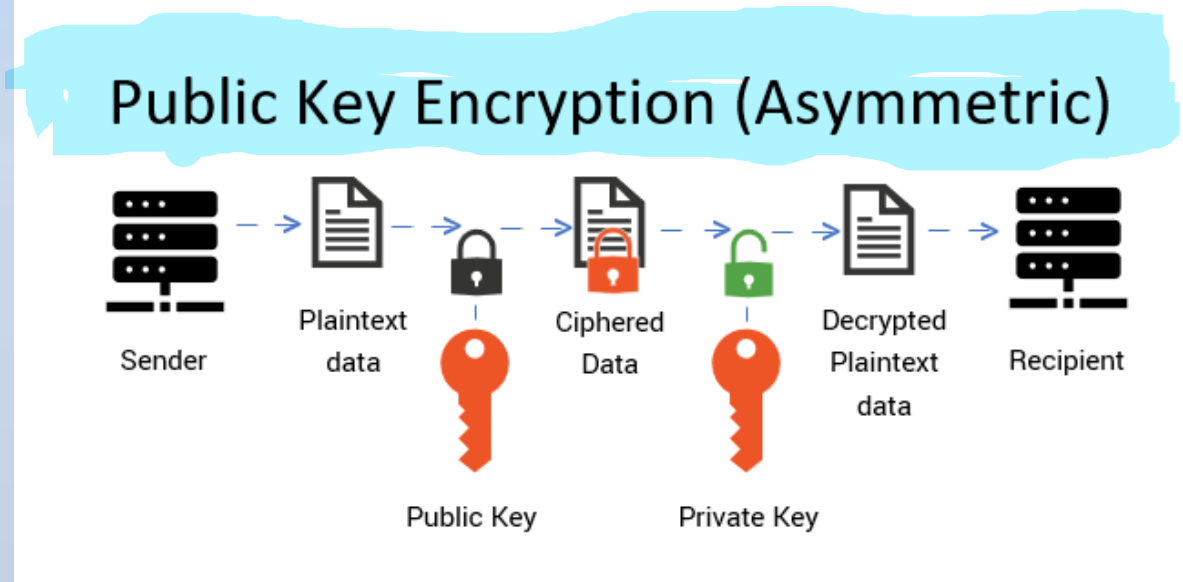
# Encryption

A digital coding system dedicated to preserving the confidentiality and integrity of data. It is used for encoding plaintext data into a protected and unreadable format.



# Symmetric vs Asymmetric Encryption

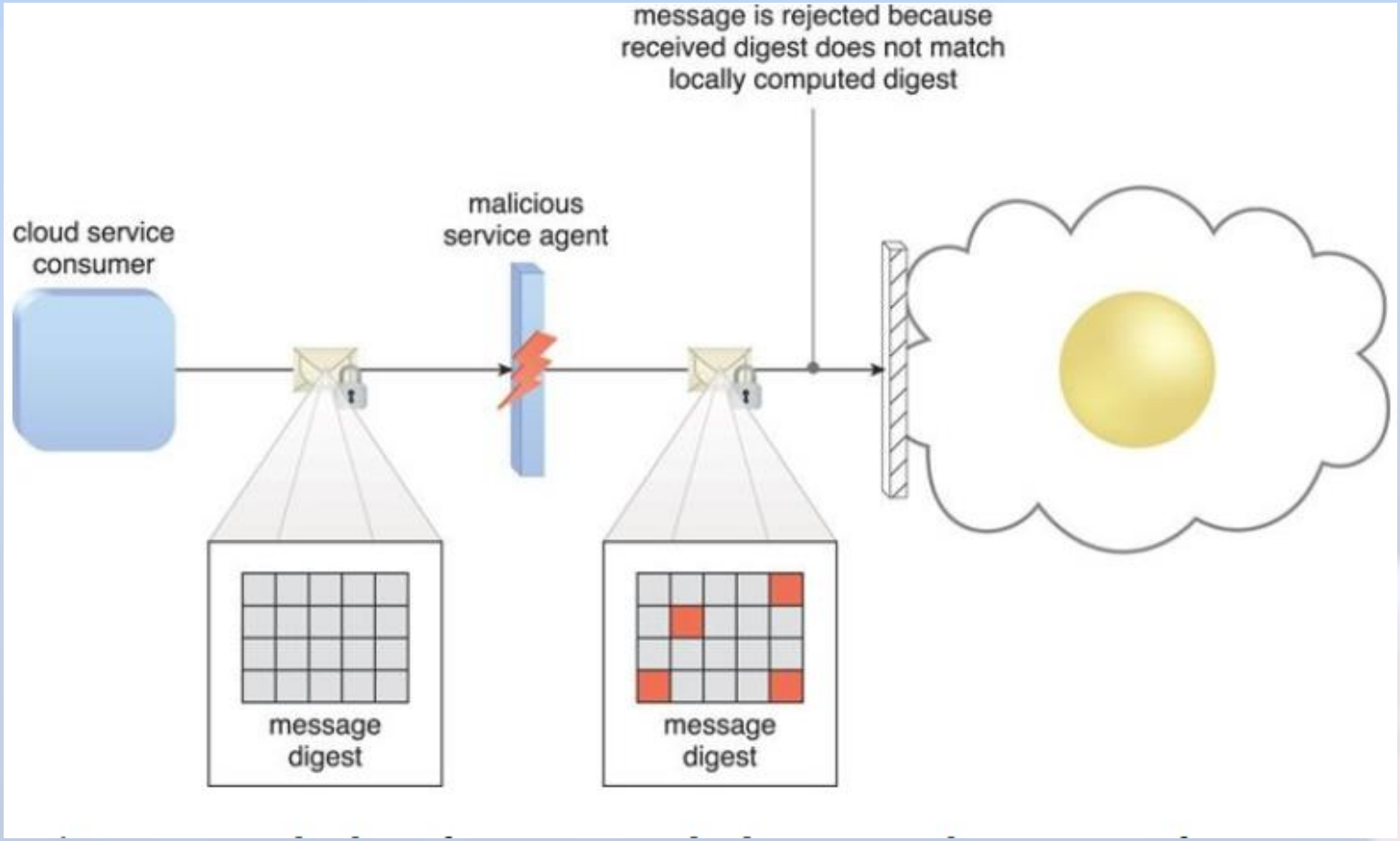


# Hashing

- Hashing technology can be used to derive a hashing code or message digest from a message, which is often of a fixed length and smaller than the original message.
- The message sender can then utilize the hashing mechanism to attach the message digest to the message.
- The recipient applies the same hash function to the message to verify that the produced message digest is identical to the one that accompanied the message.

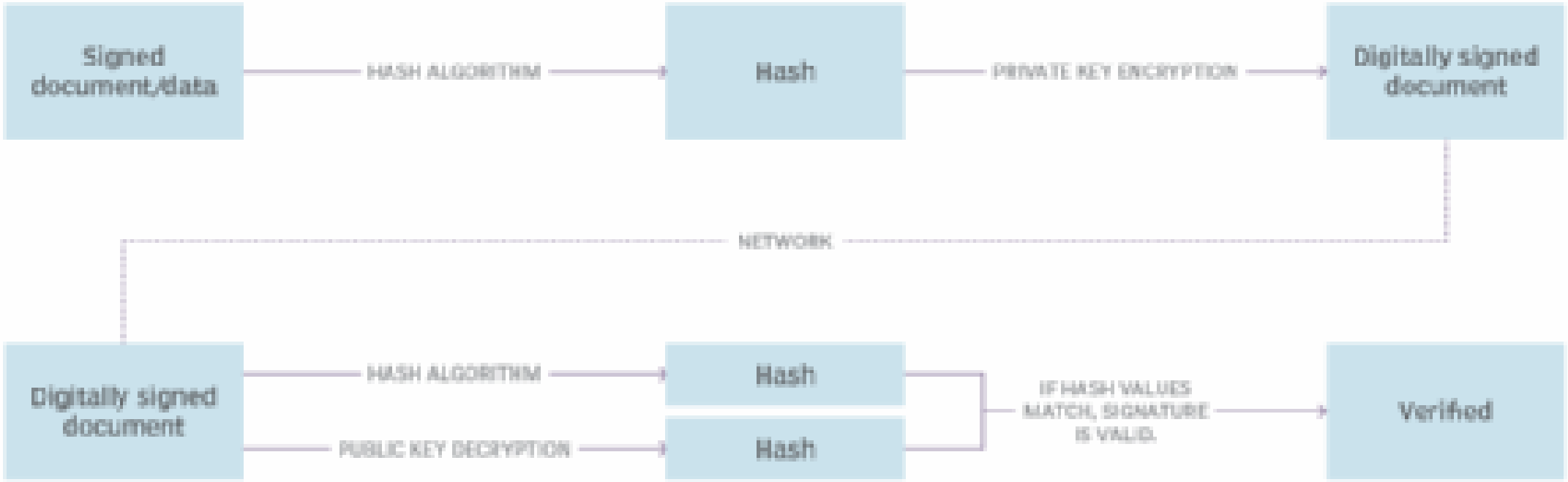
# How hashing provides integrity?



# Digital Signature

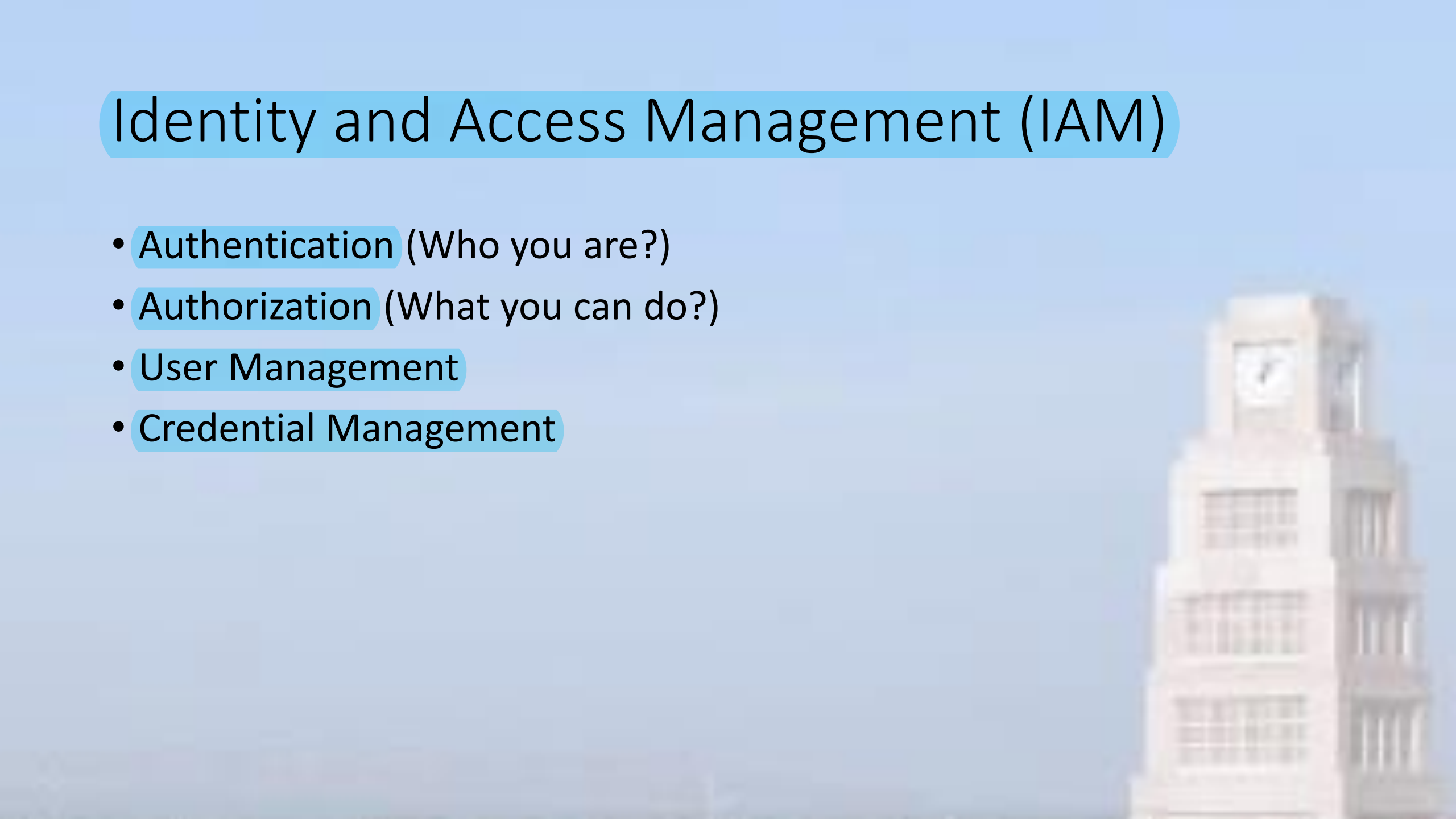
- A message is assigned a digital signature prior to transmission, which is then rendered invalid if the message experiences any subsequent, unauthorized modifications.
- Both hashing and asymmetrical encryption are involved in the creation of a digital signature, which essentially exists as a message digest that was encrypted by a private key and appended to the original message.
- Hashes are used to verify the message integrity only, digital signatures are used to verify message authenticity and message integrity both.

# The digital signature process



# Identity and Access Management (IAM)

- Authentication (Who you are?)
- Authorization (What you can do?)
- User Management
- Credential Management

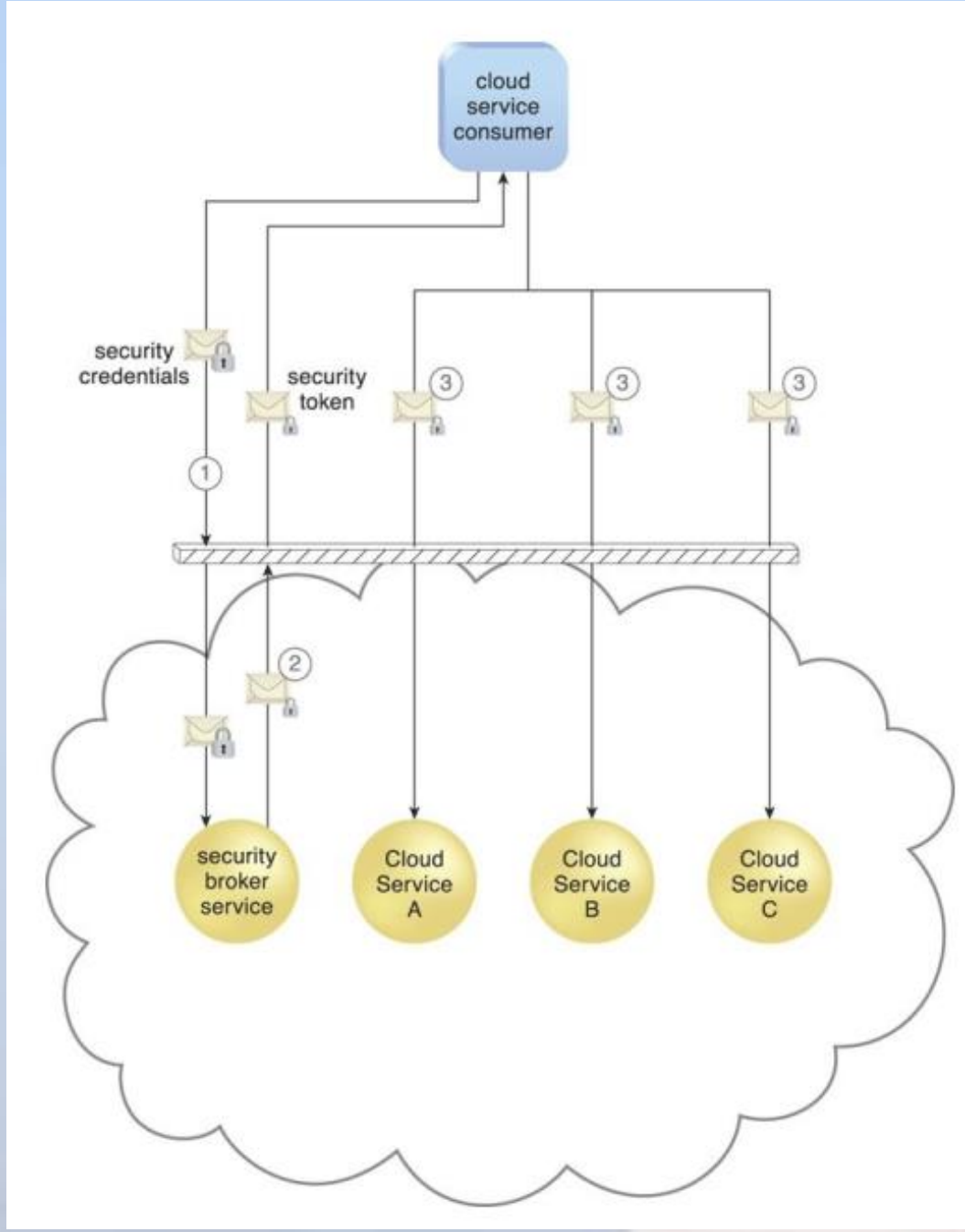


# Single Sign-on (SSO)

- Enables one cloud service consumer to be authenticated by a security broker, which establishes a security context that is persisted while the cloud service consumer accesses other cloud services or cloud-based IT resources.
- Otherwise, the cloud service consumer would need to re-authenticate itself with every subsequent request.
- Less about security per se, more about ease of security for the user.

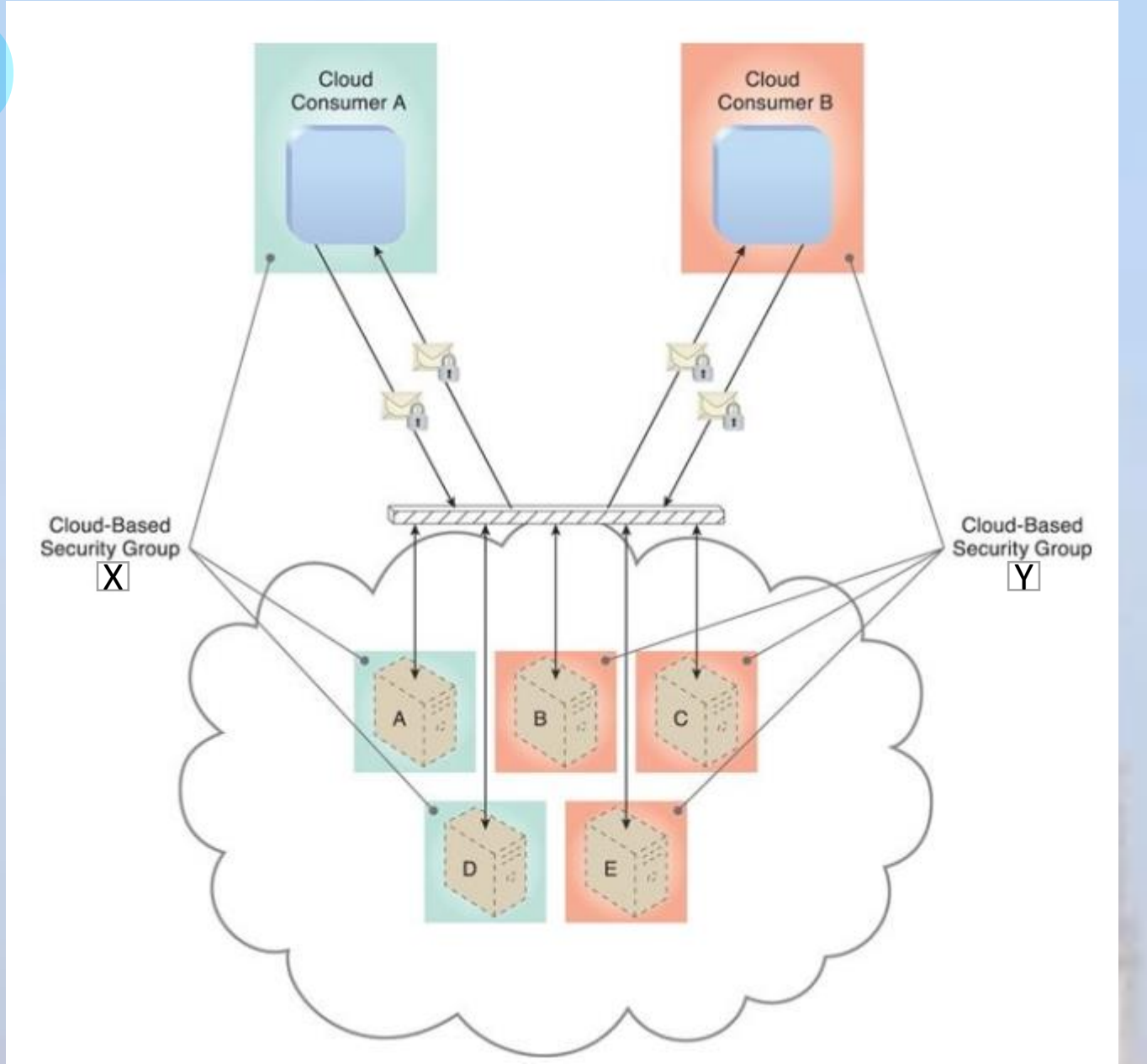
# SSO Process

1. A cloud service consumer provides the security broker with login credentials.
2. The security broker responds with an authentication token (message with small lock symbol) upon successful authentication, which contains cloud service consumer identity information
3. that is used to automatically authenticate the cloud service consumer across Cloud Services A, B, and C.



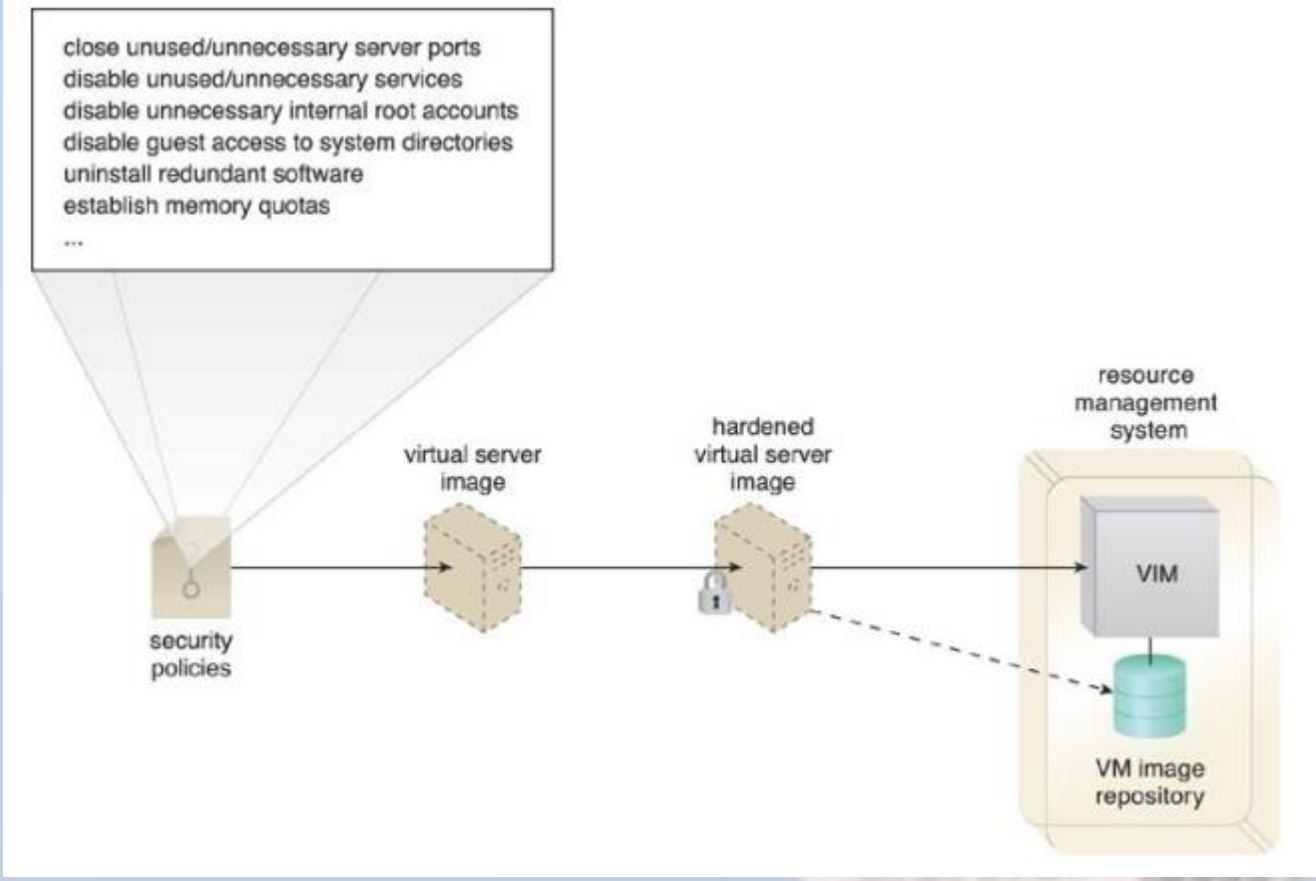
# Cloud-Based Security Groups

- Cloud resource segmentation is a process by which separate physical and virtual IT environments are created for different users and groups.
- The cloud-based resource segmentation process creates cloud-based security group mechanisms that are determined through security policies.



# Hardened Virtual Server Images

- Hardening is the process of stripping unnecessary software from a system to limit potential vulnerabilities that can be exploited by attackers.
- Removing redundant programs, closing unnecessary server ports, and disabling unused services, internal root accounts, and guest access are all examples of hardening.




I HAVE A PARTICULAR SET OF SKILLS...
NETWORK SECURITY, CLOUD SOLUTIONS,
DATA RECOVERY, AND 24/7 MANAGED SERVICES
imgflip.com