Cloud Computing Fundamentals

* An introduction to computer networking:

Computer networks are groups of computers that interconnect through infrastructure & rules to they can share data with each other. Network send, receive, and share data and resource.

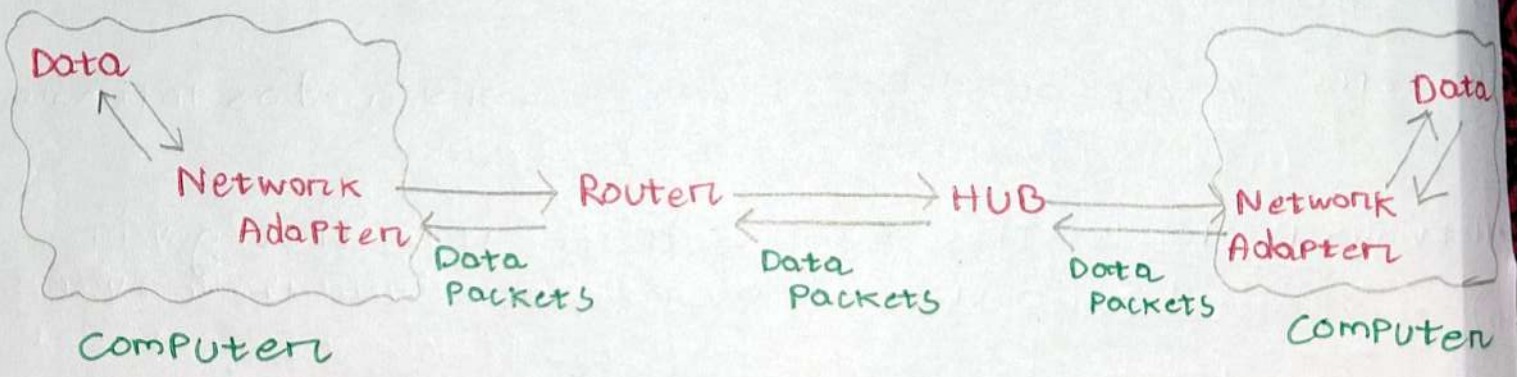
⇒ Components of network: (Taking example of road network)

- Data ⇒ It is like the vehicles that travel on road.
- Cables, fibre, optics & wireless signals ⇒ It is like roads connecting cities & towns, Physical connections such as cables etc.
- Network Adapters: Network adapters are similar to tires on a vehicle. They are interface b/w the computer & external network.
- Routers, Switches and HUBS: It can be considered as infrastructure on a road network.
- Network Protocols: These are like traffic rules that govern how devices transmit data over the network.

* Moving Data:

- collection of zeroes & ones make up all computer data, like documents, images and videos.
- Computer scientists use the binary system & the terms bits & bytes to measure the number of zeroes & ones in a piece of data.
- computers can handle very large files. computer data moves over networks like vehicles move over roadways.
- However, transporting a single file of even 1MB over a network can cause traffic jams & block the network.

- Network adapters divide files in to Packets at the source send them over the network.
- Packets are small chunks of data that the network groups together.
- Sending smaller Packets of data avoids blocking the network with a large files.
- When they reach the destination, they are ressembled in the correct order using metadata, which is info about the data.
- This way routers know the Packets back together to recreate the original file.
- Without this process, things like streaming a movie might show the ending before the beginning due to Packet disorder.



* What is cloud:

- Cloud refers to the delivery of computing services (like storage, Processing power and software) over the internet.
- These services are Provided by remote servers and accessed through a network, typically the internet.

first coined → internal document at Compaq Computer → letter merged with Hewlett - Packard Company

↓

Engineering drawings cloud as symbol of network

Innovations that cloud enables: → Global identity and access management (IAM) ③

→ Personal digital Assistants (Siri & Alexa).

→ Files & Photos everywhere & anywhere.

→ video & music streaming.

→ NLP & AI

* The Components of cloud:

• Their are 5 main components that most cloud services include as their infrastructure:

→ Physical Computers: These Performs functions like storing data & Processing info.

→ Virtual Computers: The VM emulates all the function of Physical hardware. Many VMs can run on one Physical Computer & each VM runs independently of any others.

→ Networking Devices: High Powered, intelligent network hardware & Software helps ensure that cloud systems can move data quickly & accurately over the internet.

→ management Software: Monitor cloud infrastructure & Services, Provision resource, monitor usage & enforce security Policies.

→ Service Software: Similar to GUI on an OS users use it to interact with Services Provided by cloud.

* The Role of Data Centers in cloud computing:

• A data center is a facility to house computer systems & related components, such as tele communications & storage systems.

• It is designed to Provide a secure and controlled environment for the reliable operation of cloud infrastructure,

which can include servers, network equipment, storage sy
& other hardware.

• Data centers enable cloud providers to store & proce
vast amounts of data, run complex applications, &
provide reliable connectivity to users - all the things
the cloud was designed to do well.

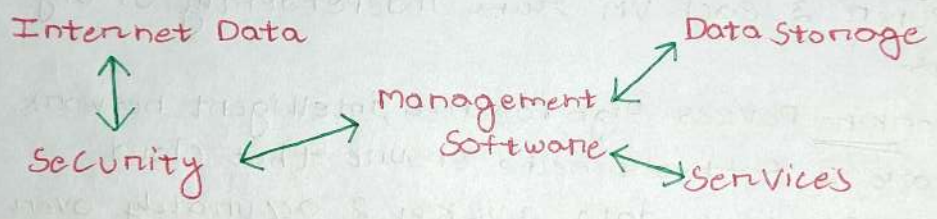
* Data centers typically have several key components:

→ Environmental controls: → Storage systems

→ Physical security → Network connectivity

→ Redudancy & disaster recovery

* How data centers work



* Key characteristics of cloud computing:

→ Scalability: Because computing in the cloud is distributed users can use as much or as little power as they need, when they need it.

→ Availability: Availability in cloud computing refers to the reliability & accessibility of resources, applications and services hosted in the cloud.

• It's all about making sure things are available when you need them, just like how your favorite apps are always ready to use on your phone.

→ Resilience: Resilience in cloud computing is like having a backup plan for your digital stuff. It's about making sure that even if something goes wrong, like a power outage or a computer glitch, your things stay safe & you can keep using them.

Benefits of cloud computing:

Benefits to users: • Convenience • Flexibility • Security
• Cost Savings • Reliability

Benefits to Business: • Innovation • Agility • Collabration

* The makeup of the cloud:

The cloud is made up of thousands of computers working together to create a seamless computing system for users & businesses.

• One software technology that some of these computers run are virtual machines (VMs)

→ VMs help the cloud to scale computing power & enable specalized tasks.

→ VMs run management software, which coordinates thousands of VM & physical computers.

→ VMs also run the service software that users acess, such as admin software for admin to manage their cloud services

* Advances in cloud technology:

• All the components that make up the cloud are constantly evolving. As these tech improve the capabilities of cloud also improve accordingly.

⇒ Computer Technology: computer tech is backbone of cloud computing.

→ computer components: RAM, CPU, hard disk, Network interface cooling system, Power supply, Ports etc.

⇒ Improvements: → Improving efficiency
→ Reducing component size
→ using more solid state components
→ Increasing Processing Power

⇒ **Virtualization Technology**: Virtualization includes virtual machines & containers. By using virtualization technology, cloud providers can reduce wasted resources & provide more fine-grained control for cloud dev over apps & services they create.

⇒ **Improvements**:
→ Increasing the use of containers
→ Adopting serverless computing
→ Virtualising hardware
→ Virtualising networks.

Virtualising Networks

ng Technology: If computer technology is the the cloud, networking technology is its mouth, .

enables computers to interact with each other a b/w computers in a data center & b/w data

⇒ **Improvements**:
→ Improving network protocols
→ Edge computing
→ Intent Based networking (IBN)

Rule Book
↓
IPV4 couldn't handle many devices
↓
IPV6 (New Protocol)

IBN → manage networks
↓
business rules & intentions
↓
makes network management easier, reduces mistake
↓
makes network work better & safer

Edge computing means doing data processing closer to where it's made, not sending it far away to a big data center.
This helps things happen faster & work better for tasks that need quick results, like real-time jobs

Serverless like renting a car.
Cloud Provider (server) car
↓
You (coding) driver
↓
Server management (parking)

← Serverless computing

Containers →

Containerization is a leight weight form of virtualization
↓
containers are portable, easy to manage and offer fast startup times.

Artificial intelligence and the cloud:

Machines that can Posses (Process) information in a way that mimics or imitates human thinking are said to be intelligent.

- Because the intelligence isn't human, scientists have called this kind of thinking ability as Artificial Intelligence (AI).

* The many faces of AI:

AI is a term that encompasses a broad range of technologies.

Technology	Application
Image Recognition	Medical Diagnosis
	National Security
Natural Language Processing (NLP)	Virtual Assistants, Chatbots
Real-time data analysis	Gaming
Deep Learning	Recommendation systems Fraud Detection

* How the Cloud enables AI technology:

→ **Data Storage:** AI systems need a ton of data to work. Like, a system that understands & talks like humans uses lots of text to learn how words fit together.

- It's like learning to make sentences from stories. To teach computers well, we need a huge amt of data & the cloud helps by giving access to tons of data everywhere.

→ **Processing Power:** For AI to handle lots of data fast, it needs strong computer brains called CPUs. and if AI wants more brain power, it can get it from cloud.

- The cloud has millions of CPUs and can give more whenever needed.

→ High Availability: Imagine the cloud as a big web of computers all around the world. It's not just the computers but also services they offer.

- Even weak devices can become strong with cloud help.

→ Experimental Opportunities: Companies sometimes struggle to try new computer stuff on their own. But with the cloud its simpler.

- Cloud providers have lots of resources from many companies and people.

* Connecting devices to the internet:

The cloud supports communication b/w devices & hosts the computer power for performing complex calculations, so the vehicles just need networking devices that can send specific and large amt of data to the cloud. Connecting devices to the internet & to each other using the cloud is called the IOT

⇒ The IOT is a networking model that describes the interconnection of physical devices, appliances & everyday objects that owner can access & control through the internet.

⇒ These devices are equiped with sensors, software, and network, connectivity, enabling them to collect and transmit data to other devices, applications, or cloud based services.

* The cloud & IOT:

The cloud plays a crucial role in enabling the IOT by providing a platform for storing, processing and analyzing the massive amounts of data generated by IOT.

→ Data & Analytics:

→ Scale & Flexibility

→ Security & Compliance

The structure of cloud services on its service models, creates an environment for business & users to create & use services like these.

The Cloud Service model:

Traditional Software	Software as Service
→ Microsoft office Pre installed in PC's or can be Purchased and installed.	→ Using cloud Person can use ms-word without downloading as software-as-a-service model.
→ installed from CD-Rom or internet.	→ Use it on any number of devices.
→ New versions need to be Purchased, installed or updated.	→ Users Purchose software through a subscription service which is continually updated.

⇒ Types of cloud service models:

Cloud Providers might apply the "as a service" name to a variety of offerings.

However, there are are four main types of service models:

* Software as a service (SaaS)

- Saas is a way of delivering software applications to users over the internet without requiring them to install or manage the software themselves.
- Instead, servers host the software in the cloud and users can access it through a web browser or internet-connected device.
- users pay a monthly subscription fee.

* Infrastructure as a Service (Iaas)

- Iaas is a cloud computing service model that Provides users with access to computing resources over the internet.
- These resources include servers, storage & networking components which are all hosted by a cloud service Provider.
- with Iaas users only pay for computing resources they use.

* Platform as a service (Paas):

- Paas is a cloud computing service model that provides users with a platform to develop, run, and manage applications over the internet.
- With Paas developers don't have to worry about managing the underlying infra or OS, because they are all taken care of by third-party provider.
- As with Iaas, users only pay for the platform services they use.

* Database as a service (DBaaS):

- DBaas is a cloud computing service model that provides users with access to a fully managed database.
- with DBaas, users don't have to manage the underlying infrastructure or database software.
- The cloud provider is responsible for ensuring there are available & operating properly.
- with DBaas users pay for database and the computing resources they use on a pay as they go basis.

=> Service models working together:

People can use the 4 cloud service models in isolation or together to create a cloud-based solution.

-> Iaas & DBaas provide foundation layer of computing resources, including servers, storage & networking components.

-> Paas builds on top of Iaas & DBaas by providing a platform for developing, running & managing applications

-> Saas works in conjuction with Paas by providing access to software applications over the internet, without users having to install or manage software locally.

Cloud Service Providers:

Cloud Providers: Cloud Providers build the devices & services that are resilient to downtime & attacks, as well as the scalable cloud services that large business needed.

* Features Cloud Providers Share:

- Global Presence
- Strong Security
- Reliability
- Scalability
- Standard Services
- Competitive Pricing.

Eg of Cloud Service Providers:
- IBM Cloud
- Microsoft Azure
- Google Cloud
- Amazon AWS
- The open source cloud
  - Next Cloud
  - OpenStack
  - OpenShift
  - Eucalyptus

mytax
MITACS

Single User (OR) Small Company → **Software as a Service (SaaS):** Enables People access software applications over the internet.

Medium sized → **Infrastructure as a Service (IaaS):** Provides virtualized computing resources over the internet.

A hobbyist (OR) Devs → **Platform as a Service (PaaS):** Provides a platform for devs to build, test & deploy applications over the internet

* Business that Scales using IaaS:

→ **Scaling Up:** Scaling Up refers to making an existing resource larger by integrating resources into them.

- This is done by adding more memory, CPUs or storage to an existing server configuration to address a specific problem.
- Typically, a configuration can't automatically scale up. A user chooses to scale up by selecting a new configuration which the cloud provider then implements.
- Scaling up is also known as vertical scaling.

→ Scaling Out: Scaling out refers to creating one or more copies of a resource to share the workload. The resource might be a physical computer or a virtual machine.

- The copy will have the same config as the original resource & be capable of performing the same tasks.

Scaling out is also known as horizontal scaling.

⇒ Their are 2 instances for scaling out:

- Scaling out to accommodate demand
- Scaling out at a specific time

* Deploying Solutions with Paas:

⇒ Using Paas to deploy a Website:

Content Management System (CMS) like Word Press

→ Azure can deploy it easily with in few clicks:

- The web server & associated services on which to run the platform.
- The database the platform needs.
- A virtual network to make the platform more secure.
- A content delivery network to make delivering media like images more efficient.

⇒ Using Pass to develop and deploy a software solution

- Application development
- API development
- Testing
- Securing Data
- Analytics & Communication
- Internal tools

Understanding Cloud Deployment models:

(13)

Infrastructure hosted on Premises:

⇒ Mainframe Computers:

- In oldays, computers were big & powerful. People connected several screens and keyboards to a single big computer, which did all the hard work.
- ~~This powerful computers were big & powerful. People connected several screens & keyboards to a single big computer~~
- This powerful computer was called mainframe, and it is shared its processing power with the connected screens, which were called "dumb" terminals. The name comes from large cabinet that held these computers.

⇒ Modern main frames:

- Mainframes are used by many people & organisations. If you've ever used an ATM, you've used a main frame.

→ Large organisations use mainframes to process large amt of data. Companies use main frame to:

- Process billions of real time calculations & web transactions every day.
- Keep track of essential financial transactions like customer billing & employee payroll information.
- Keep information safe & secure.

⇒ Some features of mainframe computers:

- High Processing Power
- Virtualisation
- Scalability
- High Availability
- Security
- Integration
- Management

- Modern mainframes power some of the most complex & demanding workloads on the cloud.
- But mainframes have uses beyond the data centers that cloud providers host.
- Business running their own data centers also use them.

* Hosting Infrastructure on Premises:

- Before cloud become mainstream, business owned & operated their own infrastructure.
- This included the hardware, like mainframes, and the software.
- This is called on-premises hosting. Everything a business needs to run their daily operations is on the premises of the business.

→ On-Premises hosting includes some of the features are:

- Environmental controls
- Physical security
- Storage systems
- Network connectivity
- Redundancy & disaster recovery.

→ Benefits of an On-Permises data center:

- High levels of security and data privacy.
- cost effective.
- Customize hardware & software
- Regulation or compliance requirements.

* Migrating to the cloud:

- over all steps for migrating from On-Premises infrastructure to a cloud managed infrastructure.

① Assess current infrastructure: The business needs to determine what hardware, software and services are currently being used on premises and how they are being utilized.

② Choose a cloud provider: The business needs to research & choose a cloud provider that meets its needs & requirements.

③ Plan the migration: The business needs to develop a plan for migrating its data & services to the cloud. This should include a timeline and contingency plan.

④ Migrate data: The business needs to move its data to the cloud. This can involve transferring data to the cloud provider storage system or using a migration tool to copy data over.

Configure cloud Services: The business needs to configure the cloud services it will use, such as VM, databases, and storage.

⑥ Test & Validate: The business needs to test & validate the cloud environment to ensure that it is working as expected & that data is being accessed & stored correctly.

⑦ Transition to the cloud: once the cloud environment is validated & tested, the business can transition to using the cloud environment for its data & services.

⑧ Decommission on-Premises hardware: After the transition to the cloud is complete, the business can decommission its on Premises hardware, including servers & storage.

* A Hybrid Approach:

- Although there are many valid reasons for hosting a data center on premises or moving entirely to the cloud, many businesses are choosing a hybrid approach.
- This will mean that a business will host some hardware & software on premises & use the cloud for many other services.

Moving to the Cloud:

- Before business can choose a cloud provider, they need to determine which cloud services they want and need.
- Choose the right cloud services depends on various factors such as business specific needs, requirements, goals & budget.

→ Business needs:

Companies identify business needs that the cloud can help meet. Some common needs include.

- Scalable storage
- Data analytics
- collabration tools
- Security

→ Scalability: As the business grow, cloud service be scalable enough to support growth. Companies need evaluate the cloud services scalability before deciding on one.

→ Security: Companies must choose cloud services that have robust security measures in places to protect data from unauthorized access, hacking & data breaches.

→ Integration: cloud services should integrate well with a business existing software & hardware system. This integration ensures a seamless workflow & easier data transfer.

Choosing a Provider:
- cost effective
- Reliable & Reputable
- Support System

Planning for a cloud migration:

→ Your cloud migration plan needs to include the following important tasks to ensure a smooth transition to the cloud.

- Assess the current infrastructure: Starting with an assessment of the existing IT infrastructure, you analyze the system applications, and data to be migrated to the cloud, aiding in the decision-making process regarding a simultaneous or phased transition.
- Identify Right cloud Provider.
- Choose the right cloud services. Infrastructure as a service (Iaas), Platform as a service (Paas) or software as service (Saas).
- Plan for resources: You strategize the allocation of resources for migration & post-migration sustainability considering the ongoing investment required for cloud deployment.

Deploying the infrastructure & applications to the cloud:

- To deploy to the cloud means to migrate or create and configure a set of computing resources, applications, services, and databases in a cloud environment.
- The cloud env could be • IBM cloud • AWS • Microsoft Azure Google cloud platform (GCP).
- Deployment involves the creation of virtual machines (vm) storage, network configurations etc.

① Design the architecture ② Configure security

③ Create virtual machines & containers

④ Set up storage ⑤ configure network settings

⑥ Deploy applications ⑦ Test & validate infrastructure

⑧ Monitor & manage the infrastructure

Optimizing a solution:

→ Example of pet dog → A cloud solution is similar, It requires regular attention, including monitoring, adjustments, and care.

→ Deploying a solution to the cloud is just the beginning. Like a pet who is well cared for, a cloud solution will thrive with continual monitoring & attention.

→ Its critical for business to monitor metrics & optimize performance to ensure their cloud solution:

- Efficient
- Reliable
- Meeting performance goals
- cost-effective.

without continual monitoring and optimization, cloud solutions can become slow & unreliable and fail to meet a business requirements.

• Deploy a migration strategy: You include in your plan detailed, step by step process for the migration. The includes timelines, resources & potential risks.

• Train the IT team: Finalize your migration plan by providing training to your IT team, ensuring they are acquainted with cloud provider's console, deployment methods and pertinent services.

Making the move:

• Migrate the company data & applications
• Validate and test the migrated system
• Monitor the cloud infrastructure
• Decommision on-premises infrastructure
• Evaluate & optimize the new cloud infrastructure

* For instance the following 6 "Rs" are a helpful way to remember essential parts of a strategy to ensure a successful cloud service migration.

→ Rehost: Identify any cloud-based systems the business already used, and the systems that must be cloned & moved to the new cloud provider.

→ Replatform: Determine system that must be optimized to work more efficiently

→ Refactor: Identify applications and services that benefit from cloud capabilities & make appropriate changes to application.

→ Repurchase: Move or replace system from one service to another.

→ Retire: Determine which application that the business doesn't need any more & should be turned off or retired.

→ Retain: Identify & retain applications that cannot be migrated for some reason.

Cloud Deployment Models:

Deployment models:

- The cloud gives these businesses the opportunity to scale their infrastructure based on need.
- Scaling can save money and provide a much better user experience for their customers.
- Cloud based innovations like artificial intelligence (AI), block-chain, & Virtualization give companies technologies such as image recognition, chatbots and reccommendation systems.

→ Cloud deployment models are the ways that cloud computing services are delivered and hosted.

→ The four main types of cloud deployment models are: Public, Private, hybrid and community.

* Public Cloud:

- A cloud deployment model where resources are available to anyone over the internet.
- The services provider owns and manages the infrastructure software, and security of the cloud.
- Public clouds are typically cheaper and more scalable than other models, but they might have less control & customisation options for users.
- Public clouds are well suited for businesses & individuals that want to use opensource software without modifying it.

* Private Cloud:

- A cloud deployment model that is dedicated to a single organization or group of users.
- Private → Service provide or organisation manages everything.
- Private clouds are typically more expensive & less scalable than public clouds, but they offer more control & customization options.

* **Hybrid Clouds:** • A cloud deployment model that combines and Private clouds

• The Service Provider or the organisation can choose which resources & applications to run on each cloud based on their needs & Preferences.

• Hybrid clouds are typically more flexible and efficient than other models but they can have more complexity & Security Challenges.

* **Community Cloud:** • A cloud deployment model where resources are shared by group of organisations or users with common goals or interests.

• The Service Provider or one of the organisations owns & manages the infrastructure, services & Security of cloud.

• Community clouds are typically more cost effective & collaborative than other models, but they might less scalability and availability.

⇒ **Scenario 1: Choosing a Public Cloud:**

Company A is StartUP → Online Platform for freelancers and clients to connect

↓

Company A decides to use Public Cloud

• Launch its Platform quickly & easily
• Scale UP or down
• Pay only for resource
• Acess Variety of cloud services & features
• Focus on its core business activities & options

⇒ **Scenario 2: Choosing a Private Cloud:**

Company B is a bank → Provides financial services

↓

Company B decides to use a Private Cloud.

• Protect its sensitive data & transactions from unauthorised access and breaches.
• Comply with strict regulation
• customize its cloud services & resources
• Have more control & visibility.
• Reduce the risk of downtime or service disruptions

The Hybrid Cloud:

A hybrid cloud deployment in a way of using different types of cloud services together to achieve the best results of a business.

- A Private cloud for sensitive data & applications.
- A Public cloud for scalable & cost-effective resources.
- A third-Party cloud for specalized services.

* Advantages of Hybrid cloud:

- More flexibility and control over their data & applications.
- Access to a wider range of features and benefits from different cloud Providers.

* Choosing a Public Cloud deployment:

A Public cloud deployment is a type of cloud computing service where a Provider offers resources over the internet to multiple customers. These resources might includes servers, storage, networking, software and applications.

→ Start UPS & Small Business → E-commerce Websites

→ Media and Entertainment → Social Media Platforms

→ Gaming companies etc.

* Situation when a business would choose Public Cloud:

- Time considerations
- Application considerations
- Cost considerations
- Data Considerations

* Choosing a Private Cloud:

- High security and compliance needs.
- High Performance and availability needs.
- High customization and integration needs.

* Choosing a hybrid cloud deployment:

- A hybrid cloud deployment it is a mixed computing environment where applications are run using a combination of computing, storage and services in different environments - Public clouds & Private clouds.
- This includes on-premises data centers or edge locations.
- "Edge computing" is a way of processing data closer to where it is generated or used, instead of sending it to a central server cloud.

=> considerations can lead a business to choose to deploy a hybrid cloud.

- Reduce costs
- Minimize Risk
- Extend Capabilities

Some sectors:
- Healthcare Providers
- Financial institutions
- Retailers

Virtualisation:

Virtualisation is the Process of creating a virtual representation of a Physical resource, such as a server, storage device, or a network.

• Virtualization in a cloud environment offers a lot of benefits to users.

→ It enables multiple virtual computers to run on the same Physical host computer, each on its own OS & applications.

→ It can improve efficiency, scalability, and flexibility of information technology (IT) resources, as well as reduce costs & environmental impact.

→ It enables cloud customers to access services over the internet, without having to manage or maintain the underlying Physical infrastructure.

→ It also enables cloud customers to scale up or down their resources on demand, depending on their needs & requirements.

* Cloud Providers Provide 3 types of Virtualisation:

• Virtual machines

• Virtual Storage

• Virtual Networks

Virtual machines:

The situation changed with development of virtual machines. A virtual machine or VM is a software based emulation of a Physical computer that can ~~draw~~ run diff OS & applications.

→ Run on a Physical computer & each Physical computer can run, or host, multiple VMs.

→ Have their own virtual hardware, such as CPU, memory, disk, and network devices that are isolated from host system & other VMs.

→ Orginally virtual machines were primorily used in b[illegible] scenarios. But today, the technology is also being regu[illegible] used in cloud.

- Testing and development.
- Disaster recovery & backup
- Server consolidation
- Security and isolation

* How does virtual machine works:

- Virtual machine work with help of virtualization software called a hypervisor.
- The hypervisor manages & allocates the physical resources of the host computer, like CPU, memory & storage, to the virtual machines.

→ There are 2 main types of hypervisors:

- Type 1 hypervisors: Runs directly on the host hardware. They provide the best performance since there are no additional layers b/w the VM & the hardware.

  Eg: Citrix Hypervisor & microsoft Hyper-V

- Type 2 hypervisors: Runs with in an OS as an application. They are easier to install & use but provide slightly worse performance since all VM requests have to go through the host OS first,

  Eg: VM ware workstation & oracle virtual box.

→ The hypervisor abstracts physical hardware & presents virtual hardware to the guest VMs.

→ This allow each VM to run as if it is its own dedicated physical computer.

→ The hypervisor schedules and manages the execution of VMs so they can share the host computer's resources efficiently.

Main components of VM are:

Virtual CPU • Virtual memory • Virtual Disk • Virtual network adapter.

Virtual Storage:

• Computers work by processing digital data. whether that data in the form of a spreadsheet or a streaming movie the main function of a computer is to store, send and retrieve, and process large amount of 1s and 0s.

→ The virtual storage refers to the pooling of physical storage from multiple networked devices in to what appear to the user as a single storage device.

(OR)

→ "Virtual storage" generally refer to a storage mechanism that stimulates physical storage using software or hardware abstraction, often allowing the user or software to interact with it.

→ Virtual storage can serve various purposes, including isolating data, creating backups, or providing scalable storage solutions.

Eg: In a future with self-driving cars, the problem of finding parking might disappear.

• Cities could pool their parking so any car can use any of available parking spots in the city.

• A car would simply drop someone off at their home & then drive itself to an available parking space.

• People are no longer constrained by the available parking spaces near where they need to be.

Eg: Similarly, virtual storage is a way to store data from a device & retrieve it back over a network or the internet.

• Virtual storage enables devices connected to the network to store and acess large amounts of data virtually, without needing large amounts of storage space on the device itself.

* How do virtual storage work?

Virtual storage uses remote servers to store data, such as files, business information, videos and images.

- Upload data
- Manage data
- Increase storage space
- Access Data

- Virtual storage enables organisation to store, access and maintain data so that they don't need to own & operate their own data center.
- Virtual storage is scalable, allowing organisation to expand or reduce their data footprint depending on need.

* Virtual storage on cloud:

There are 4 main models of cloud storage available.
→ Public → Private → hybrid → multi cloud.

* Public cloud storage:

- In the public cloud storage model, an organisation stores data in a service providers data centers.
- Data in public cloud storage is spread across multiple regions. Cloud providers offer it on a subscription or pay-as-you-go basis.
- Public cloud storage is "elastic". This means that users can scale their data storage up or down depending on the needs of the business.
- Public cloud providers typically make data available from any device such as a smart phone or web portal.

→ Private cloud storage → Hybrid cloud storage.

→ Multi cloud storage.

an org uses multiple public cloud providers to store diff ~~type~~ of data

Helps avoiding vendor lock in, optimize costs, improve performance & enhance security.

more sensitive data on private cloud

less sensitive on public cloud.

Virtual Networks:

A virtual network is a network that uses software instead of physical hardware. It behaves and operate like a regular network, but it exists only in the digital world, not in the physical world, Virtual networks:

→ Use virtualisation technology, which allows engineers to create a network using software based network components.

→ Can simulate all the functionality of a physical network, including routing, switching, firewall & load balancing.

* How do virtual networks work?

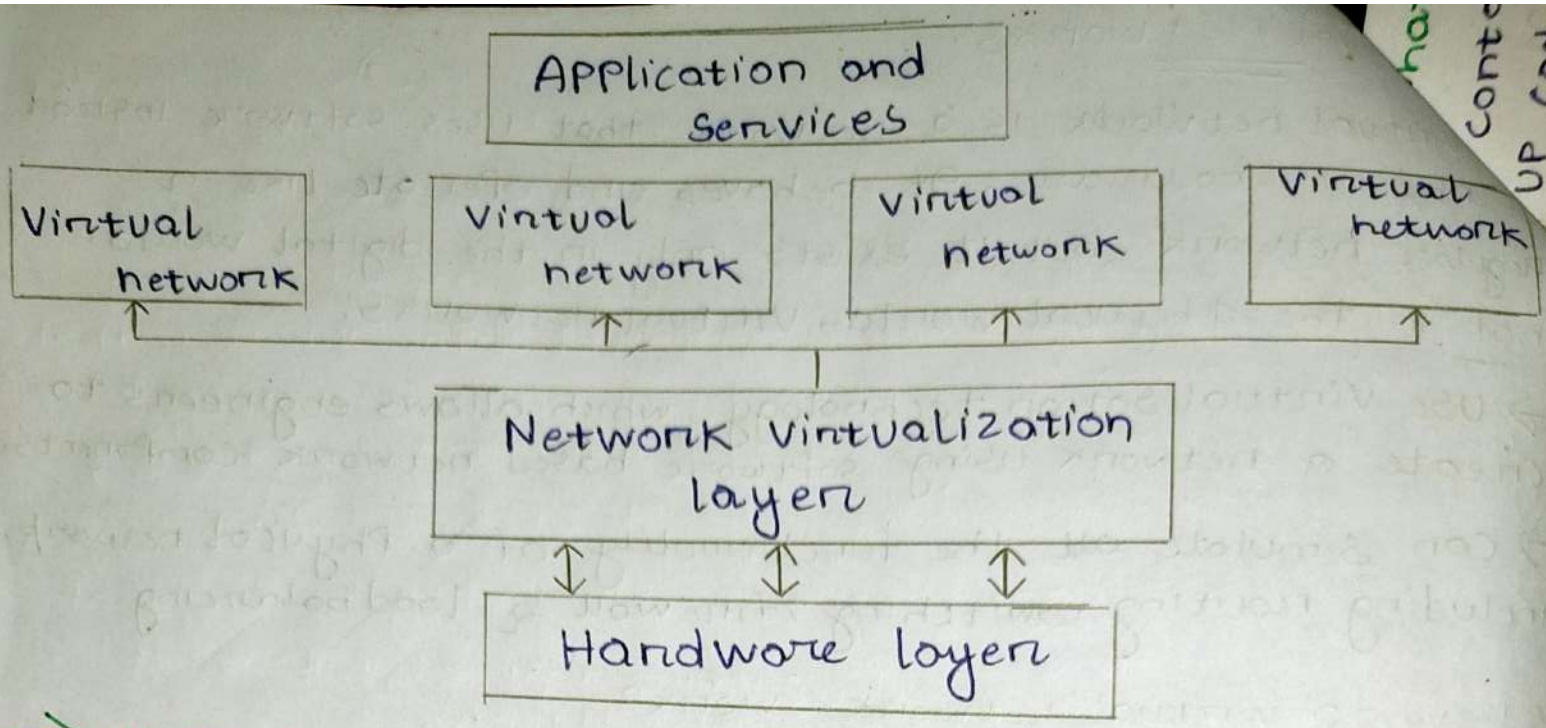
- Virtual networks use virtual routers, virtual switches & virtual firewalls in the same way that physical networks use physical components.
- They exist in a layer b/w physical network components and the workloads that use them.

→ **Hardware layer**: Physical network components like routers and servers. These provide the foundation for the virtual network.

→ **Network virtualisation layer**: Software component
↓
Creates & manages virtual networks on top of physical infrastructure.
↓
multiple virtual network coexist & work independently, while sharing same resource.

→ **Virtual network layer**:
↓
Contains virtual routers, switches, firewalls & other devices
↓
This layer includes additional network services like DHCP and DNS

→ **Application and Services Layer**:
↓
At top layer, there are applications & services, or workloads that rely on the underlying virtual network infrastructure & services to provide network connectivity.



⇒ Users commonly use virtual networks for various purposes:

- Isolating and securing network segments.
- Connecting different locations and cloud services.
- Enhancing performance & availability of network devices/services
- Experimenting with new network configurations & technologies.

Containers: • Containerization is a light weight form of virtualization that enables applications to run in isolated environments on a single host OS. Containers are portable easy to manage, and offer fast startup times.

- By using containers in cloud environments, cloud developers don't have the cost and management associated with a full physical computer or even a virtual machine.
- This means they can make their application & services run faster & require less resources.

What is a container?

A container is a standard unit of software that packages up code & all its dependencies so the application runs quickly & reliably from one computing environment to other.

Eg: • Docker is a popular containerization platform that allows developers to create, deploy & run applications in a container.

• Developers can package their applications and all the dependencies in to docker containers, ensuring consistent behaviour across diff env.

• These containers that can be easily moved and run by various systems that support Docker.

Containers provide many benefits compared to using physical computers.

• **Lightweight and Portable** → containers use a shared OS & only contain the application code & dependencies

→ computer have their own OS & hardware resources.

• **Isolated and Secure**: → containers run in sandboxed env

↓

limit their access to other containers and the host system.

→ By contrast, malware & other security threats can affect computer.

reduces risk of code running in a container impacting other applications or the OS itself

• **Scalable and efficient**:

→ Developers can easily deploy, replicate & update containers across multiple hosts.

→ Computers require more time & effort to set up, maintain & upgrade.

• **Compatible and interoperable**:

→ containers can run on any platform that supports the container software technology.

→ By contrast, computers might have compatibility issues with different hardware or software configurations.

* Containers and virtualization:

Containerization & virtualization are two methods of creating isolated environments for running software applications.

They both aim to improve the efficiency, security & portability of software development & deployment.

→ Virtualising computer resources typically means creating one or more virtual machines to provide a resource for performing various tasks.

→ Containerization means creating containers that run applications & services for performing tasks.

Containers	Virtual machines
1) containerization involves creating containers that share the same OS and hardware as the host server. (virtualise OS)	1) virtualization involves creating VM that emulate the complete operating system & hardware on a physical server. (virtualise hardware)
2) Each container has its own applications, libraries & config files.	2) Each VM has its own OS applications, libraries and config files.
3) Each container is a lightweight and self contained package of software that can run anywhere that supports the same OS.	3) Multiple VMs can run on the same physical server, each with its own resources & settings.
4) enables users to run multiple applications on the same server each with its own dependencies & environment variables and to isolate applications from each other.	4) enables users run diff OS such as windows and Linux on same physical hardware at the same time.
	5) It also enables users to isolate diff applications from each other & the host.

Example of container tools:

- **Docker:** which is the most popular tool for creating & running containers.
- **Kubernetes:** which is a system for orchestrating multiple containers across diff machines or clouds.

"orchestration" is a way to manage & automate tasks across multiple cloud platforms.

- **Podman:** which is a newer alternative to docker for creating & running containers that offers some advantages in security and simplicity.

→ **Docker:**

- Docker is a tool for creating & managing containers using a client server architecture.
- It has a background process called the Docker Daemon that handles container operations & exposes an API for communication with other tools & services.
- Users can interact with the daemon using the Docker command line interface or graphical user interface tools.
- Dockers also supports Docker Swarm, a native orchestration tool for managing multiple Docker hosts & containers.

→ **Kubernetes:**

- Kubernetes is a tool that help users to manage groups of servers & containers.
- It automates tasks like deploying & scaling containers & makes sure they are balanced and healthy.
- Kubernetes uses Pods, which are groups of containers that share resources.
- Users can interact with Kubernetes using CL or graphical tools.

→ Virtualisation uses hardware of the host computer but has its own OS & software, this is called as "Hardware abstraction level".

→ Containers uses hardware and OS of host computer but has its own software, this is called as "Operating System abstraction level".

Docker, Kubernetes, and Podman are different tools for different purposes.

→ Docker is suitable for developers who need a simple and comprehensive tool to create & run containers locally or on a single host.

→ Kubernetes is suitable for operators who need a powerful & scalable tool to manage clusters of servers and containers across different environments.

→ Podman is suitable for anyone who needs a secure and lightweight tool to run containers individually or in pods without a daemon.

* Benefits of using containers in the cloud:

- Containers enable faster innovation, lower costs & higher quality.
- Containers are compatible with the principles of DevOps.
- Containers make it easier to test, deploy & update applications in the cloud.
- Cost savings → 10 applications in 10 VM, would require 10 copies of OS.
  → 10 containers can share the same OS, reducing costs substantially.
- Increased Portability: → On-Premises data centers
  → Public clouds like AWS, GCP, Azure
  → Developer machines.

  Containers abstract the applications from underlying infrastructure, ensuring portability.
- Clustering support: Containers can be clustered together to work as a team of microservices.

  → Easy horizontal scaling of cluster → Dynamic resource allocation across the cluster

Containers allow you to optimize your cloud infrastructure & deploy applications in an efficient and agile manner.

→ **Podman**: • Podman is a tool that can manage & run Containers without needing an additional Program to do so.

• It is based on a model used by Kubernetes, which allows it to run multiple containers together.

• Users can interact with Podman using a command-line tool or graphical tools.

⇒ Differences that impact how users use them in terms of security, architecture & functionality:

	Docker	Kubernetes	Podman
Security	Docker needs access to the core of the host OS or root priviliges to run its background process which can be a security risk.	Kubernetes also uses role-based access control to enforce security policies.	Podman & Kubernetes on the other hand, run as non-privileged users by default & don't need a background process. This makes them more secure & less vulnerable to attacks.
Architect	Docker bundels all its container features in to a single tool.	Kubernetes seperates its containering features in to different components.	Podman uses existing Linux features to run containers without needing a background process. This makes Podman architecture more light weight than the others.
Functionality	Docker is mainly for managing containers, but can also do basic orchestration with Docker Swarm.	Kubernetes is mainly for orchestrating containers, but users can also do basic container management with its command line tool "Kubectl".	Podman is mainly for running containers but can also do basic Pod management using the Podman command from the command line.

Microservices:

* Software goes modular:

- In traditional computing, software packages encompass all necessary components for their tasks or rely on the OS.
- For instance, an image editing app may require custom code for adding online images. Such specific functions known as services, are integral to software applications, often comprising multiple bundled services.

* Breaking software in to pieces:

- In earlier software development, all necessary code for a task was included with in the application itself or OS.
- Engineers began creating libraries, which are collections of software functions designed for specific tasks.
- Libraries house services that multiple applications can use such as file management, spell checkers and font management.
- Applications can call upon these library services to perform tasks, receiving results or data in return.
- Bundling standard code into libraries lets multiple applications share the same functionality, reducing code duplication.
- The approach minimizes the amount of code applications need to store and allow users to become familiar with standardized functions.

* Modular software & the cloud:

- Microservices are like the shops in a mall, working together to provide a seamless experience while operating independently.
- They are used in cloud-based applications as small, independent and loosely coupled services.
- Loosely coupled mean services are connected but perform specific functions & communicate with each other.

- Communication b/w microservices is done through application Programming interface (API)
- API is define how microservices or applications can interact with each other.
- API specify how data and requests should be structured & handled.
- Microservices architecture enables scalability, flexibility and easier maintainence.
- Each microservice can be developed, deployed & updated independently.
- It allows for better management of complex applications and faster development cycles.

⇒ Microservices offer benefits to developers:

- They enable faster deployment, development & more flexible scaling of cloud applications.
- They allow developers to use diff technologies & long for different, services, depending on their needs & preference.
- They help deliver agile & resilient software for the cloud

* Using containers to deploy micro services:

- One of the challenges of developing & maintaining microservices is ensuring that they can run reliably & consistently across different environments
- Developers can use containers to deploy microservices in a consistent and reliable way.
- By using containers to deploy microservices, developers can avoid problems of incompatible software versions conflicting versions (dependencies) & varying OS that can cause error & inconsistencies

Reasons: • Isolation • Scalability • Portability

• Fast startup times. • Ease of management. (37)

* How microservices communicate:

An API is set of definitions & protocols that enable two software components to communicate with each other.

For eg: Weather App $\xrightarrow{\text{Request}}$ API $\longleftrightarrow$ Weather Service

Weather App $\xleftarrow{\text{Response}}$ API

→ API define
- how microservice can exchange info and request services
- type of data that can be sent & recieved
- format of data and protocols to follow.
- work together as a cohesive system.
- maintaining their autonomy & scalability

* By using APIs to communicate, microservices can achieve several benefits.

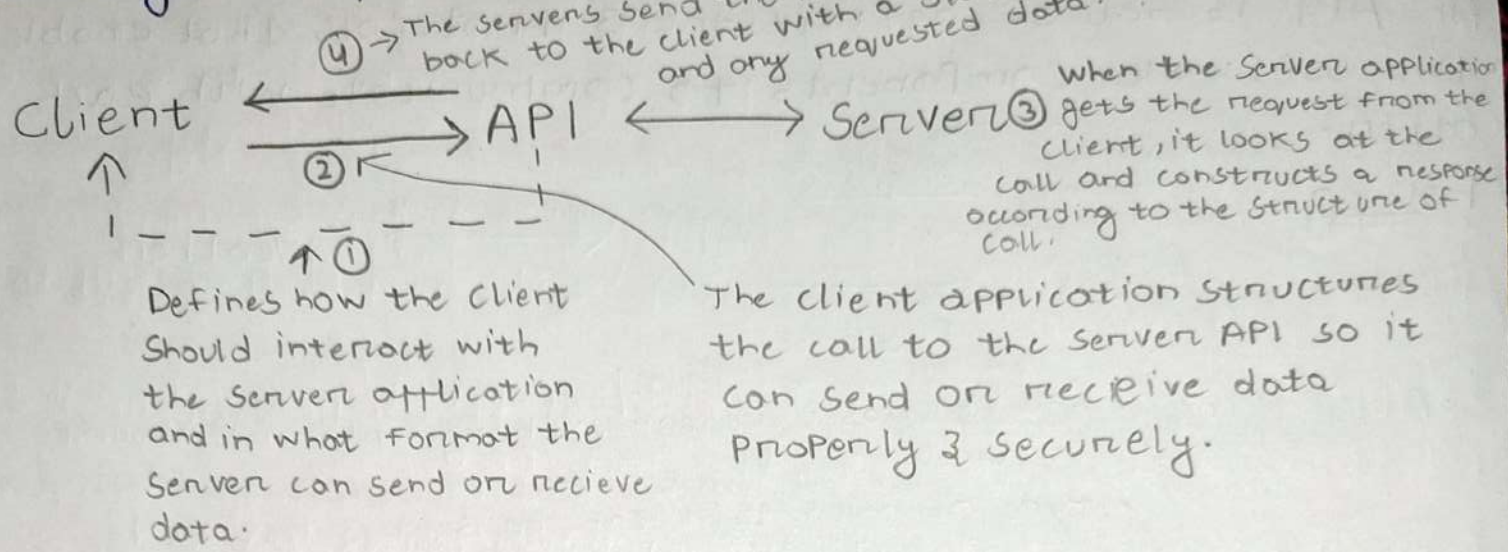
- Modularity
  - test, deploy & update each microservice independently
- Reusability
- Scalability
- Reliability
  - Each microservice can handle errors & failures gracefully
- Flexibility
  - Each microservice can use different technologies & frameworks that suit its needs. without being constrained by the choices of other microservice developers

APIs:

* Data in, Data out:

- APIs enable computer program & services to exchange data.
- They are sets of rules & instructions for different software applications to communicate and share data
- APIs acts as translators or messengers that bridge communication b/w parties.

- For instance, travel websites use APIs to send booking requests to airline systems & retrieve available options & prices.
- APIs streamline process by facilitating efficient data exchange b/w applications.



* APIs in cloud computing:

- They enable the development, integration & management of cloud-based applications & services.
- APIs allow developers to acess & use the functionality & resource provided by cloud service providers such as AWS, microsoft Azure, GCP.
- APIs facilitate connections b/w various cloud services, platforms & applications.
- They enable integration b/w cloud services & on-premises applications.

* The 3 key types of APIs:

⇒ **Service APIs**: Service APIs provide access to specific cloud services, such as storage, messaging & analytics.

Eg: The AWS S3 API allows users to store and retrieve objects in the AWS S3 cloud storage service.

⇒ **Application APIs**: Application APIs provide access to specific cloud applications, such as email, calendar, and social media.

For eg: The Email API allows users to send & receive emails using Email cloud applications.

Infrastructure APIs:

- Infrastructure APIs provide access to low level cloud infrastructure components, such as virtual machines, containers, and networks.

For eg: The AWS EC2 API allows users to launch and manage virtual servers in the AWS EC2 cloud computing service.

* Automating cloud tasks using APIs:

- APIs enable developers to automate cloud tasks in a faster, easier, and more efficient way.
- This is because they can use existing code libraries & frameworks that support various API standards and formats.

Use Cases and Best Practices:

* Using containers, microservices and APIs to migrate legacy apps to the cloud.

- containers help separate the program from the computer it runs on and include all the resources & configuration settings that software needs to run independently.
- microservices divide program in to small parts that can work together.
- And APIs help these parts talk to each other & to other programs.

Developing and Deploying software in Cloud

* Software Development in Cloud:

- Software development is the process of creating, designing, deploying & supporting software.
- Software is set of instructions or programs that tell a computer what to do, and from a user perspective, software is the applications they use to perform their task.
- Cloud based development involves cloud computing to develop software.
- Cloud computing is the delivery of computing services such as servers, storage, databases, networking, software, analytics, and intelligence over the internet.

⇒ Cloud computing offers many benefits for software development.

- **Scalability:** ↓ Easily adjust resources based on demand without hardware concerns
- **Cost efficiency** ↓ No upfront investment, pay as you go model, access to affordable tools
- **Collabration** ↓ Remote work, cloud-based platforms, real-time sharing & feedback
- **Innovation** ↓ Access to latest technologies like AI, ML, bigdata IOT.

⇒ Cloud-based development versus traditional development:

→ Development environment:

Traditional: Developers use a local computer with an OS, programming language, IDE & tools.

Cloud: Enables remote work from any device with internet access worldwide.

→ Development cycle:

Traditional: Developers follow a linear cycle with phases like planning, analysis, design, implementations, testing & deployment.

Cloud: • Developers follow iterative cycle (agile) with frequent iterations of planning.
• Enables faster deployment of new and updated apps due to iterative development

→ Development Model:

Traditional: Developers use a monolithic or centralized model building a single large application for a single server or private network.

Cloud: This approach offers faster development, easier deployment & flexible scaling of applications.

* Developer Operations (DevOps) in the Cloud:

- Developer Operations or DevOps is a culture and practice of collabration b/w developers and operation team.
- It's a software development approach that combines collaborative principles, tools, and practices to enable frequent updates & rapid evolution of products.

→ DevOps originated in on-premises development environments. Teams using traditional DevOps strategies can face challenges:

- Limited scalability
- Reliability
- Cost-efficiency
- Lack of standarization & automation of their processes
- Difficulty sharing knowledge & best practices across their teams.
- DevOps on cloud gives businesses a centralised, standard platform to manage & automate their infrastructure, data and security.

→ **Benefits:**
- Multiple Environments
- Better Delivery
- Continuous, Agile Process
- Valuable Tools

* Best Practices for Cloud Software development:

- Cloud software development is the process of creating & delivering software applications that run on remote servers & users access over the internet.
- Some of the practices are:

n for Portability • Use ~~service~~ Serverless computing

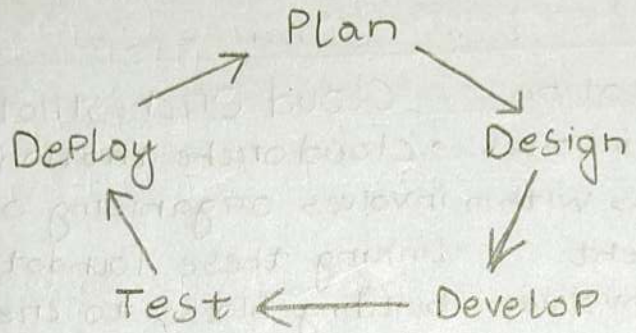
Choose the appropriate Design • Provide Security

• Considder different IT environments

* The software development lifecycle (SDLC) in the Cloud

• The software development lifecycle (SDLC) is a methodology with clearly defined Processes for creating high-quality software.

• SDLC helps software developers Plan, design, develop, test & deploy software in a systematic & efficient way.



When software dev. use SDLC in the cloud they need to understand how the cloud works and how it can benefit their software development process.

They can use the cloud to store data, run, applications, host websites, and more

* Orchestration Software development on the cloud:

• Orchestration: It is a way of managing and automating the different tasks and processes involved in running applications & work loads.

• Cloud orchestration: • Cloud orchestration involves coordinating applications and workloads across different cloud Platforms, like IBM cloud, AWS, and Azure.

• It helps developers manage various components in their cloud environment to achieve goals like app deployment or updates.

• components can include servers, storage, networking, security and software.

• **Automation**: It is the process of using software to perform tasks that would otherwise require human intervention, such as sending emails, updating databases or testing applications.

• **Cloud Automation**: Cloud automation is software automation that operates on cloud platforms, offering computing resources & storage.

• It offers benefits like scalability, reliability, security and cost effectiveness compared to travel automation

• Businesses can enhance efficiency, productivity and innovation by automating processes & workflows in the cloud.

Cloud Automation	Cloud Orchestration
• Cloud automation involves performing tasks within a cloud environment without human involvement. • Developers use it to automate tasks like creating VM or config fire walls. • It serves as a foundational tool for building intricate & connected operations.	• Cloud orchestration involves organising and linking these foundational building blocks to create a sequence that accomplishes a particular business task. • For instance, a developer might orchestrate the app deployment process by automating tasks like VM creation, software installation etc

* Cloud orchestration:

There are different methods that developers can use for cloud orchestration, depending on the needs of their project.

• **Imperative orchestration**: methods, in which developers specify the exact steps and order of execution for their automation tasks.

Declarative orchestration: methods, in which developers specify the desired outcome & left the tool they are using figure out the best way to achieve that outcome.

⇒ Cloud orchestration has many benefits for business and IT organisations.

- Reduce manual works, errors and delays
- Improve standarization and consistency
- acceleration delivery and innovation
- Enhance visibility and control.
- Optimize resource utilization & performance across a cloud environment.

* The imperative orchestration method:

- In imperative cloud orchestration, developers specify the exact steps & commands to execute to achieve a certain goal.
- For eg: To deploy an application on a cloud platform, they need to write a script or a workflow that tells the cloud orchestration tool what to do in each step, such as creating a VM, installing software & then configurig settings.

→ An example workflow that a developer might follow to deploy a web application in an imperative orchestration.

Provision a server on a public cloud service. → configure the network settings and security policies

→ Install the required software & dependencies → Deploy an application on the server

→ Start the server & monitor its performance.

→ Imperative cloud orchestration gives a developer control & flexibility over the process, but it also requires more knowledge & skills to write & maintain the scripts or workflows.

→ Developers will also need to update the orchestration whenever there are changes in the cloud environment or application requirements.

The imperative method can provide you with distinct benefits if your deployment approach calls for it. Consider these two advantages.

- Control => By using the imperative approach, you have more control over the process.
When deploying a new service, more control can help you ensure things go the way you intend.

- Specific steps => When deploying a new service, you might want to create very specific steps so you are sure the service does exactly what you want it to do.

* The declarative orchestration method.

Another way to achieve cloud orchestration is by using a declarative method.

- Developers outline the desired outcomes & goals of their cloud service.
- Specifies like config, performance, security, availability and cost are defined.
- Detailed step by step instructions are not necessary in this approach.
- Cloud orchestration tools (eg: Kubernetes, Jenkins) interpret developer specifications.
- Tools automatically execute the necessary operations & procedures.
- Cloud resources are orchestrated to meet the defined goals efficiently.

* Useful & Scenarios: -> A developer
-> An IT operator
-> A Business user.

Using the declarative method:

A developer can deploy a web application to the cloud by:

→ Defining the components of their application, such as the web server, databases, load balances & firewall.

→ Specifying the properties & policies of each component, such as the number of server instances, scaling rules, access controls, and backup schedules.

⇒ Declarative method for deployment can be essential consider the following.

- Complexity: A developer would use a declarative method for complex tasks that involve multiple steps and resources, such as deploying an application or managing a network.
- Optimization: The declarative method allows the computer to optimize the execution of the deployment and handle errors automatically.
- This enables the developer to focus on the desired outcome rather than the details of the process.

* Cloud orchestration automation software:

- Developers use cloud automation to perform individual operations on components of a cloud environment, such as servers, databases, or switches.
- Using automation tools in cloud orchestration scenarios helps reduce the amount of manual work, errors, and delays that IT teams face when managing complex cloud environments.
- Automation tools can also help IT teams implement Infrastructure as Code (IaC).
- IaC is a way of defining & configuring resources using scripts or Line of codes instead of manual actions.

Some eg: • Cloud orchestration Platforms that use automation tools are Kubernetes, Docker, Swarm & Ansible.

• These platforms allow IT teams to input commands or scripts to set up monitor, and manage cloud resources & applications.

* Automating cloud orchestration with Kubernetes:

• Kubernetes is a tool that automates deploying, scaling & managing applications.

• It does this by grouping containers in to logical units, making it easier for developers to manage their apps.

• Developers can specify how many copies of each container they need, where they should run, and how they should work together.

⇒ The Requirements:

• Imagine you are part of team that develops a web application for a large company. Your app needs to run on hundreds of servers across diff regions & handle millions of requests per day. How do you manage such a complex system?

⇒ Kubernetes handles the workload:

① Container Management: It destributes your containers (where your apps run) across diff servers.

② Monitoring: It keeps an eye on the health & performance of your containers.

③ Auto-Replacement: If a container fails or needs an update Kubernetes replaces it automatically.

④ Load Balancing: It evenly distributes incoming requests to your app, ensuring it runs smoothly even with high traffic.

⑤ Reliability: All of this makes your app fast & reliable for user

The Result: By using Kubernetes, you can focus on developing your app's features & functionality, while letting Kubernetes handle the operational aspects of running it in the cloud.

(45)

Introduction to Data Management & Security in the Cloud.

* Security in a wired world:

- Some devices & applications require users to provide two or more methods of authentication.

For eg: when you access your email you might need to enter your password & then enter a code that email provider sends to your mobile phone.

- This is known as two-factor authentication (2FA) or multifactor authentication (MFA).

* Data Security in cloud:

- Some systems encrypt data as it moves over the internet. This is known as encryption in transit. For eg: messaging apps encrypt messages in transit to prevent anyone else from viewing the messages

- Some systems encrypt data on the storage system itself. This is known as encryption at rest. For eg: A business might choose to encrypt employee data that they store in the cloud.
- Even if hacker accesses a data, without the decryption key they won't be able to read it.
- Detecting patterns and then using those patterns to predict future behavior is sometimes called heuristics.
- Heuristics comes from a greek word meaning discovery.

• Engineers define what behaviours would be useful to observe & then figure out how to apply those observations to create security alerts.

• when you want to protect your personal computer, you might install a virus scanner or a firewall.

• Websites need similar protection too, people with malicious intent might try to steal data or cause a website fail.

For eg: A denial of service (DoS) attack attempts to overload a website by sending an enormous amt of fake requests

→ Prevention Tools: detect DoS Attack and then either prevent the fake requests from reaching website or alert the cloud engineer about the attack so they can respond.

→ Monitoring tools: Examine the status of web services cloud engineers use them to view every aspect of their cloud service so they can detect if anything is under attack.

→ Development tools: Web dev use to create websites have built in features that can alert cloud engineers about problems with their code that could cause security issues.

* Complying with security regulations:

• Security Regulations are rules for standards that aim to protect the confidentiality, integrity, and availability of data and systems in cloud.

⇒ Complying with security regulations when developing cloud based solutions can:

• Help prevent or mitigate the -ve consequences of security incidents. These might include legal penalties

...rational damage, customer loss, or operational disruption

- Enhance the trust & confidence of users in the solutions
- Enable the solutions to meet the expectations & needs of different market & regions.

→ Developers need to follow some best practices to comply with security regulations for their cloud based solutions.

- Assess.
- Control.
- Monitor
- Educate
- Review.

* Impact of data breaches:

- A cloud security breach is a serious incident that can expose sensitive data, disrupt business operations, and damage customer trust.
- A company's reputation depends on how well it protects its data & its customers from cyberattacks.

=> -ve consequences of cloud security breaches:

1) Loss of credibility 2) Legal Liability 3) Brand damage.

Cloud Based security vulnerabilities:

* Types of cloud vulnerabilities:

- A vulnerability in a cloud-based service is a weakness or flaw in its security.
- Threat actors exploit vulnerabilities in software in several ways, called attack vectors.
- An attack vector in cloud security is a way that cyber criminals can access or damage cloud data or applications.

* Types of vulnerabilities:

→ Misconfiguration → Poor access management

→ Insecure APIs → System vulnerabilities → Lack of monitoring

* Ways to mitigate vulnerabilities:

- Cloud security is a critical concern for businesses and organisations that use cloud computing to store & process their data.
- Cloud engineers follow several key approaches to help mitigate cloud vulnerabilities & protect company data from attacks.

=> Some approaches are:

- The shared responsibility model
- The defence depth strategy
- The principle of least privilege
- Patching & updating.

=> Shared Responsibility model:

- Shared responsibility model in cloud security involves both the CSP & the cloud customer.
- CSP is responsible for securing infrastructure.
- Cloud customer is responsible for securing data, application & access.
- Responsibilities include encrypting data, using strong passwords and configuring access policies.

=> Defense in Depth strategy:

- Defense in depth strategy involves multiple layer of security controls.
- Examplex of these controls include firewalls, IDS/IPS, antivirus software, WAF, encryption, backup etc.
- This approach reduces the attack surface & enhances attack detection & prevention.

Principle of least Privilege:

Principle of least Privilege restricts users & applications to minimal necessary access & Permission.

- It minimizes Potential damage from compromised accounts or applications.
- users & applications are granted access only to what is required for their tasks

Eg: Read Only access for a user.

⇒ Patching & Updating:

- Patching & updating are processes of applying fixes or improvements to software or systems.
- These fixes address known Problems or vulnerabilities.
- unpatched software can be exploited by threat actors.
- Applying security Patches can Prevent vulnerabilities from being exploited.
- Eg: A security Patch on a web server Prevents hackers from injecting malicious code in to a website hosted on the cloud.

IDENTITY AND ACCESS MANAGEMENT:

* Accessing systems & resources:

⇒ Gaining access to a system

Authentication: • Authentication (AuthN) strengthens access control.

- It permits authorized individuals or systems to access a network or device.
- common methods include usernames & Passwords.
- Biometrics like finger Prints, facial recognition, and retinal scans can also be used.

• Lock Screens on devices serve as an authentication meas

⇒ Gaining access to resources:

Authorization

• Authorization (Auth z) manages access to resources with in a system.

• It controls whether users or systems have permission to use specific resources.

• Authentication determines if access is granted, while authorization governs what actions users can perform after access is granted.

• Analogous to a child lock on an appliance, it restricts certain actions even after access is granted for safety & control.

* Authentication and Authorization work together:

• In consumer focused cloud services, like file storage & mobile devices, authenticated users often receive automatic authorization for various resources.

• For instance, when you log in to your mobile phone, you are granted permission to read & write files, and download apps

• Cloud management tools provide IT professionals with the ability to finely control resource access, tailoring to meet the organization needs & security policies.

* Authenticating and Authorizing users in the cloud:

→ Pass-through authentication

• Pass through authentication is a process that allows a user to access a system or application using the same credentials they have already provided.

• It's often used to simplify user access & reduce the need for users to remember multiple sets of login credentials.

eg: In corporate network, Paas-through network authentication might enable a user who has already logged in to their work station to access network resources without needing to enter login credentials again.

- Paas through authentication relies on initial authentication, typically handled by a central authentication server, to grant access to other system or services without additional login steps.

→ Multifactor Authentication:

- Multifactor Authentication (MFA) adds an extra layer of security to the login process
- It requires users to provide two or more auth factors.
- Factors can include something you know (like Password, fingerprint etc)
- MFA enhances security by making it harder for unauthorized users to access accounts.
- It's commonly used in online banking, email services etc.

* Enforcing access Policies & procedures:

- Cloud adminstrators are also responsible for managing who can access cloud resources and what they can do with them.
- They use "Policies" and "Procedures" to enforce access rules and protect data from unauthorized or malicious users.

→ Policies are sets of conditions and actions that define what users can or can't do in a cloud service.

→ Procedures are steps or instructions that cloud adminstrators follow to implement.

→ Cloud adminstrators can also use Policies and Procedures to grant different levels of access to different users or group of users.

→ By using Policies & Procedures, cloud adminstrators can:

- Control & monitor access to cloud resources & data
- Comply with security standards & regulations that apply to their organisation or industry.

* Generating Reports:

3 examples scenarios in which a cloud adminstrator would need to write a report.

- A user or group exceeds their allocated cloud storage.
- A cloud service or application experiences an outage or a performance issue due to misconfiguration or improper deployment.
- A cloud resource or an account is compromised or accessed by an unauthorized users or part of a breach.

* What's in a report?

Cloud administrators need to write their reports in a clear, concise and accurate manner, using simple and non technical language.

- They need to explain what happened, why it happened, what they did to fix it, and what should change to prevent it from happening again.
- They also need to provide evidence & data to support their findings & recommendations

* Zero Trust Model:

- The Zero Trust model is a way of securing modern organisation by removing the assumption of trust & enforcing strict verification & authorization.
- In this model, every user, device & component is considered untrusted at all times, regardless of whether they are inside or outside of an organisation work.
- The zero trust model is designed to adapt to the complexities of the cloud environment, where data & applications can be accessed from anywhere & by anyone.

The Zero trust model is based on 3 main Principles:

→ **Verify explicity**: The Services must authenticate & authorize every access request based on multiple factors such as identity, location, device, health & data sensitivity.

(49)

→ **Use least Privilege access**: Users & devices should only have the minimum level of access they need to Perform their tasks and that they should only gain access for a limited time & under certain conditions.

→ **Assume breach**: Design security measures to minimize the impact of a Potential attack. Do this by encrypting data, Segmenting networks, and monitoring for anomalies.

⇒ The Purpose of the Zero trust model:

The Zero trust model can help organizations to:

- Improve their Security
- Empowered Productivity
- Enable digital transformation
- Comply with regulations
- Reduce costs & complexity.

However, implementing the Zero trust model requires a strategic approach covers six key elements:

- **Identities**: This element focuses on verifying the identity of every user before granting access to resources.
- Adminstrator can do this by using multifactor authentication & identity management solutions.
- **Devices**: This element focuses on ensuring that only secure and compliant devices can access resources.
- Adminstrator can use device management and endpoint security solutions to implement this.
- **Applications**: This element focuses on securing the applications that user access. Adminstrators can use application security & access control solutions for this.

• **Data:** This element focuses on protecting the data that users accesses & share. Adminstrators use data encryption and data loss prevention solutions to protect data.

• **Networks:** This element focuses on securing the networks that connect users to resources.
Adminstrators can secure networks by using network segmentation and network security solutions.

• **Infrastructure:** This element focuses on securing the underlying infrastructure that supports the organisation operations.
Adminstrators use infrastructure security & compliance solutions to secure this.

Databases and DBAAS:

• **Simplified Data Management:** Store & management data online without technical hassles.

• **Provider's Role:** DBaas Provider handles software, hardware & maintenance.

• **Tenant's Customisation:** Users choose database features, akin to renting an apartment.

• **Maintenance-Free:** No worries about security, utilities or infrastructure.

* **Benefits of using DBaas:** • Cost savings • Flexibility • Availability • Security • Reliability.

* **Managing databases with DBaas:**

• Database management is the process of creating, maintaining and securing databases.

• can be complex, especially for large databases requiring specialized skills & tools.

* **Securing databases with DBaas.**

⇒ **On-Premises:**

• **Control:** Organisations have greater control over security protocols.

& Responsibility: Companies are entirely responsible for maintaining updating security measures.

⇒ DBaaS (Database as Service):

- Provider Handling: Service Providers manage and implement security measures.
- Advanced Security: DBaaS Providers offer advanced security features
- Maintenance & Updates: Providers handle routine maintenance & updates.
- Trust Factor: organisations must trust the provider's security competence & vigilance.

* Security features of DBaaS:

- Encryption
- Backup & Recovery
- Access and control

Managing data in the cloud:

⇒ Managing data effictively involves two interrelated activities: data governance & data compliance.

Data Governance	Data Compliance
• Data governance involves: → Process → Policies → Roles → Metrics → Standards • It's purposes are: → Ensuring data is clean, accurate secure, and available for authorized users. → Aligning data management practices with organizational goals. → complying with external regulations.	• Data compliance involves: → Adherence to rules & regulations for data in the cloud. → Compliance with industry standards, gov laws, contracts or ethics. • It's purposes are: → Protecting data from unauthorized access, misuse or loss. → Avoiding legal risks & reputational damage from data breaches or violations.

* The importance of data governance & compliance:

- Personal experience of a data breach, like credit card misuse or social media hacking, indicating the impact on individuals.
- Data governance and compliance breakdowns are costly & harm a company's reputations & customers.
- Effective data management doesn't always prevent unauthorized access but is crucial for data safety.
- Proper governance and compliance ensure essential security measures like encryption, access controls and backups.

Cloud support for data governance & compliance:

- Cloud service providers offer different levels of support for data governance & data compliance depending on the type of service they offer & the contract they have with the customer
- Some ways that cloud service providers support data governance & data compliance.

→ Certifying their compliance

→ Providing tools & documentation for customers

→ collaborating with customers & regulators.

⇒ Certifying Compliance:

- Federal Risk and Authorization Management Program (FedRAMP) is a US government program.
- It standardizes security assessments for cloud services.
- Cloud providers can achieve FedRAMP certification.
- Certification demonstrates compliance with strict security standards.
- It helps federal agencies ensure data security in cloud.

Providing Tools: cloud Service Providers offer tools & features that help customers to manage their data.

- These might Include tools for encryption, backup, recovery, access control, logging & auditing.

(51)

⇒ Providing Documentation:

- Cloud service Providers ~~collaborate with customers & regulators to address~~ offer documentation for data governance & compliance.
- This includes SLAs, TOS and Privacy Policies.
- These documents clarify customer and provider responsibilities.
- They help ensure data security and compliance in the cloud.

⇒ Collaborating:

- Cloud Providers work with customers and regulators on data governance and compliance.
- collaboration involves handling data subjects requests, breach notifications, and audits.
- This ensures adherence to data Protection regulations in the cloud.

* Cloud security tools that support governance & compliance:

- Encryption: It is the Process of transforming data in to a secrete code that only authorized parties can read.
- Key Management: It is the Process of creating, storing and managing the keys or passwords used to encrypt & decrypt data.
- Identity and access management (IAM): IAM is the Process of defining & enforcing who can access what resources in the cloud, and under what conditions.
- Data loss Prevention (DLP): DLP is the Process of detecting & Preventing the unauthorized exposure or leakage of sensitive data from cloud.
- Security information and event management (SIEM): SIEM is the process of collecting, analyzing & correlating security related data from various sources in cloud, such as logs, alerts, events & incidents.