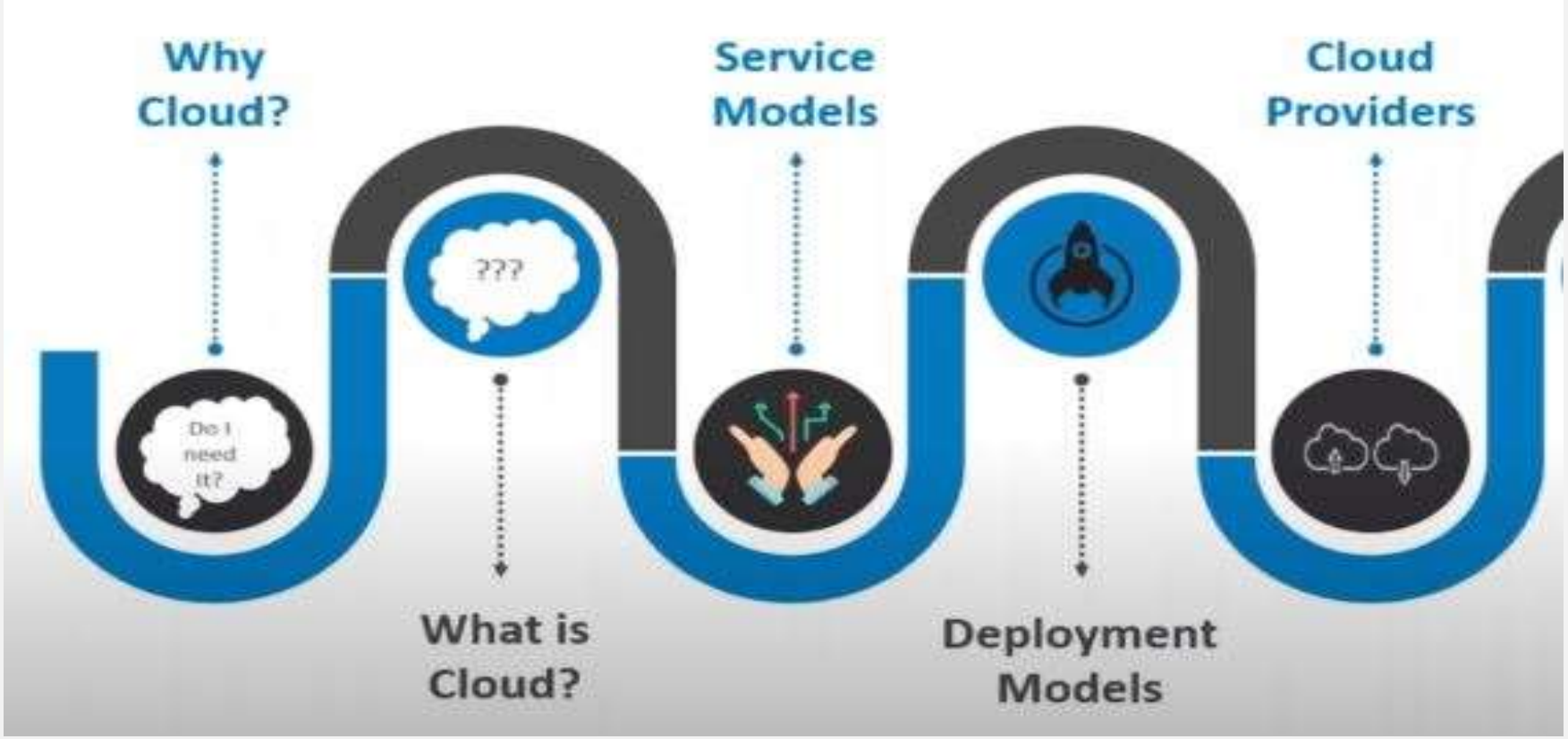
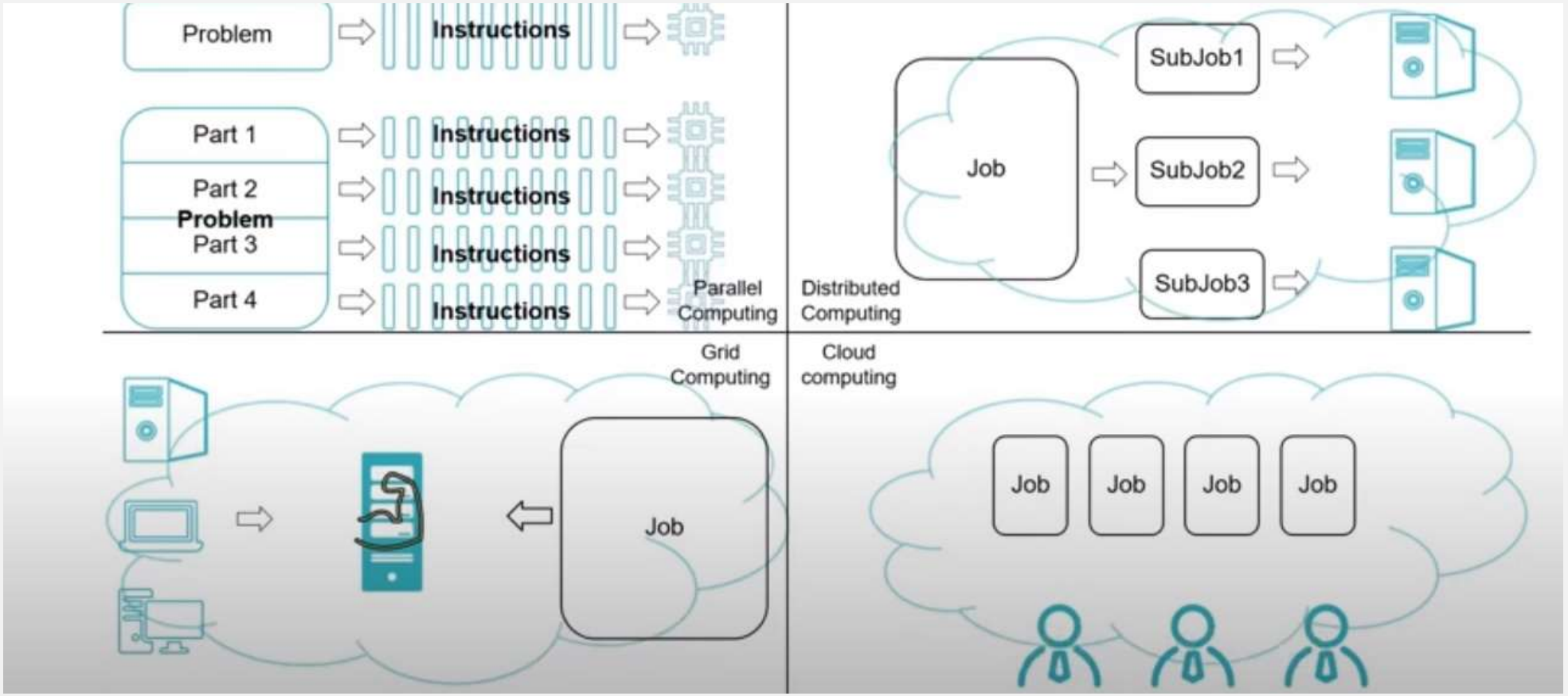
Introduction to Cloud

Dr. Mukti Padhya
Assistant Professor, NFSU

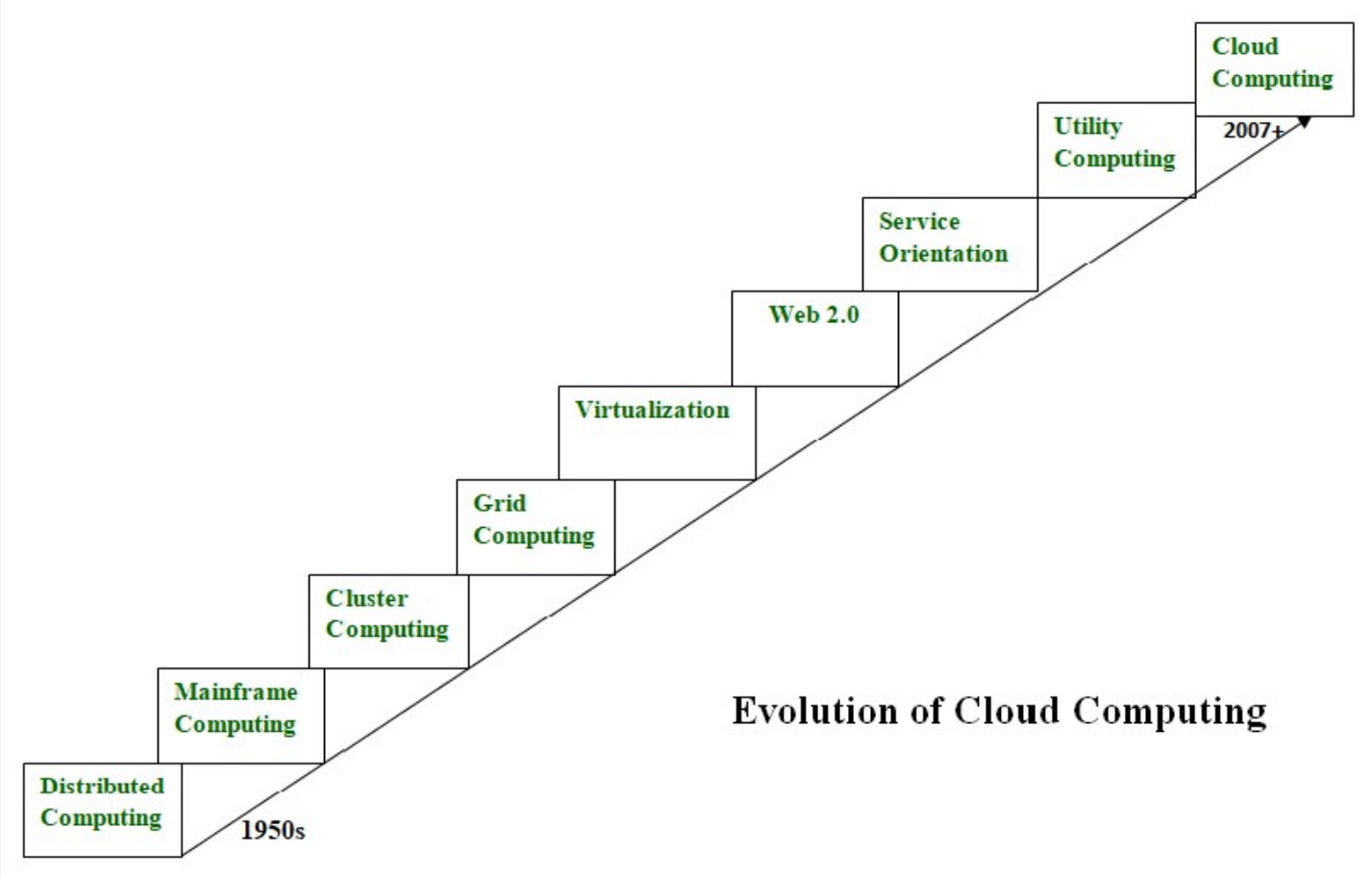
Offerings of This Session : Unit I



Evolution of Cloud Computing



Evolution of Cloud Computing

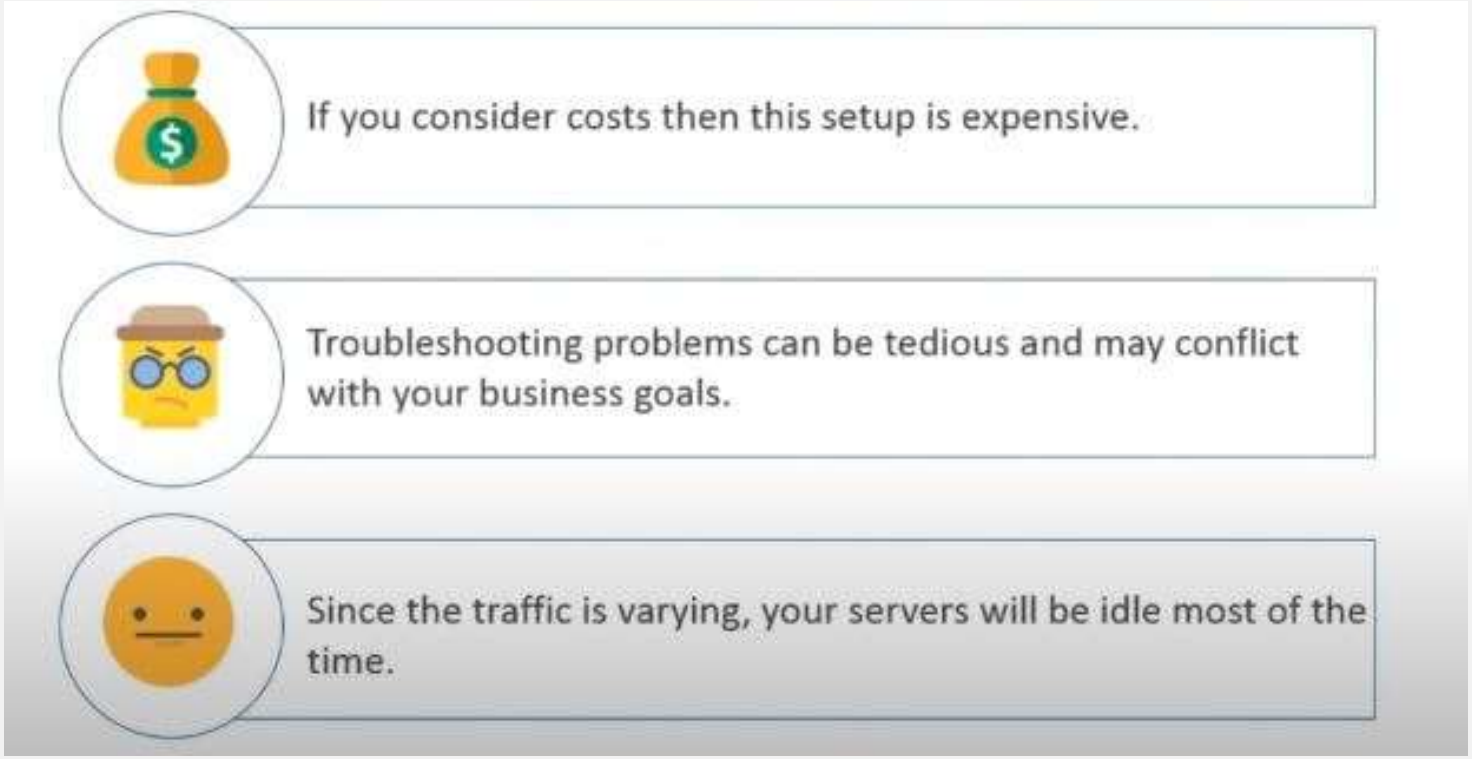


For Details Refer : https://www.geeksforgeeks.org/evolution-of-cloud-computing/

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?

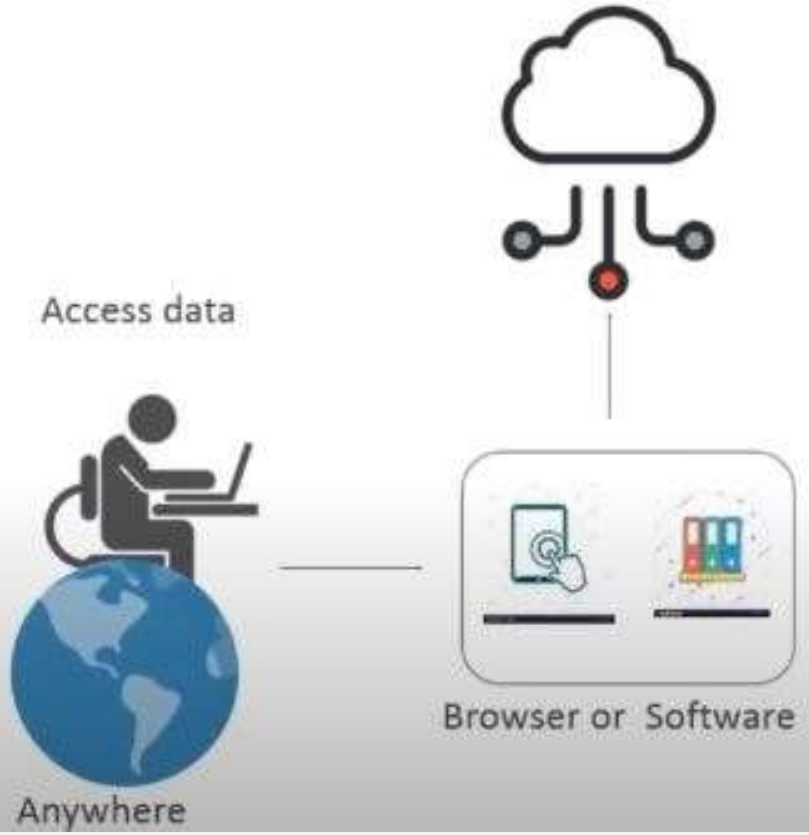
What is Cloud?

- 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."

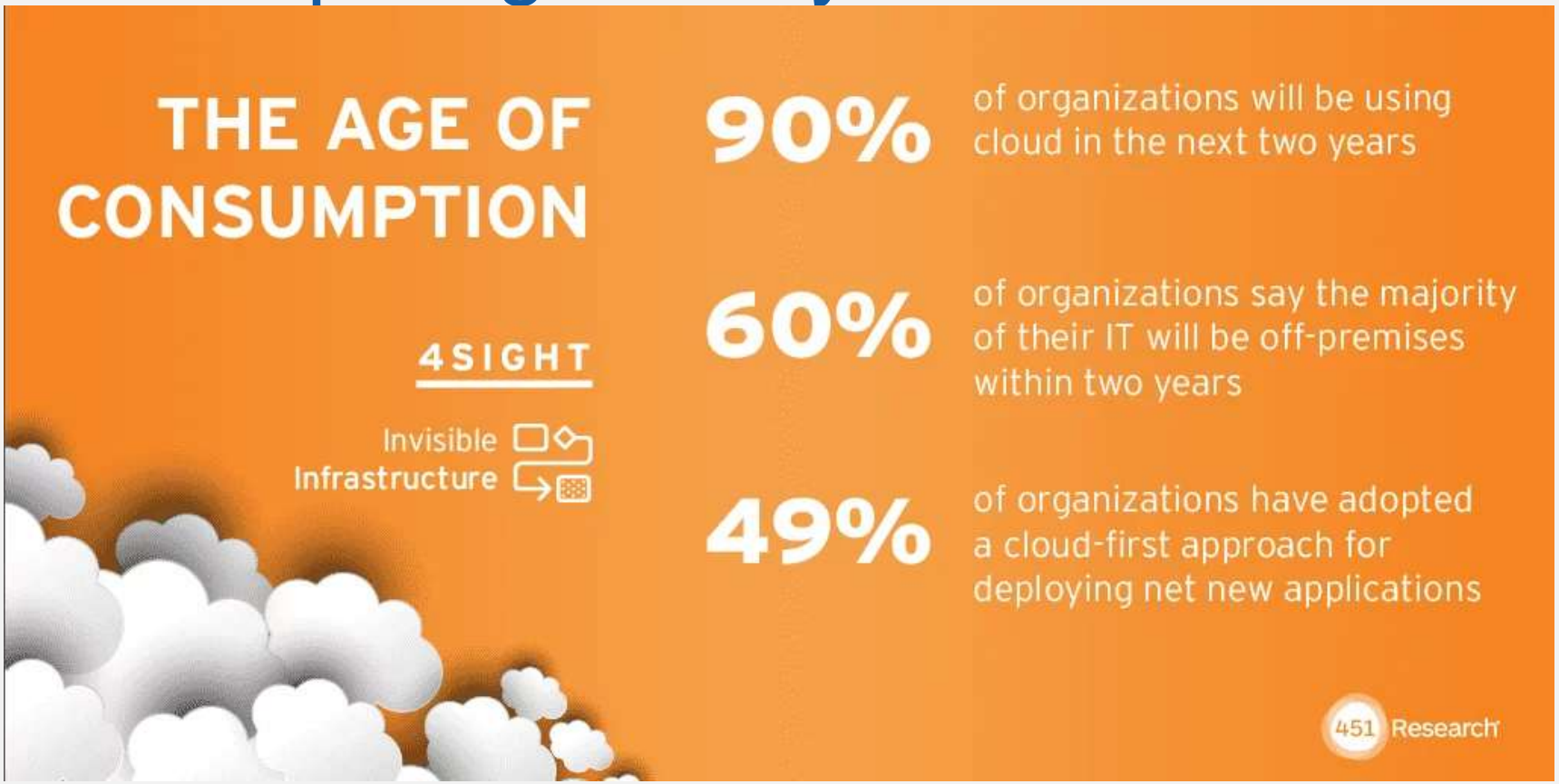
- National Institute of Standards and Technology (NIST)

Cloud : DataCenter

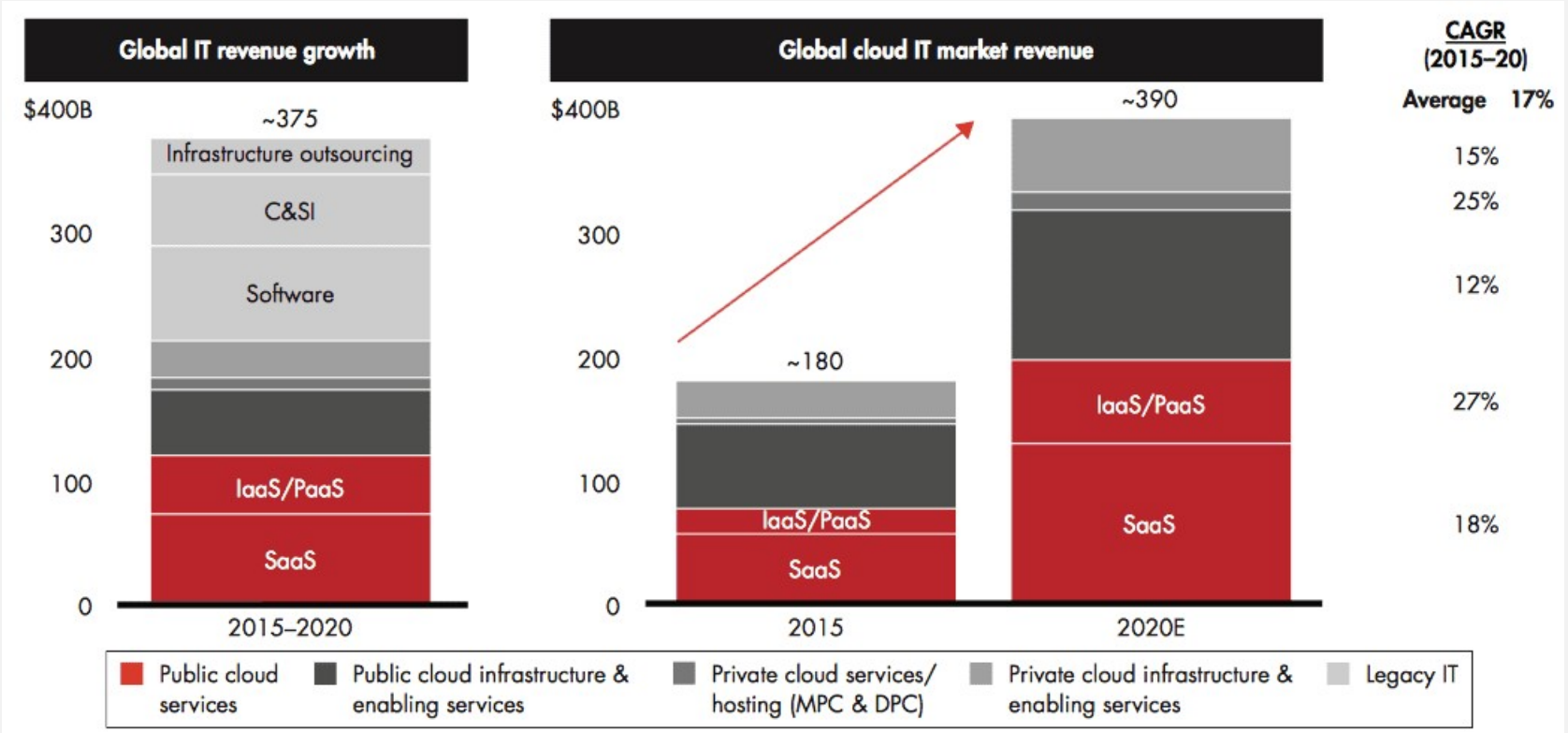
- Clouds can be built with physical or virtualized resources over large data centers that are distributed systems. Cloud computing is also considered to be a form of utility computing or service computing.

- 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



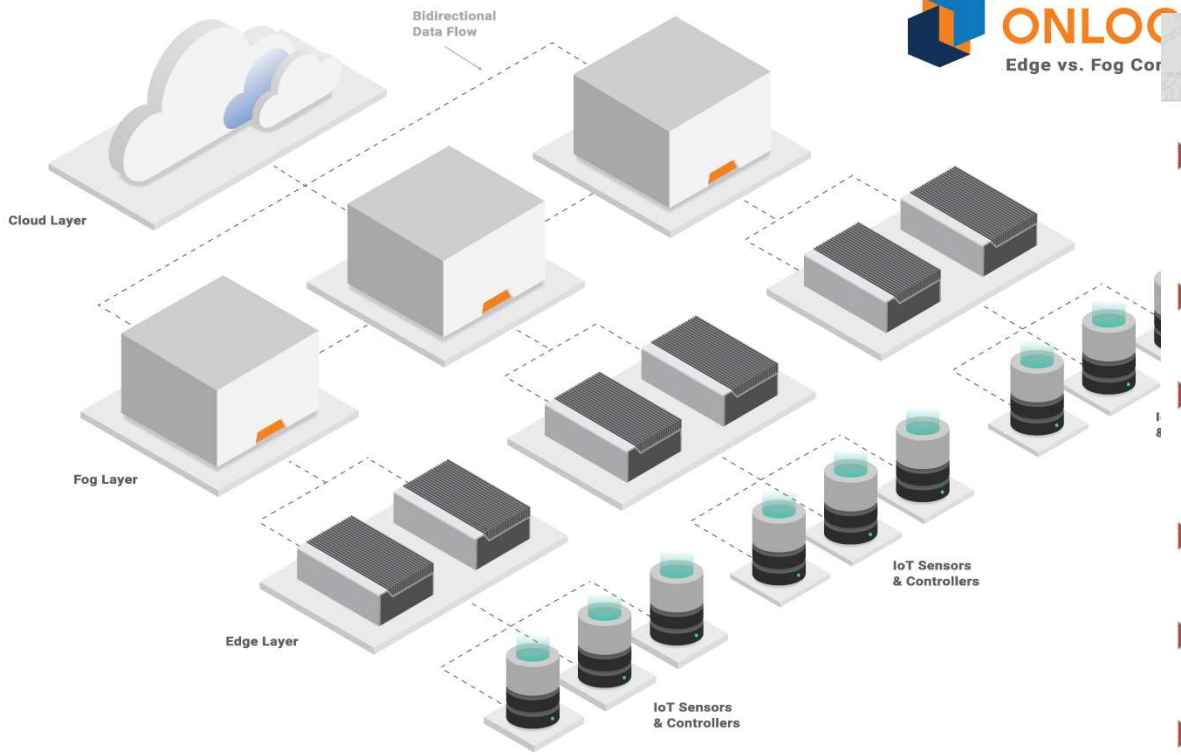
Cloud Computing : Today



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



Introduction to Fog Computing

- IoT is all about the data. The factors that affect data are the four Vs - variety, velocity, veracity and volume.
- All IoT applications require instant analysis and action.
- Most of the time, the action would be corrective in nature, it would be business critical.
- In case the data volume is high and it reaches the cloud after some delay.
- So we may lost the opportunity to use the data appropriately.
- In such cases, fog computing serves the solution.

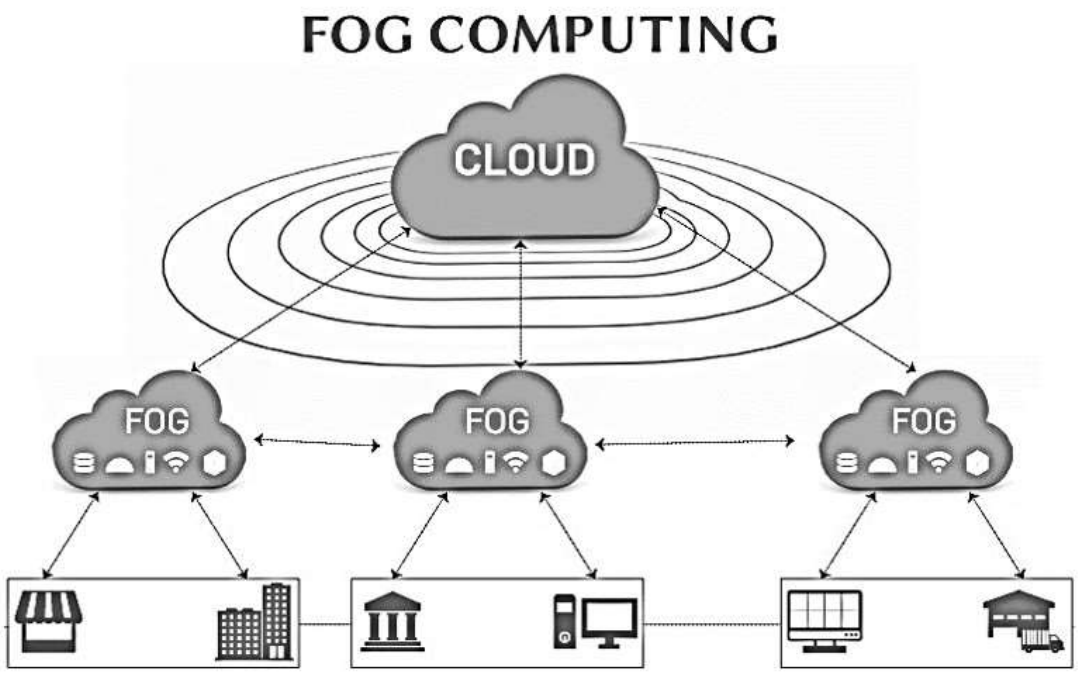
Cloud Computing : Recent Trends

- 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.

Introduction to Fog Computing

- The most sensitive data should be analyzed in the area closer to the place where it is generated.
- With fog computing, it is possible.
- Using fog computing we can process the data locally and to avoid the trouble by not sending the data to the cloud.
- Respond much faster because of data is moving locally so data travel is reduced considerably.
- It thus process the data in milliseconds.

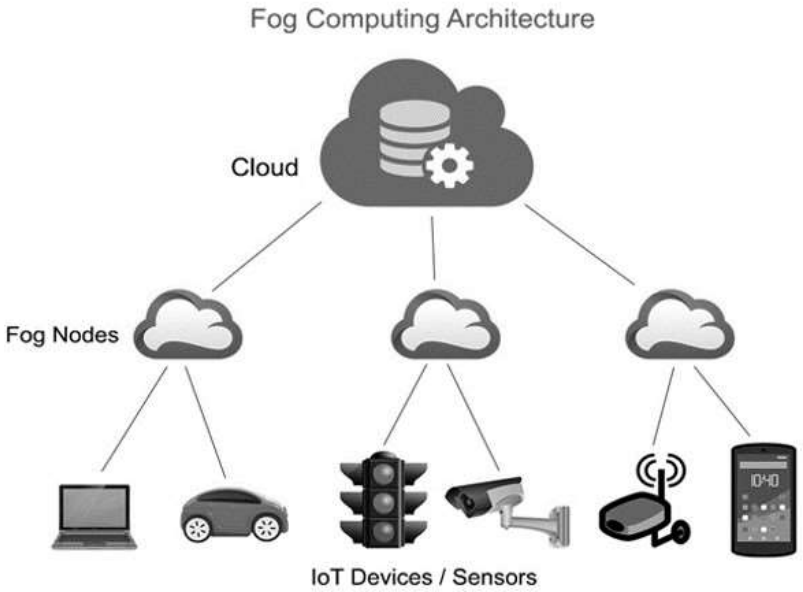


Introduction to Fog Computing

- Only the required data will be sent to the cloud.
- This will be based on storage requirements and guidelines.
- Predictive analytics can also be carried out with the data stored in the cloud.
- The fog is below cloud, which means it is closer to the elements that generate data.
- After analysis, the data stored is pushed on to the cloud.
- Results in increased efficiency and safety both physical and asset safety.
- Some examples where faster response time is extremely important are factory or manufacturing line, oil and gas tube lines fault analysis, on-flight diagnosis, and healthcare.

Working of Fog Computing

- Sensors/devices generate data transmit it to the middle layer, which is very close the data source.
- These nodes in the middle layer are capable of handling the data.
- This requires minimum power and lesser resources.
- All the data need not go to the cloud at the instant.
- Also, sensitive data gets processed very fast, which results in an instant response.
- Fog is not meant for hefty storage. It is still the cloud that does the task of storing big data.
- Fog is just an intermediary layer for faster data processing, and the faster response time.



Summarize the concepts

Concept of fog nodes

- It receives the data feed from the sensors, in real-time.
- Response time is minimal, ideally in milliseconds.
- Fog computing is transit, where data is stored for a limited time only.
- Data is then sent to cloud as a summary.
- It is important to note that not all data goes to the cloud.

Concept of cloud computing platform

- It receives the data summary from the fog.
- Data prediction, data analytics, data storage, etc. takes place here.

Benefits of fog computing model

- Minimal amount of data sent to the cloud.
- Reduced bandwidth consumption.
- Reduced data latency.
- Improved data security. When limited data goes to cloud, it is easier to protect it.
- Immediate processing of data in real time (this is very much needed in industrial applications).

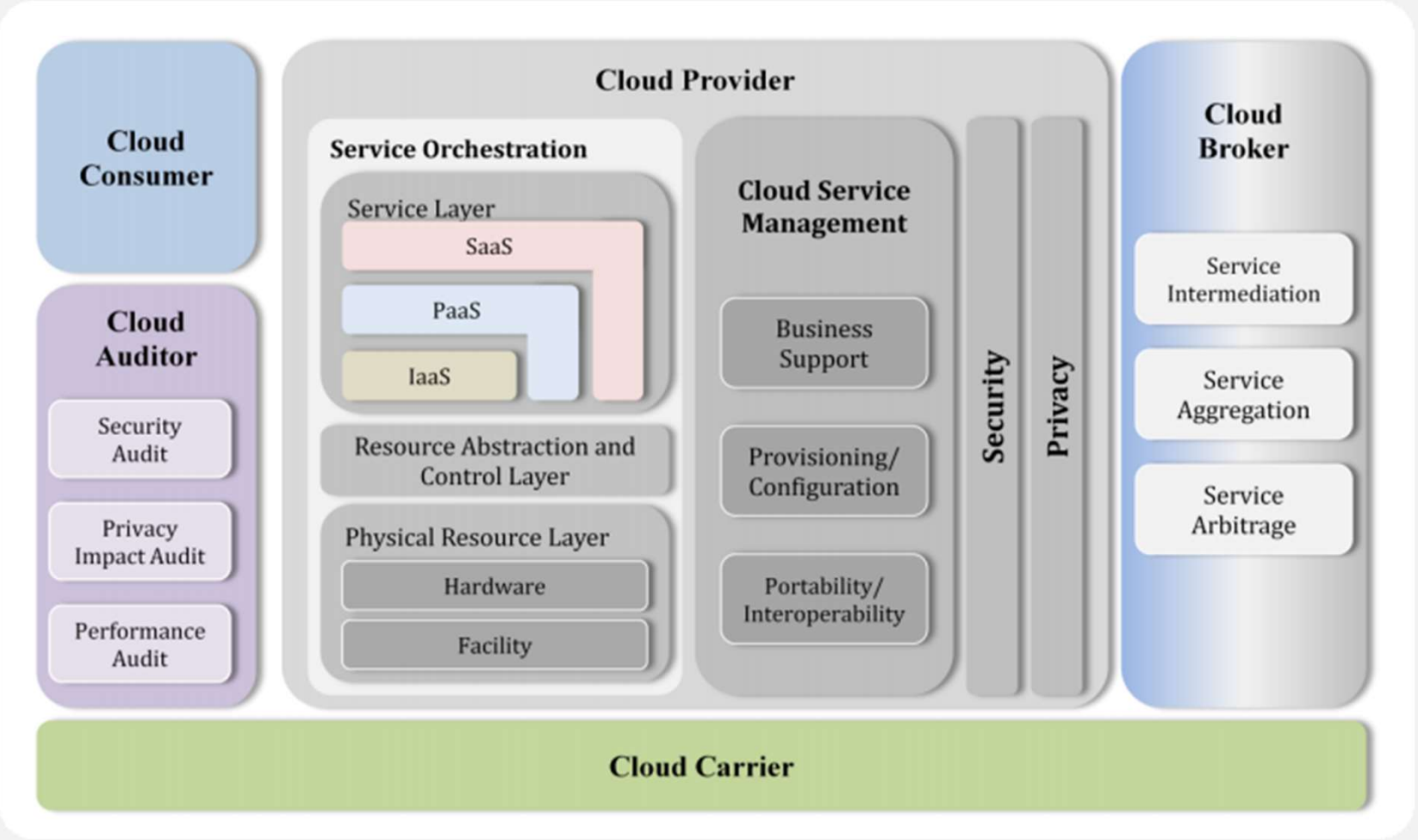
Difference between Edge and Fog Computing

- Both fog and edge are concerned with the computing capabilities to be executed locally, before passing it to the cloud.
- Both aim at reducing complete dependency on the cloud to perform computation.
- Analyzing data and processing it at the cloud is to be avoided.
- Both these reduce the time delay for making faster decision for real-time applications.
- The main difference between edge and fog computing is where data processing takes place.
- Edge computing is the computing carried out at the device itself, where all the sensors are-connected.
- In fog computing, data processing is moved to the processors that are connected to the local area network (LAN), making it a little farther from the sensors and actuators.
- Thus, the main difference between edge and fog computing is the distance.

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

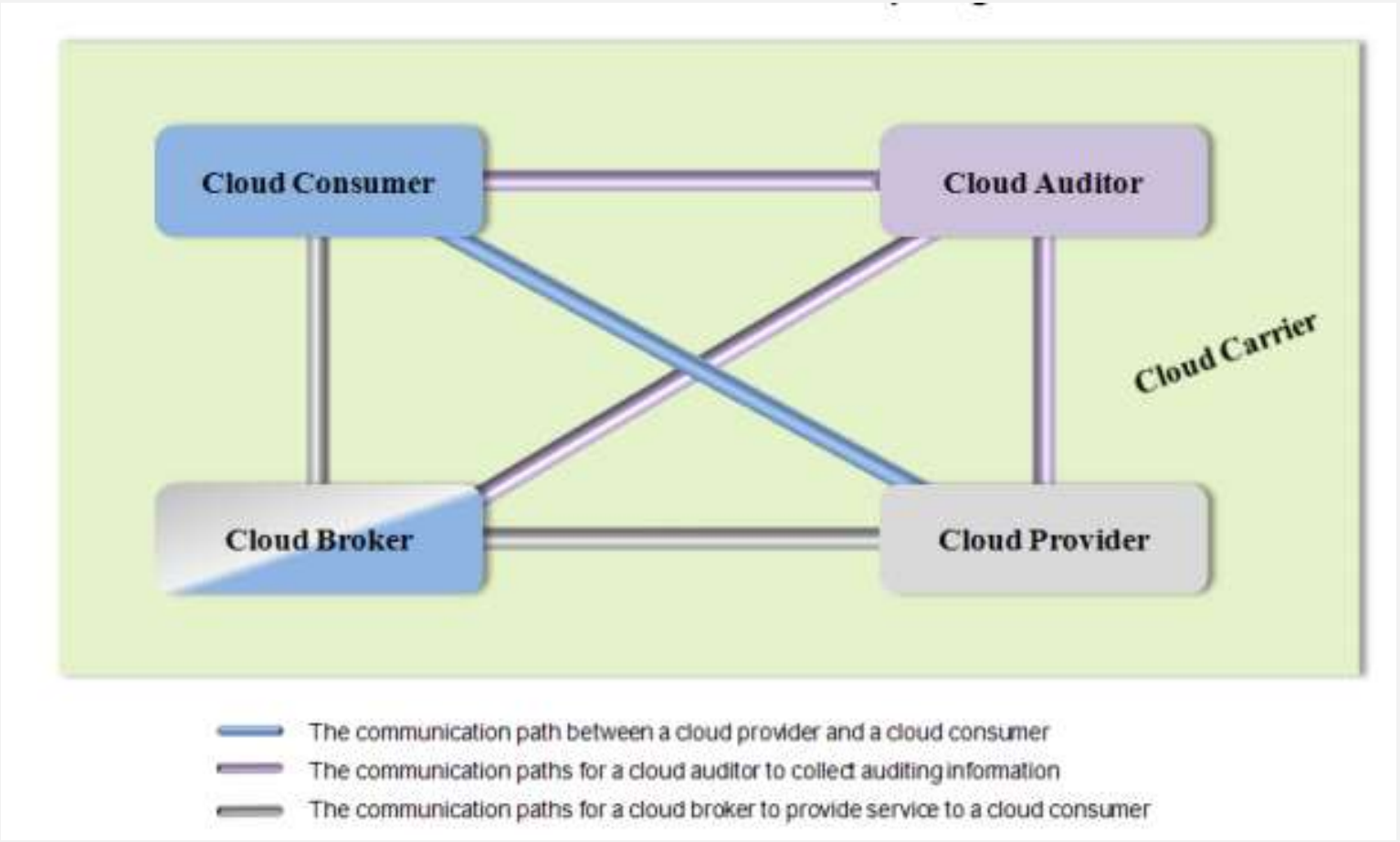
Cloud Architechture : NIST



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 :

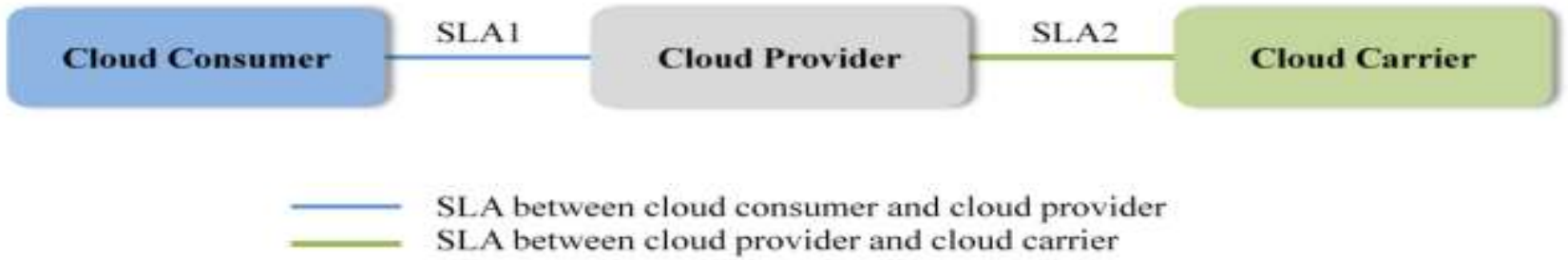
- **Service Intermediation:** A cloud broker enhances a given service by improving some specific capability and providing value-added services to cloud consumers. The improvement can be managing access to cloud services, identity management, performance reporting, enhanced security, etc.

- **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.



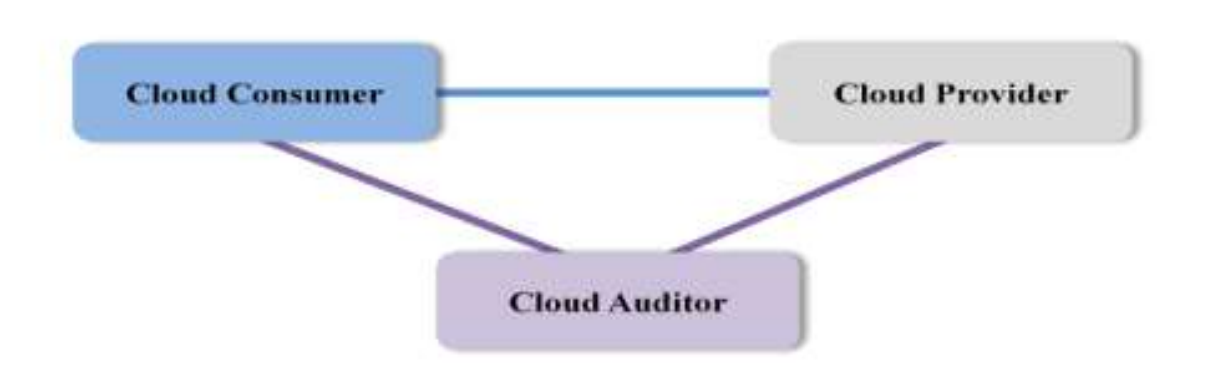
- **SLAs can cover terms regarding the quality of service, security, remedies for performance failures. A cloud provider may also list in the SLAs a set of promises explicitly not made to consumers, i.e. limitations, and obligations that cloud consumers must accept.**

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

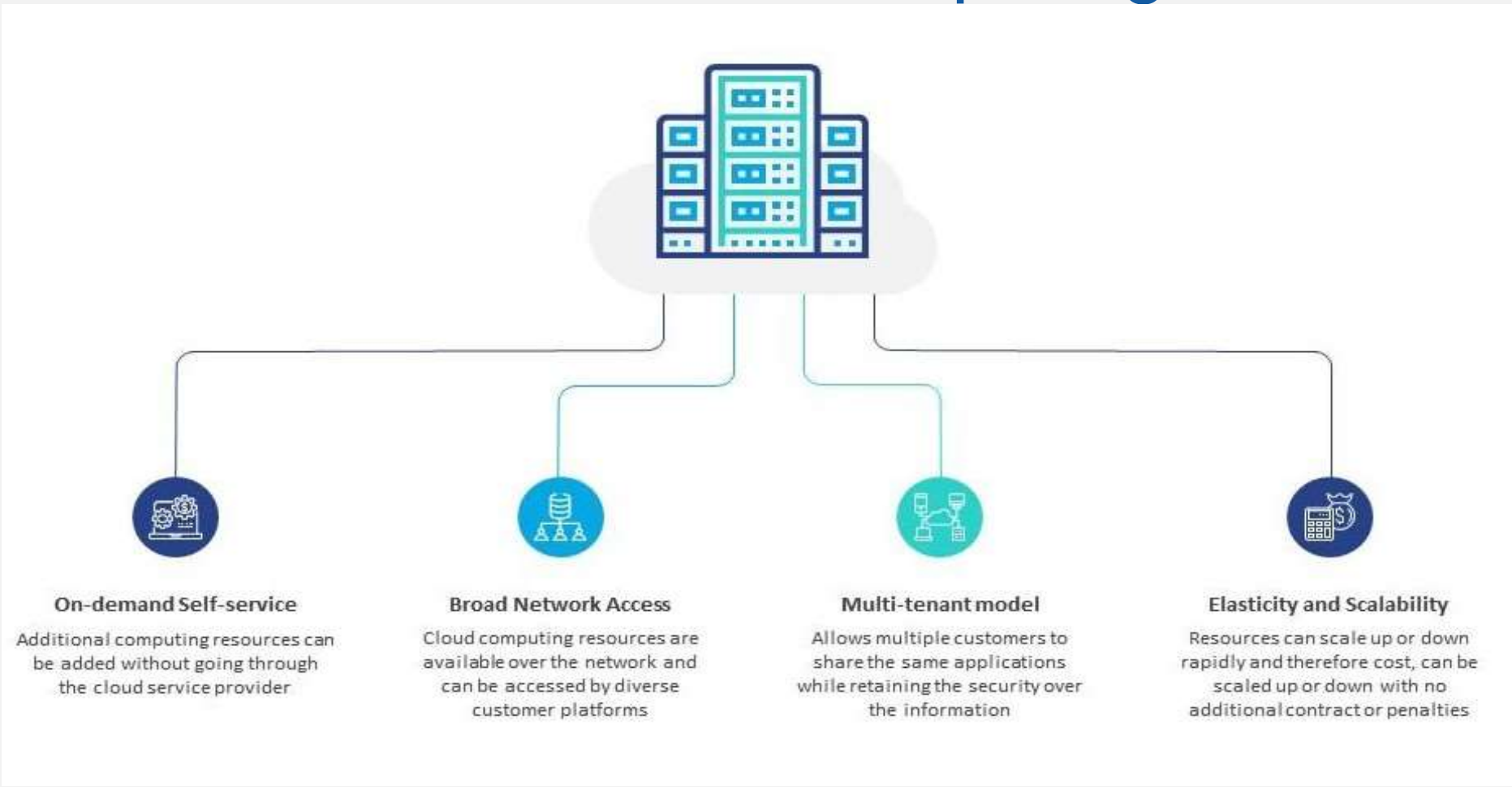
- For a cloud service, a cloud auditor conducts independent assessments of the operation and security of the cloud service implementation. The audit may involve interactions with both the Cloud Consumer and the Cloud Provider.



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

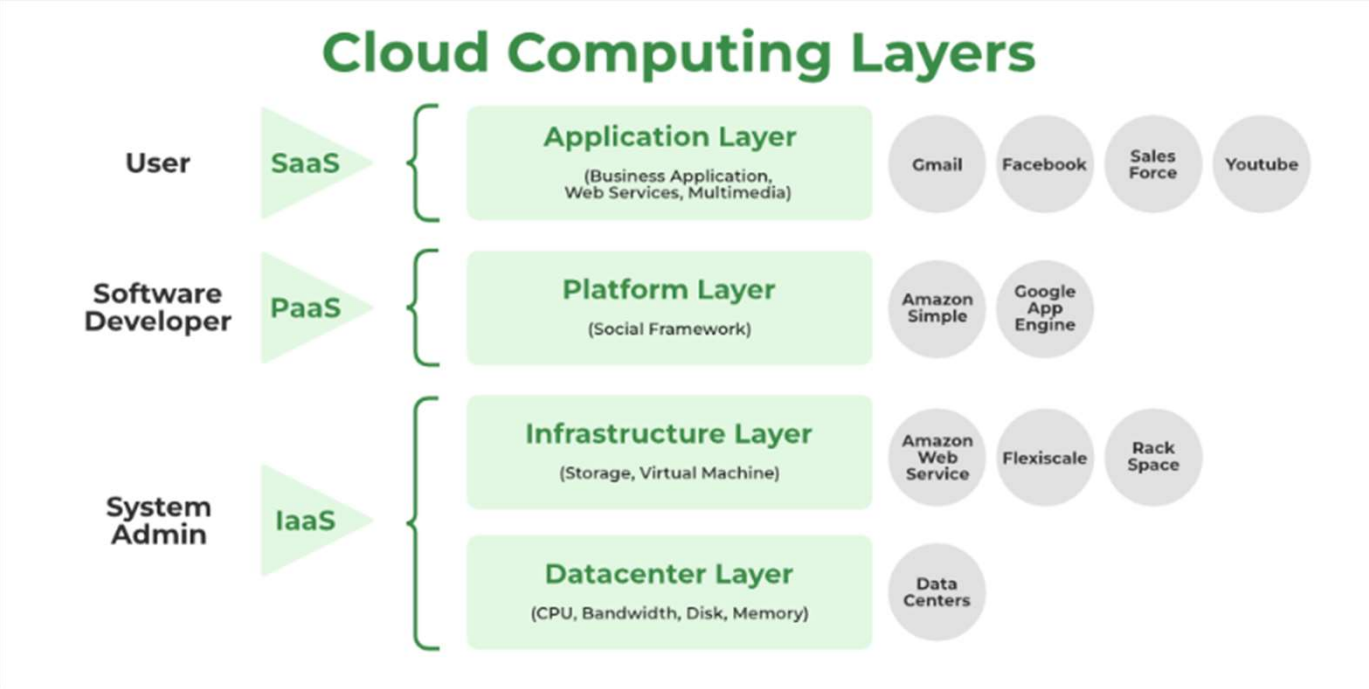
Cloud Computing : Advantage

- 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

Layers of Cloud Computing



Layers of Cloud Computing

- **Application Layer**

1. The application layer, which is at the top of the stack, is where the actual cloud apps are located. Cloud applications, as opposed to traditional applications, can take advantage of the **automatic-scaling** functionality to gain greater performance, availability, and lower operational costs.
2. This layer consists of different Cloud Services which are used by cloud users. Users can access these applications according to their needs. Applications are divided into **Execution layers** and **Application layers**.
3. In order for an application to transfer data, the application layer determines whether communication partners are available. Whether enough cloud resources are accessible for the required communication is decided at the application layer. Applications must cooperate in order to communicate, and an application layer is in charge of this.
4. The application layer, in particular, is responsible for processing IP traffic handling protocols like Telnet and FTP. Other examples of application layer systems include web browsers, SNMP protocols, HTTP protocols, or HTTPS, which is HTTP's successor protocol.

Layers of Cloud Computing

- **Platform Layer**

1. The operating system and application software make up this layer.
2. Users should be able to rely on the platform to provide them with **Scalability, Dependability, and Security Protection** which gives users a space to create their apps, test operational processes, and keep track of execution outcomes and performance. SaaS application implementation's application layer foundation.
3. The objective of this layer is to deploy applications directly on virtual machines.
4. Operating systems and application frameworks make up the platform layer, which is built on top of the infrastructure layer. The platform layer's goal is to lessen the difficulty of deploying programmers directly into VM containers.
5. By way of illustration, Google App Engine functions at the platform layer to provide API support for implementing storage, databases, and business logic of ordinary web apps.

Layers of Cloud Computing

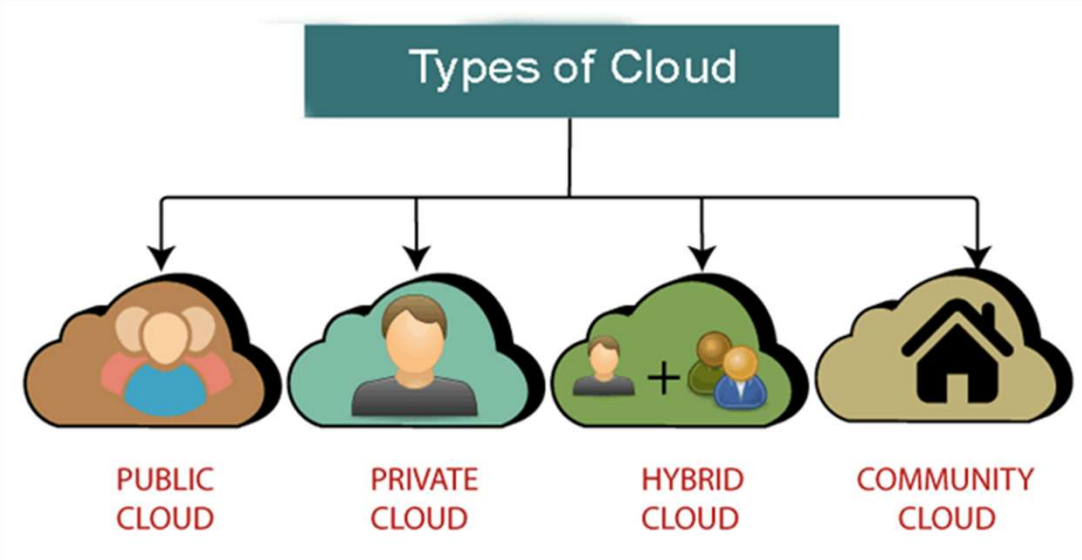
- **Infrastructure Layer**

1. It is a layer of virtualization where physical resources are divided into a collection of virtual resources using virtualization technologies like Xen, KVM, and VMware.
2. **This layer serves as the Central Hub of the Cloud Environment**, where resources are constantly added utilizing a variety of virtualization techniques.
3. A base upon which to create the platform layer. constructed using the virtualized network, storage, and computing resources. Give users the flexibility they want.
4. Automated resource provisioning is made possible by virtualization**,** which also improves infrastructure management.
5. The infrastructure layer sometimes referred to as the virtualization layer, partitions the physical resources using virtualization technologies like **Xen, KVM, Hyper-V, and VMware** to create a pool of compute and storage resources.
6. The infrastructure layer is crucial to cloud computing since virtualization technologies are the only ones that can provide many vital capabilities, like dynamic resource assignment.

Layers of Cloud Computing

- **Datacenter Layer**
- In a cloud environment, this layer is responsible for **Managing Physical Resources** such as servers, switches, routers, power supplies, and cooling systems.
- Providing end users with services requires all resources to be available and managed in data centers.
- Physical servers connect through high-speed devices such as routers and switches to the data center.

Types of Cloud

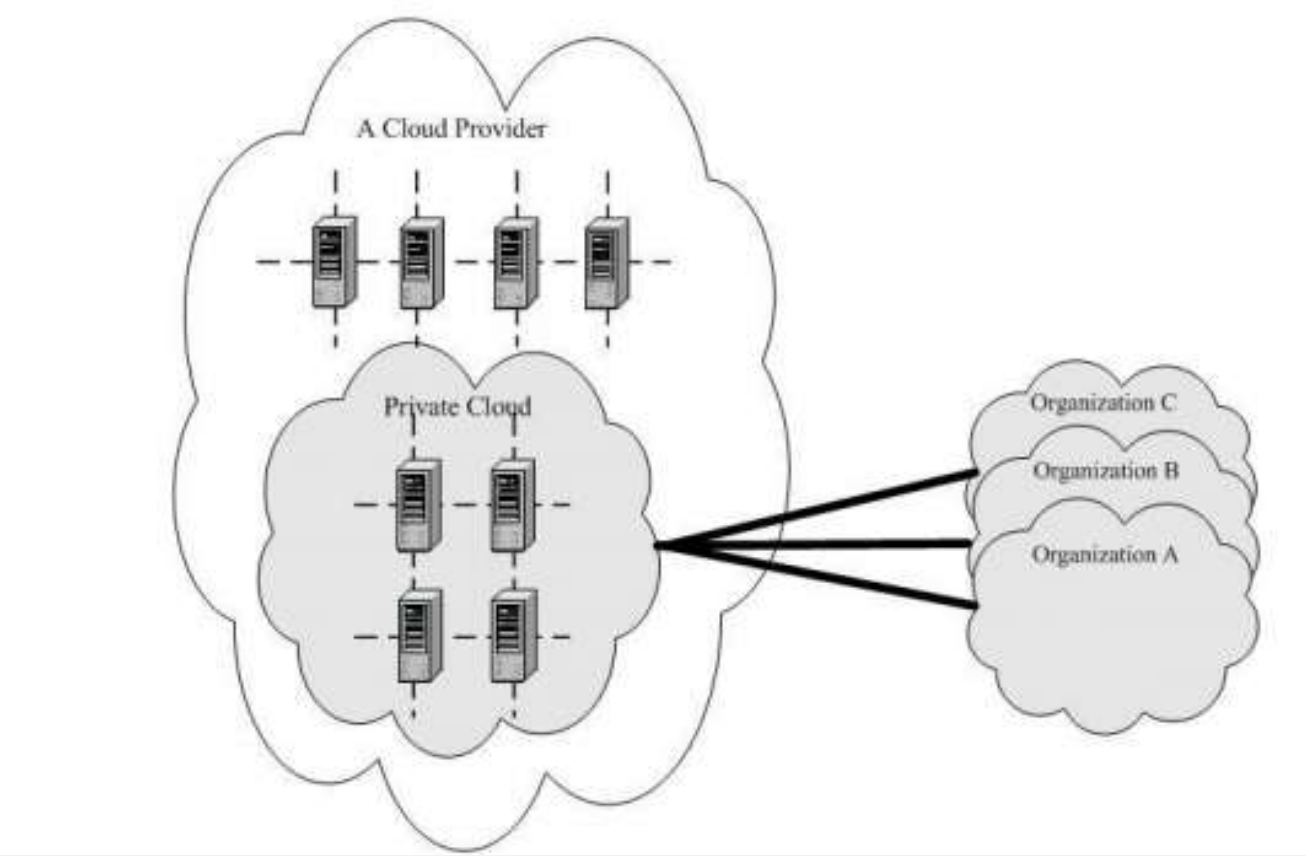


Public Cloud

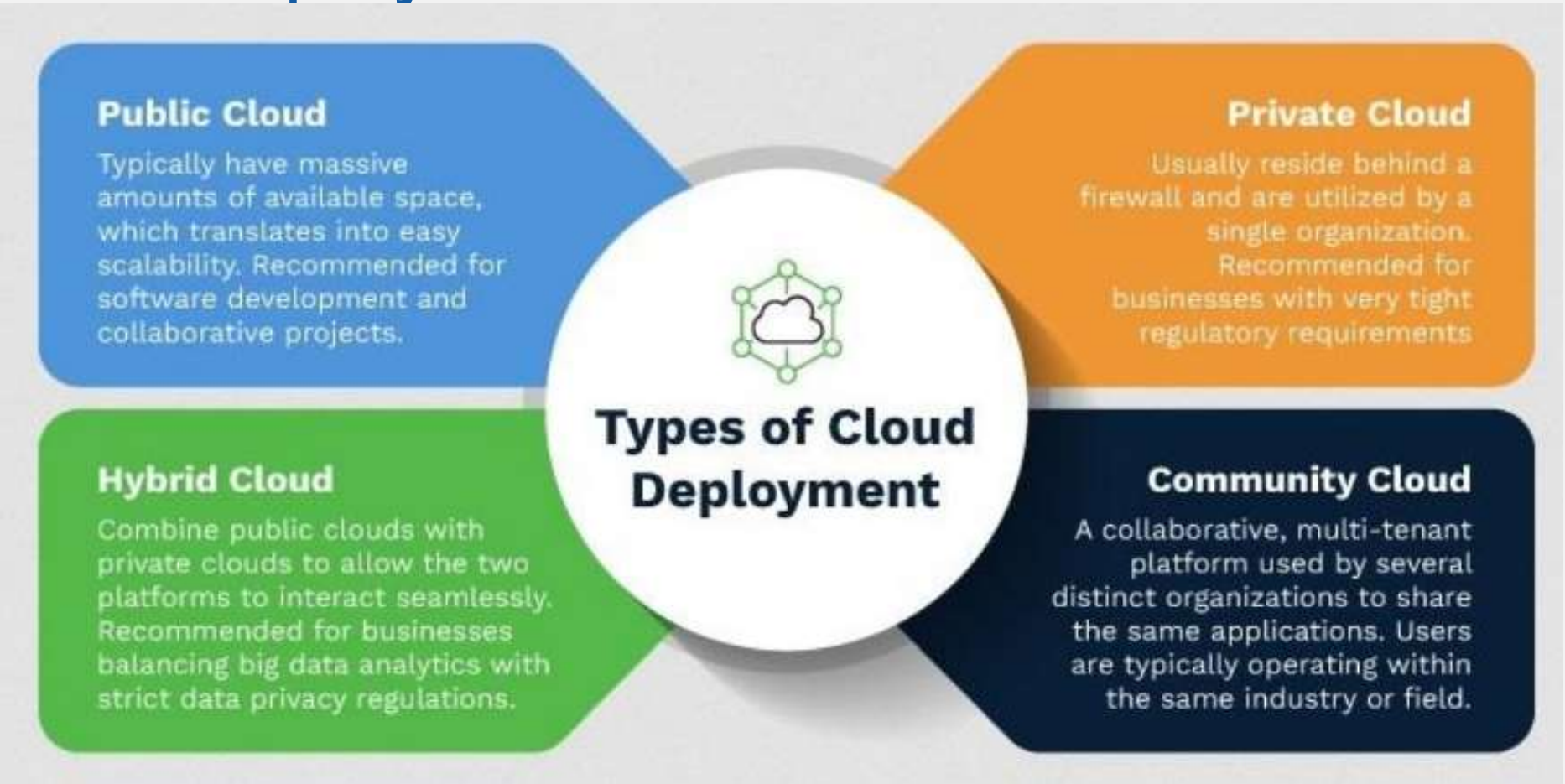
Private Cloud

Hybrid Cloud

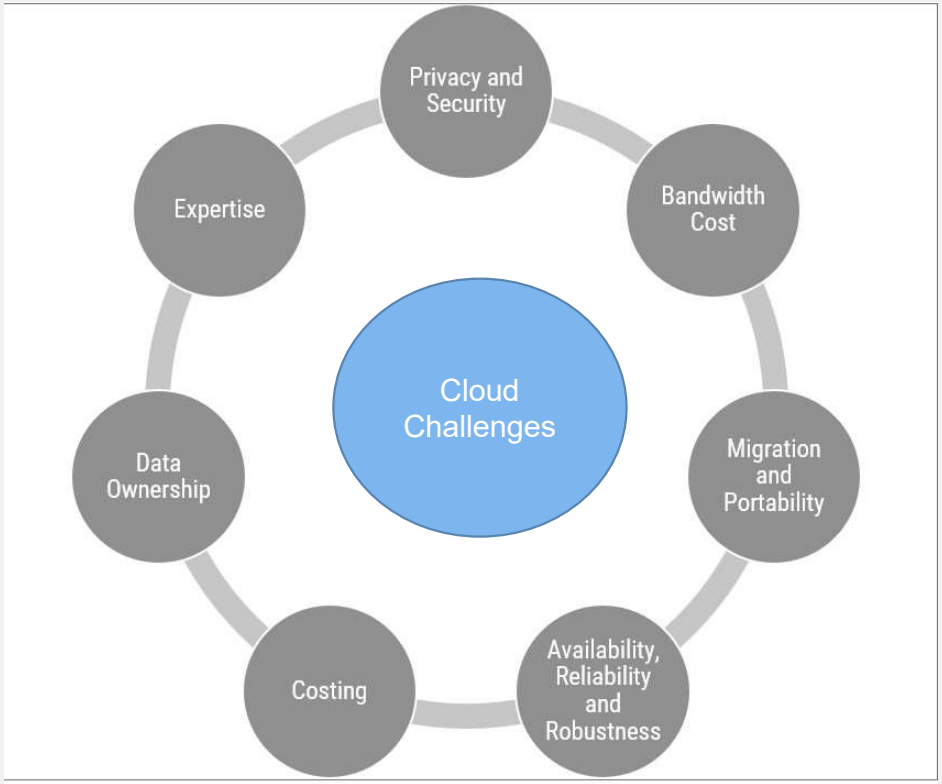
Community Cloud



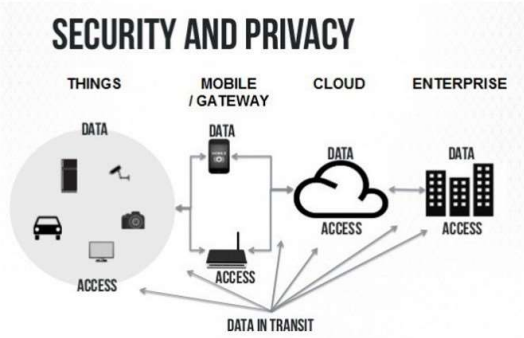
Cloud Deployment Models



Cloud Challenges



Cloud Challenges



The following are solutions to this privacy and security challenge.

- Periodic monitoring of the network activities
- Select private cloud if the data is confidential
- To reduce the risk of being exposed, use recognized antivirus solutions.
- Before signing the contract with a cloud service provider, it is necessary to read and understand the regulations involved in the service being provided.

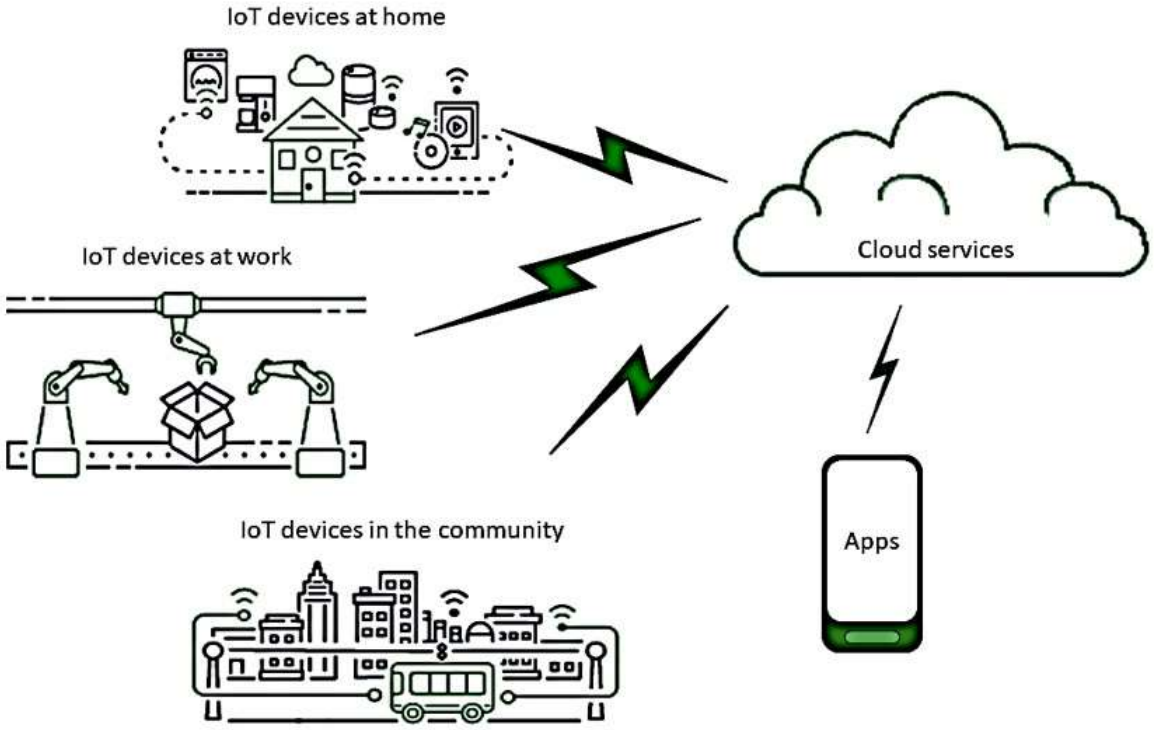
Security & Privacy

Availability, Reliability and Robustness

- In downtime, it would miss critical data so reliability of the process has to be monitored.
- The process should be robust towards handling data at different rates.
- Data could be flooded or slowed at anytime, in the both situations it should be handled effortlessly.

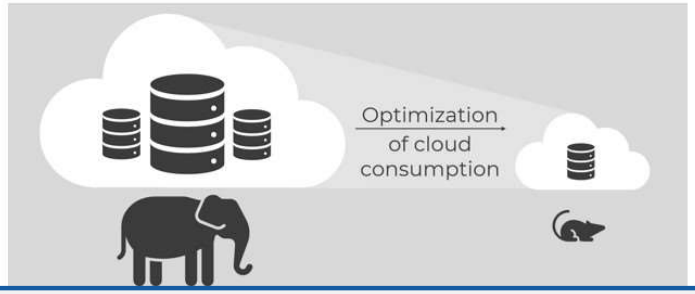
Cloud Challenges : Bandwidth Cost

- Bandwidth is one of the challenges because of continues data transferring from the IoT devices.
- IoT is all about data, and in most cases, this would be big data. Hence, huge investment in storage is needed.
- Cloud computing is preferred for storage and processing in IoT.
- Small-scale IoT application demanding lesser resources.
- But if the application is data concentrated, then the investment in bandwidth would be considerable.



Cloud Challenges

- One of the main advantages of cloud is that it can scale up with rising demand.
- While it is scalable and flexible, an organization should plan its budget carefully.
- Wrong selection for subscription without having clear vision and planning, it may lead to unnecessary cost.

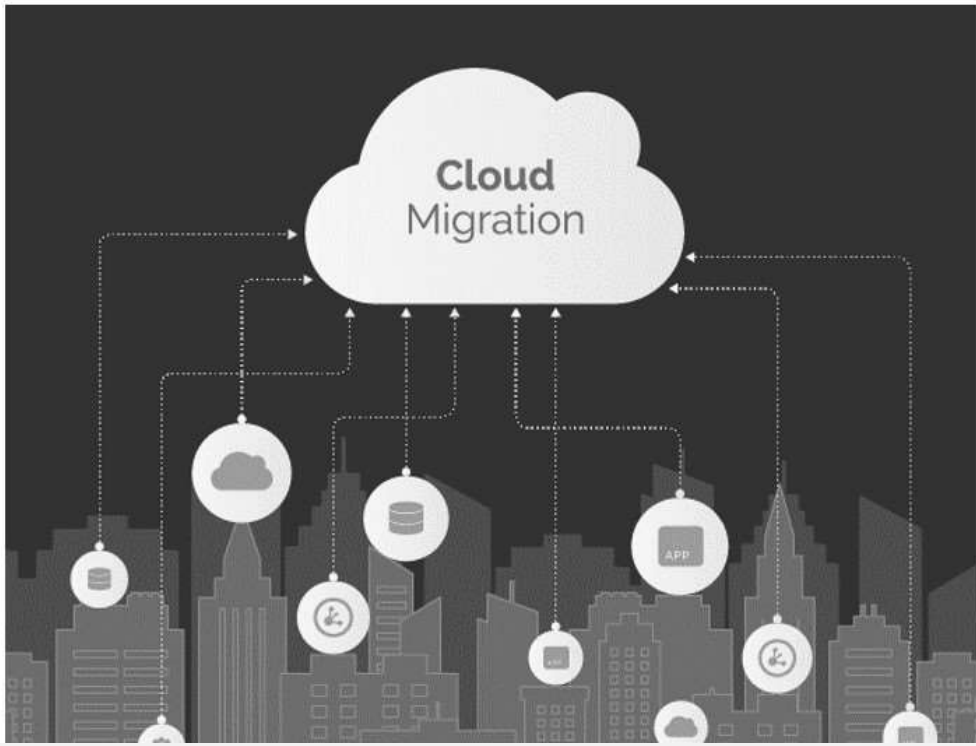


Cost

Data Ownership

Cloud Challenges : Cloud Migration

- When data is to be moved to or migrate from the cloud, we have to take care of the followings.
  - How easy and safe is it to move the data?
  - How much downtime would this process require?
  - What is the strategy to migrate data to the cloud?
  - Will it be easy to select out of the cloud and take data back to the infrastructure?
  - How much would it cost?
  - Would there be support offered to migrate smoothly to another cloud service provider?



Cloud Migration

- A cloud migration strategy is the plan an organization makes to move its data and applications from an on-premises architecture to the cloud.
  - To get advantages Scalability, Cost, Performance, Digital experience

- Cloud Migration Challenges
  - Data Security and Compliance
  - Downtime
  - Interoperability
  - Cost Management

For Details Refer: https://www.cisco.com/c/en_in/solutions/cloud/what-is-a-cloud-migration-strategy.html#~process

The Cloud migration process

- Planning your migration:
  - List out reasons for the move and which strategy can best support them.
  - calculate your cloud server requirements based on current application resource requirements

- Choosing your cloud environment:
  - Decide what kind of cloud model you want to adopt.
  - Whether you choose public cloud, hybrid cloud, private cloud, or multicloud

- Migrating your apps and data:
  - complying with security policies and planning for data backup and recovery

- Validating post-move success:
  - comparing pre- and post-move application performance, from both a technical and business perspective, in a low-risk test environment

The Cloud migration strategies

- **Rehosting ("lift and shift"):** lifting your stack and shifting it from on-premises hosting to the cloud. You transport an exact copy of your current environment without making extensive changes

- **Replatforming:** making a few further adjustments to optimize your landscape for the cloud.

- **Repurchasing:** moving your applications to a new, cloud-native product, most commonly a SaaS platform (for example, moving a CRM to Salesforce). The challenge is losing the familiarity of existing code and training your team on the new platform.

- **Refactoring:** rebuilding your applications from scratch. This is usually driven by a business need to leverage cloud capabilities that are not available in your existing environment, such as cloud auto-scaling or serverless computing

The Cloud migration strategies

- **Retiring:** Once migration is somplete, find some applications which are not longer useful and simply turn them off. The resulting savings might even boost your business case for applications

- **Retaining:** For some organizations, cloud adoption does not yet make sense. In this case, plan to revisit cloud computing at a later date

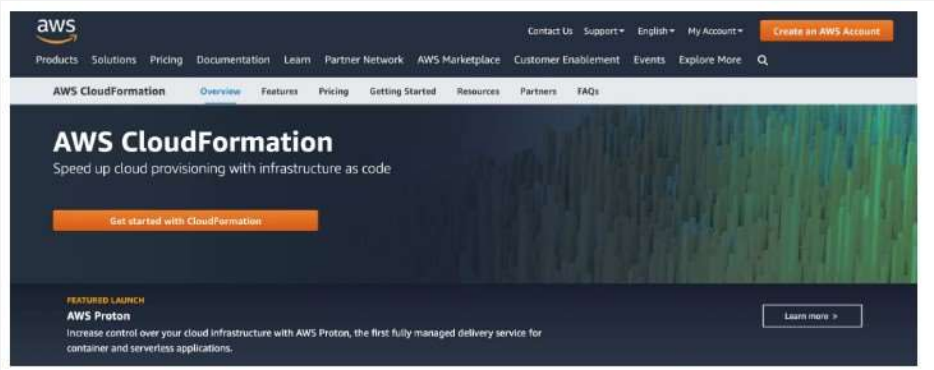
Cloud Orchestration

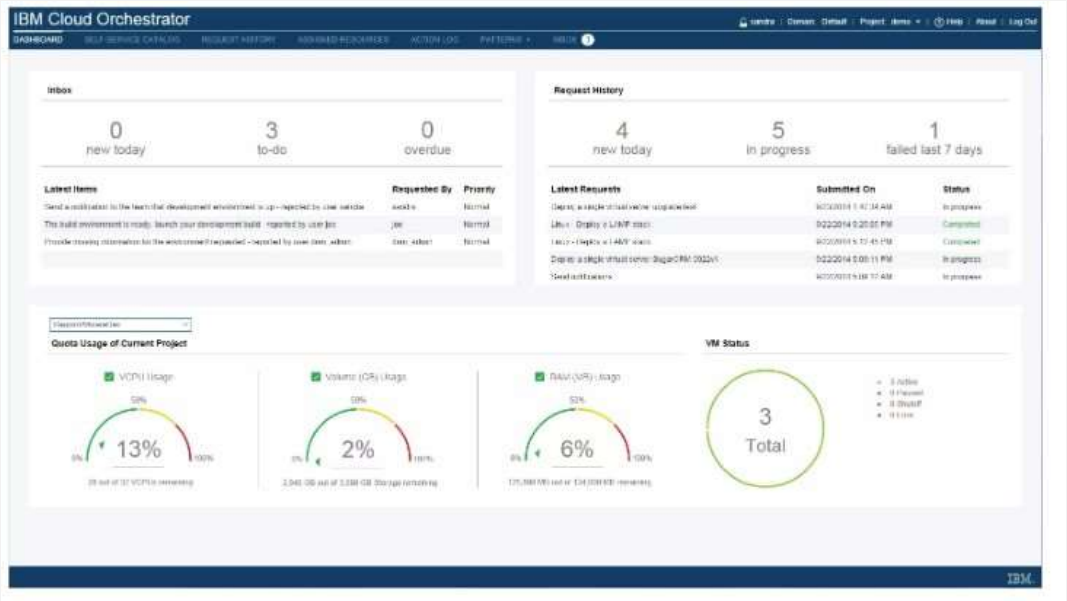
- Cloud orchestration is the coordination of multiple tools, processes, and APIs an organization uses in a cloud environment, from start to finish. This involves coordinating many automated tasks to occur within a single, synchronized IT process.
- Automated tasks are orchestrated by aligning appropriate resources, timing, security protocols, and other deployment mechanisms to ensure they start and run correctly.
- Cloud orchestration is often a complex, automated cloud infrastructure management technique. It brings together complex computing systems, including instances in multi-cloud and hybrid cloud environments, server instances in different physical locations, and automation at scale.
- That coordination takes place in what's referred to as an orchestration layer. The orchestration layer governs, controls, and coordinates service delivery among servers, networks, security protocols, virtual machines, and storage options.
- Cloud platform users generally have no access to the orchestration layer, which is only accessible by cloud provider engineers who maintain and update it.

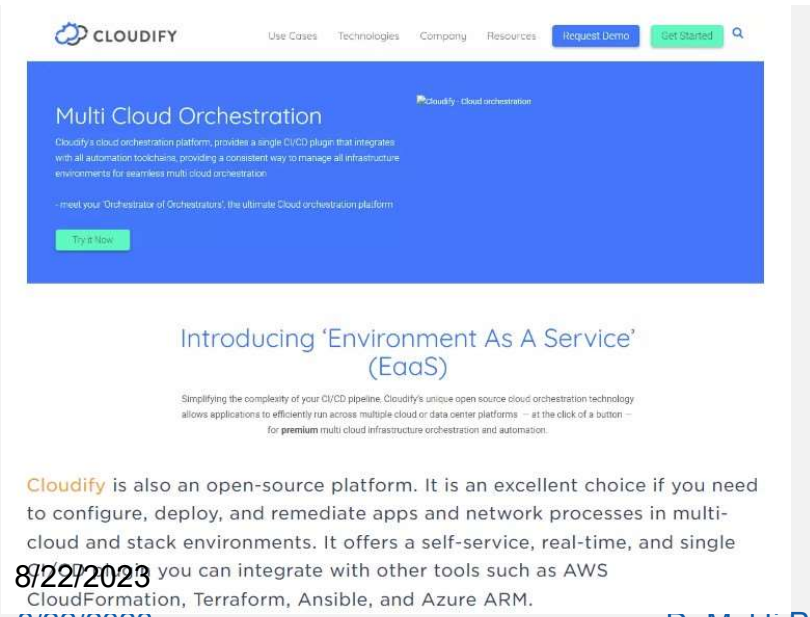
Cloud Orchestration

- Cloud orchestration includes two types of models:
  - Single Cloud model
  - Multi-cloud model
- In Single cloud model, all the applications designed for a system run on the same IaaS platform (same cloud service provider).
- Applications, interconnected to create a single workflow, running on various cloud platforms for the same organization define the concept of multi-cloud model.
- IaaS requirement for some applications, though designed for same system, might vary. This results in availing services of multiple cloud service providers.
- For example, application with patient's sensitive medical data might reside in some IaaS, whereas the application for online OPD appointment booking might reside in another IaaS, but they are interconnected to form one system. This is called multi-cloud orchestration.
- Multi-cloud models provide high redundancy as compared to single IaaS deployments.
- This reduces the risk of down time.

Cloud Orchestration : Provider







Cloudify is also an open-source platform. It is an excellent choice if you need to configure, deploy, and remediate apps and network processes in multi-cloud and stack environments. It offers a self-service, real-time, and single [illegible] you can integrate with other tools such as AWS CloudFormation, Terraform, Ansible, and Azure ARM.

Cloud Security

Cloud Computing: Security Aspects

- The security of any computing platform including cloud computing depends on
  - Software security,
  - Infrastructure security,
  - Storage security, and
  - Network security,
- If any of these is compromised, it would result in security violation and could cause damages.
- Let us discuss these security aspects briefly.

Cloud Security

Cloud Computing: Security Aspects

1. Software Security:

- Software is the core component and plays a vital role in presenting and ensuring a secure environment.
- If there are defects created/generated during the development phase, it is a software security threat.
- Defects such as simple software implementation defects, memory allocation, design issues, and exception handling all contribute to security issues.
- This can be ensured by complete and comprehensive testing carried out at all-stages.

Cloud Security

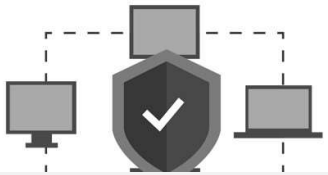
Cloud Computing: Security Aspects

2. Infrastructure Security:

- Making sure that the infrastructure provided by the CSP is safe is a must.
- Third party could also contribute to the infrastructure.
- It is extremely important to check the security vulnerabilities with the infrastructure.
- All infrastructure related guidelines should be mentioned clearly in the agreements and should be made transparent to the customer.
- If data is damaged, everything is damaged and lost.
- Hence, care should be taken to protect the infrastructure.

3. Storage Security:

- It is important to be informed of who owns the data and the location where it is stored.
- Data leak, snooping, malware attacks, etc. are all threats to the stored data and can be listed under storage security.
- Appropriate antivirus software and periodic monitoring, should help protect the data.



4. Network Security:

- Data is stored in the cloud via the Internet, and hence all network threats become a possibility.

Security Terminology

- Security Vulnerability
- Threat/ Attack
- Attack Types:
  - Passive attack
  - Active AttackThreat

Security Terminology

- Security Vulnerability : It is a weakness, flaw, or error found within a security system that has the potential to be leveraged by a threat agent in order to compromise a secure network.
  - Broken Authentication:
  - SQL Injection:
  - Cross-Site Scripting:
  - Security Misconfiguration:

- Threat/ Attack: A threat refers to the hypothetical event wherein an attacker uses the vulnerability. An attempt to gain unauthorized access to information resource or services, or to cause harm or damage to information systems.

- Attack Types:
  - Passive attack
  - Active AttackThreat

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

1. Accenture. In August of 2021, Accenture fell prey to a LockBit ransomware attack. The culprits claimed to have stolen 6TB worth of data, for which they requested a ransom of $50 million.

The largest exposed server appeared to contain credentials linked to Accenture customer accounts. One backup database contained nearly 40,000 passwords – the majority of which were in plain text.

"This cloud leak shows that even the most advanced and secure enterprises can expose crucial data and risk serious consequences," wrote security researcher Chris Vickery.

Lesson learned: Ensure that IT departments and/or cyber security personnel check to ensure correct configuration of AWS cloud servers. Attacks on misconfigured servers can cause extreme reputational, client and financial damage.

3. Cognyte. In May of 2021, the cyber analytics firm Cognyte left a database unsecured without authentication protocols. In turn, hackers managed to expose 5 billion records. Information such as names, email addresses, passwords, and vulnerability data points within their system were leaked. Information was even indexed by search engines.

Lessons learned: The company managed to secure the data within four days, but the incident highlighted how persistent cyber attackers can effectively exploit the smallest of flaws. In this instance, the importance of cyber attack prevention cannot be overstated. Prevent as many attacks as possible through a combination of policies, tools, education and vigilance.

4. Facebook. In April of 2021, Facebook reported a breach affecting hundreds of millions of user records, which were publicly exposed on Amazon's cloud computing service. Although Facebook confirmed that it identified and resolved the issue immediately, the attack managed to impact founder Mark Zuckerberg.

In precipitating the incident, two third-party Facebook app development companies posted the records in plain sight. The database exposed contained private information that social engineers could use in targeted attacks or within hacking attempts.

Lessons learned: In resolving this issue, Facebook reached out to Amazon, which took down the exposed servers. "...If you're still opening AWS buckets [to the public], you're not paying attention," says business advisor Corey Quinn.

Cloud cyber attack :Example

5. Raychat. In February of 2021, Raychat, an online chat application, survived a large-scale cyber attack. A cloud database configuration breach gave hackers free access to 267 million usernames, emails, passwords, metadata and encrypted chats. Shortly thereafter, a targeted bot attack erased the entirety of the company's data.

According to reports, a MongoDB misconfiguration left the data openly available. The attack highlighted how NoSQL databases can function as easy targets for bot threat actors.

Organizations need to ensure that databases are secure. NoSQL databases in particular represent targets for malicious actors who wish to steal or wipe content, unless given a ransom payment. In Raychat's case, a README ransom note appeared, demanding roughly $700 USD.

Lesson learned: Database security requires a range of tools controls and measures that can protect the database itself, the actual data embedded within, its database management system and the assorted applications that access it. End-to-end compliance technologies and cybersecurity penetration tests can help.

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

- **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
- **For Details Refer : https://www.apriorit.com/dev-blog/523-cloud-computing-cyber-attacks**

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

Privacy & Security in Cloud Storages

- Is Google Drive secure?
- **In Transit**
  - To mitigate this threat, Google encrypts your data using TLS encryption before it's uploaded.
  - Google also encrypts your data whenever it is in transit within its internal network. This means that your data is always encrypted when it moves from one Google server to another, and during synchronization with your various devices.
- **At Rest**
  - Once your data arrives with Google, it's encrypted to keep it secure within its cloud servers – and Google uses 128-bit AES encryption for all data that is at rest. Although this isn't as strong as 256-bit encryption
  - Google encrypts the AES encryption keys used to encrypt your data with a rotating set of master keys.
  - Google holds the key to your files on your behalf, which means that the firm can take a look in your files if it really wants to.
- **Privacy policy**
  - Google asks for consent to access everything you upload, it can't claim HIPAA compliance.

- Is iCloud secure?
  - Apple states that all communication with iCloud servers is protected with TLS 1.2 encryption with Forward Secrecy.
  - For additional security, when you access iCloud services using native Apple apps such as Mail, Calendar, or Contacts, authentication is handled using a secure token.
  - Apple states that all data is stored on its servers using AES-128 encryption.
  - Apple's privacy policy makes it clear that iCloud user data may be accessed under some circumstances

Privacy & Security in Cloud Storages

- For data stored in the cloud (i.e., storage-as-a-service), referring to IaaS and not data associated with an application running in the cloud on PaaS or SaaS.
- **Confidentiality**:
  - AWS S3 does not encrypt a customer's data. Customers are able to encrypt their own data themselves prior to uploading, but S3 does not provide encryption.
  - If a CSP does encrypt a customer's data, the next consideration concerns what encryption algorithm it uses. : Symmetric encryption or Asymmetric encryption
  - what key length is used.
- **Integrity**
  - integrity also requires the use of message authentication codes (MACs).
  - The simplest way to use MACs on encrypted data is to use a block symmetric algorithm (as opposed to a streaming symmetric algorithm) in cipher block chaining (CBC) mode, and to include a one-way hash function.
- **Availability**
  - many cloud storage providers do not back up customer data, or do so only as an additional service for an additional cost. For example, "data stored in Amazon S3, Amazon SimpleDB, or Amazon Elastic Block Store is redundantly stored in multiple physical locations as a normal part of those services and at no additional charge." However, "data that is maintained within running instances on Amazon EC2, is all customer data and therefore AWS does not perform backups."

	Total downtime (HH:MM:SS)		
Availability	Per day	Per month	Per year
99.999%	00:00:00.4	00:00:26	00:05:15
99.99%	00:00:08	00:04:22	00:52:35
99.9%	00:01:26	00:43:49	08:45:56
99%	00:14:23	07:18:17	87:39:29

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

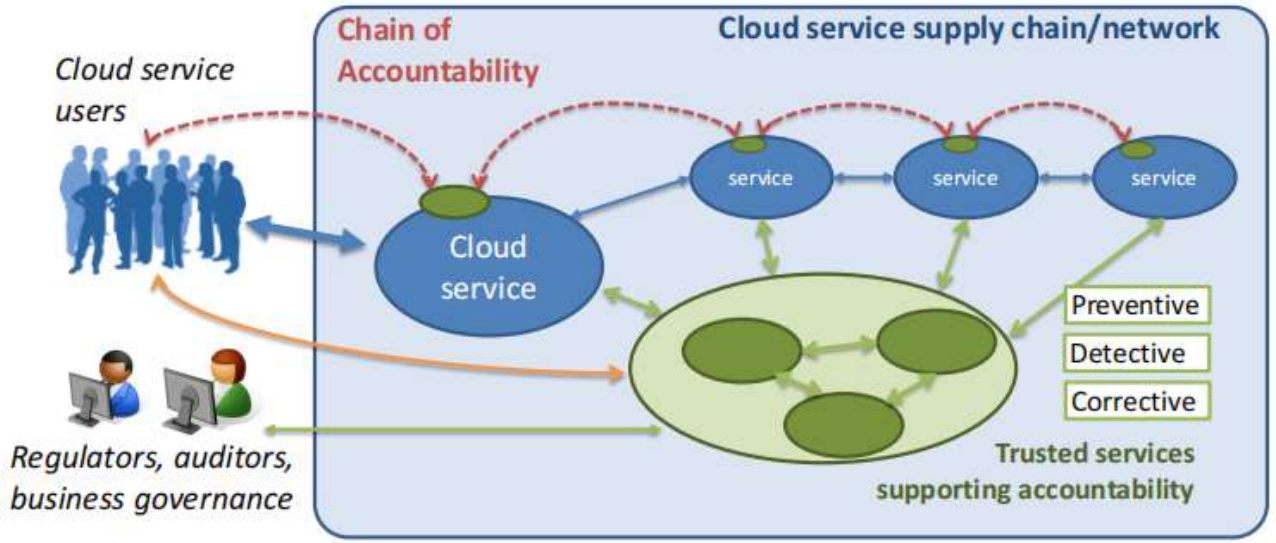
What is Accountability?

– "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

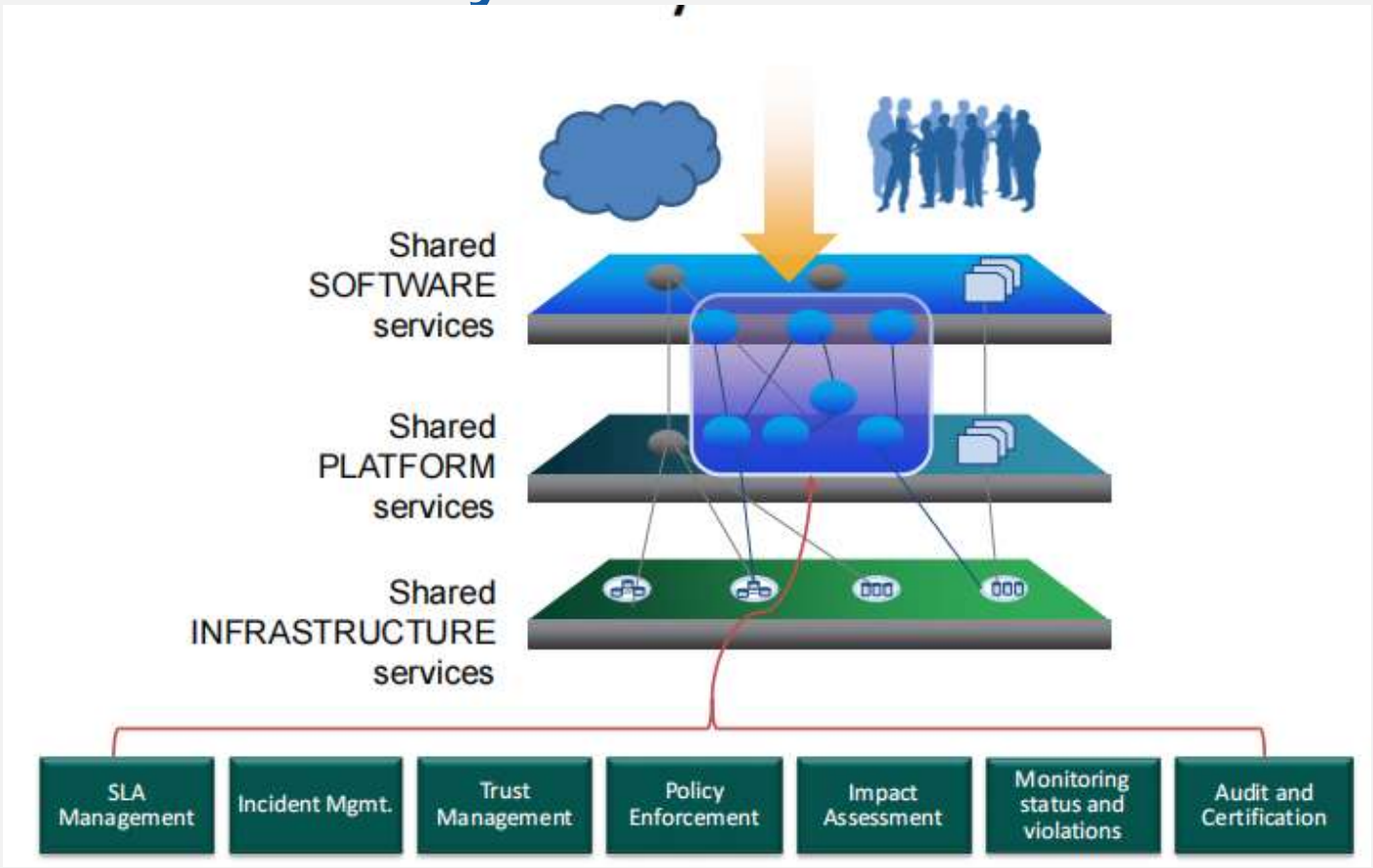


Cloud service users: control and transparency over how their data is used, and support in obtaining redress

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

Summary

- Cloud computing has become one of the most used technology components in modern day applications, which not only provides storage but also supports data analytics.
- Cloud services could be any one of the following:
  - **Software as a Service (SaaS):** Complete software application as a service is provided to the user.
  - **Platform as a Service (PaaS):** Development tools, APIs, libraries, etc. will be divided by the cloud service provider. User have to build, manage and maintain the applications.
  - **Infrastructure as a Service (IaaS):** User should be provided with virtual machine support, where the user does not need to know and worry about the infrastructure. Everything should be taken care by the service provider. User will manage the machines, select the OS and underlying applications.
- The three deployment models generally used for public, private and hybrid
- Private cloud deployment model can be opted wherever confidentiality matters the most.
- When its come to public cloud deployment model, the cloud service provider owns all the resource which include hardware/infrastructure and software. Cloud service provider will take care of all resource management.

Summary

- Hybrid development is a mix of both public and private deployment model. In this approach the resource offered and manage are both in-house and third party based.
- There are many challenges one could face while opting for cloud storage with IoT applications some of these are as follows:
  - Privacy and security
  - Bandwidth cost
  - Migration and portability
  - Reliability and availability
  - Costing
  - Data ownership
  - Expertise
- Selecting a CSP is not easy. Many parameters are to be considered before choosing the best option.