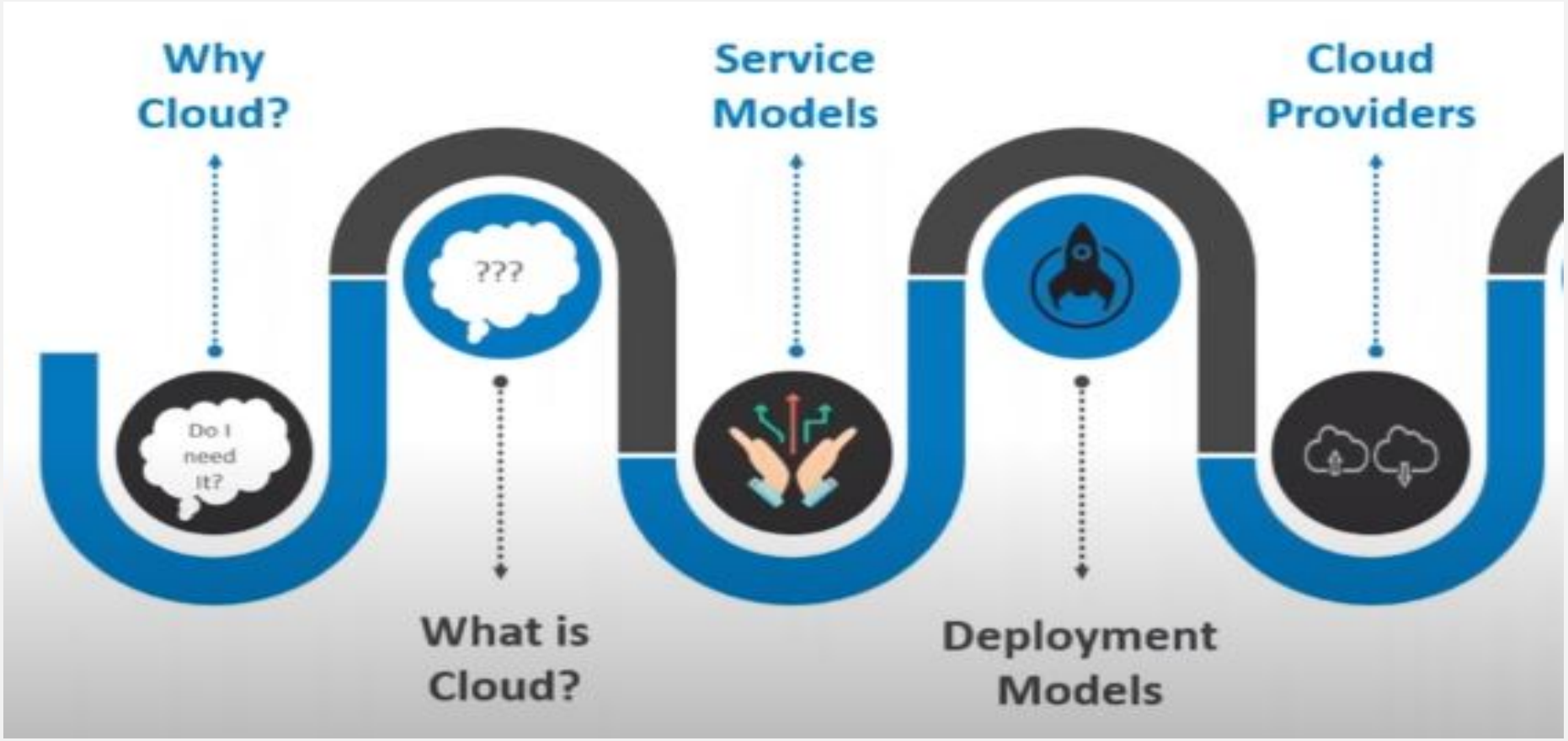
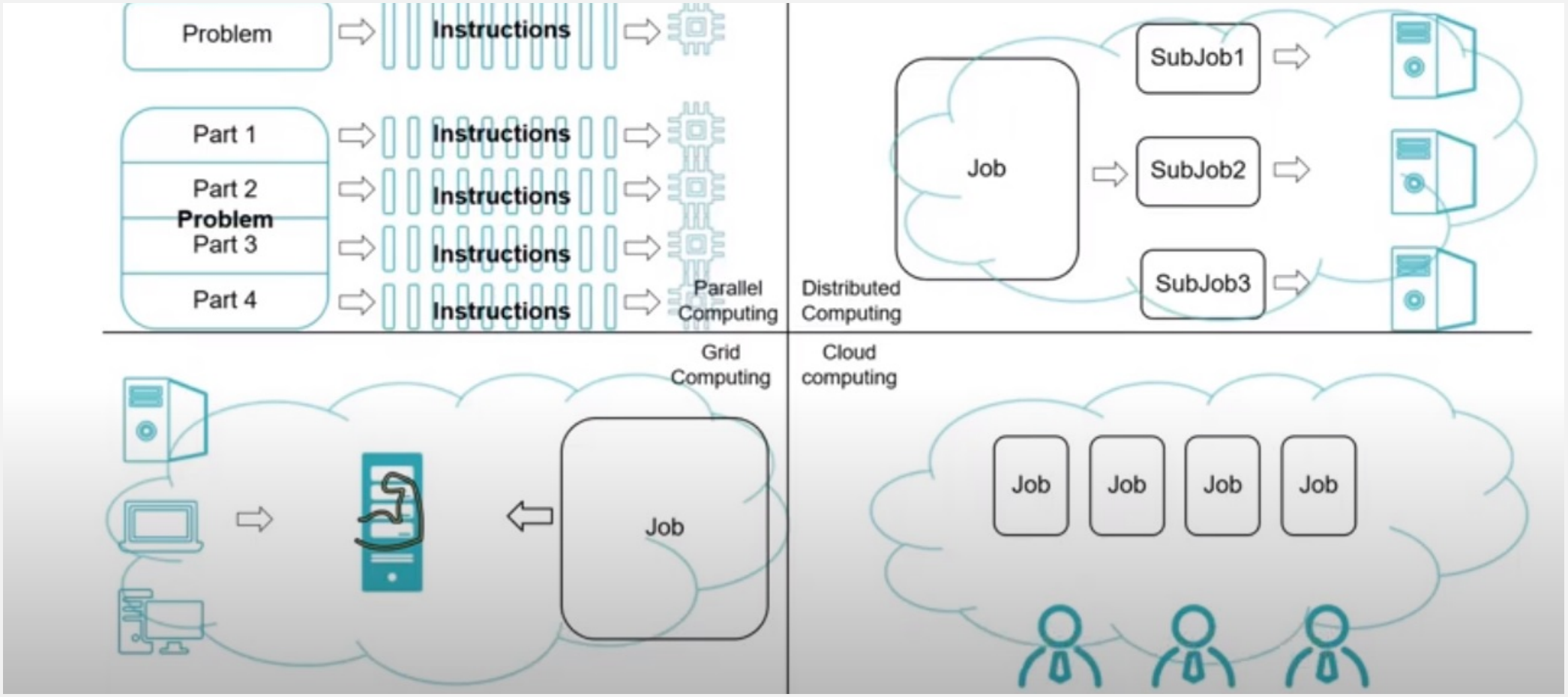
Introduction to Cloud

Dr. Mukti Padhya
Assistant Professor, NFSU

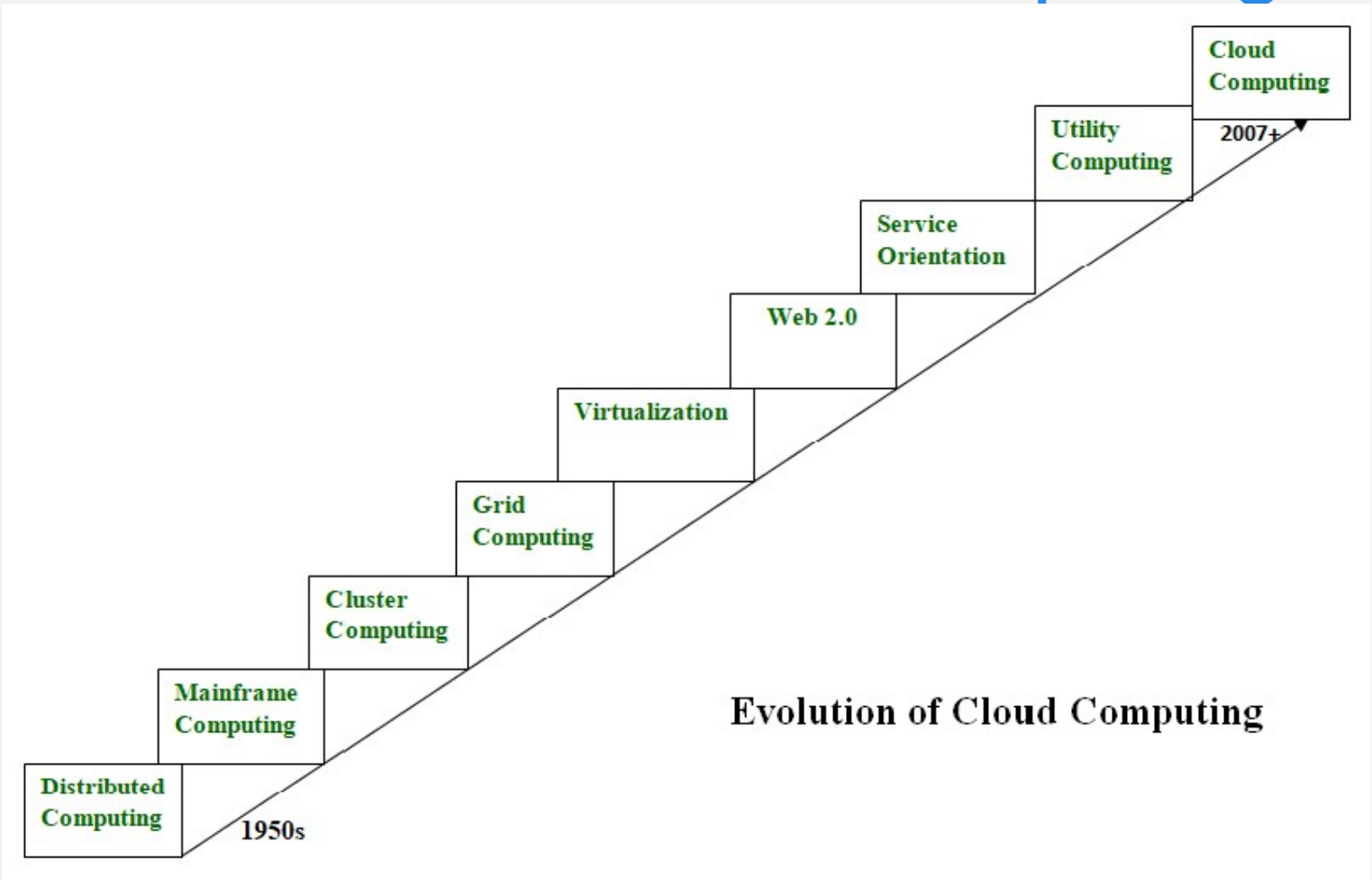
Offerings of This Session : Unit I



Evolution of Cloud Computing



Evolution of Cloud Computing

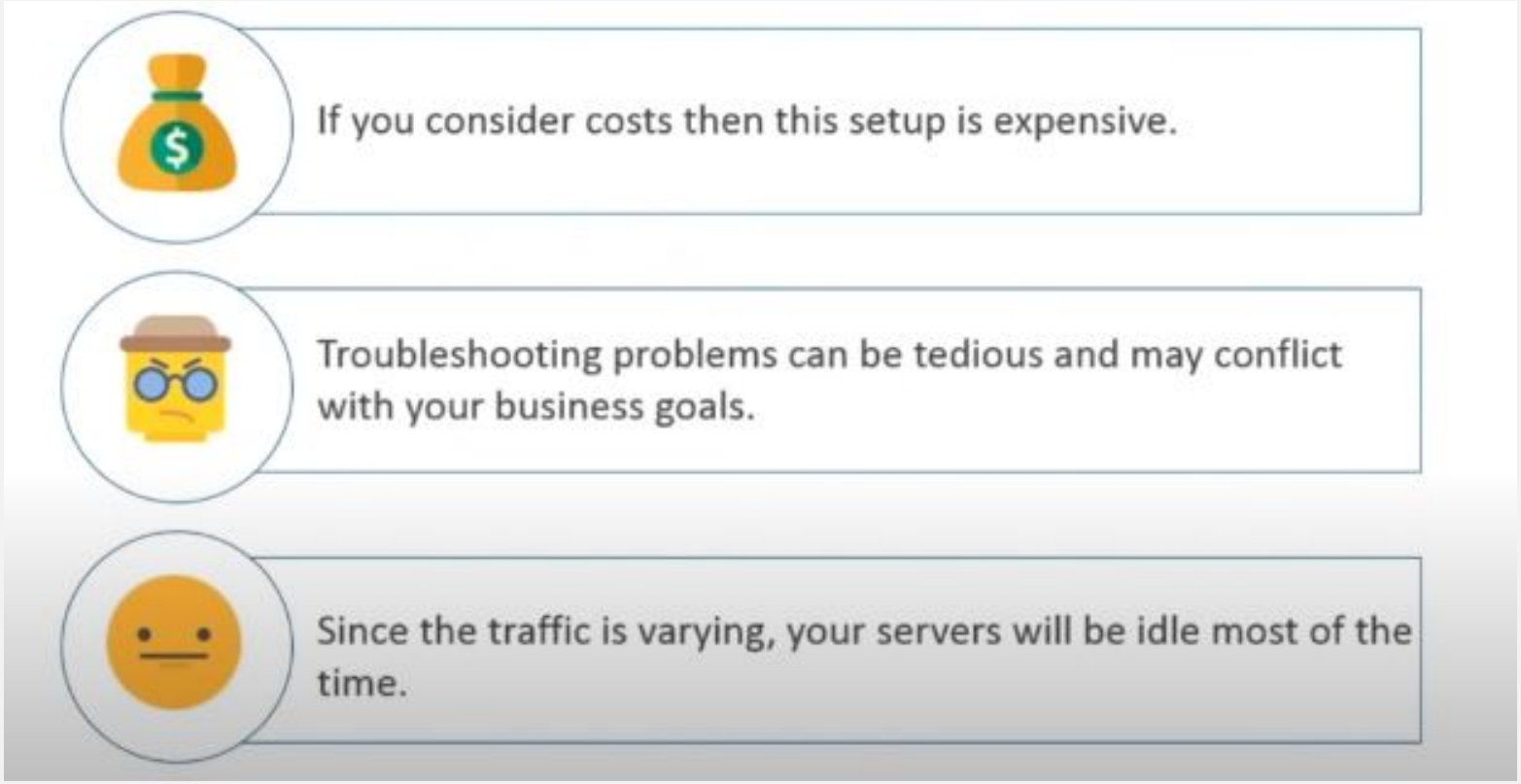


For Details Refer : https://www.geeksforgeeks.org/evolution-of-cloud-computing/

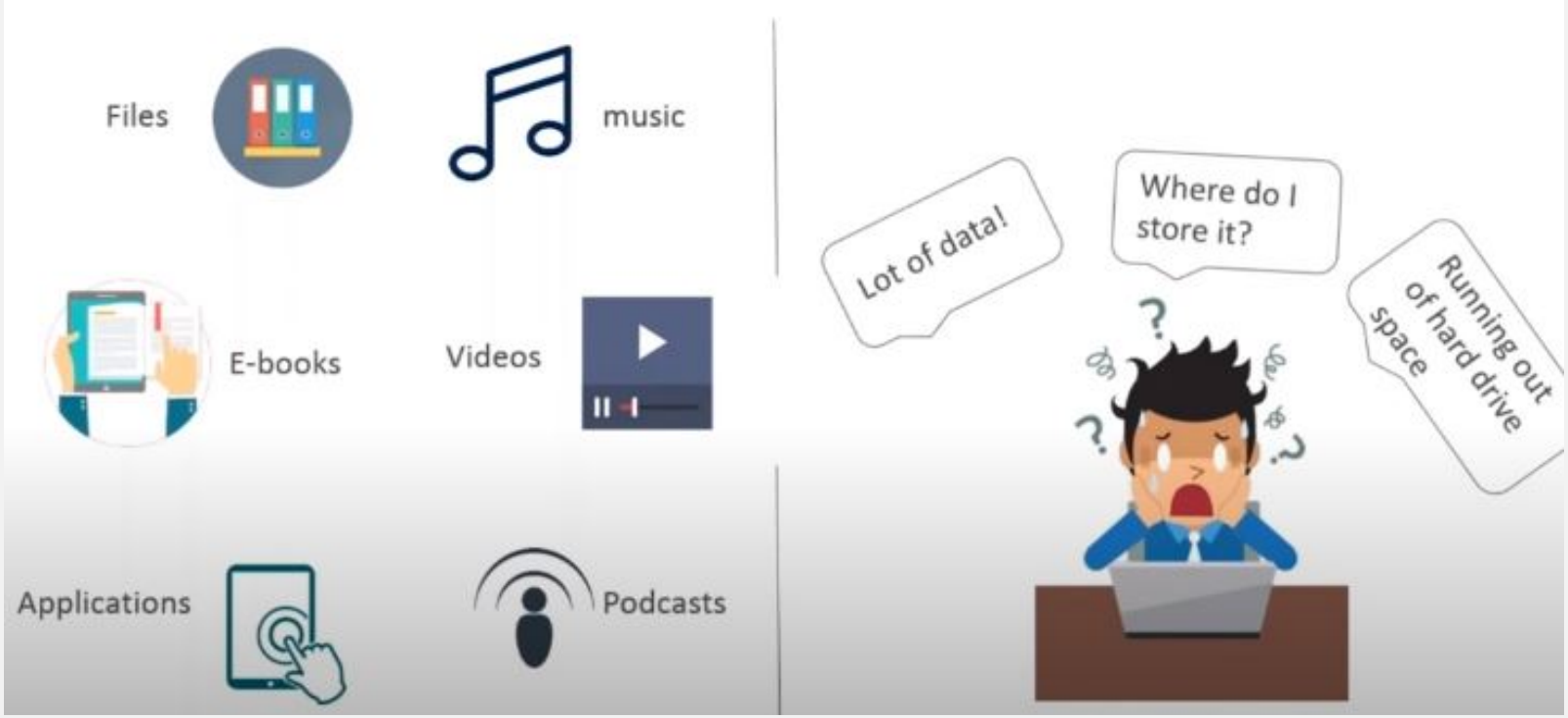
Before cloud computing

- Suppose you want to host a website , there are following things that you would need to do
  - Buy a stack of servers
  - High traffic? More servers
  - Monitoring and Maintain Servers
- Big Data - Internet seamlessly generating High amount of data
  - Where to store data
- High computing jobs
  - Computional resources?

Disadvantages



Why Cloud?


Files
music
E-books
Videos
Applications
Podcasts
Lot of data!
Where do I store it?
Running out of hard drive space

What is Cloud?

- The term ‘cloud’ in technical terms, was used to refer to distributed computing as early as 1993.
- Cloud computing is basically the on-demand provision of computing resources like storage, applications, networking capabilities, databases, software and services, development tools, processing capabilities, and more, by service providers (known as Cloud Service providers or CSP), to its users, via the internet.
- These services can be provided with minimum management effort or service provider interaction. Cloud computing is often referred to as internet-based computing.
- In simple terms, users can access data, applications, and services hosted in remote services, instead of accessing it from their computer’s hard drive.

What is Cloud?

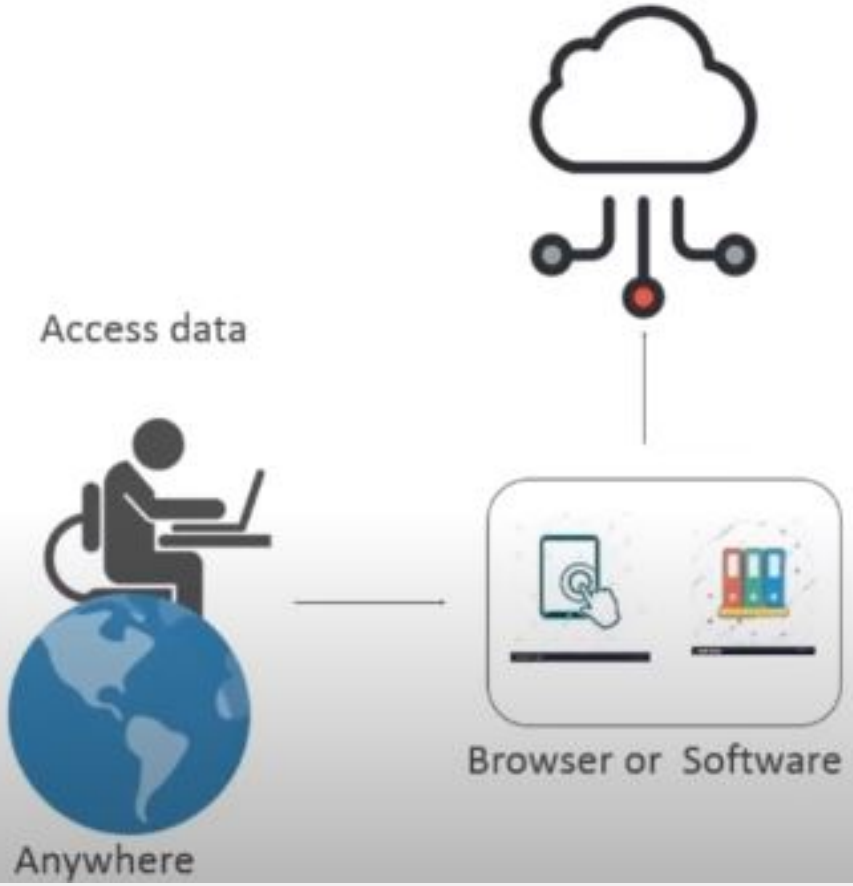
What is Cloud?

- Global network of servers each with a unique function
- Cloud is not a physical entity - Virtualization
- It is a vast network of remote servers around the globe which are hooked together and meant to operate as a single ecosystem
- The information will be available anywhere you go and anytime you need it
- Cloud is nothing but a server that we access over the internet, it contains a large amount of data such as text files, video, audio, images, docs, pdfs, and so on.
- It is just like developing software for millions to use as a service rather than distributing software to run on their PCs.

What is Cloud Computing?

Cloud computing is:

- Storing data/applications on remote servers
- Processing data/applications from servers
- Accessing data/applications via Internet



What is Cloud Computing?

"Cloud computing is a model for enabling ubiquitous convenient, on-demand network access to a shared pool of configurable computing resources (e.g.,networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction."

- National Institute of Standards and Technology (NIST)

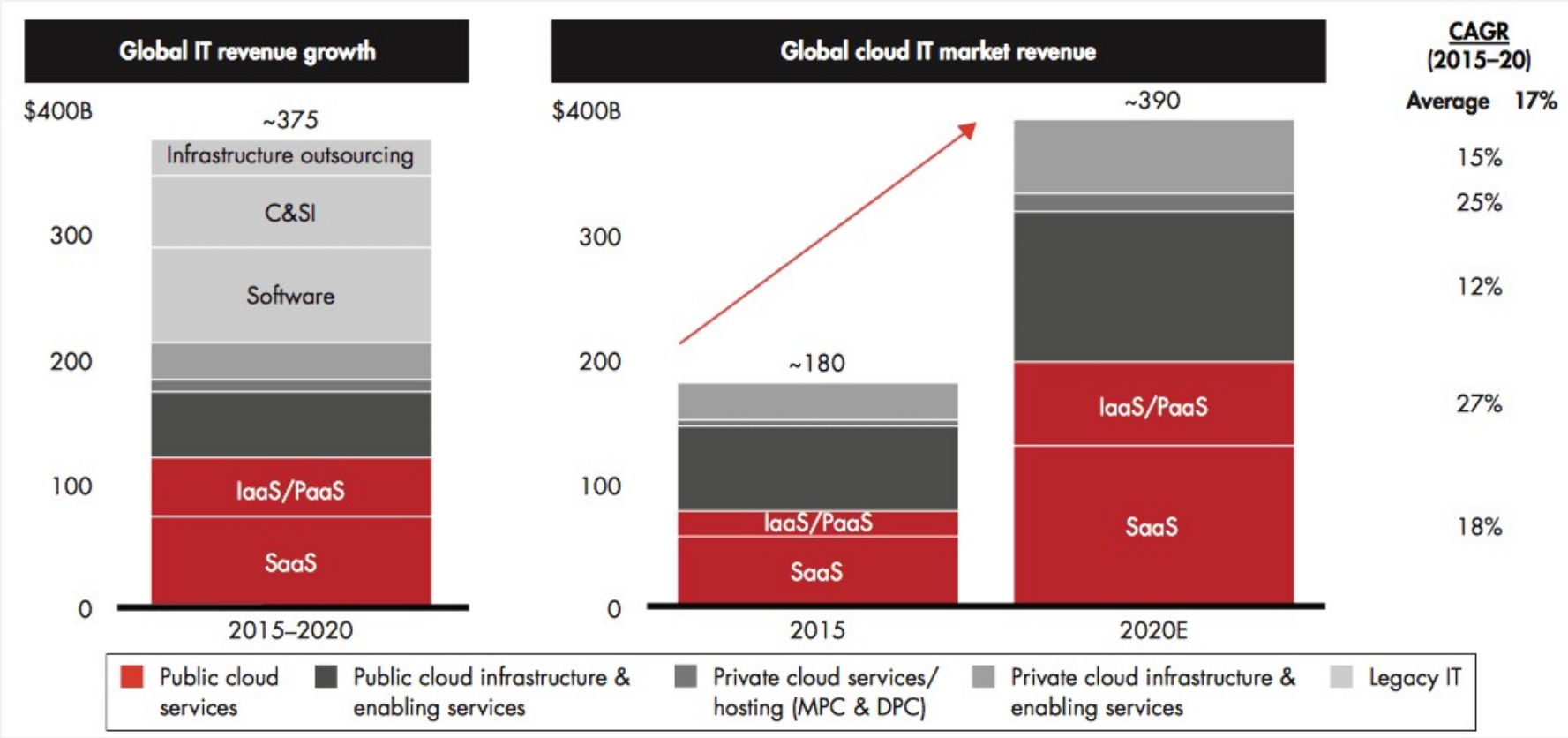
Cloud : DataCenter

- Clouds can be built with physical or virtualized resources over large data centers that are distributed systems. Cloud computing is also considered to be a form of utility computing or service computing.

- A single-site cloud (as known as a “Datacenter”) consists of
  - Compute nodes (grouped into racks).
  - Switches, connecting the racks.
  - A network topology, e.g., hierarchical.
  - Storage (backend) nodes are connected to the network.
  - Front-end for submitting jobs and receiving client requests.
  - Software Services.

Cloud Computing : Today

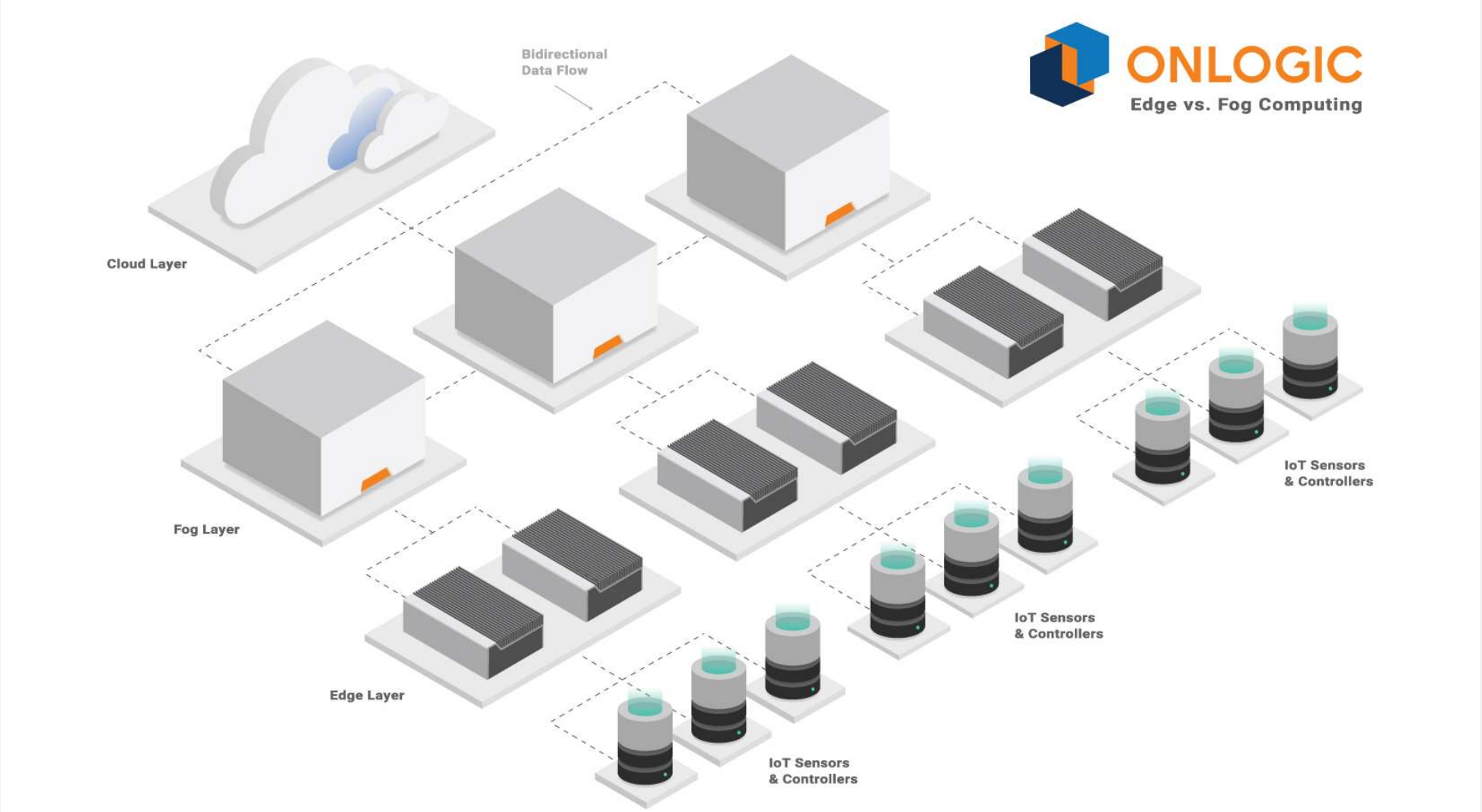
Cloud Computing : Today



The Number of Cloud-based Services and Solutions Will Continue to Rise

Indeed, they will. According to Bain & Company, subscription-based SaaS solutions will grow at an 18% CAGR by 2020, IaaS/PaaS at 27%, and public cloud infrastructure and enabling services at 12%. In all, cloud computing hardware, software and services are capturing 60% of all IT market growth.

Cloud Computing : Recent Trends



Cloud Computing : Recent Trends

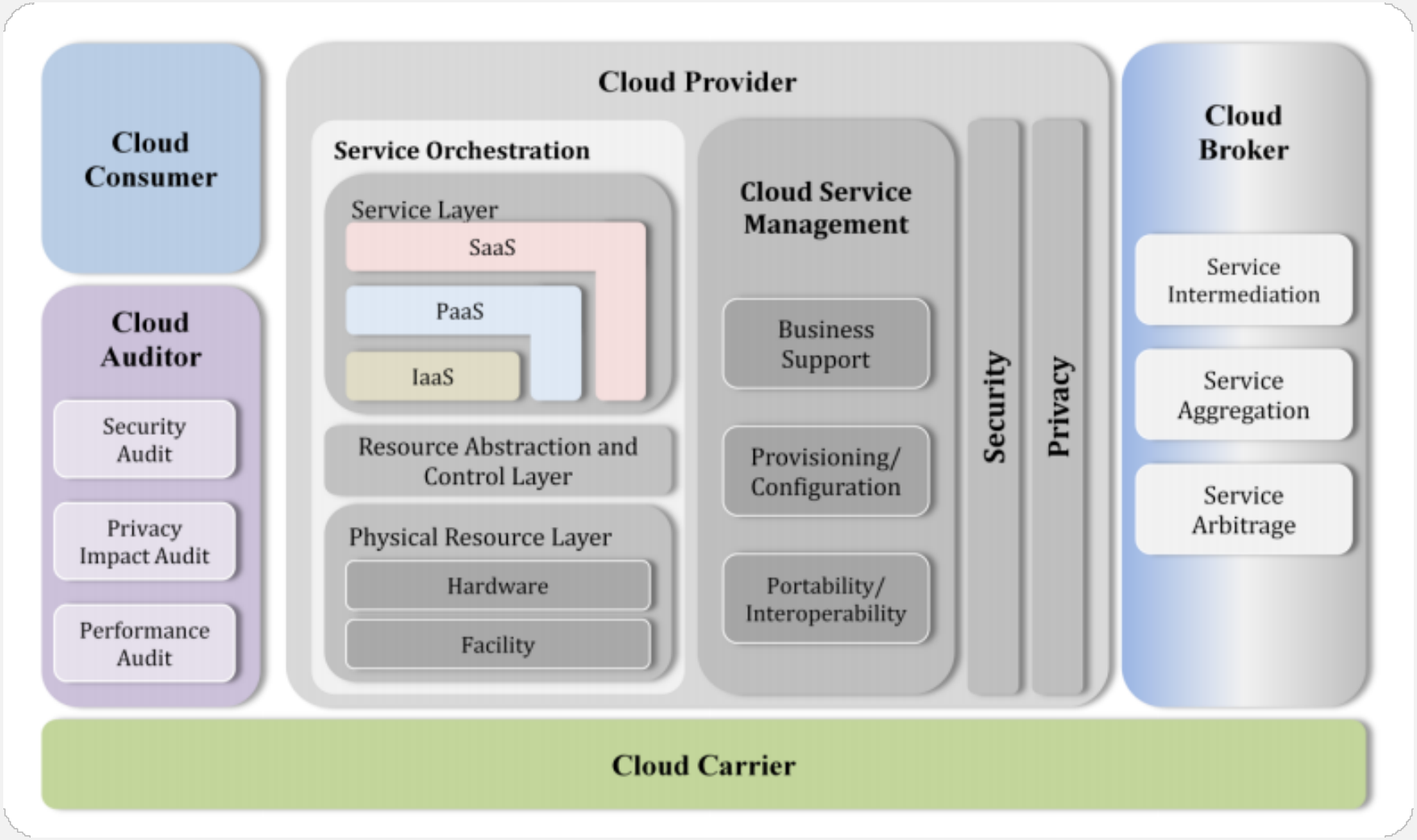
- An edge is a computing location at the edge of a network, along with the hardware and software at those physical locations. Cloud computing is the act of running workloads within clouds, while edge computing is the act of running workloads on edge devices.
  - Clouds are places where data can be stored or applications can run. They are software-defined environments created by datacenters or server farms.
  - Edges are also places where data is collected. They are physical environments made up of hardware outside a datacenter.
  - Cloud computing is an act; the act of running workloads in a cloud.
  - Edge computing is also an act; the act of running workloads on edge devices.

- Fog computing is a compute layer between the cloud and the edge. Where edge computing might send huge streams of data directly to the cloud, fog computing can receive the data from the edge layer before it reaches the cloud and then decide what is relevant and what isn't. The relevant data gets stored in the cloud, while the irrelevant data can be deleted, or analyzed at the fog layer for remote access or to inform localized learning models.

Cloud Computing?

- NIST defined cloud model is composed of five essential characteristics, three service models, and four deployment models
- If a cloud does not have any of these essential characteristics and deployment models it is likely not a cloud
- It is a convenient, on-demand way to access a shared pool of configurable resources (networks, servers, storage, applications and services)
- Enables users to develop, host and run services and applications on demand in a flexible manner in any devices, anytime, and anywhere

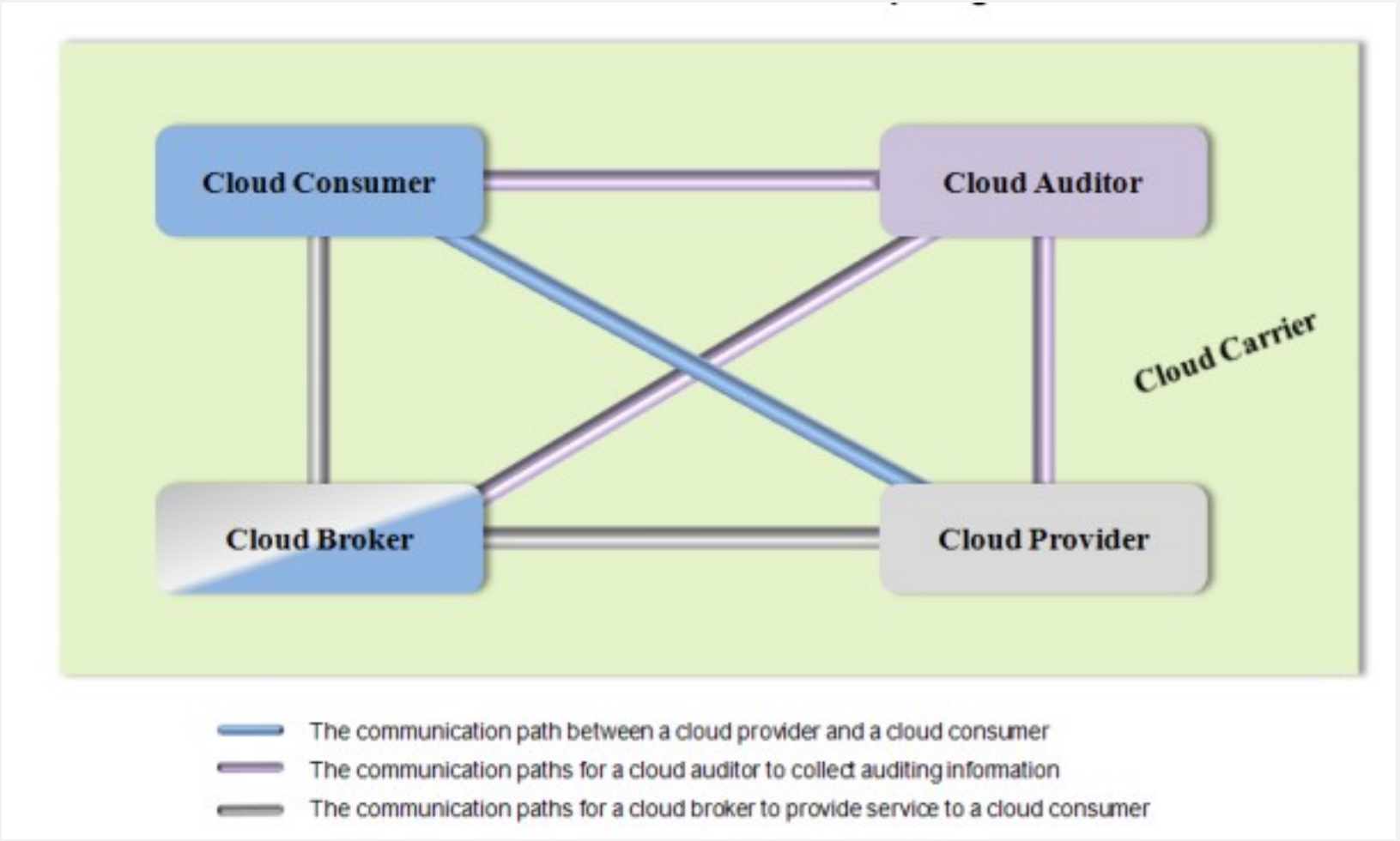
Cloud Architechture : NIST



Cloud Stakeholders : NIST

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

Interaction between Stakeholders



Example Usage Scenario : 1

- **Example Usage Scenario 1**: A cloud consumer may request service from a cloud broker instead of contacting a cloud provider directly. The cloud broker may create a new service by combining multiple services or by enhancing an existing service. In this example, the actual cloud providers are invisible to the cloud consumer and the cloud consumer interacts directly with the cloud broker.

Cloud Broker

- A cloud broker can provide services in three categories :

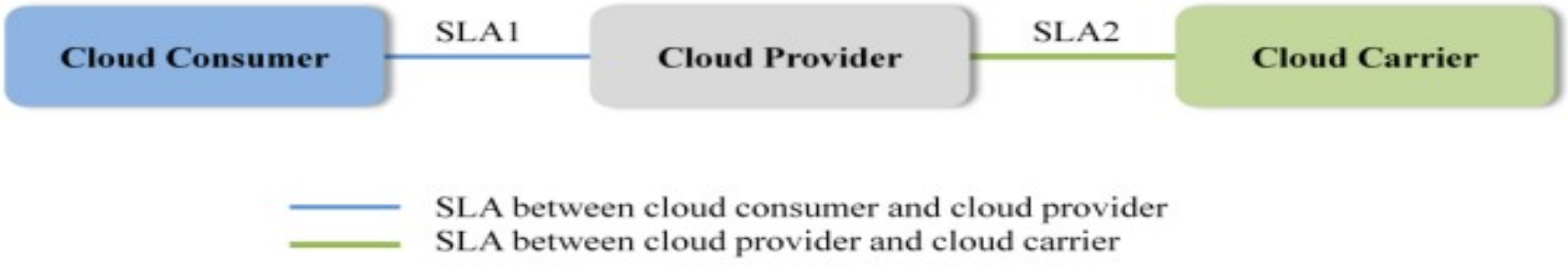
- **Service Intermediation:** A cloud broker enhances a given service by improving some specific capability and providing value-added services to cloud consumers. The improvement can be managing access to cloud services, identity management, performance reporting, enhanced security, etc.

- **Service Aggregation:** A cloud broker combines and integrates multiple services into one or more new services. The broker provides data integration and ensures the secure data movement between the cloud consumer and multiple cloud providers.

- **Service Arbitrage:** Service arbitrage is similar to service aggregation except that the services being aggregated are not fixed. Service arbitrage means a broker has the flexibility to choose services from multiple agencies. The cloud broker, for example, can use a credit-scoring service to measure and select an agency with the best score.

Example Usage Scenario : 2

Example Usage Scenario 2: Cloud carriers provide the connectivity and transport of cloud services from cloud providers to cloud consumers. As illustrated in Figure 4, a cloud provider participates in and arranges for two unique service level agreements (SLAs), one with a cloud carrier (e.g. SLA2) and one with a cloud consumer (e.g. SLA1). A cloud provider arranges service level agreements (SLAs) with a cloud carrier and may request dedicated and encrypted connections to ensure the cloud services are consumed at a consistent level according to the contractual obligations with the cloud consumers. In this case, the provider may specify its requirements on capability, flexibility and functionality in SLA2 in order to provide essential requirements in SLA1.



- **SLAs can cover terms regarding the quality of service, security, remedies for performance failures. A cloud provider may also list in the SLAs a set of promises explicitly not made to consumers, i.e. limitations, and obligations that cloud consumers must accept.**

Cloud Carrier

- A cloud carrier acts as an intermediary that provides connectivity and transport of cloud services between cloud consumers and cloud providers.
- Cloud carriers provide access to consumers through network, telecommunication and other access devices.
- For example, cloud consumers can obtain cloud services through network access devices, such as computers, laptops, mobile phones, mobile Internet devices (MIDs), etc .

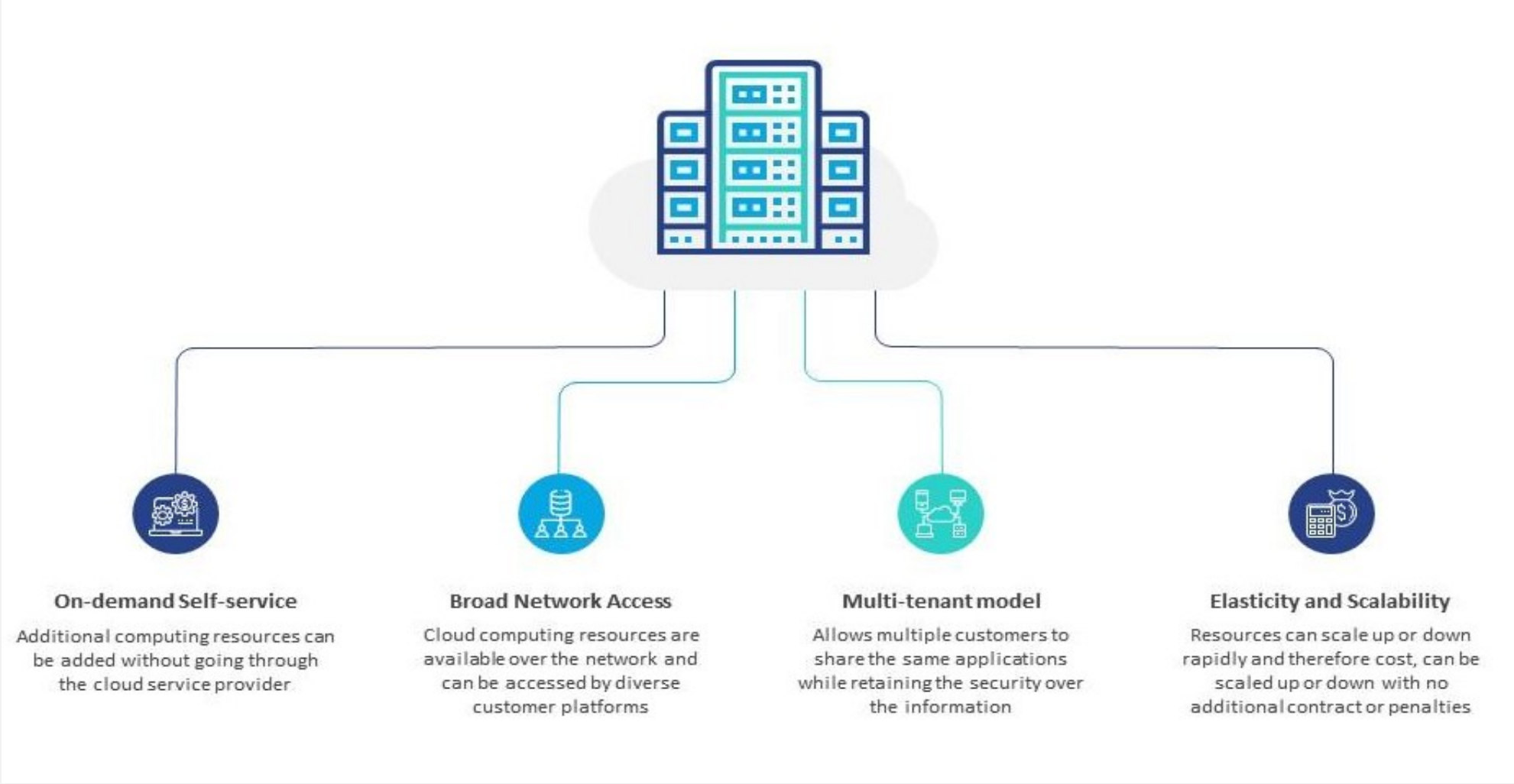
Example Usage Scenario : 3

- For a cloud service, a cloud auditor conducts independent assessments of the operation and security of the cloud service implementation. The audit may involve interactions with both the Cloud Consumer and the Cloud Provider.

Cloud Auditor

- Audits are performed to verify conformance to standards through review of objective evidence.
- A cloud auditor can evaluate the services provided by a cloud provider in terms of security controls, privacy impact, performance, etc.
- For security auditing, a cloud auditor can make an assessment of the security controls in the information system to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to the security requirements for the system.
- The security auditing should also include the verification of the compliance with regulation and security policy.
- For example, an auditor can be tasked with ensuring that the correct policies are applied to data retention according to relevant rules for the jurisdiction.
- The auditor may ensure that fixed content has not been modified and that the legal and business data archival requirements have been satisfied.

Characteristics of Cloud Computing



On-demand Self-Service

- Cloud computing resources can be provisioned without human interaction from the service provider
- In other words, a manufacturing organization can provision additional computing resources as needed without going through the cloud service provider
- This can be a storage space, virtual machine instances, database instances, and so on

Broad Network Access

- No geographical boundaries.
- Cloud computing has a vast access area and is accessible via the internet.
  - You can access your files and documents or upload your files from anywhere in the world
- Cloud computing resources are available over the network and can be accessed by diverse customer platforms

Multi-tenancy & Resource Pooling

- Cloud computing resources are designed to support a multi-tenant model

- Multi-tenancy allows multiple customers to share the same applications or the same physical infrastructure while retaining privacy and security over their information
  - E.x. : people living in an apartment building, sharing the same building infrastructure but they still have their own apartments and privacy within that infrastructure.

- The IT resource (e.g., networks, servers, storage, applications, and services) present are shared across multiple applications and occupant in an uncommitted manner. Multiple clients are provided service from a same physical resource.

Rapid Elasticity

- Dynamically adjust to capacity requirement
- Cloud computing resources can scale up or down rapidly
- Elasticity is a landmark of cloud computing and it implies that manufacturing organizations can rapidly provision and de-provision any of the cloud computing resources
- Rapid provisioning and de-provisioning might apply to storage or virtual machines or customer applications.

Measured Service

- Cloud computing resources usage is metered and manufacturing organizations pay accordingly for what they have used
- Resource utilization can be optimized by leveraging charge-per-use capabilities
- This means that cloud resource usage - whether virtual server instances that are running or storage in the cloud—gets monitored, measured and reported by the cloud service provider
- The cost model is based on pay for what you use

Other Characteristics of Cloud

- Simplicity
- Flexibility
- Automation
- Scalability (Rapidly adjust to accommodate growth)
- High availability and reliability
- Agility
- Device and Location Independence
- Maintenance
- Low Cost
- Services in the pay-per-use mode

How does Cloud computing work?

- Cloud computing is possible because of a technology called virtualization
- Virtualization allows for the creation of a simulated, digital-only "virtual" computer that behaves as if it were a physical computer with its own hardware
  - Such Computer sustem is called virtual machine
- VMs don't interact with each other at all
- The files and applications from one virtual machine aren't visible to the other virtual machines even though they're on the same physical machine

How does Cloud computing work?

- Virtual machines also make more efficient use of the hardware hosting them.
- By running many virtual machines at once, one server becomes many servers, and a data center becomes a whole host of data centers, able to serve many organizations
- Thus, cloud providers can offer the use of their servers to far more customers at once -- at a low cost

Virtualization

- Virtualization uses software to create an abstraction layer over computer hardware that allows the hardware elements of a single computer—processors, memory, storage and more—to be divided into multiple virtual computers, commonly called virtual machines (VMs).

- Each VM runs its own operating system (OS) and behaves like an independent computer - running on just a portion of the actual underlying computer hardware.

Virtualization

- Virtualization reduces the burden of workloads of users by centralizing the administrative tasks and improving the scalability and workloads
- Every available resource is seen as a utility
- It increases the total computing power and decreases the overhead
- It reduces the hardware acquisition & maintenance cost

Cloud Computing : Advantage

- Backup and Restoration of Data – Data stored on cloud is easy to backup and restore
- Improved Collaboration – Applications on cloud allow quick and easy sharing of info via shared storage
- Easy Accessibility – Data stored on cloud is easily accessible without any geographic boundaries 24 X 7 □
- Low maintenance cost – Hardware and Software maintenance cost is reduced in cloud computing
- Pay-per-use Model – Allows user to pay for service being used thereby saving huge costs
- Unlimited storage – Nearly unlimited storage is available to user for storing photos, movies, etc

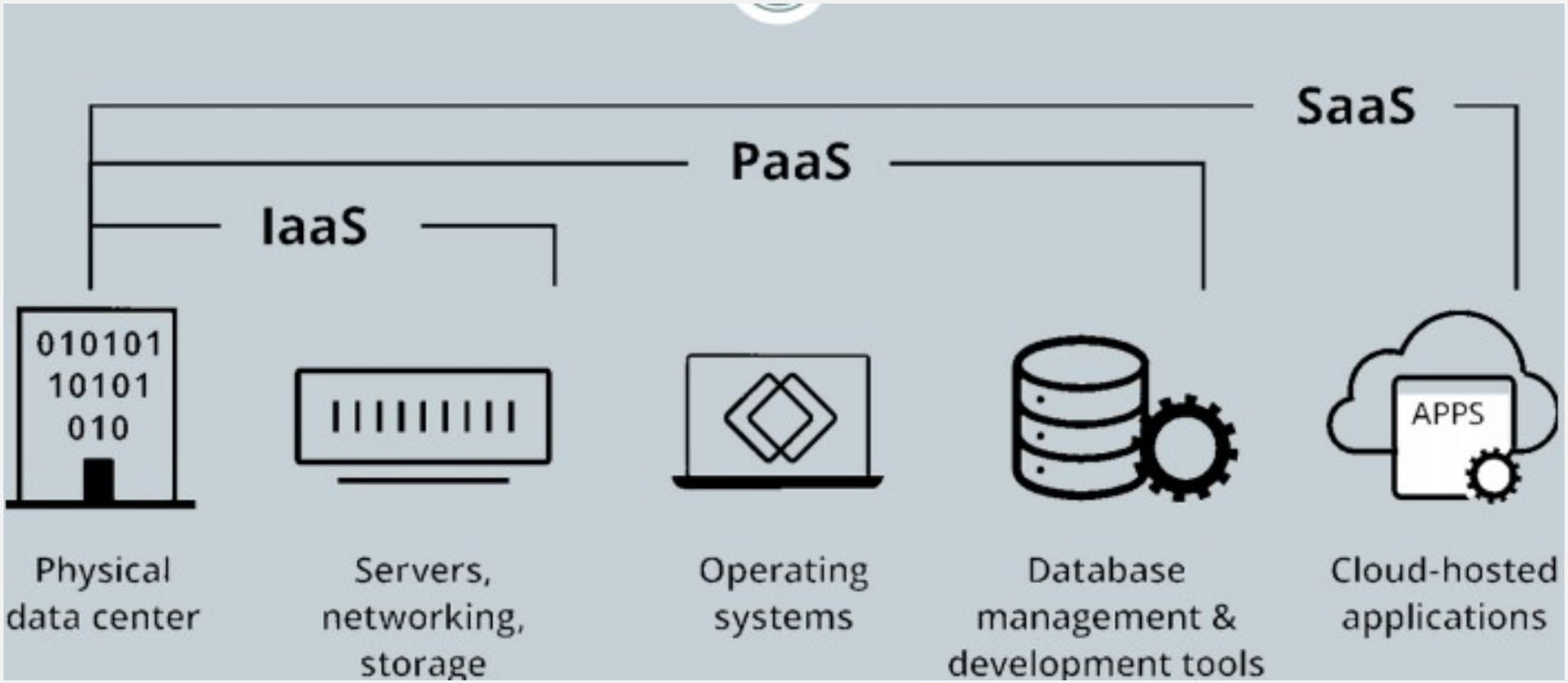
Cloud Computing : Disadvantage

- Internet Connection – A reliable and high speed internet connection is required for accessing cloud resources
- Vendor Lock-in – Cross compatibility of platforms provided by different vendors is an issue
- Limited Control – Cloud resources are managed by service providers hence user has limited control
- Security – Sensitive information of an organisation stored in the cloud can be misused by hackers
- Loss of data – Due to natural calamity/ incident

Cloud Service Models

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

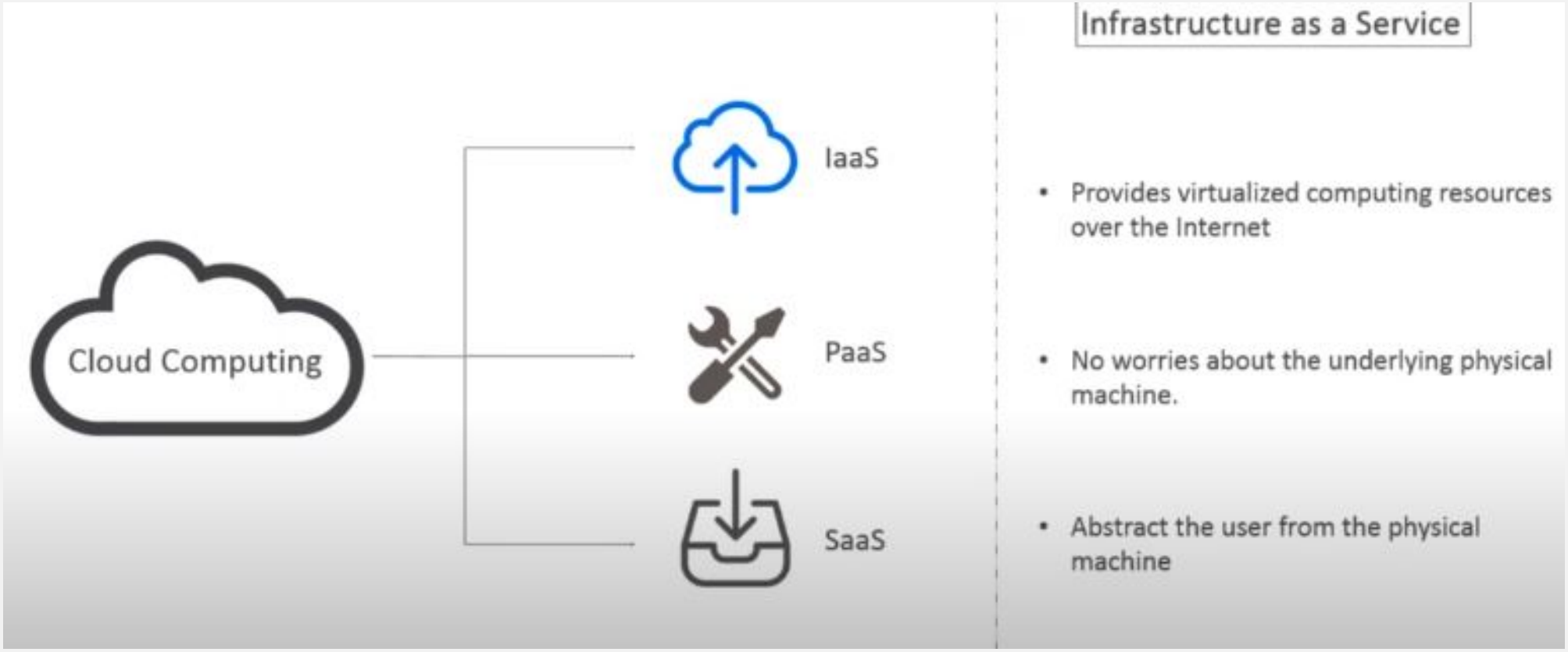
Service Models



Service Models

Type of Cloud Service	What It Does	Examples
Infrastructure as a service (IaaS)	Compute power, networking, and storage provided over the internet	Amazon Elastic Compute Cloud (Amazon EC2), Rackspace, Google Compute Engine
Platform as a service (PaaS)	Tools provided over the internet for making programs and applications	AWS Elastic Beanstalk, Microsoft Azure, Google App Engine
Software as a service (SaaS)	Applications and programs that are accessed and provided over the internet	Dropbox, Slack, Spotify, YouTube, Microsoft Office 365, Gmail

Service Models : IaaS



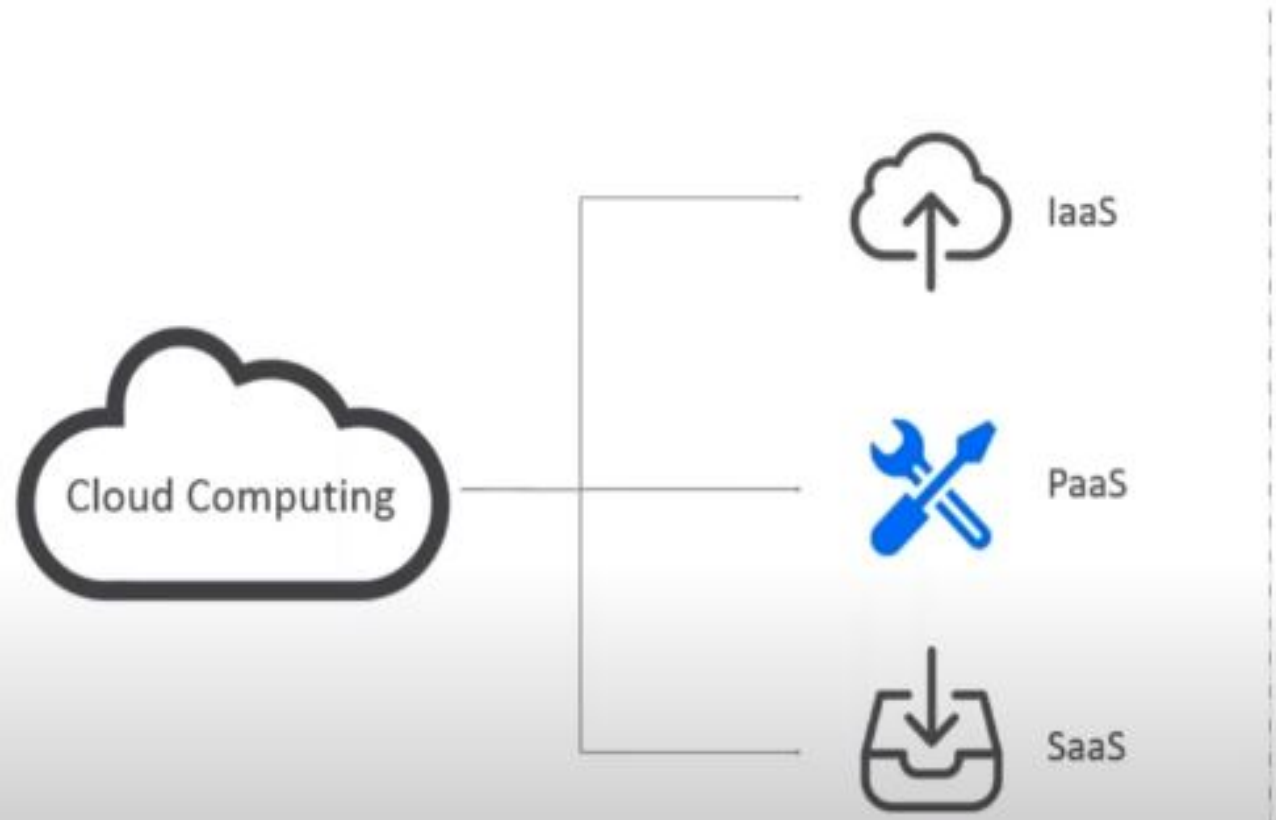
Service Models : IaaS

- A standardized way of acquiring computing capabilities on demand and over the web
- Resources include storage facilities, networks, processing power, and virtual private servers.
- This is a Pay as you go model

Service Models : Why IaaS?

- IaaS is the most flexible of cloud models
- It gives the best option when it comes to IT hardware infrastructure
- If control is required over the hardware infrastructure such as in managing and customizing according to requirements
- Ideal for Startups as it gives access to computing resources without the need to invest in them separately. □
- However, the only downside with IaaS is that it is much costlier than SaaS or PaaS cloud models

Service Models : PaaS



Platform as a Service

- No control over the underlying architecture including OS, storage, servers etc.
- The Cloud Provider gives the ability to the customer to deploy customer created apps using programming languages, tools etc that are provided by the Cloud Provider.

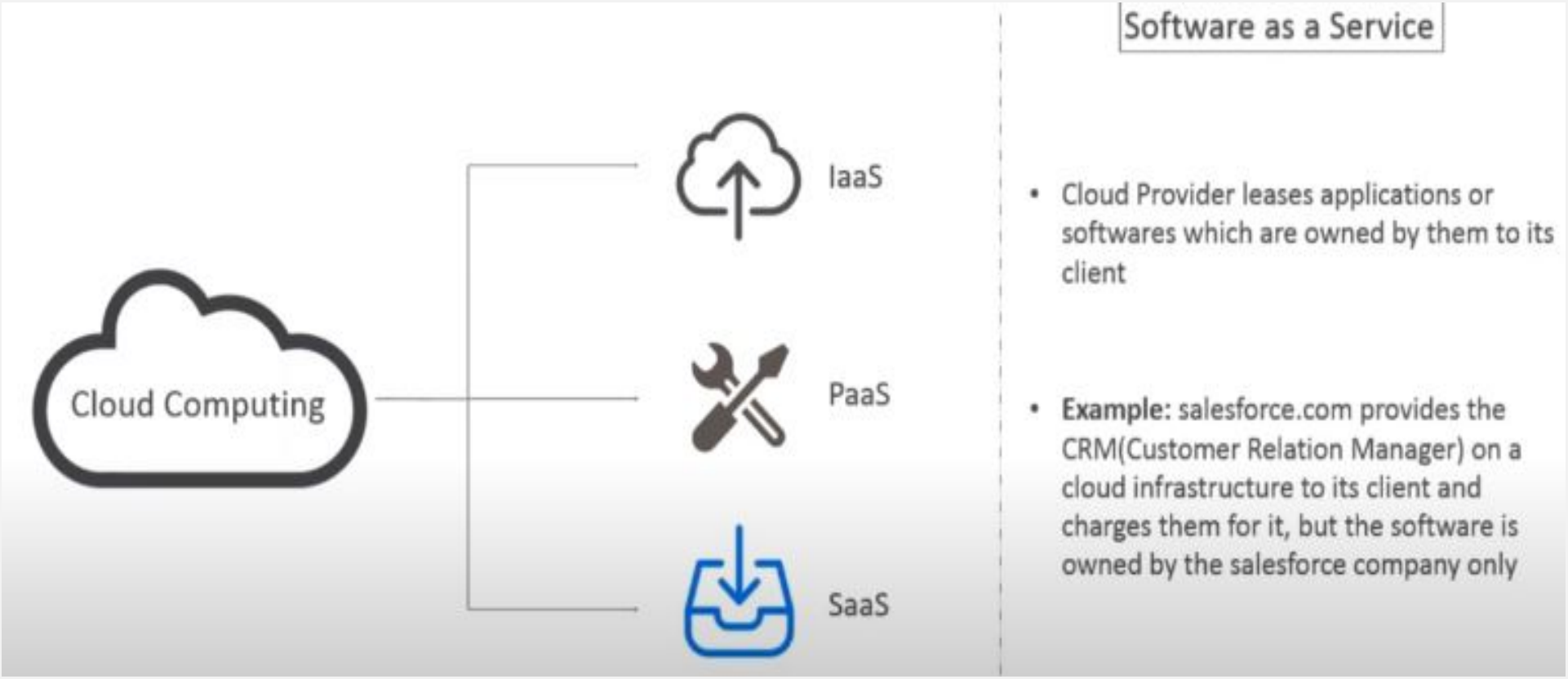
Service Models : PaaS

- In this model, companies don't pay for hosted applications; instead they pay for the things they need to build their own applications
- PaaS vendors offer everything necessary for building an application, including development tools, infrastructure, and operating systems, over the Internet
- PaaS can be compared to renting all the tools and equipment necessary for building a house, instead of renting the house itself
- PaaS examples include Heroku and Microsoft Azure

Service Models : Why PaaS?

- Preferred option for projects involving multiple developers and vendors
- Easy to create customized applications as it leases all the essential computing and networking resources
- PaaS simplifies the app development process that minimizes organizational costs
- It is flexible and delivers the necessary speed in the process, which rapidly improves development times
- Less flexible compared to the IaaS cloud model

Service Models : SaaS



Service Models : SaaS

- Instead of users installing an application on their device, SaaS applications are hosted on cloud servers, and users access them over the Internet
- SaaS is like renting a house: the landlord maintains the house, but the tenant mostly gets to use it as if they owned it
- Examples of SaaS applications include Salesforce, MailChimp, and Slack

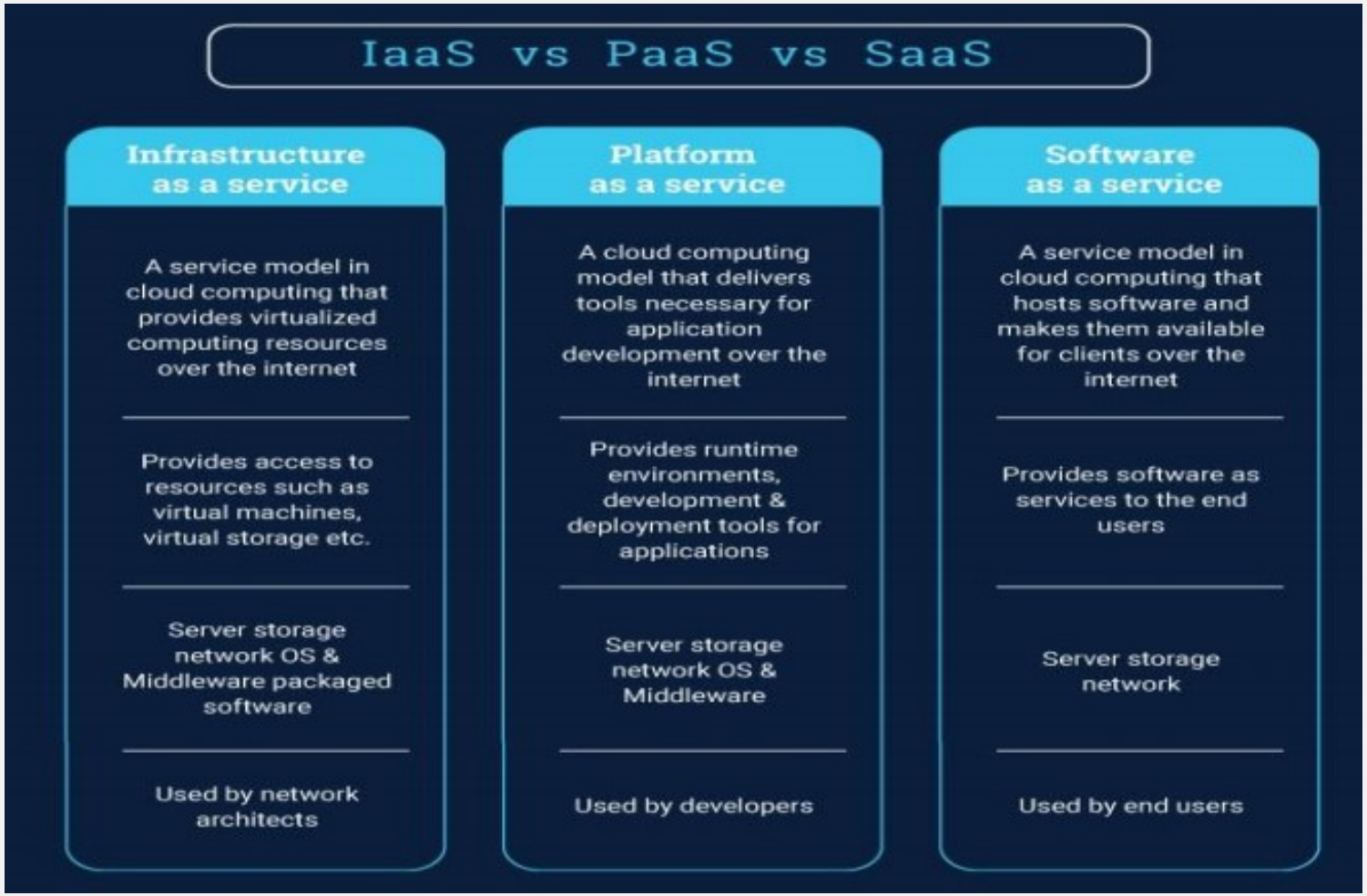
Service Models : Why SaaS?

- With SaaS, communication, transferring of content, and scheduling meetings are made easy
- Ideal choice for small-scale businesses
- Companies that do not have the necessary budget and resources to deploy on-premise hardware
- Organisations requiring frequent collaboration on their projects will find SaaS platforms useful
- Supply Chain Management, Business Intelligence, Enterprise Resource Planning (ERP), and Project and Portfolio Management are some high growth SaaS applications

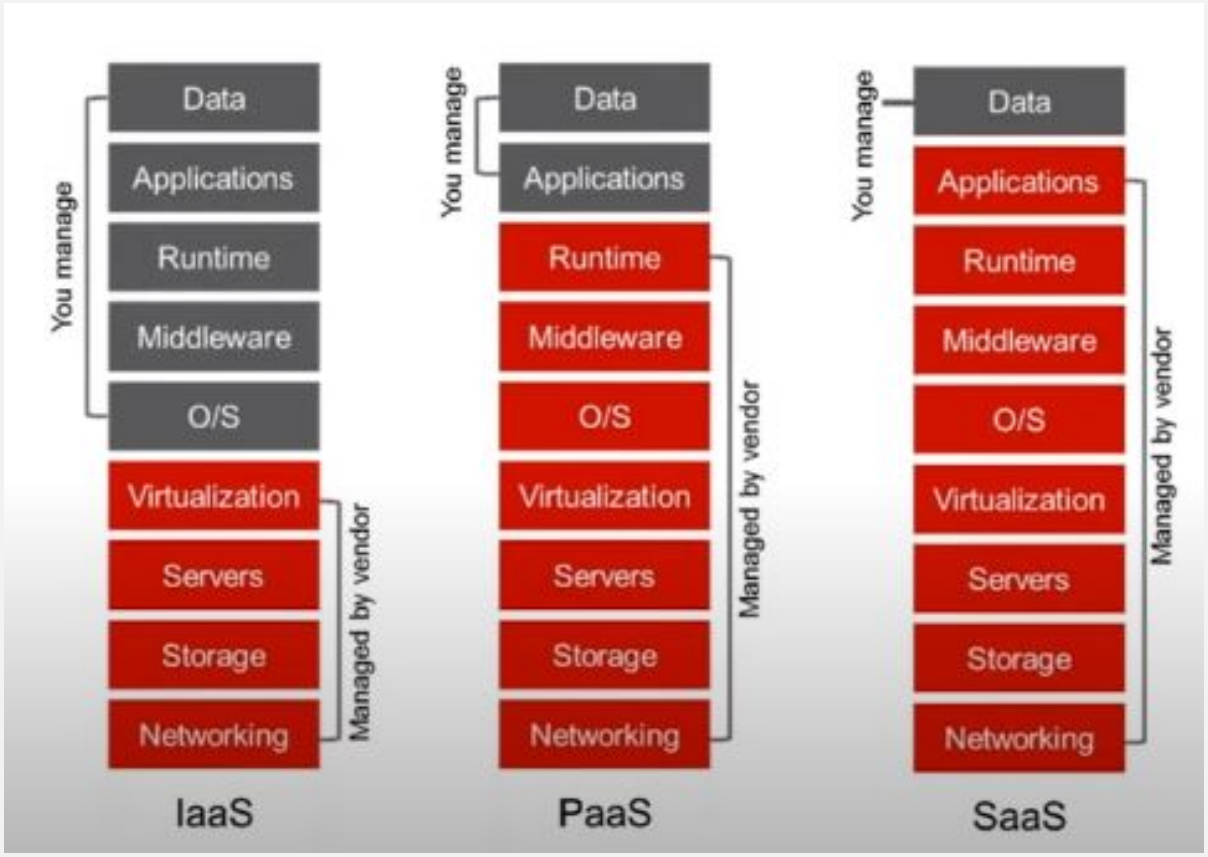
Service Models : Comparison

- IaaS - Best option where a complete virtual computing platform with powerful resources is required
- PaaS – Perfect choice if need is there to develop and test software and applications
- SaaS – Ideal for cloud-based software like email, CRM, and productivity tools

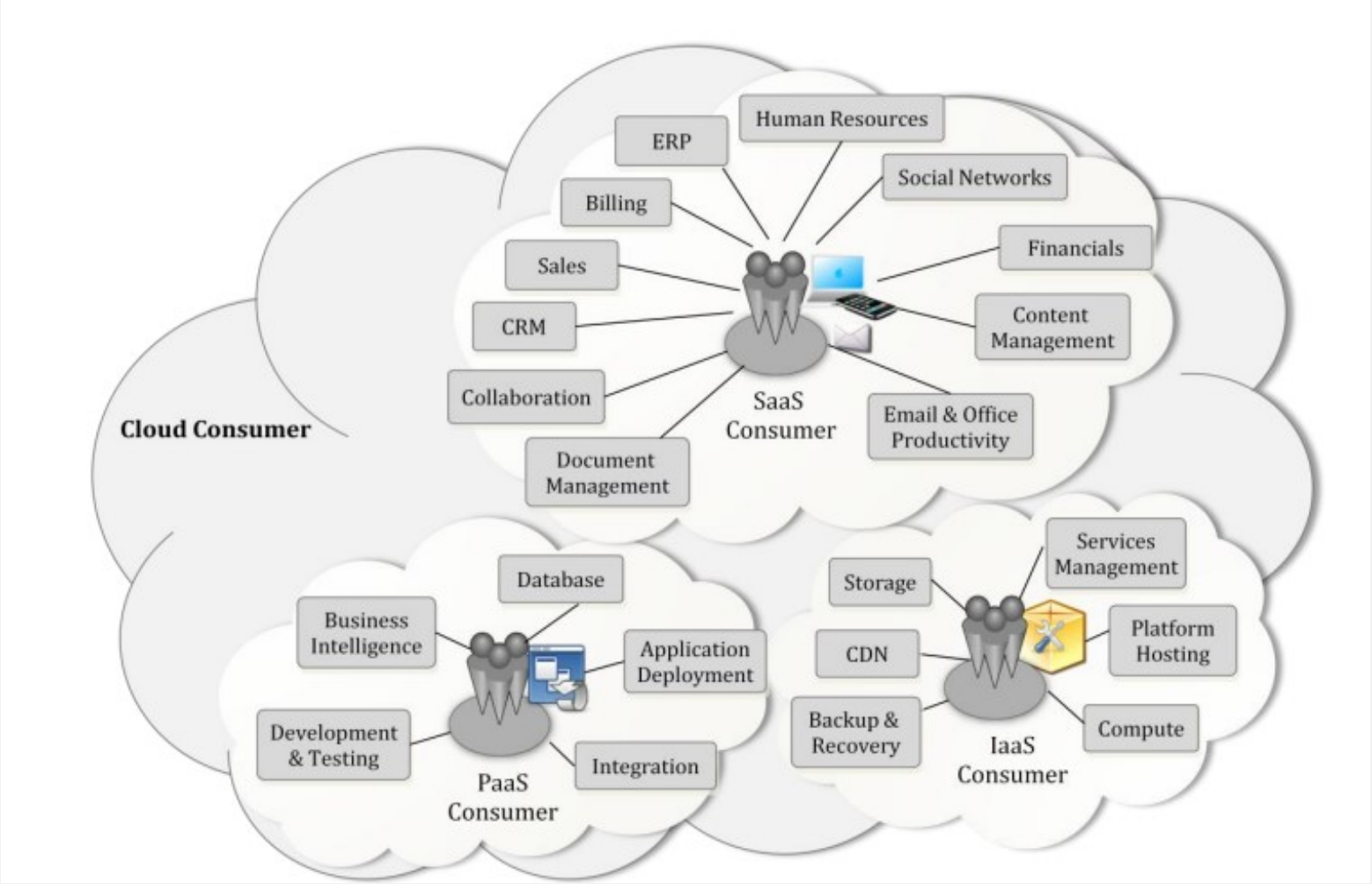
Service Models : Summary



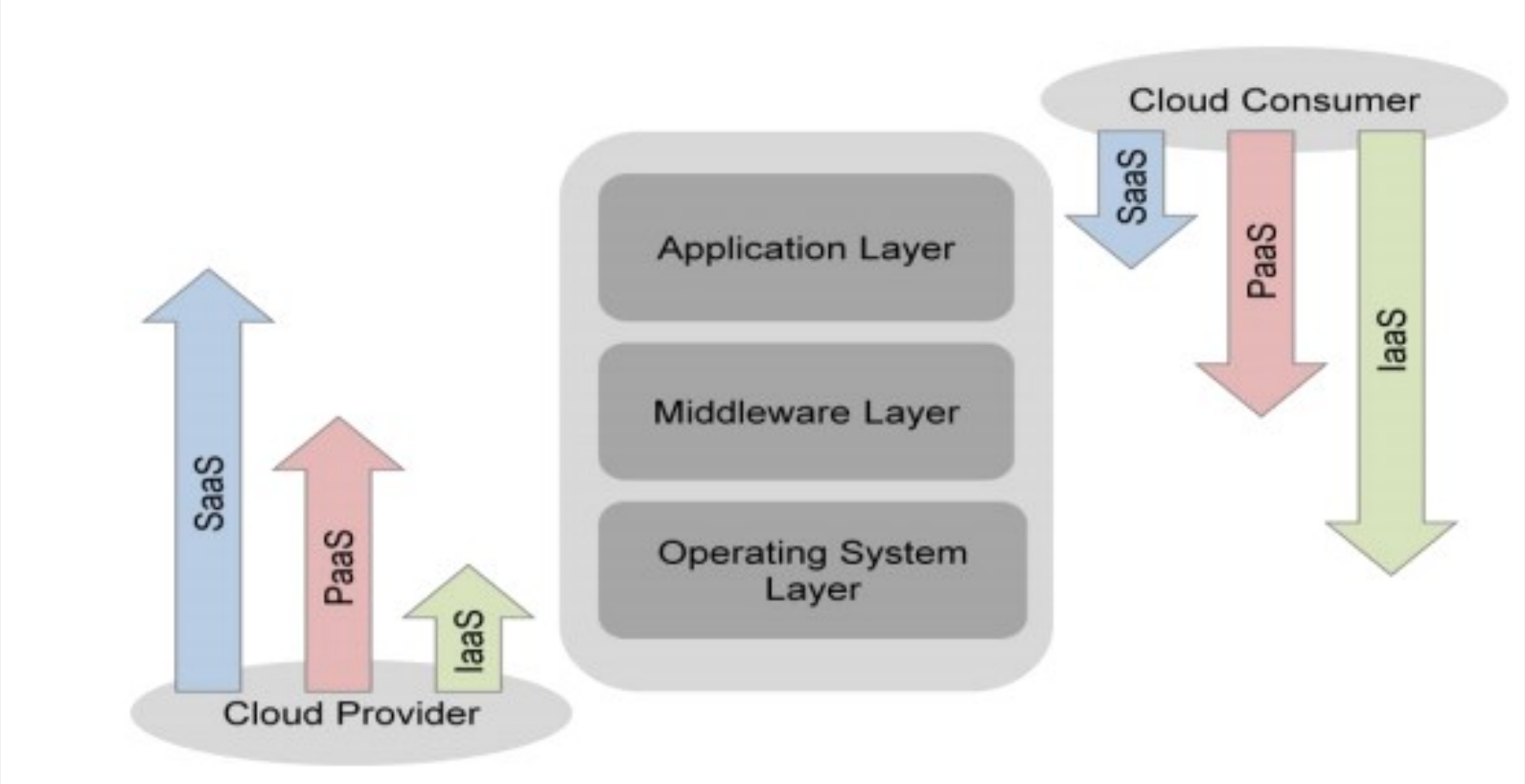
Service Models



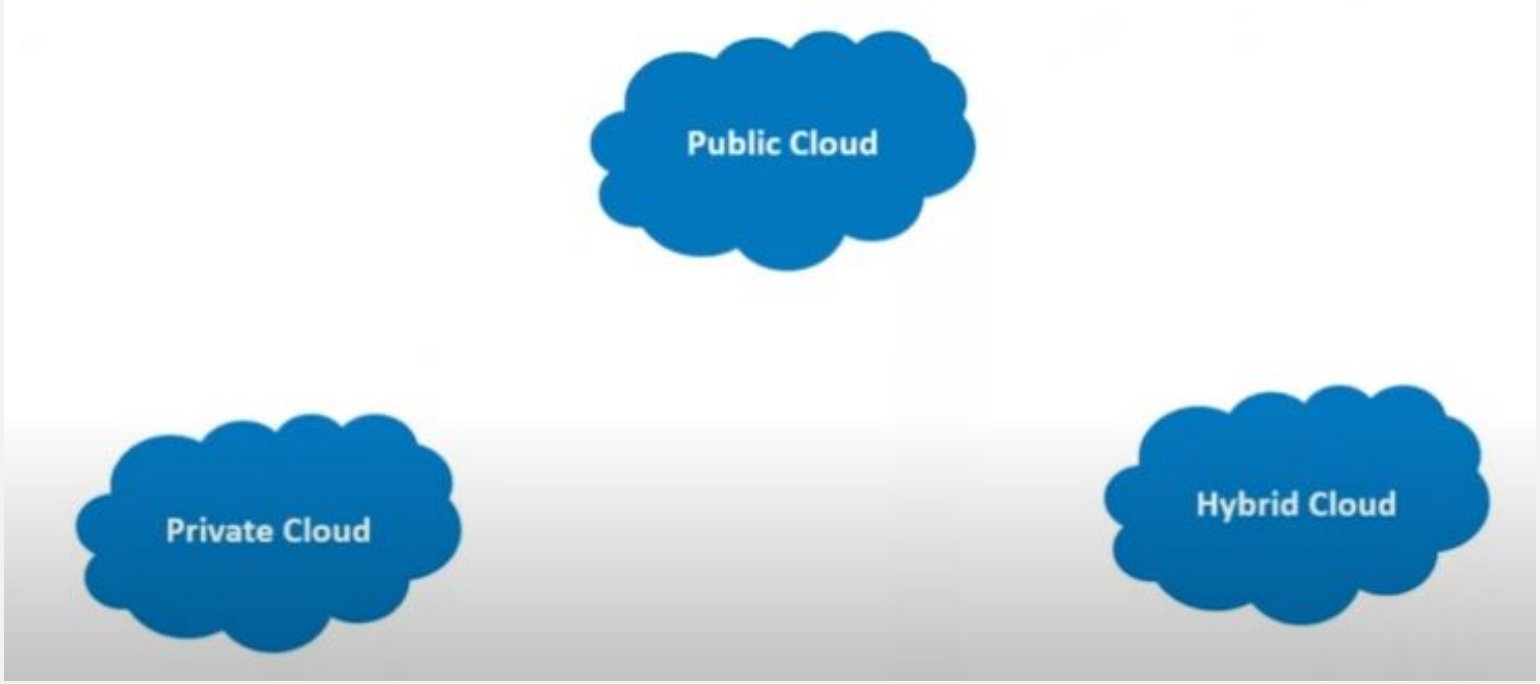
Cloud Consumer



Scope of Service Control : Provider & Consumer



Deployment Models



Cloud Deployment Models

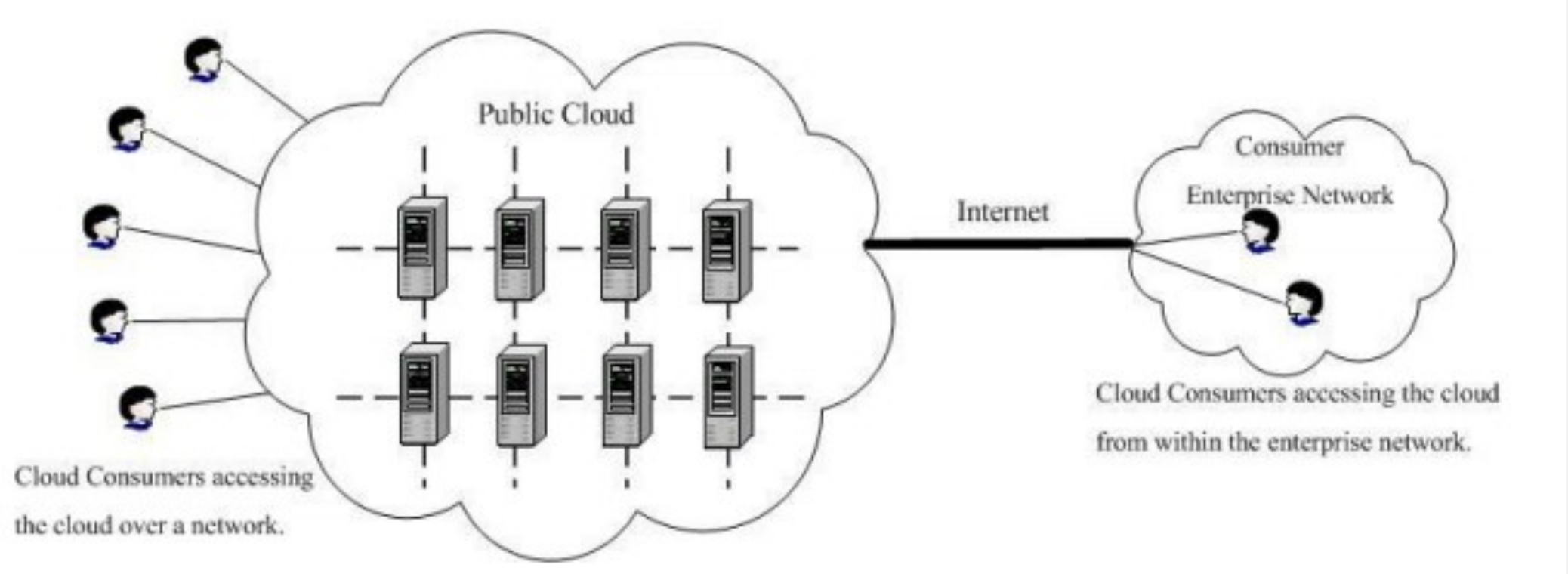
- Cloud deployment describes the way a cloud platform is implemented, how it's hosted, and who has access to it

- All cloud computing deployments operate on the same principle by virtualizing the computing power of servers into segmented, software-driven applications that provide processing and storage capabilities

- Types are
  - Public
  - Private
  - Hybrid
  - Community

Public Cloud

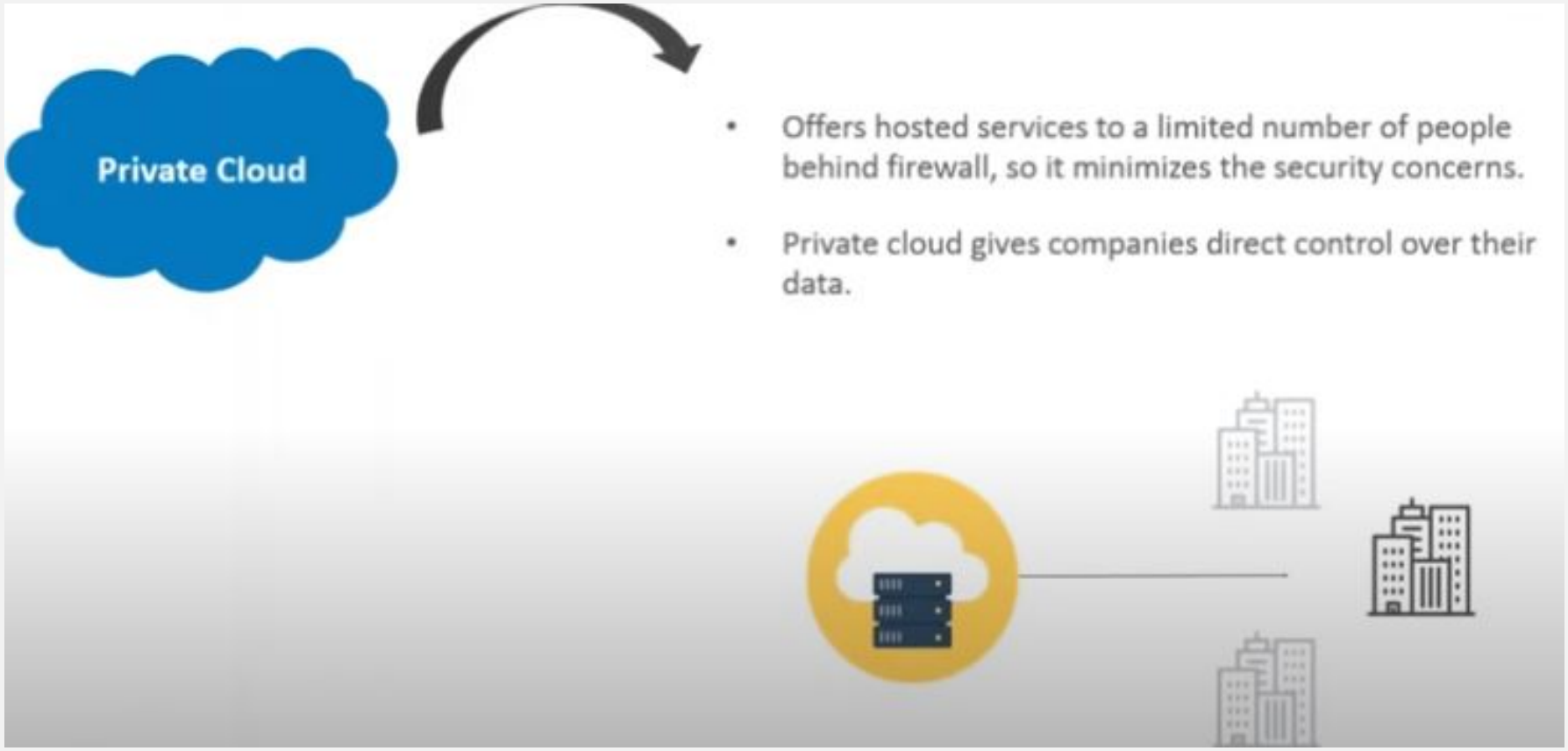
Public Cloud



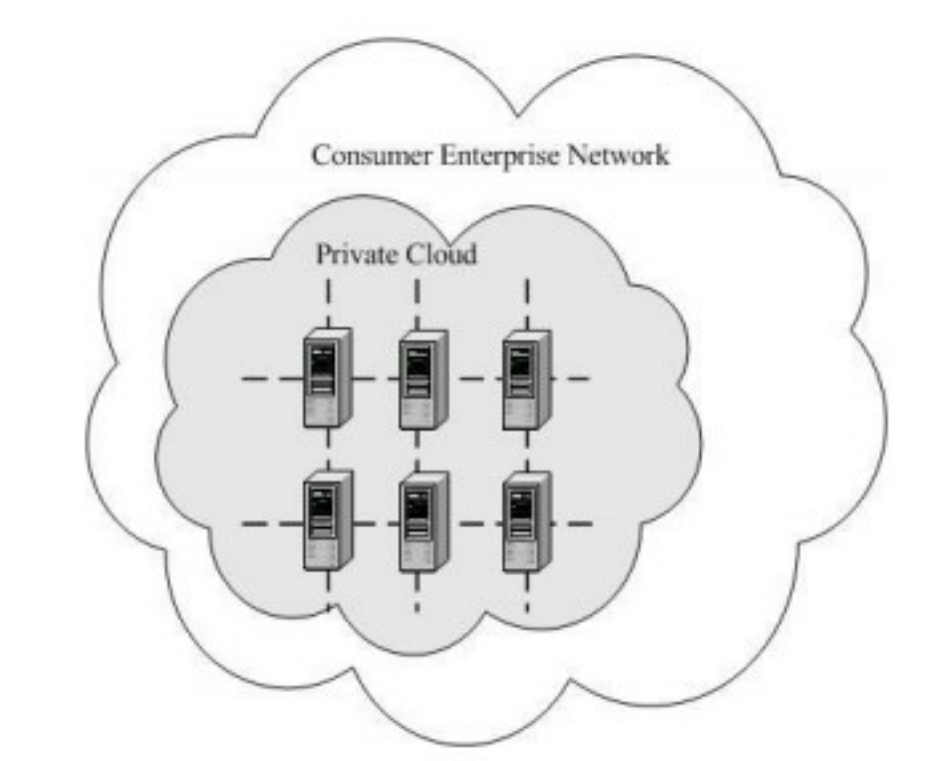
Public Cloud

- Cloud services provided for public use : Data is stored on third party servers
- Resources such as virtual machines, applications or storage are available to users remotely
- Services may be free/through subscription
- Versatility and “pay as you go” structure that allows customers to provision more capacity on demand
- It is also popular among businesses of all sizes for their web applications, webmail, and storage of nonsensitive data
- Public Cloud examples include those offered by Amazon, Microsoft, or Google

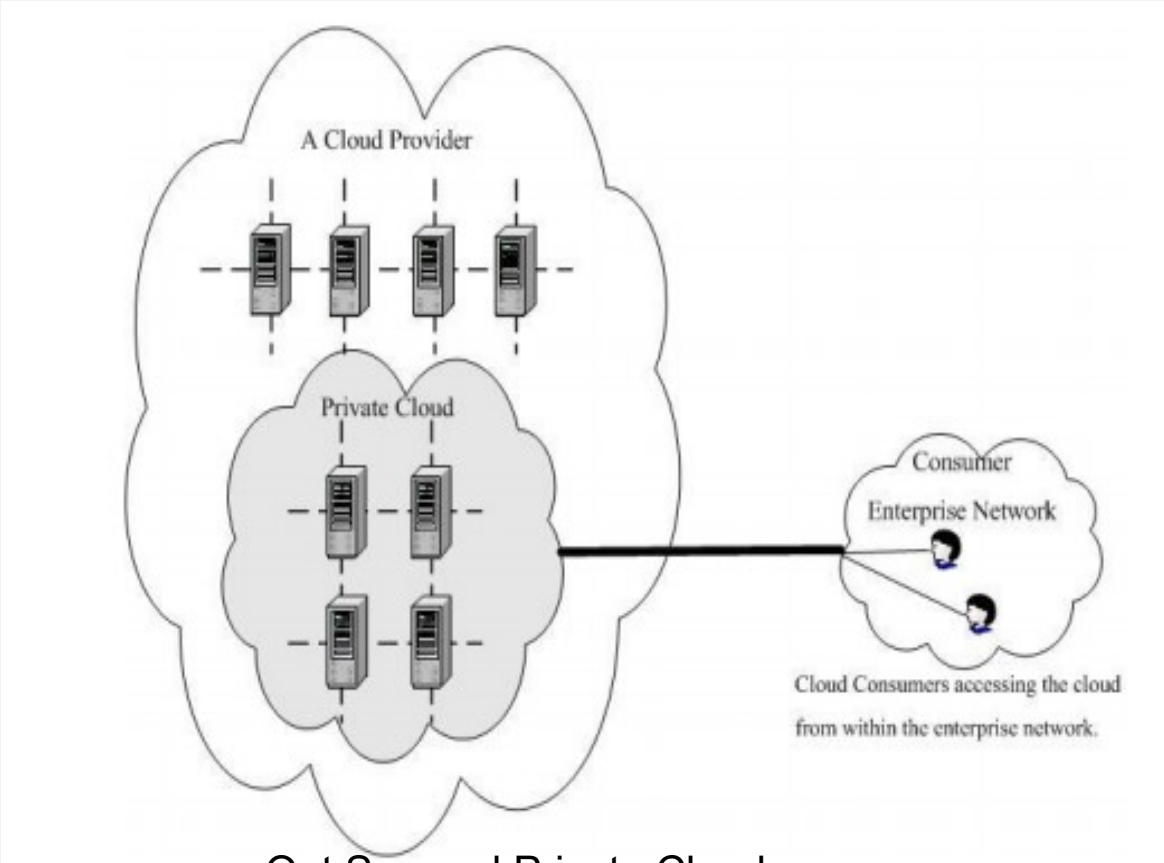
Private Cloud



Private Cloud



On Site Private Cloud

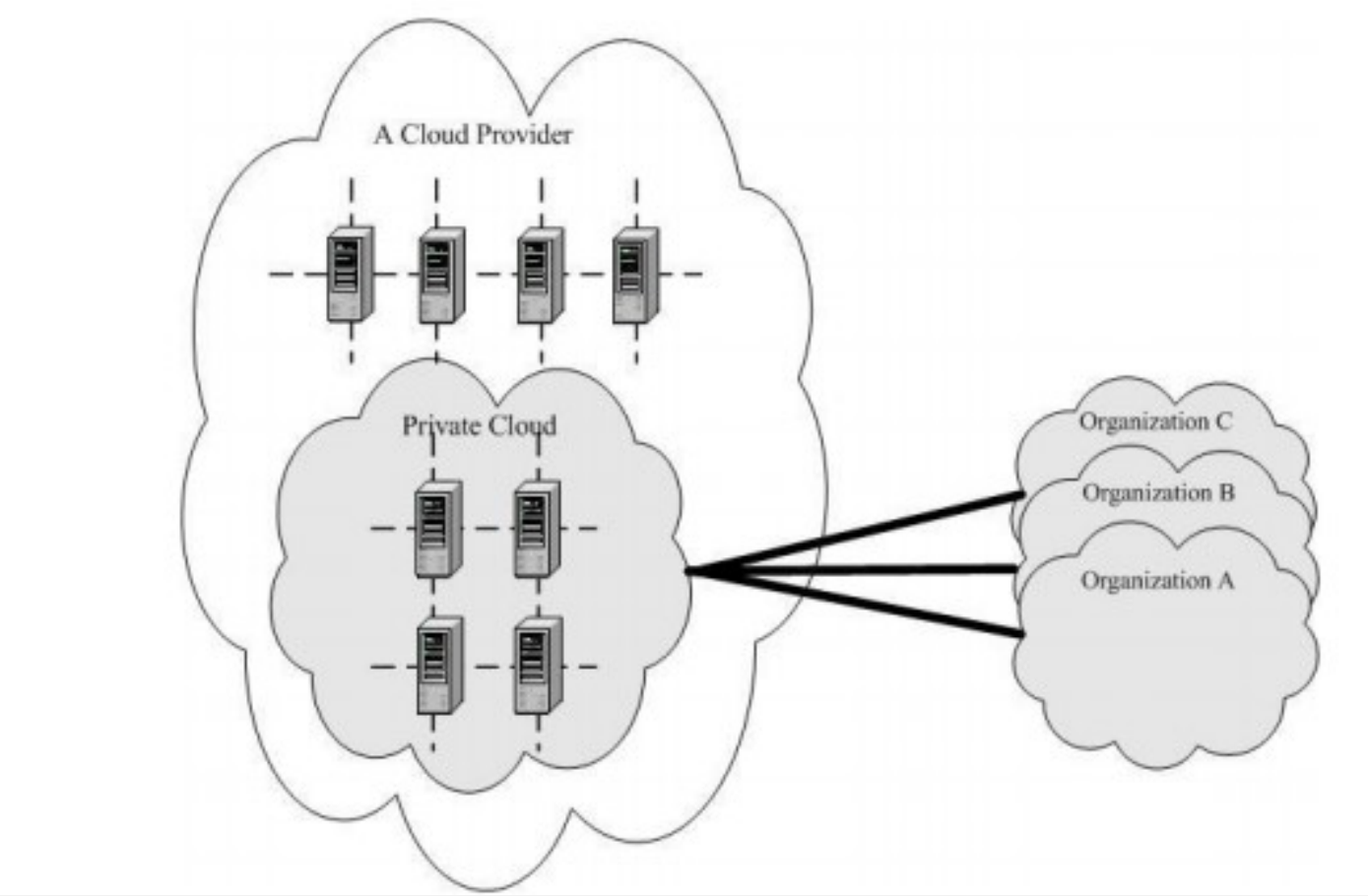


Out Sourced Private Cloud

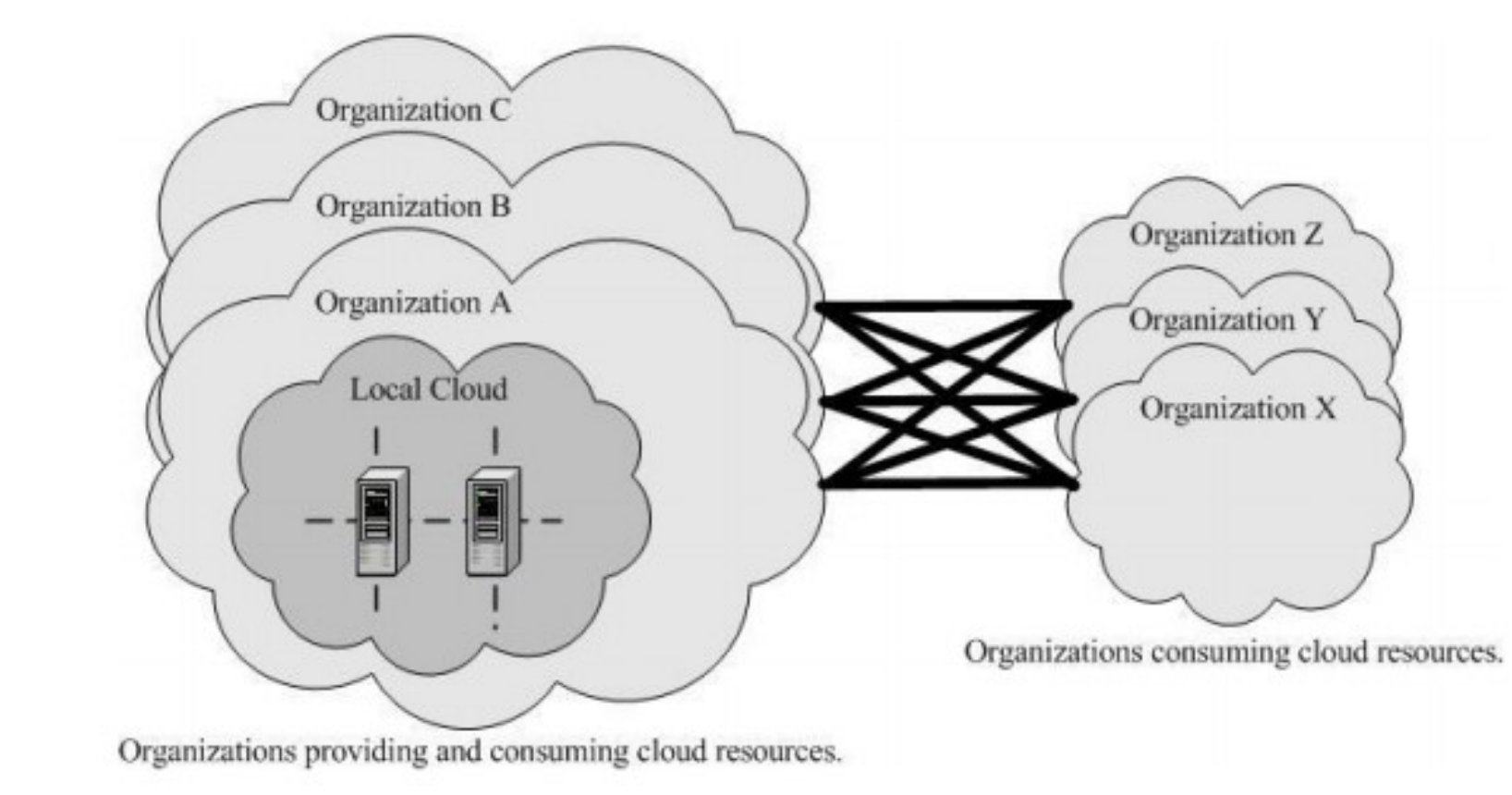
Private Cloud

- A private cloud is a cloud service that is not shared with any other organization
- The private cloud user has the cloud to themselves
- It offers greater control over security
- Private clouds are perfect for organizations that have high security requirements, high management demands and availability requirements
- The server can be hosted externally or on the premises of the owner company
- Multiple public cloud service providers, including Amazon, IBM, Cisco, Dell and Red Hat, also provide private solutions
- Highly scalable, secure, reliable and with privacy but at a high cost

Community Cloud



Community Cloud

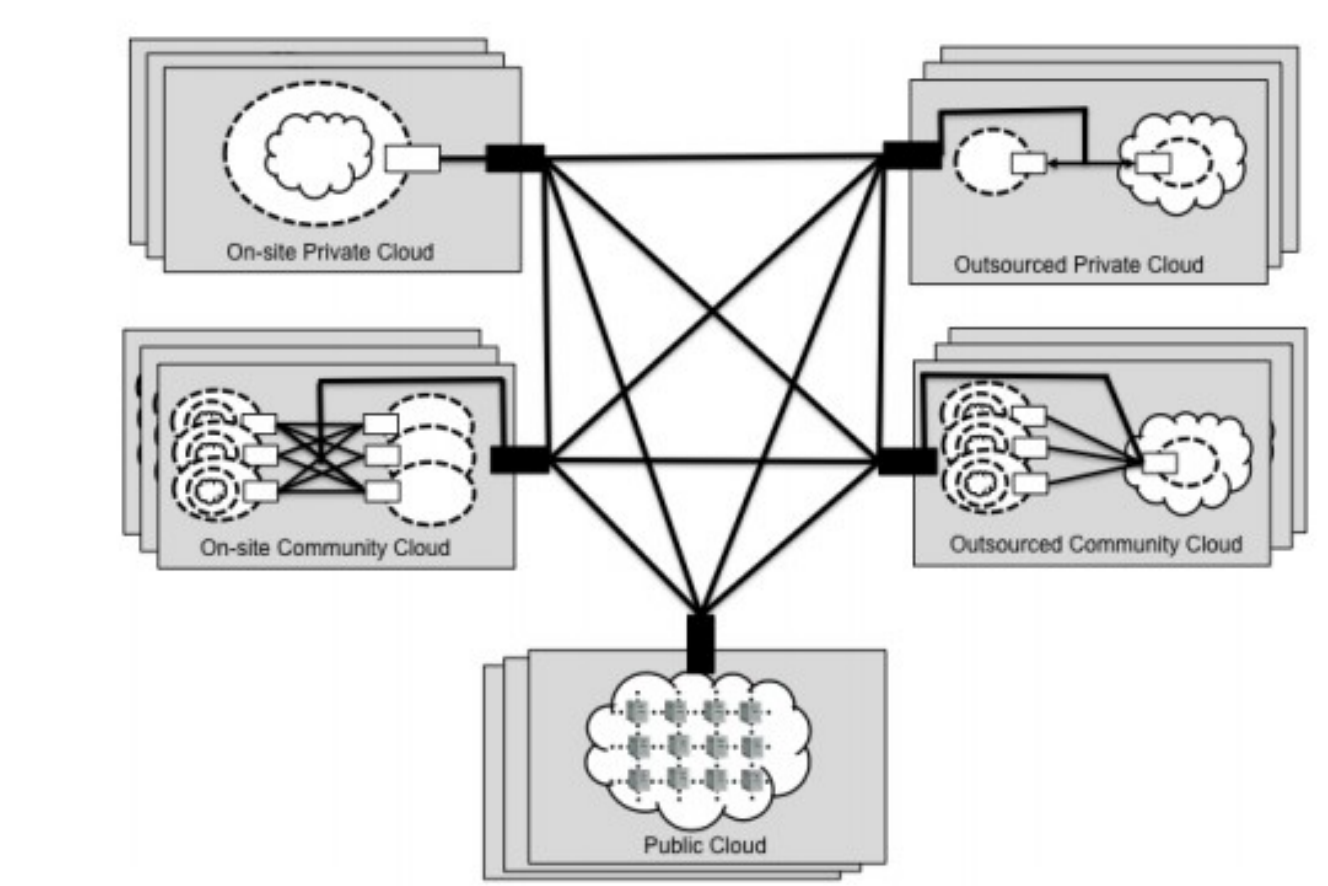


Community Cloud

- A community cloud is a private cloud that functions much like a public cloud
- Collaborative, multi-tenant platform used by several distinct organizations to share the same applications
- Users are typically operating within the same industry or field and share common concerns in terms of security, compliance, and performance
- Cost reduction, Improved security, privacy and reliability, Ease of data sharing and collaboration
- E.g. Government agencies, healthcare organizations, financial services firms, and other professional communities

Hybrid Cloud

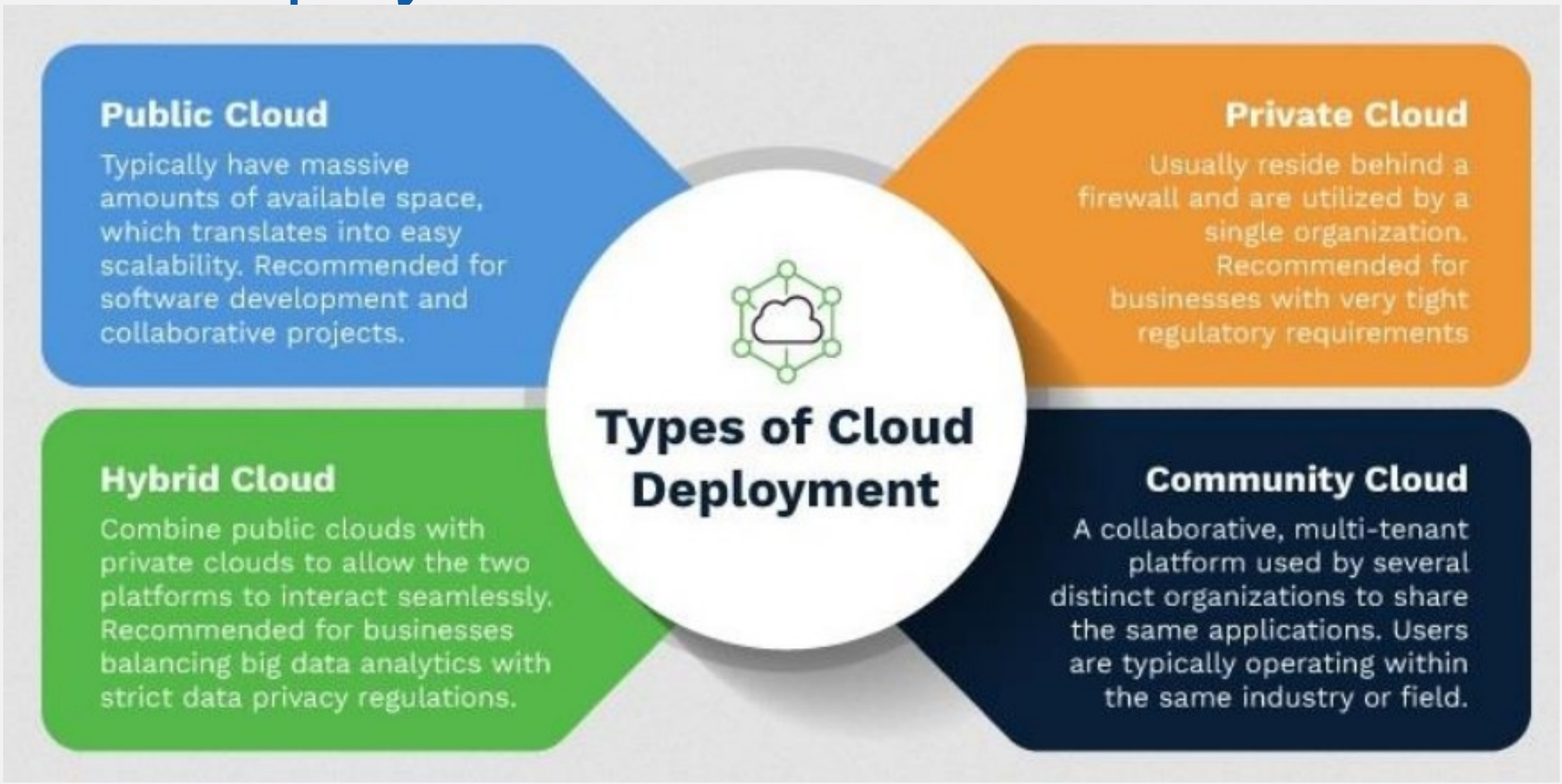
Hybrid Cloud



Hybrid Cloud

- A mixture of public and private cloud
- The critical activities are performed using private cloud while the non-critical activities are performed using public cloud
- The best features of the three deployment models is taken
- Mission-critical workloads on a secure private cloud and deploying less sensitive ones to a public one
- Benefits are Improved security and privacy,
- Enhanced scalability and flexibility and Reasonable price

Cloud Deployment Models



Research Challenges

- Denial of service
- Security & privacy
- Lack of standards
- Reliability - No Direct Control over Outsourced Data
- Semi-Trusted Cloud Server - Verification of Computational Result

Cloud Security??

- Cloud security is the set of strategies and practices for protecting data and applications that are hosted in the cloud
- Like cyber security, cloud security is a very broad area, and it is never possible to prevent every variety of attack.
- However, a well-designed cloud security strategy vastly reduces the risk of cyber attacks
- The goal of a cloud security strategy is to reduce the threat posed by these risks as much as possible by protecting data, managing user authentication and access, and staying operational in the face of an attack

Cloud cyber attack

"Any cyber attack that targets off-site service platforms that offer storage, computing, or hosting services via their cloud infrastructure can be classified as a cloud cyber attack. This can include attacks on service platforms that utilise service delivery models like SaaS, IaaS, and PaaS."

Cloud cyber attack :Example

- **CAM4—2020**
  - CAM4 is an adult live streaming website that fell victim to a cloud cyber attack in March 2020 that exposed 10.8 billion sensitive entries amounting to 7 TB of data. The leaked database included location details, email addresses, IP addresses, payment logs, usernames and more.

- **Keepnet Labs—2020**
  - One of the more ironic cloud data breaches of 2020, the Keepnet Labs data breach involved a leaky ElasticSearch database that contained entries that were previously exposed by various data breaches across the globe. The database included two data collections containing 5 billion and 15 million entries respectively.

- **Microsoft—2019**
  - On January 22, 2020, Microsoft announced that one of their cloud databases was breached back in December 2019, resulting in the exposure of 250 million entries, including email addresses, IP addresses, and support case details.

Cloud computing vulnerabilities

- Data threats
  - data is susceptible to loss, breach, or damage as the result of human actions, application vulnerabilities, and unforeseen emergencies.
- Cloud API vulnerabilities
  - vulnerabilities in APIs may significantly impact the security of cloud orchestration, management, provisioning, and monitoring
- Malicious insiders
- Shared technology vulnerabilities
  - Weaknesses in a hypervisor can allow hackers to gain control over virtual machines or even the host itself.
- Weak cryptography
- Vulnerable cloud services

Attack Vectors for Cloud Computing

- When arranging attacks in the cloud, hackers usually intrude into communications between cloud users and services or applications by:
  - exploiting vulnerabilities in cloud computing;
  - stealing users' credentials somewhere outside the cloud;
  - using prior legitimate access to the cloud after cracking a user's passwords;
  - acting as a malicious insider.
  - compromise the cloud by brute-force attacks and/or DDoS
  - compromise of the cloud by phishing campaigns

Cloud Threats

- Cloud malware injection attacks
  - infected service implementation module to a SaaS or PaaS solution or a virtual machine instance to an IaaS solution.
  - General Forms are : cross-site scripting attacks and SQL injection attacks
  - XSS attack against the AWS cloud computing platform in 2011.
  - Sony PlayStattion was victim of SQL injection attack in 2008

- Abuse of Cloud Services
  - use cheap cloud services to arrange DoS and brute force attacks
  - Bryan and Anderson arranged a DoS using Amazon's EC2 cloud infrastructure in 2010, by spending only $6 to rent virtual services.

Cloud Threats

- Denial of service attacks
  - DDoS attacks may be even more dangerous if hackers use more zombie machines to attack a large number of systems.
- Side channel attacks
  - malicious virtual machine on the same host as the target virtual machine
- Wrapping attacks
- Man-in-the-cloud attacks

Cloud Threats

- Insider attacks
- Account or service hijacking
  - Access to user's credential's using fishing to spyware to cookie poisoning
  - an employee of Salesforce, a SaaS vendor, became the victim of a phishing scam which led to the exposure of all of the company's client accounts in 2007
- Advanced persistent threats (APTs)
- New attacks: Spectre and Meltdown
  - With the help of malicious JavaScript code, adversaries can read encrypted data from memory

Cloud Threats

- **Data Breaches.** If access to event logs is not there then it can be nearly impossible to identify who has been affected by a data breach and what data was compromised. CSP has to have event logging solutions and should provide access to those event logs in case of a data breach

- **Misconfiguration and Inadequate Change Control.** In 2017, a misconfigured AWS Simple Storage Service (S3) cloud storage bucket exposed detailed and private data of 123 million American households

- **Lack of Cloud Security Architecture and Strategy.** Lack of security controls during migration to cloud. Cloud migration is not a “lift-and-shift” endeavor of simply porting existing IT stack and security controls to a cloud environment

Cloud Threats

- **Insufficient Identity, Credential, Access and Key Management.** Traditional IAM practices do not work on clouds. CSP and consumer need to work in sync
- **Account Hijacking.** Malicious attackers can gain access to and abuse accounts that are highly privileged or sensitive
- **Insider Threat.** 58 percent of companies attribute security breaches to insiders
- **Insecure Interfaces and APIs.** Cloud providers expose a set of software user interfaces and APIs to allow customers to manage and interact with cloud services. Poorly designed APIs could lead to misuse or data breach

Cloud Threats

- **Weak Control Plane.** A weak control plane means the person in charge is not in full control of the data infrastructure's logic, security and verification

- **Limited Cloud Usage Visibility.** Limited cloud usage visibility occurs when an organization does not possess the ability to visualize and analyze whether cloud service use within the organization is safe or malicious

- **Abuse and Nefarious Use of Cloud Services.** Cloud computing resources can be used to target organizations or users. Malicious attackers can also host malware on cloud services

Cloud Threats : Prevention Techniques

- Enhance security policies
- Use strong authentication
- Implement access management
- Protect data
  - at the source (on the user's side)
  - in transit (during its transfer from the user to the cloud server)
  - at rest (when stored in the cloud database)
- Detect intrusions
- Secure APIs and access
- Protect cloud services

Cloud Accountability

- In the context of cloud computing, **accountability** is all about developing a **holistic approach** to achieving trust and security in the cloud, encompassing
  - Legal,
  - Regulatory, and
  - Technical

  mechanisms

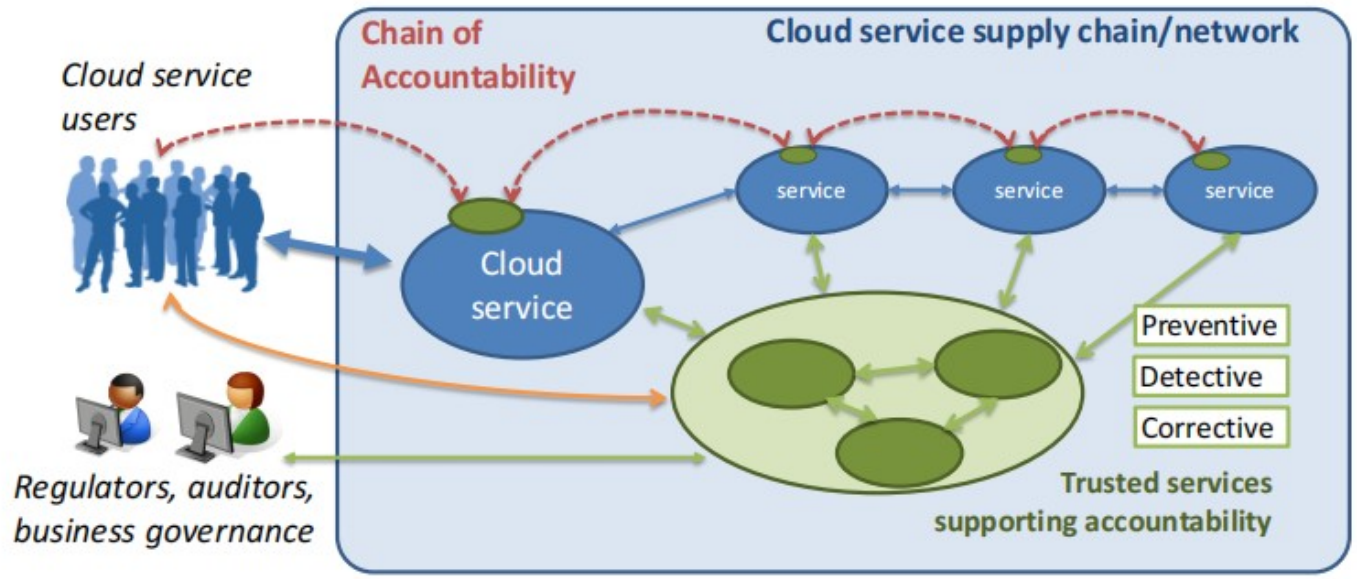
What is Accountability?

– "Accountability is the obligation to act as a responsible steward of the personal information of others, to take responsibility for the protection and appropriate use of that information beyond mere legal requirements, and to be accountable for any misuse of that information."

Accountability in the Cloud

- In the context of cloud, accountability is a set of approaches to addresses two key problems:
  - **Lack of consumer trust** in cloud service providers
  - **Difficulty** faced by cloud service providers **with compliance** across geographic boundaries
- Emphasis is on **data protection,** but the notion of accountability encompasses more than just privacy

Accountability in the Cloud

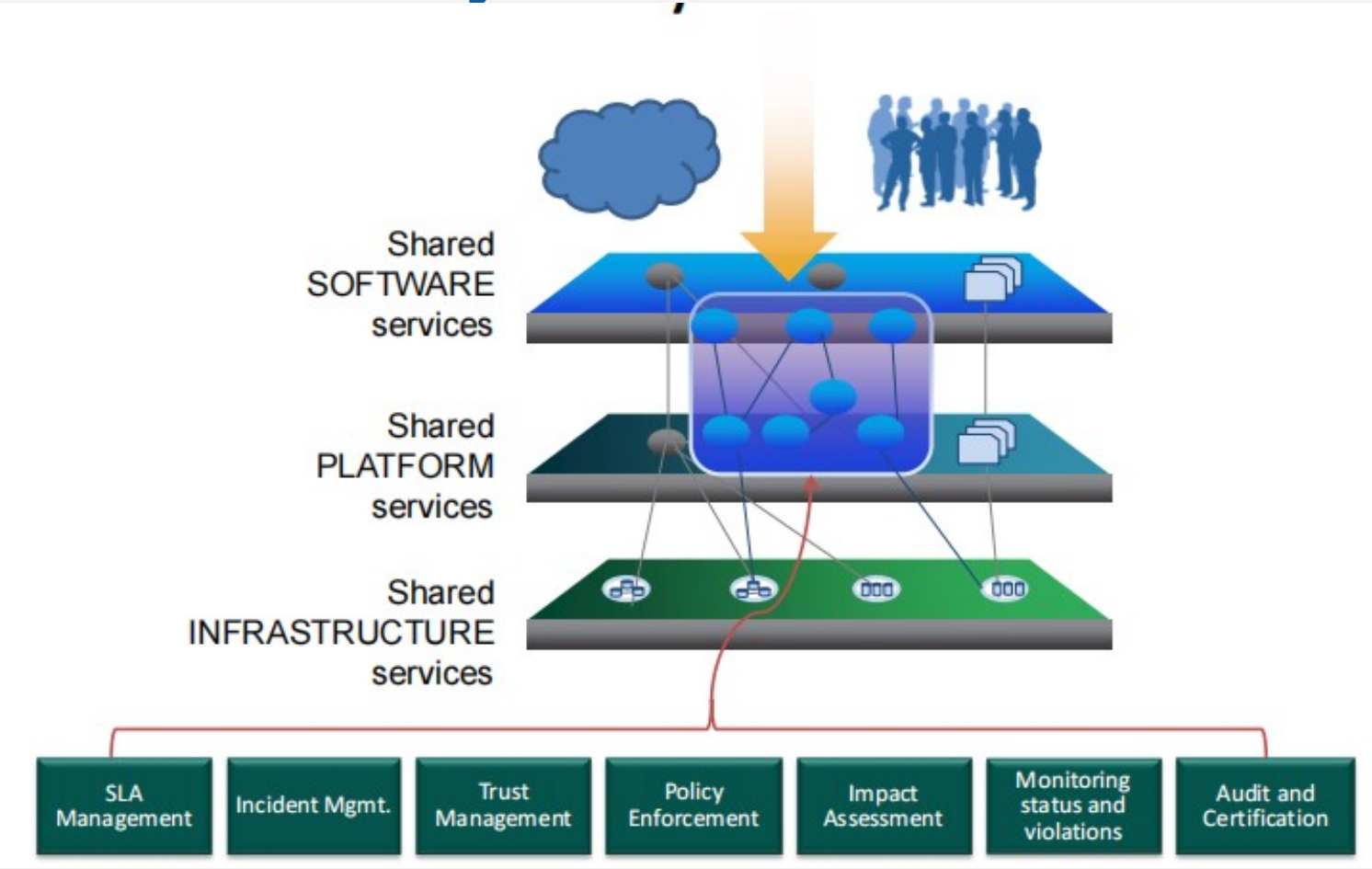


Cloud service users: control and transparency over how their data is used, and support in obtaining redress

Service providers: techniques to make services more trustworthy, satisfy business policies and allow differentiation

Regulators/auditors: assurance about compliance with policies and regulations

Solution : Mechanism for Achieving Accountability in the Cloud



Technical Mechanisms for Accountability in the Cloud

- **Preventive controls**
  - Risk analysis and decision support tools
  - Policy enforcement mechanisms (access control, obligations, ...)
  - Data Obfuscation
  - Identity management
- **Detective controls**
  - Intrusion detection systems
  - Transaction logs
  - Language frameworks for expressing security properties
  - Verification tools
- **Corrective controls**
  - Incident management plans
  - Dispute resolution methods
  - Other forms or remediation