Unit : 03.

Q.1) Describe the structure & types of Virtualization ?

→ Virtualization is a technology that allows you to create a virtual version of something, such as Hardware, a Server or an operating system (OS).

- it means Running Multiple virtual machines or systems on a single physical machines allowing better resources use & flexibility.
- it uses Software to create a virtual environment
- Virtualization is a technology that allows you to create a virtual version of a resources, such as a server, storage, devices or NW using Software.
- This helps improve efficiency, Scalability & flexibility in managing IT resources.

- Characteristics of Virtualization →

1) Isolation → each virtual machine (VM), or env. is independent of others, ensuring that issues in one VM don't affect other running on the same physical hardware.

(each VM is separate, so problems in one won't

Unit : 03.

Q.1) Describe the structure & types of Virtualization ?

→ Virtualization is a technology that allows you to create a virtual version of something, such as Hardware, a Server or an operating system (OS).

- it means Running Multiple virtual machines or systems on a single physical machines allowing better resources use & flexibility.
- it uses Software to create a virtual environment
- Virtualization is a technology that allows you to create a virtual version of a resources, such as a server, storage, devices or NW using Software.
- This helps improve efficiency, Scalability & flexibility in managing IT resources.

- Characteristics of Virtualization →

1) Isolation → each virtual machine (VM), or env. is independent of others, ensuring that issues in one VM don't affect other running on the same physical hardware.

(each VM is separate, so problems in one won't

affect other.

2) Resource Sharing →

Multiple VMs share the physical Hardware Resources (CPU, Memory, storage), efficiently. optimizing usage & reducing hardware Costs.

(Multiple VMs Can Share the Same physical Computer. using its Resources efficiently)

3) Encapsulation →

VM or env are encapsulated as files, Making them easy to copy, move or Back up

(A VM is like a file that you Can easily move, Copy or Back-up)

4) Flexibility →

VM Can run different operating Systems or apps on the Same physical hardware, providing flexibility in managing workloads.

(you Can run diffr OS or applications on the Same Machine, making it easier to manage)

5) Portability →

VM or env Can be easily migrated betn physical hosts, allowing for better load balancing & minimizing downtime.

(VMs Can be moved easily betn diffr Computers, helping balance the workload)

6) Scalability →

Virtualization allows quick Scaling of Resources, enabling the addition of more Virtual Machines or env. Without significant hardware changes

(its easy to add or remove VM Based on your needs)

7) Security →

Each VM Can have its own security setting, allowing for greater Control & reduced risks of attacks spreading across the System.

(each VM Can have its own Security, reducing the risk of Spreading attacks)

• Benefits →

The benefits of Virtualization include:

1) Cost Saving → By running multiple VM on a Sing physical Server, you reduce the ne for physical Hardware

2) Better Resource Utillization →

Virtualization help fully use the resources (CPU, M Storage) of a physical Server, reducing waster

3) Scalability →

It easy to add or remove VMs, allowing businesses to quickly scale up or down based on their needs.

4) Flexibility →

5) Improved Disaster Recovery →

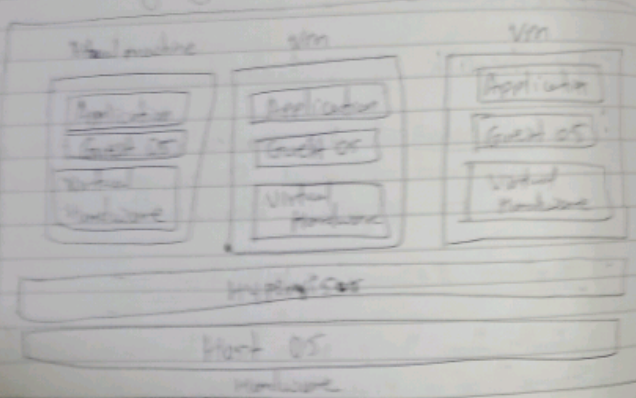
VMs can be easily backed up & restored, making disaster recovery faster & simpler.

6) Less Downtime → VMs can be moved between servers with minimal disruption, reducing downtime for maintenance or upgrades.

7) Energy efficiency →

8) Easy to Test →

- The following fig the concept of virtualization technology:



- Types of Virtualization →

1) Hardware Virtualization
2) Software "
3) Server "
4) Storage "
5) NIW "
6) Operating System(s) "

1) Hardware Virtualization →

- Hardware Virtualization is a technology that allows a single physical Computer (or server) to run multiple Virtual Machines (VM) at the same time.

- each VM acts like a separate Computer, with its own (OS) & applications, but they all share the physical hardware (CPU, Memory, Storage) of the main Computer.

- A special software Called a Hypervisor Controls this, dividing the hardware so that each VM gets what it needs.
This way, you Can use one Computer to do many tasks, Saving money, energy & space.

; It's like having several Computers inside one.

- Hypervisor are of two types. These are as follow:

- Type-1 Hypervisor
- Type-2 "

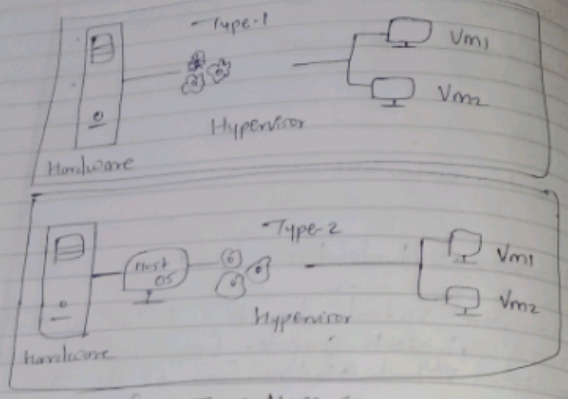


fig: Type Hypervisor

- Types of hardware Virtualization

Hardware Virtualization can be broadly divided into three types:

1) Full Virtualization
2) Para "
3) Hardware assisted "

1) ~~Full Virtualization~~ →

disadvantage ↓

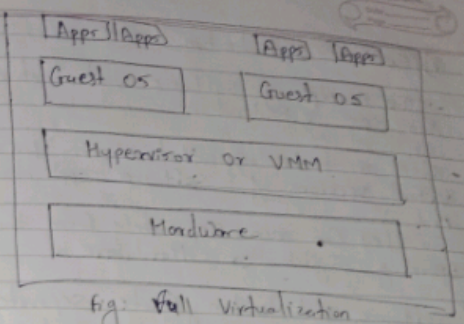


fig: Full Virtualization

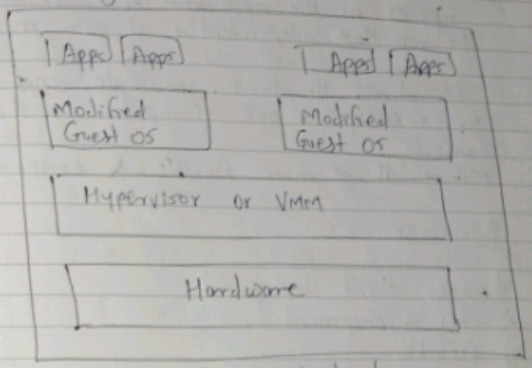


fig: Para- Virtualization

2) Software Virtualization →

- The Concept of Software Virtualization is the same as Virtualization
- It is a technology that allows you to create virtual versions of software application or env.
So they can run separately from the underlying operating system or Hardware

[Software Virtualization Create : Separate, Virtual Spaces for the application or Software env to run independently of your main System]

- This allows you to run multiple apps, versions or settings on one Computer without Conflicts.
Making things more flexible & easier to manage

- Advantage →

1) easier client deployment
2) easy management
3) flexible
4) Backup
5) Running Multiple Os
6) " diff^n Versions of Software

- Types of Software Virtualization →

1) Operating System Virtualization
2) Application "

3) Service "

3) Server Virtualization →

- It is a technology that allows one physical server (a powerful Computer that manages data & services)
to be divided into multiple virtual servers.
- each Virtual Server works like a Separate, independent server.
- Every physical server has its own Os, memory, & hardware resources including CPU & hard disk.
- In Server Virtualization all these resources are Hidden from the users.

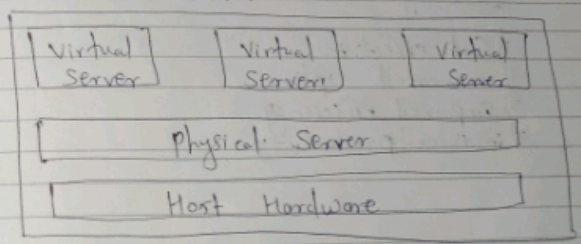


fig: Server Virtualization

- In server Virtualization, the physical server is divided into multiple Virtual server
- All these server are diff^n & work like Unique devices

- They seem to be real physical devices to the users.
- The Central Server administrator uses a software to divide the physical server into more than one virtual env.

Each virtual env run it own OS independently.

- The physical server is also known as Host.

- Types of Server Virtualization →

1) Virtualization at the OS level
2) Virtual Machine model
3) para - virtual Machine

- Advantage →

1) Cost effective
2) increased uptime
3) improved efficiency
4) increased productivity

4) Storage Virtualization →

- It is a technology that combines diff physical storage devices into one virtual storage system.

Making it easier to manage & use all that storage as if it were a single, unified space.

-

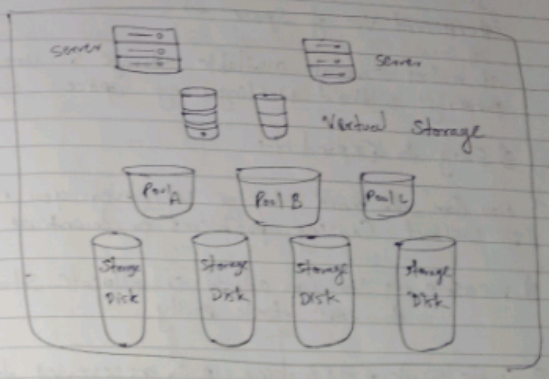


fig: Storage Virtualization

- Storage Virtualization is also know as Cloud Storage.
- It helps us to manage data & store devices efficiently & in less time.

It enables users to maintain a backups of their data & ensures recovery of the data.

- Organizations should implement Storage Virtualization for better Storage management & improved Storage virtualization.

- Characteristics →

1) Easier Management →

It Combines Many storage devices into one virtual space, making it simpler to manage everything as if it's one big storage system.

2) efficient Use of Space →

It makes sure all available storage is used properly, without wasting any space

3) Easy to Expand →

You can add more storage whenever you need it without causing problems or downtime

4) Flexible → You can adjust or allocate storage to diff tasks easily.

5) Simple Backup → Backing up & recovering data is easier because everything is managed in one place

6) faster performance.
7) more Reliable

- Benifit →

1) Highly Scalable
2) easy data migration
3) Better management
4) easy & Secure Storage

4) Network Virtualization →

- It is a technology that combines diff physical nlw resources, like routers, switches & servers into one virtual nlw.
- This virtual nlw works like a single unit, even though it is made up of diff pieces of physical hardware
- In Nlw Virtualization, hardware & software nlw resources & their functionalities are encapsulated into a Software-based administrative entity.

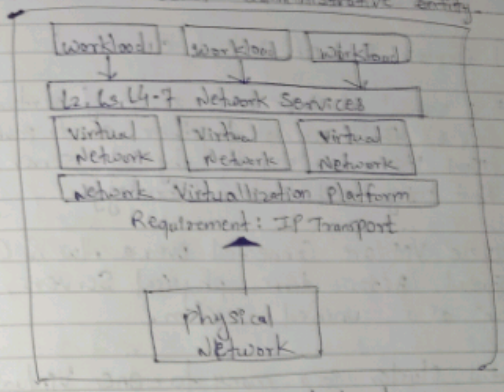


fig: Network Virtualization.

- Network Virtualization Can be classified into the following two classes as follows:

1) external Nlw Virtualization
2) internal Nlw Virtualization

3) Virtualized Network interface Cards(VNIC)
4) Isolation
5) Abstraction.

- Characteristics →

1) Centralized management
2) Resource efficient
3) Flexibility
4) Scalability.
5) Isolation
6) Fault Tolerance

Q 2) Explain in brief Virtual clusters ?

→ A Virtual clusters is a group of Virtual Machines (VMs) that work together as to perform tasks. Much like a traditional physical Server cluster, but using virtualization technology.

- These VM are Connected over a Nlw & Can be Spread Across diffn physical Servers, they run as a unified system.

- Virtual Cluster is a many-to-one Virtualization technology, which Can form a Routing System from multiple Common devices Connected through a switching Nlw.

- In Cloud Computing, a Virtual cluster is a group of Virtual machines (VM) that are deployed as a single logical unit.

- They share the same Virtualization software & hardware.
& they appear as a single unit to the end-user.

- Virtual clusters provide the ability to scale operations easily.
you Can add or remove VMs to meet changing demands & you Can move VM to optimize the use of hardware.

- Clusters provide the Computational power through the use of parallel programming, a technique for Coordinating the use of many processors for a single problem.

- A Cluster of Virtual Servers will be used to host the services to support high availability & resources utilization.

- Virtual Clusters also provide flexibility in adding more services in the future, with minimal Code & Configuration changes.
An additional standby virtual cluster is also used.

- Virtual clusters works by enhancing the server utillization.

- Instead of using seperate physical Computers, it uses virtualized environments on a single physical Server or across multiple servers.
These VMs Can share resources, Communicate with each other & run applications allowing for flexibility easy Scaling & efficient use of hardware.

-

- Virtual clusters are common in cloud computing for handling workloads & making sure resources are used efficiently.

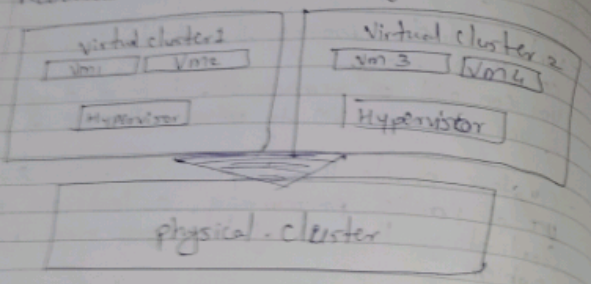


fig: Virtual cluster

Q a) Explain Resource management ?

→ Resource management in cloud computing is about controlling & allocating resources like computing power, storage & n/w bandwidth efficiently to meet users needs.

- In the cloud, resources are shared among many users, so resource management ensures everyone gets the performance they need without wasting capacity.

- It involves tracking demand, adjusting resources automatically & optimizing usage to prevent overloading.

- Good resource management keeps cloud systems efficient, responsive & cost-effective.

- In CC, resource management ensure that each application or services gets just the right amount of resources, like CPU, memory, storage & n/w BW when needed.

It involves several key tasks:

1) Resource Allocation
2) Load Balancing
3) Auto scalling
4) monitoring & optimization

Q b) Difference

→

Virtual cluster	physical cluster
1) Uses virtual machine on shared physical hardware, running as if they were separate computers	1) Uses multiple physical computers or servers connected to work together
2) Multiple VMs share the same physical hardware resource	2) each machine has its own dedicated hardware
3) easier to scale by adding more VMs as needed without new hardware	3) Scaling required adding more physical machines & which can be costly & time-consuming

2) More Cost-effective 2) less Cost	2) more Cost because more physical hardware
3) Managed Centrally, often with automated tools, Making it Simpler to update & maintain	3) each machine needs individual maintenee
5) Highly flexible.	6) limited flexiblity

(1) 5) Difference →

→ Cloud Computing	Virtualization
1) Cloud Computing is used to Provide pools & automated Resources that Can be Accessed on-demand	1) Virtualization is used make Various Simulated env. through a physical hardware System
2) Cloud Computing Setup is Completed	2) Simple
3) Cloud Computing is high Scalable	3) Low Scalable
4) In the Condition of desaster recovery, CC Relies on Multiple machines	4) In the Condition of desaster recovery, Virtualization relies on Single peripheral device.
5) In CC, the workload is Stateless	5) in Virtualization, the Workload is Sateful

6) Cloud Computing is very Flexible	6) less flexible
7) The total Cost of CC is higher than Virtualization	7) The total Cost of Virtualization is lower than CC.
8) CC requires many dedicated hardware	8) in Virtualization, Single dedicated hardware.
9) CC provides unlimited Storage Space	9) Storage space depends on physical server Capacity in Virtualization
10) CC is of 2 types: Public Cloud & Private cloud	10) Virtualization is of 2 type: Hardware & Application Virtualization
11) in CC, Configuration is Image Based	11) in Virtualization, Configuration is template Based
12) Delivers on-demand IT Services over the internet	12) creates virtual versions of hardware, storage or NIW within a Single physical system
13) Uses a NIW of Servers managed by Provides like AWS or Azure	13) Runs virtual machine on a Single physical server with a hypervisor
14) less Cost	14) more Cost.

Q 6) Virtualization Architecture & level ?

→ - Virtualization allows multiple applications or operations to gain Access to the hardware resources / software resources of the host machine.

- Virtualization is a layer bet^n the hardware & the operating system.
& it also provides access transparency

- The hypervisors also known as the VMm (Virtual machine monitor), manages the applications & the operating system in general.

- Hypervisors are hardware virtualization techniques that allow multiple guest operating system (OS) to run on a single host.

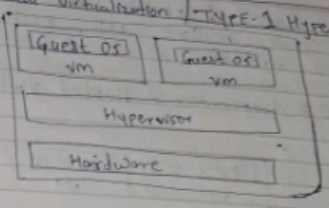
- Virtualization architecture is the setup that enables multiple virtual machines (VM) to run on a single physical machines.
sharing its resources like CPU, memory & storage.

- It uses a layer of software called a hypervisor to manage & control these VM.

- A hypervisor is sometimes also called a Virtual machine manager (VMm)

- There are two types virtualization architecture :
Bare metal Virtualization & Hosted Virtualization

1) Bare Metal Virtualization : TYPE-1 Hypervisor →



- The hypervisor runs directly on the underlying host system.
- It is also known as "Native hypervisor" or "Bare metal Hypervisor".
- It does not required any base server OS
- It has direct access to hardware resources
- Example of Type 1 hypervisor include VMware ESXi & microsoft Hyper-V hypervisor

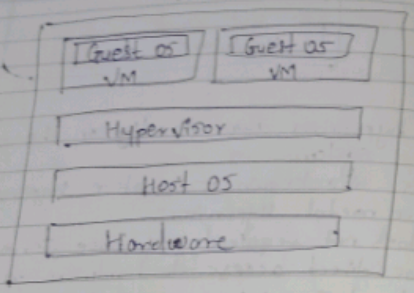
- a) Hardware layer → This is the physical hardware (CPU, memory, storage) of a server or computer.

b) Hypervisor → Also known as a bare metal hypervisor this software site directly on the hardware, not on an operating system.
It Controls & manages the hardware resources & Creates multiple VM.

3) VM → Each VM runs on the hypervisor as if it were a separate Computer
each VM has its own Guest OS, meaning each VM can run diff^n OS (like windows, Linux)

The Type 1 hypervisor diff" uses the hardware to create multiple VMs, each with its own OS & applications.

2) Type 2 hypervisor / Hosted Virtualization →



- A Host operating System runs on the underlying host System.
- It is also known as "Hypervisor".
- Ex; KVM, Microsoft Hyper V, Windows Virtual PC.

- i) Hardware layer → This is the Actual, Physical hardware of the Computer (CPU, memory, storage)

ii) Host OS → This is the primary OS installed on the physical hardware (e.g. windows, Linux) It acts as the main OS running on the Computer

3) Hypervisor → The hypervisor here runs on top of the Host OS like an application

it Creates & manages VM on the Computer.

4) VM → Each VM created by the hypervisor acts like an independent Computer. Each has its own Guest OS (eg. Windows, Linux) running within the VM.

- In this Setup, the Type-2 Hypervisor depends on the Host OS. The hypervisor is installed like any other application on the host OS & allows you to create VMs.
Each VM can have its own OS separate from the host.

3) Level of Virtualization. →

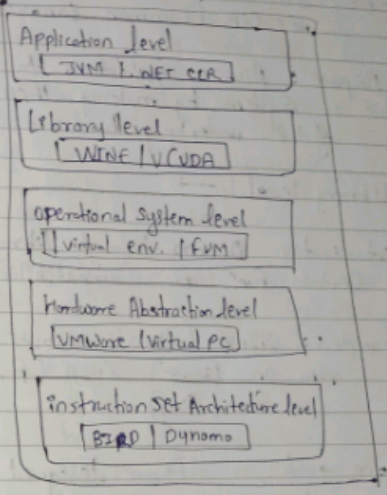


fig: Implementation levels of virtualization

- The diagram shows the level of implementation Virtualizations.
- The diff^n layers at which Virtualization can be implemented.

1) [Application level] →

- Virtualization happens at the application layer
- This type of Virtualization allows applications to run on various OS without needing to modify the software for each OS
- Ex: JVM (Java Virtual Machine) & .NET CLR (Common Language Runtime)
- Purpose: Allows applications to run on any system by making them independent of the underlying hardware & OS

2) [Library level] →

- Virtualization occurs through library that supp~~o~~rt~~s~~ Certain fun^n for Compatibility
- Examples: WINE (allows windows applications to runs on Linux), CUDA (for parallel Computing)
- Purpose → Allows software designed for one env. to work on another by using Compatible library.

3) [OS level] →

- Virtualization at the OS level enables multiple isolated env. on a single OS.
- Example: Virtual env, JVM
- Purpose: Allows applications to run in their isolated space without affecting other parts of the system

4) [Hardware Abstraction level] →

- Virtualization is done closer to the hardware. abstracting hardware resources
- Examples: VMware, Virtual PC
- Purpose: Allows multiple OS to run on the same physical hardware, each as if it were running on its own machine

5) [Instruction set Architecture (ISA) level] →

- Virtualization happens at the instruction level for Compatibility with diff^e Architectures.
- Ex; BIRD, Dynamo
- Purpose: Translates instructions from one architecture to another; allowing software to run across diff^n hardware platforms

- These level represent diff^n ways to Achive Virtualization, from Running Software across diff^t OS env. (application & library level) to running multiple OS instances on the same hardware (hardware & ISA level)

Each level provides flexibility & compatibility at diff^n level layers of the Computing Stack

Q 7) Describe the Components of VM ?

→ A Virtual Machine (VM) is made up of several main Components that allow it to act like a real Computer.

1) Virtual Hardware →

- This is the "Virtual" version of Computer hardware created by the VM Software (or hypervisor)

- Virtual CPU (vCPU) → A Part of the physical CPU that the VM uses to process data
- Virtual Memory (vRAM) → A Portion of the physical RAM dedicated to the VM
- Virtual Storage → A Part of physical storage (like a hard drive) allocated to the VM. where it stores its files, OS & applications
- Virtual NIW interface → This enables the VM to Connect to NIW & Comm^n with other devices.

2) Guest OS →

- This is the OS installed within the VM (like window, linux) it runs independently inside the VM, just like it would on a physical Computer

3) Hypervisor →

- This is the Software layer that manages the VM & allocates the physical resources (CPU, memory, etc) from the host system to the VM.

There are two types:

1) Type 1 Hypervisor → (Bare-metal): Run directly on the physical hardware
2) Type 2 Hypervisor → (Hosted): Runs on top of a Host OS

4) VM Configuration file →

- This file stores all the settings for the VM, such as how much memory, CPU & storage it should use.

5) VM disk image →

- This is a virtual Copy of the VM's storage, including its OS, applications & data.

Q) 8) Write a short note on:

1) CPU Virtualization →

- It is a way to share a single physical CPU with multiple VMs.
- It lets each VM act like it has its own CPU.

•) Virtual CPU (vCPU):

Each VM gets a part of the real CPU called a virtual CPU, which it uses to do its tasks.

2) Hypervisor → A software called a hypervisor controls how much CPU time each VM gets, making it feel like each VM has its own processor.

3) efficient use → This sharing ~~called a hypervisor~~ controls helps makes better use of the CPU, allowing multiple VMs to run on one computer.

- CPU virtualization lets one CPU work for many VMs so they can all run smoothly on the same machine.

2) Memory Virtualization →

- Memory virtualization allows multiple VM to share the same physical memory (RAM) as if each VM has its own dedicated memory.

•) Virtual Memory → each VM is given a "virtual" memory space that feels like its own, even though they share the same real memory.

2) Hypervisor Control → A special software called a hypervisor, manages the memory, giving each VM a part of it & adjusting as needed.

3) Better Use → This allows many VMs to run on one machine without needing separate RAM for each.

- Memory virtualization makes one memory source work for many VMs, so they all the have enough to run.

3) Desktop Virtualization →

- Desktop virtualization allows users to access their desktop (like windows or mac) from any devices, like a laptop, tablet or phone.

•) Virtual Desktop: instead of being on one computer the desktop is stored on a server

or in the cloud.

c) Access Anywhere: Users can open their desktop from anywhere & find everything just as they left it.

d) Easy management: IT teams can updates & protect all desktops from one place.

- Desktop Virtualization allows you to use your desktop from any devices, making remote work easy & secure.

4 Unit

4).

Q.) Explain in detail Design principle of CDA ?

→

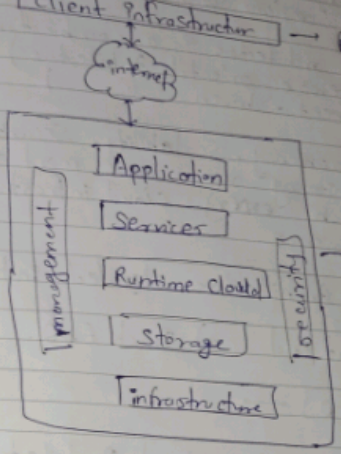


fig: Architecture of cloud computing

- CC, which is one of the most demanding technology of the current time. & which is giving a new shap to every organization. by providing on demand virtualized Servers.

- Starting from Small to medium, & medium to large every organization use CC. Services for storing info & accessing it anywhere & anytime only with the help of internet

- [The cloud Computing used both small & large organization to stored the info & access anywhere & anytime with the help of internet connection]

- CC architecture is a Combination of SOA (service-oriented Architecture) & EDA (event-driven ")

- Transparency, Scalability, Security & intelligent Monitoring are some most imp constraint which every cloud infrastructure should experience

- CC Architecture divided into 2 parts →

1) front end 2) Back End.

1) [Front End] →

FrontEnd of the Cloud Architecture refers to the client side of the cloud Computing System.
It includes all the user interfaces & applications which are use the by the client to access cloud services or resources

- for ex, using web brower like (chrome) or firefox to access a cloud platform. is a part of front end.
It provides tools & interfaces that let users interact with the cloud system easily.

- The front end include web services (like chrome, Firefox, internet explorer etc), thin & fat client, tablets & mobile devices

- client infrastructure - client infrastructure is a part of the front end Component

- In other words, it provides a GUI (Graphical user interface) to interact with cloud.

2) [BackEnd] →

- The Backend refers to the cloud System Managed by the Service provider.
It includes all the Resources needed to run & manage cloud Services.

- It handles Resource management, Security, data Storage, Virtual Machines, virtual Applications, traffic management & diff deployment models.

- It is responsible for storing data, running applications, & ensuring that everything works properly.

• Application →

+ Application in Backend refers to a software or hardware Platform to which client access it provides services to clients based on their needs (requirement).

- Services →

Services in Backend refers to the major 3 types of cloud based services like SAAS, PaaS, IaaS. Also manages which type of services the user access

- Runtime Cloud →

Runtime Cloud in Backend provides the execution & Runtime platform/env to the Virtual Machine.

- Storage →

Storage in Backend provides flexible & scalable storage, service & Management of stored data.

- Infrastructure →

Cloud infrastructure in Backend refers to the hardware & software components of cloud like including servers, storage, NW devices, virtualization software etc.

- Management →

Management in Backend refers to the managem of Backent components like application, servi runtime cloud, storage, infrastructure & other security mechanisms, etc.

- Security →

Security in Backend refers to the implementation of diffn security mechanisms. in the Backend for secure cloud resources, system, file & infrastructure to the end-user

- Internet →

Internet connections acts as the medium or bridge betn front end & backend & establishes the interaction & commn betn frontend & backend.

- Benefits of Cloud Computing Architecture:

1) make overall CC system simpler
2) improves data processing requirements
3) Helps in providing high security
4) Makes it more modularized
5) Gives good user accessibility
6) result in better disaster recovery.
7) reduces IT operating costs

Q2) Why we need CC Solutions?

→ By using CC solutions, we get various Benifits, some of which are as follows

- Improved Software & Hardware performance :

Through the CC solutions one can easily make out what will be the best Software & hardware specification for the Better Performance of the application running on the cloud.

- Flexibility & affordability →

CC gives users many options to choose from, allowing them to pick the Best Services for their application.

Cloud services more affordable Compared to the other options.

- ~~Increasing~~ :

- Increased UpTime & Availability :

- CC is highly available & has excellent uptime, which helps handle more traffic at the same time.

- Better Collaboration with Real time :

CC allows easy real time sharing; Making it easier to collaborate with others.

(13) Draw & explain cloud Computing life cycle.

- CC Architecture ~~DIG~~.

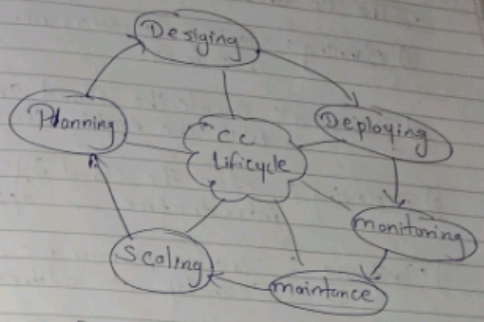


fig: CC lifecycle

- CC is the Booming industry of the Present time & will Continue to grow by many folds in the futures.

- Nowadays, its really hard to find a safe, secure & yet cost-effective place to store your data & Business critical ideas.
But with the growth of CC, this Problem is Vanishing exponentially.

- cloud provides us with a place where your data can not be only stored but can also be acce easily over the internet.

Using cc you can also host & Manage your applications.

- The cc lifecyle consists 6 stages →

1) Planning : Identify Business needs & required resources

2) Designing : Create the Cloud architecture with the Right Services & tools

3) Deploying : setup the cloud System, including Infrastructure & applications

4) Monitoring : Track performance, Usage & Security to address issues

5) Scaling : Adjust Resources Based on demand

6) Maintenance : Keep the System running Smoothly with updates & fixes.

- Life Cycle of cc Solution →

To create such Cloud platform, it takes a long number of steps & dedicated time. Let now look at the steps involves of the life cycle of cc solutions.

Step 1 : Define the purpose :

The first & most imp step is to Define the Purpose for which you want to create a Cloud.

For this, you have to first understand your Business requirement & what type of application you want to run on the cloud.

After this, you have to decide whether you want your cloud to be Public, Private or hybrid.

Step : 2 : Define the Hardware

Deciding what type of hardware you will need. & most imp part.

You need to Decide which type of hardware & Computing Services will support your cloud & help your application run smothly.

Step 3 : Define the Storage

every application needs a good amount of data storage. where its data can be stored safely.

choose a Storage Service that Allows you to safely Backup & Archive your data online

Step 4 : Define the Network

Networking is the key that will be deliver your data to the End-users.

So, the Network must be well-configured, Secure & fast to ensure data, Video & apps are delivered efficiently without Security issues

Step 5 : Define Security

Security is the key aspect of any Application. set up security measures like user Authentication & limit access to Specific users to keep your resources safe

Step 6 : Define the Management Process & Tools

The developer should have Complete Control over there resources & Applications on the Cloud.
These management tools allow you to Control & Configure your cloud evn.

Step 7 : Testing the Process

Testing is the another imp thing in the lifecycle of deploying any applications.

All the faults are figure out only through the testing Process involved in it.

During testing, you should verify your application using various developer tools. Where you build, test & deploy your code quickly

Step 8 : Analysis

Finally, in this step, you analyse & visualize your data using Analytics tools.

You can quickly query data & get instant results

once the analysis is Complete, your application is ready to be deployed

Advantage →

1) Cost Saving
2) High Speed
3) Backup & restore of data
4) Reliability

Disadvantage →

1) downtime
2) Performance Can Vary.

Q(4) What is Service-oriented Architecture (SOA)

→

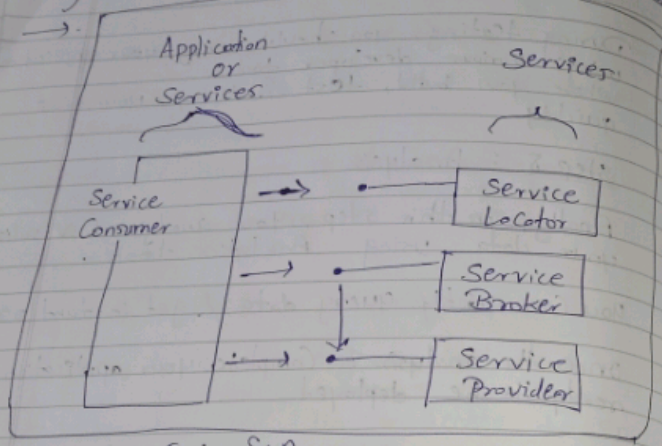


Fig: SOA.

- A Service oriented Architecture or SOA is a design pattern which is used to designed Build distributed system that delivers services to other applications through the protocol.
It is only a concept & not limited to any Programming language or platform.

- A Service is a well-defined, self Contained Fun^n that represents a unit of functionality.

- There are 2 major ~~Components~~ roles within SOA →

1) Service Provider : The Service Provider is the organization that Create & manage the services. They make the available one or more services for others to use.
They can publish details about it in a registry, including how to use the service, its requirements & any fees involved.

2) Service Consumer :

The Service Consumer is the user or Application that finds the service in the Registry & creates the necessary Components to use it.

[It can be called as a requestor or client that ~~called~~ calls a Service provider.
A Service Consumer can be another Service or an end user application].

Other roles are :

1) Services : The Services are the logical entities defined by one or more published interfaces.

2) Service locator :

It is a Service Provider that acts as a registry. It is responsible for examining Services Provider interfaces & Service locations.

3) Service Broker :

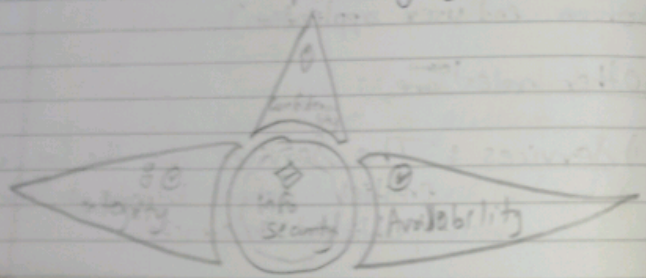
It is a Service provider that pass service requests to one or more additional Service providers

- Characteristics of SOA →

1) They are loosely Coupled
2) They support Interoperability
3) They are location transparent
4) They are Self Contained

5) What is Cloud Security ?

→ Cloud CIA model
(Confidentiality, Integrity & Availability)



Confidentiality, Integrity & availability also known as the CIA triad, is a model designed to guide policies for information security within an organization.

- In this context, Confidentiality is a set of rules that limits access to information.
Integrity is the assurance that the info is trustworthy & Accurate, &
Availability is a guarante of Reliable Confidentiality, Integrity, Availability.

1) Confidentiality →

It means protecting Sensitive ~~data~~ info from Unauthorized Access
sometimes, people who handles sensitive data need Special training to Understand risks & how to protect against them.

This training can include:

- Creating Strong Passwords & following best practices for using them.
- learning about techniques, like Social Engineering, which trick people into breaking data Security rules
So they can avoid making mistakes even with good intentions

[Understanding the Social engineering helps prevent Mistakes that Compromise data Security]

- A good example of methods used to ensure Confidentiality is required for transit channels or traveling data when Banking online.

- Data encryption is another common method of ensuring Confidentiality & another standard method is two-factor authentication (2FA), which adds an extra layer of security.

* Key Aspects :

1) Data Encryption → Encrypts data when stored (at rest) & during transfer (en route) to prevent unauthorized Access without a decryption key.

~~2)~~ (Protects data from Unauthorized access)

2) Access Control → Limits Access to Authorized User only

3) Secure Comm^{n} → Uses protocol like HTTP, SSL/TLS, & VPN to keep data private & securing during transmission.

2) Integrity →

- These measures includes file permissions & Access Controls.

- In Cloud security, Integrity ensures that data is accurate, consistent & has not been altered or tempered with without Authorizations.

It ensures the information stays Correct throughout its use, whether its stored, Processed or transmitted.

* Key Assep Aspects :

1) Hashing fun^{n} → Data is processed to create a unique fingerprint. If the data is modified, the hash value changes.

2) Access Control → Restricts who Can edit data to prevent unauthorized changes

[limits who Can edit data to prevent unauthorized changes]

- By ensuring integrity Organization maintain trust in their data, preventing errors fraud alterations.

c) Availability →

Availability ensures that data, applications & services are Accessible to authorized users whenever needed, without interruption.

It focuses on minimizing downtime & ensuring reliability in delivering resources

Key Aspects :

1) Redundancy & Replication →

Ensures continuous service by using backup systems.

2) Scalability → Adjusts resources to meet growing demand without performance loss.

6) Explain Cloud Computing Security Architecture

→ CC Security Architecture refers to the designs framework & components used to ensure the protection of data, applications & infrastructure within a CC env.

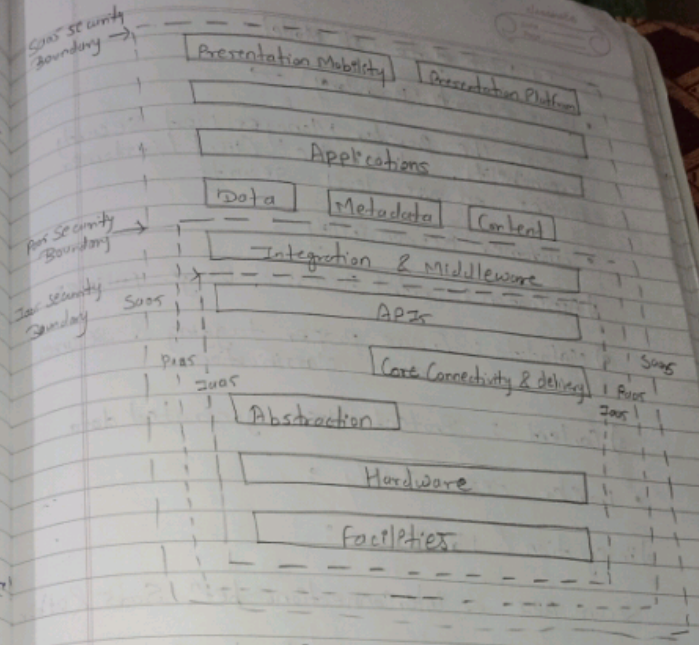


fig : CC Security Architecture

Key Points to CSP Model :

- **Saas Security Boundary** →

In Saas, the Provider Manages Most Security responsibility, while the Client / Customer focuses on user-level security

- Customer Responsibility :

1) Application : Control Access & Usage Policies

2) Metadata : Ensure proper tagging & secure data classification

3) Content : Protect User-generated data

- Provider Responsibility :

1) Integration & Middleware :

Secure API & InterConnections bet^n Saas & other

2) APIs : Provide Secure endpoints for application Integration

3) Core Connectivity & delivery :

ensure Secure data transmission & availability.

- **Paas Security Boundary** →

In Paas, the provider manages the Platform while Customers is Responsible for Building & Security applications

- Customer Responsibility →

1) Applications : Secure Custom developed apps hosted on the platform.

2) Integration : Manage API calls & third-Party service Connections.

3) Data : ensure Proper encryption & secure access.

- Provider Responsibility →

1) Platform middleware :

Secure frome works, Runtime env. & API.

2) Connectivity & Delivery :

ensure Secure Comm^n & Scalability.

• Iaas Security Boundary →

In Iaas, the provider offer hardware & Virtualization, while the customer manages operating system (os), application & data

Customer Responsibility →

1) Application & Data :

Install, secure & Maintain Software & data

2) Middleware :

Configure & Secure any additional layer like databases

3) Operating System :

Ensure Patches, updates & Configurations

• Provider Responsibility →

1) Abstraction : Manage hypervisors & resource allocations

2) Hardware & Facilities : Provide Secure physical infrastructure & Nlw

7. 2) What are the security issues in cloud service providers ?

1) Denial of Sevice (DoS) & Distributed Denial of Service (DDoS) Attacks :

These Attacks try to Block Access to internet services for legitimate users, disrupting Service.

2) Excessive Traffic & Resource Depletion :

Infected machines, overload systems, causing issues.

3) BGP Routing Attacks :

Redirect traffic to steal data

4) DNS Info Misuse :

Criminals Sometimes use DNS to Redirect traffic to Malicious sites for their Benefit

5) Device Compromise :

Attackers Can Break into Critical Infrastructure Components & change their settings, leading to Vulnerabilities

6) Size of the Nlw :

Large Nlw Make Security Implementation h

7) Higher Number of targets & Entry Points :

more targets for attacks increase risk

8) Defending Multiple Targets :

Service providers must be Able to protect many diff^n targets from Multiple Attacks at the Same time

9) Securing Transit paths :

Services providers must secure the Infrastructure Carrying data, not Just the Access points.

Q 8) What are Security issues in CC ?

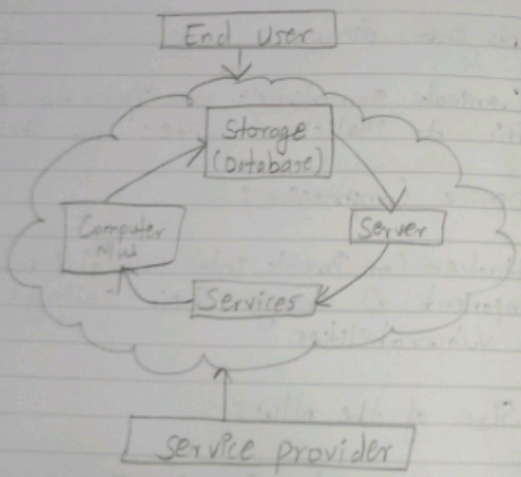


Fig: Cloud security issues

- CC is a type of technology that provides remote services on the internet to manage, access & store data Rather than storing it on servers or local drives.

This technology is also known as serverless technology. Here the data can be anything like Image, Audio, Video, documents, files etc.

- There is no doubt that Cloud Computing provides various Advantage but there are also some security issues in cloud Computing.

Below are Some following Security issues in issues in CC as follow :

1) Data loss :

Data loss is one of the issues faced in Cloud Computing. This is also known as data leakage.

As we known that our sensitive data is in the hands of somebody else, & we don't have full Control over our database.

So, if the Security of the cloud service is to Break by hackers then it may be possible that hackers will get access to our sensitive data or personal data.

2) Interference of Hackers & insecure API's :

As we know if we are talking about the cloud & its services it means we are talking about the Internet.
Also we know that the easiest way to communicate with cloud is using API. So it is important to protect the interfaces & API which are used by an external user.

But also, In cc, few services are available in the Public Domain.
And is the vulnerable part of cc. because it may be possible that these services are accessed by some Third parties.
So, it may be possible that with the help of these services hackers can easily hack everything.

3) User Account Hijacking :

Account Hijacking is the most serious security issue in cc.
If somehow the Account of User or an Organization is Hijacked by Hacker.
Then the Hacker has full authority to perform Unauthorized Activities.

4) Changing Service provider →

"Vendor lock" in is also an imp security issue in cc.

Many organizations will face diff^n problems while shifting from one vendor to another vendor.
For Example, An Organization wants to shift from AWS Cloud to Google cloud services then they are various problems like shifting of all data, also both cloud services have diff^n techniques & fun^, so they also face problems regarding that.
Also it may be possible that the charges of AWS are diff^n from Google Cloud, etc

5) Lack of Skill →

while Working. Shifting on another Service Provider, need an extra feature, how to use a feature, etc.
are the Main problem caused in IT Company who doesn't have skilled Employee. So it requires a skilled person to work with cc.

6) Denial of Service (DoS) Attack →

This type of Attack occurs when the system receives to Much traffic.
Mostly DoS attacks ocurrs in large Organizations such as the Banking sector, government Sector, etc. When a DoS attack occurs, data is lost.

So in order to recover the data. It required a great amount of Money as well as time to handle it

Q 7) Explain Host Security ?

→ - Host security describes how your Server is Setup for the following tasks:

1) Preventing Attacks
2) Minimizing the impact of a successful Attack on the overall System
3) Responding to Attacks when they occurs
4) updating software with security patches

- Defination :

Host security refers to the Method & Practices used to protect a Computer System (Server/Host) from unauthorized Access, Attacks & Vulnerability.
It ensures that the System operates securely while Minimizing Risks.

- Example : A Bank's Server Handles Customer data.

- Prevention : A firewall & antivirus protect against unauthorized access
- Minimizing impact : Strick user permissions limit damage to one service.
- Response : The IT team applies updates to fix vulnerabilities quickly.

Conclusion :

Host Security is essential to Maintain the integrity & Reliability of any System by minimizing risks & ensuring prompt responses to potential threats.

- on the cloud, Rolling out a Patch Across the infrastructure takes 3 steps simples:

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

Q 8) Explain Data Security ?

→ - Data, a word which is now spoken everyday & ~~every~~ everytime one or other way.

People in Corporate throughout the day with Small Scale figures keeping in find that our Company data should not be leaked by any chance or by any external force but they haven't thought of their data being in-secured.

Why our data is not Secured ?...

We feel free while using Apps especially social Media apps like facebook, whatsApp which is not normal because we logins on diff devices which is not a favorable Condition in terms of our Personal data

& also if the People linked through it

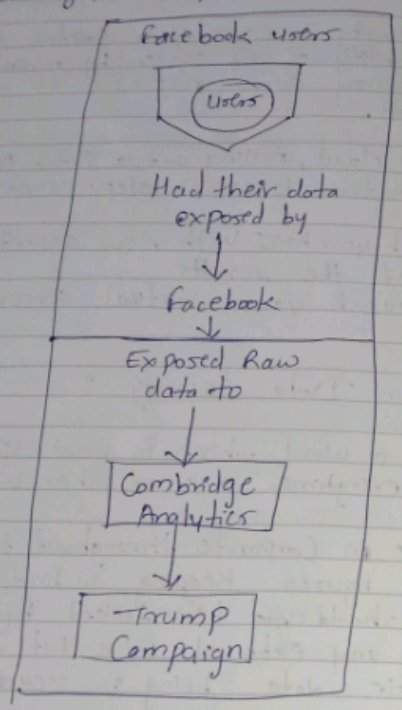


Fig: Flowchart of Data Seamty

• How data will be Secured ?

1) use firewalls
2) use encrypted systems
3) use VPN
4) never give authorization to external Parties
5) use strong Password & change them often
6) public Nlw should be Avoided as much as we Can like wifi on metros, airports.
7) Do make trust issues while logging in another devices

• Types of Data Security :

1) Access Controls :

Limiting who Can enter or Access important system & spaces to only authorized people

2) Authentication :

Verifying users before they can access data, using methods like passwords or fingerprints.

3) Backup & Recovery :

Keeping Backup Copies of data in Safe places (like disks or the cloud) so you Can recover it if Something goes wrong.

4) Data Erasure :

Permanently deleting data to prevent unauthorized recovery.

5) Data Masking :

obscuring sensitive data with random characters to keep it safe from unauthorized Access

6) Data Resiliency. :

ensuring systems can recovers from failures without compromising security.

9) Encryption :

A Computer algorithm transformation text characters into an unreadable format via encryption keys

9) Explain firewall ?

→

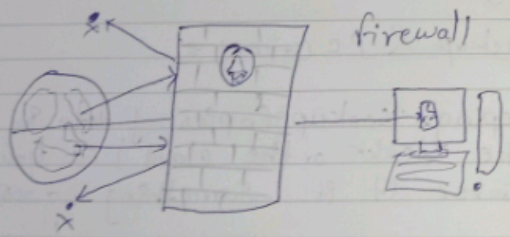
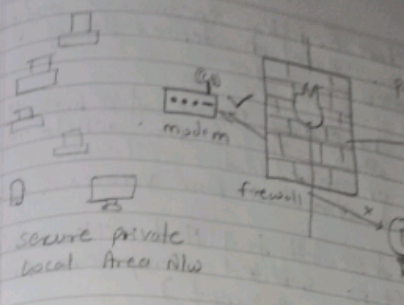


fig: Firewall Architecture



- ✓ = Specified Traffic Allowed
- ✗ = Restricted unknow Traffic

fig: Firewall working

- Nowadays, it is a big challenge to protect our sensitive data from unwanted & unauthorized sources.
- There are various tool & devices that can be provides diffn security level & help keep our private data secure.
- one such tool is "Firewall" that provides unauthorized access & keep our Computer & data safe & secure.
- A firewall can be defined as a special type of Nlw security device or software program.

that Monitors & filters incoming & outgoing nlw traffic. Based on defined set of security rules.

- Purpose: The primary purpose of a firewall is to allow safe traffic while Blocking harmful or unwanted data.
- To protect Computers from Viruses & Attacks.
- It is a Cyber Security tool that filters nlw Traffic & Stops infected Computers from Connecting to the Internet)
- [This is one of the most Problematic questions Whether a firewall is a Hardware or Software
- (As stated above, a firewall can be a nlw Security device or Software program.
- This means that firewall comes at both level, i.e hardware & Software.
- each format (a firewall implemented as a Hardware or Software) has Diff^n functionality but same purpose.
- In the Hardware firewall: is a Physical devices that attaches Bet^n Computer nlw & gateway for example, a Broadband Router.

In the Software is a Simple Program installed on Computer.

Apart from that, there are Cloud based firewall they are Commonly referred to as Firewall as a Services)

Why we need a firewall?

- A firewall protects your Computer & nlw from harmful Attacks & unauthorized Access
- It checks all the data entering your system & only allows the trusted Sources
- ~~what~~ the Some of the imp Risks of without using firware:

1) Open Access → Anyone can Access your devices without permissions
2) Data loss → Hackers can steal or Delete your personal data
3) Nlw Problems → Attackers can shut down your nlw & Causing delay & extra costs

Therefore, it is imp to use firewware & keep our nlw, Computer & data Safe from unwanted Sources.

Imp ◦ fun^n of firewall →

- The Main fun^n of firewall is to protect your Nlw & Info. by Controlling incomming traffic, Blocking unwanted traffic & checking data for harmful things like Hackers & malware

- Most operating System (like windows) & security Software already include Built-in Firwall support

- Firewalls are Now very Powerful & have many features, including:

1) Nlw Threat prevention
2) Application & identity - Based Control
3) Hybrid Cloud Support
4) Scalable Performance
5) Network Traffic Management
6) Access validation
7) event logging & Reporting

Imp ◦ Type of firewall →

1) Proxy firewall
2) Cloud firewall
3) Packet filtering firewall
4) Stateful Multi layer Inspection (SMLI) firewall
5) Unified threat management (UTM) ,,
6) Next-generation firewall ,,
7) Nlw address translation (NAT) firewall ,,
8) Application level Gateway ,,
9) Circuit ,, ,,

Unit 5

=>

1) Explain diff^n Services Provided by Google cloud Platform ?

1) [Google App engine] →

[Google app engine (GAE) is a Paas cloud computing platform for developing & hosting web applications in google managed data centers

- It is the way to write your own web Application & have them hosted on google servers]

- Google cloud Provide 2 env to use App engine one is Standard evn with Constrained env. & Supports for language Python, Go, Node.JS

second is the Flexible env allows Custom runtimes, extended timeouts, Custom software & SSH access

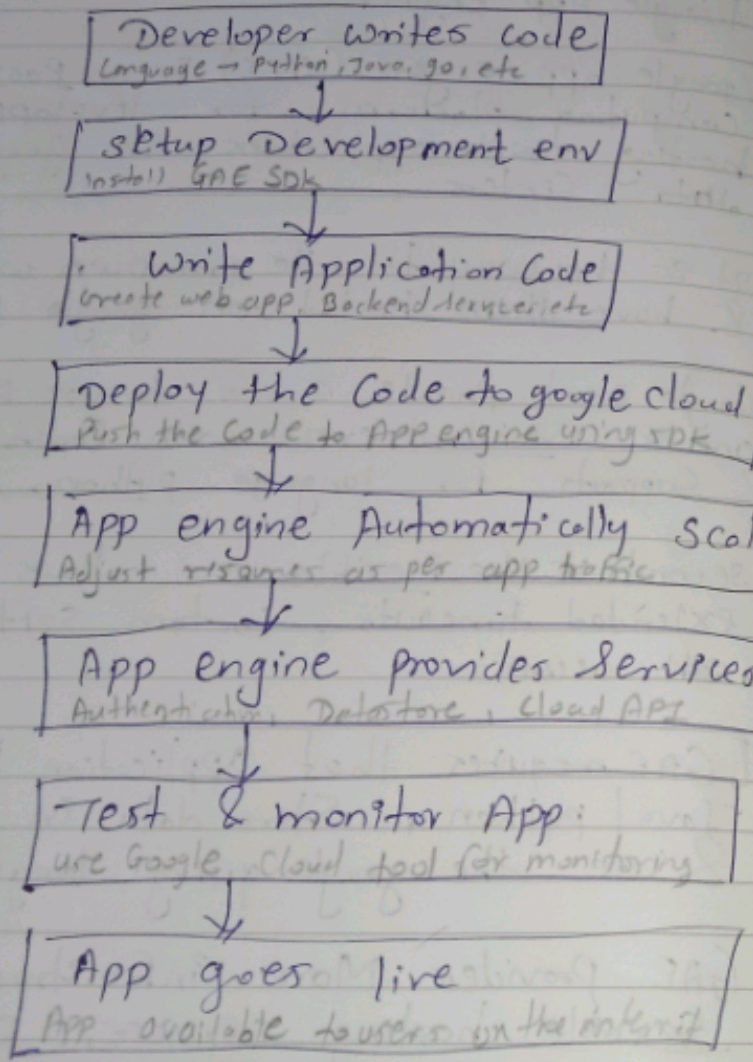
- [GAE requires that application be written in Java / python, Store data in google BigTable & use the google query language]

- GAE Provides More infrastructure than other Scalable hosting services, such as Amazon EC2.

- Users Can create GAE account, setup Software development kit & write application Code.

- then use GAE to test & deploy the code in cloud.

- Simple Flowchart of GAE →



- Feature of GAE →

1) Automatic Scaling : Scales your appl° Based on demand
2) Managed infrastructure : No Need to manage Servers or Hardware
3) Multi-language Support : Python, Java, Go, Node.Js, PHP, etc.
4) Seamless Google Cloud integration
5) Automatic load Balancing
6) Buit in Security
7) Real time Monitoring & logging
8) Flexible env.
9) cost efficiency
10) easy Deployment

a) Amazon Web Services (AWS) →

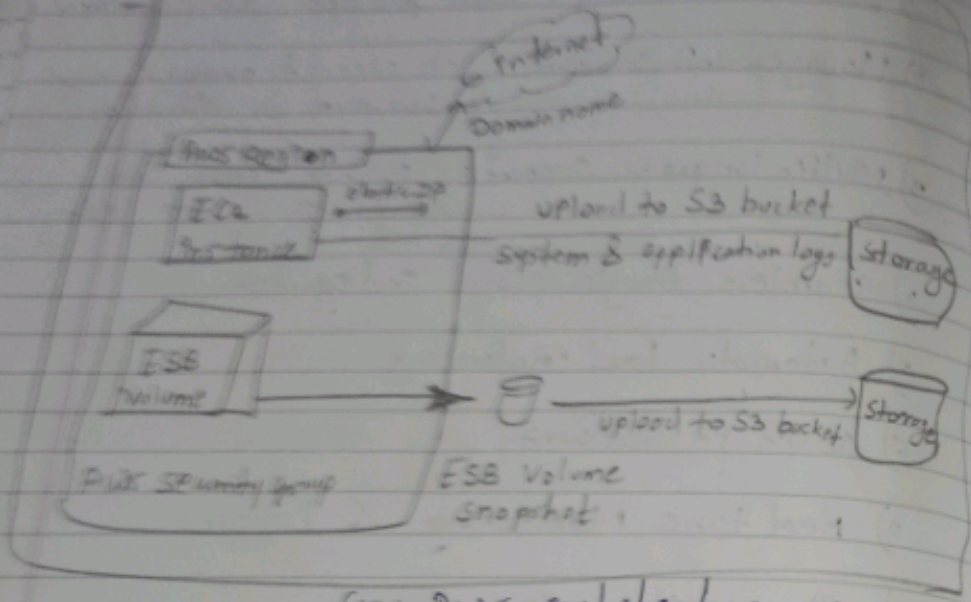


Fig: AWS architecture

- The diagram shows a Basic AWS Architecture as shown in fig.
- Core Components →

1) EC2 instance : This is like a virtual Computer running in the cloud. It hosts your application or website

2) EBS Volume : This is like hard drive attached to the EC2 instance. Used to store data

3) S3 Bucket : This is cloud storage for backup & other files

- Networking →

1) Elastic IP : A static IP address for your EC2 instance. If it restarted

2) Security Group : A firewall that Controls allow traffic to your instance

- Database →

1) ~~Cpnam~~ Domain Name : A alo SSL database for fast Access

- How it work →

Users access the application
↓
requests go to EC2
↓
Data is stored on EBS & Backup to S3.
↓
Dynamo DS.

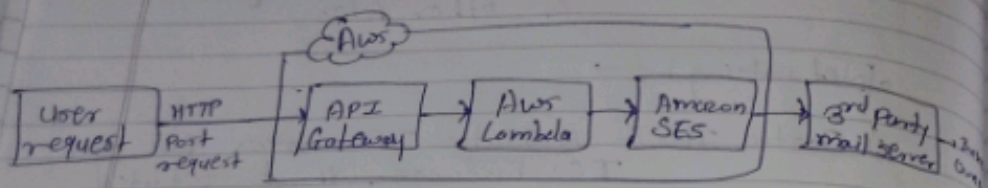
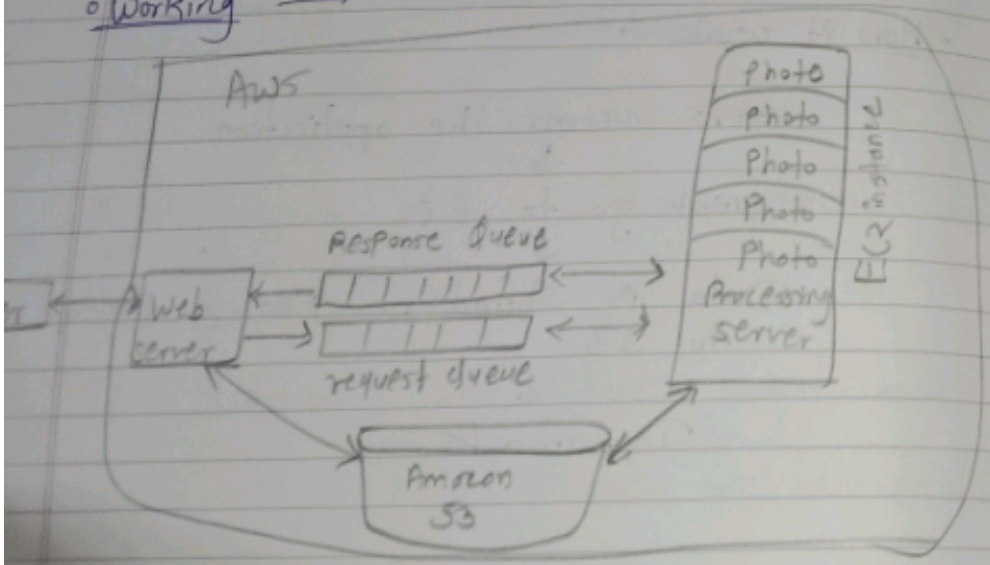


fig: Block Diagram of AWS (Architecture)

- AWS Consists of many cloud Services that Can you use in Combination with Business & ~~ob~~ organizational needs

- Working →



- Amazon Web Services (AWS) is a cc platform from Amazon that Provides Customers with wide range of cloud services

- It is Provides diff^n Services such as Iaas, Paas, & Saas.

- features of AWS →

1) Flexibility
2) Cost-effective
3) Scalable & elastic
4) secure

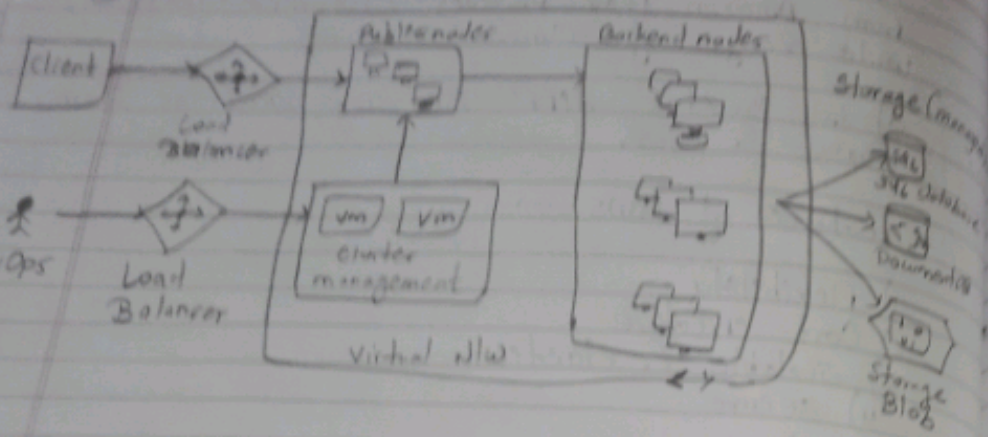
- Advantage →

1) AWS allows organization to use already familier programming models, OS, databases, etc

2) It is Cost effective Services

3) you don't requires money for running & Maintaing data centers

3) Microsoft Azure →



- (Microsoft Windows Azure is Cloud OS Built on top of Microsoft data centers Infrastructure
- It supports Computing, Storage & Networking to application connectivity, etc
- It provides developers with Collection of Services for building applications with Cloud Technology)

[Microsoft Azure is a cloud Computing platform create by Microsoft.
It provides a wide range of Services to host existing applications, develop new one more easily, & impore On-premises applications.

Azure helps organizations to Build, test, deploy & Manage application & Services using Microsoft data Centers.
eto need for physical infrastructure)

It is Faster & easier development of Solutions
Azure helps developers learn key services, Prepare for Job Interviews & earn Certification
Making powerful tool for Building cloud Based solutions

- Azure Services →

1) [Compute Services] :

for Processing data on the cloud using virtual Machine (VM), Websites, Mobile services, etc

2) [Data Services] :

for Storing & Scaling data with tools like Azure Storage, SQL Database & Redis cache

3) [Application Services] :

for Building & Managing apps using Active Directory, Service Bus, Scheduler & Media Services

4) [NW Services] :

- for Connecting cloud system with virtual NW
CDN & Traffic Manager.
- Connecting Private & public NW

5) Storage →

flexible cloud storage for file, database & Backups

6) Mobile app →

Build & Deploy mobile apps using AI & Cognitive tools

6) Databases →

options for MySQL & more.

- Azure Makes Complex technology Accessible & Scalable on demand.
- Wide range services it provides over 100 Services, including Computing Power, Storage, Networking & AI Tools, to meet diff needs
- Azure helps Business reduce Cost & Complexity by offering Scalable Solutions, meaning you only pay for what you use.

5) Describe the steps involved in Create an EC2 instance ?

→ Step 1 : Signup for AWS

Create an AWS Account to Access all services including Amazon EC2.

Step 2 : Create an IAM user

Setup a user with permissions to Access AWS resources, instead of using your root Account

Step 3 : Create a key pair

Use public key cryptography for secure login to your EC2 instance.

step 4 : Create a Virtual Private Cloud (VPC)

setup a Private Nw for your AWS resources

Step 5 : Create a Security group

setup rules for Controlling the inbound & outbound Traffic for your EC2 instance

6) Launch an EC2 instance : step 6

Use the AWS Management Console to launch a new VM

7) Step 7 : Connect to the Instance

Access the Instance using SSH (for linux) or RDP (for window).

8) cleanup the instance : Step 8

Terminate the instance one you're done to ~~stop~~ Stop incurring charges.

Q3) Describe Amazon EC2 Cloud following Points:

1) Amazon Machine Image →

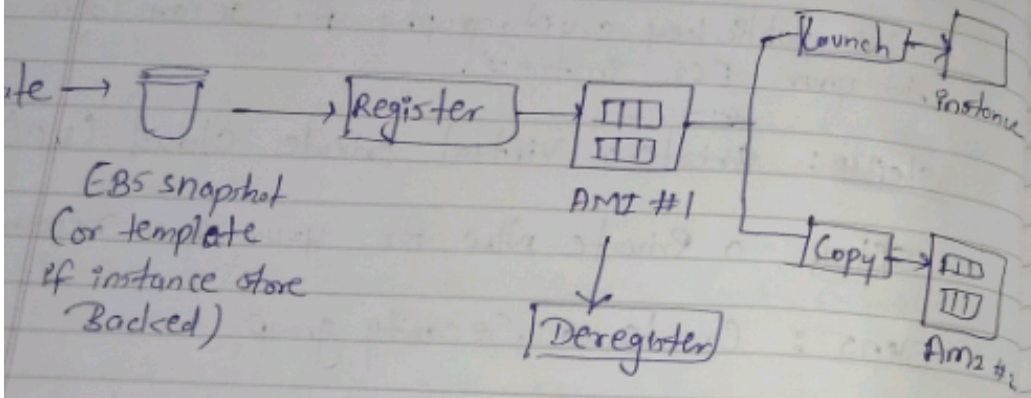


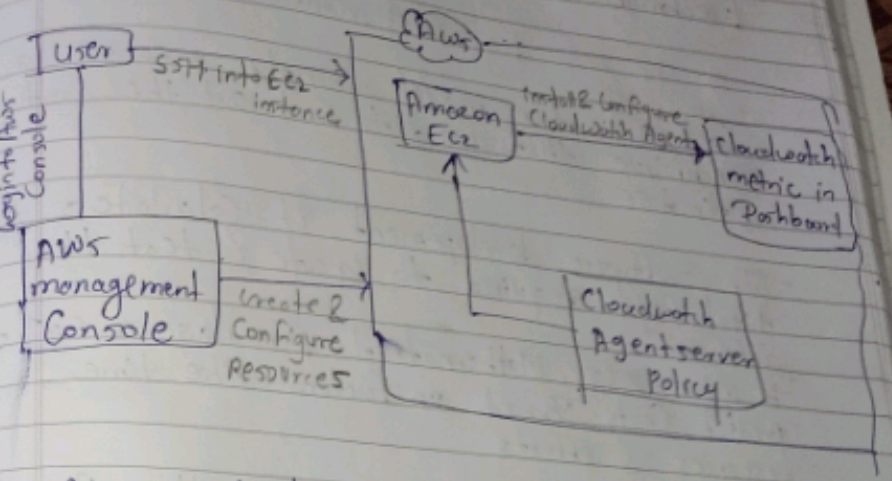
fig: AMI.

An AMI is a template used to Create VM. (EC2 instances) on Aws.

Contains the OS, Software & Configurations needed to run your application.

- Think of it as a Snapshot or Blueprint of your system setup.
- you can Create your own AMI or use Pre-Configurable once provided by Aws.

2) Amazon CloudWatch →



- Amazon Cloudwatch is a Monitoring Services that helps you track the performace & health of your EC2 instance & other Aws resources.

It Collects & Provides data on metrics like CPU usages, Memory, disk activity, & Nlw traffic.

You can Set alarms to get notifications, If any certain thresholds are reached. ensuring your system run smoothly & efficie

Q 6) Explain Diff Cost Model in CC ?

→

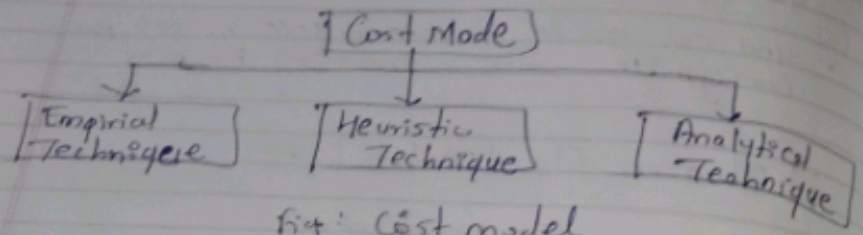


fig: Cost model

- Cost estimation model simply means Technique that used to find out the Cost estimates.

- In Software developement, it Calculates the total Cost required to create & test the Software
it often uses Mathematical formulas or eq" to predict Costs Based on factors like time, resources & efforts

It is helps plan the Budget for the Project

- (Cost model are method used to predicts the Cost of software projects)

- Types of Cost Model →

1) Empirical Technique →

- Uses past data & experience to Predicts the project costs

- Based on the reduction guesses, Assumptions, & the size of the software.
- Examples: Delphi Technique (group discussions to reach a Consensus) & Expert Judgement (relaying on experienced individuals)
- It is Simple & Practical but relies heavily on past data & expertise.
- (It uses Past project knowledge & logical asumptions to predict costs)

2) Heuristic Technique →

- The Heuristic Technique is a Methode used for solving problems or Making decisions quickly & practically.
- The word "heuristic" Comes from a Greek word meaning "to discover".
- it uses shortcuts & approximate Calculations to Make decisions, especially when dealing with Complex data.
- This Method helps to achive goals but may not always give the best results.
- A popular example of this Technique is the Constructive Cost model (Cocomo).

which is used to help analyzing & speeding up decisions about Costs & investments.

3) [Analytical Technique] →

- The Analytical Technique is a Method used to calculate the effort or Cost of a task by breaking it down into Smaller parts :

(i) The task is divided into Basic Components or Steps

(ii) If standard time predicts are Available from Previous Sources, they are Applied to each part.

(iii) If no standard times exist, the work is Predicts Based on past experience.

- This Technique is Based on logical & Scientific principles, often making certain asumptions about the project.

An examples of this is Halstead's Software Science,
Which uses formulas to analyze software metrics

[Analytical estimation Breaks work into smaller pieces, uses past data or logical asumptions to calculate effort, & has a Scientific approach]

(13) Explain steps to Create & manage associated objects for the Amazon S3 Bucket ?

→ Step1 : Create An S3 Bucket

- Open the AWS Management Console & go to the S3 Service.
- click on "Create Bucket"
- Use the AWS Console to create a uniquely named Bucket. choose a region, & set permissions.

Step 2 : Upload objects (files)

- Select the Bucket, Click "Upload", and add files with optional settings like permissions.

Step 3 : Set permissions for objects

- Control file Access using Bucket or ACL policies

Step 4 : Organize files with folders

Create folders inside the Bucket to keep files Organized

Step 5 : Enable Versioning

Turn on versioning to track & recover previous file versions.

Step 6 : Apply Lifecycle Rules

Step 7 : Monitor & Track usage

use cloudwatch & S3 metrics to track storage & costs

Step 8 : Delete file / Bucket

Remove unwanted files & empty the Bucket before deleting it

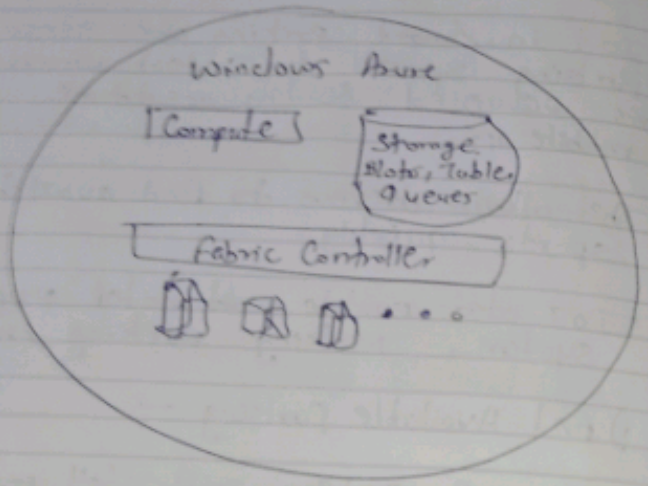
Q1) Diff^n bet^n Google cloud platform & Aws ?

→

Parameter	GCP	AWS
1) Full form	google cloud platform	Amazon web Services
Company	google	Amazon
Computing	Compute engine, App engine	EC2, elastic Beanstalk, Aws lambda
tabase	Cloud SQL, Bigtable (NoSQL), Datastore	RDS, DynamoDB, (NoSql), SimpleDB
rage	cloud Storage, Persistent Disk.	S3, elastic Block Store.
ing	Virtual Private Cloud, Cloud load Balancing	Amazon VPC, Root 53, Direct Connect
	more frequent than Aws	Less

used by	Spotify, Coca-cola, Snapchat, HSBC	Netflix, Facebook, Twitch
Market leadership	Newer but growing fast. Backed by google's expertise on ML & data analytics	oldest & largest cloud Provider with a wide range of services

(1) Windows Azure Platform ?



*RPC (Remote Procedure Call)
*) RMI (Remote method invocation)

Unit : 6

6.

(1) Diff^n

	Cloud Computing	Distributed Computing
Definition	Cloud Computing is a way to use Computing Services (like Storage, Servers & Software) over the Internet. It Combines various ressources like hardware, software & internet tools into one system. Accessible through the n/w like the Internet	Distributed Computing is a field of CS that studies distributed systems. A distributed system is a system whose components are located on different networked computers, which communicate & coordinate their actions by passing messages to one another. CC uses this Concept with virtualization to provide shared resources over the Internet
Goals	• Reduced Initial Investment & Proportional Costs • Increased Scalability • " Availability • " Reliability	• Resource sharing • openness • Transparency • Scalability
Types	• public clouds • private " • Community " • Hybrid "	• Distributed Computing systems • " Information " • " Pervasive "
Characteristics	1) Shared Resources for users 2) On-demand Access anytime 3) Managed by providers 4) Accessible via the Internet	1) Task are processed on Multiple Machine Simultaneously 2) uses RPC & RMI for distributed Computing

5) Disadvantage	1) High elasticity, less control 2) service limitations depends on the provider	1) more node failures 2) Slow Nlw affect algorithms 3) High overhead for some tasks
6) benifit	• There are many benifit in CC like Cost effective, elasticity & reliable, economies of scale, Access to the global market, etc	• like flexibility, reliability, improved performance etc
7) refers	CC refers to providing on demand IT resources/services, storage, database, networking, analytics, software, etc. over Internet.	Distributed Computing refers to solve a Problem over distibuted autonomous computers & They Comm^n bet^n them over a Nlw.

Q1) write short Note on Distributed Computing ?

→ (types,

• Definition:

Distributed Computing refers to a System where diff^n sevices & data storage devices are Spread out in various locations Around the world.

These Components work together, Communicating & Collaborating to Achive a Common goals

• In Simple words, its like having Multiple Computers or systems working together to solve a Problem, even though they are located far apart.

• Examples:

1) The Internet (world wide web) www

2) Telecomm^n Nlw with Multiple devices like antenna & amplifiers that work together as one system for users.

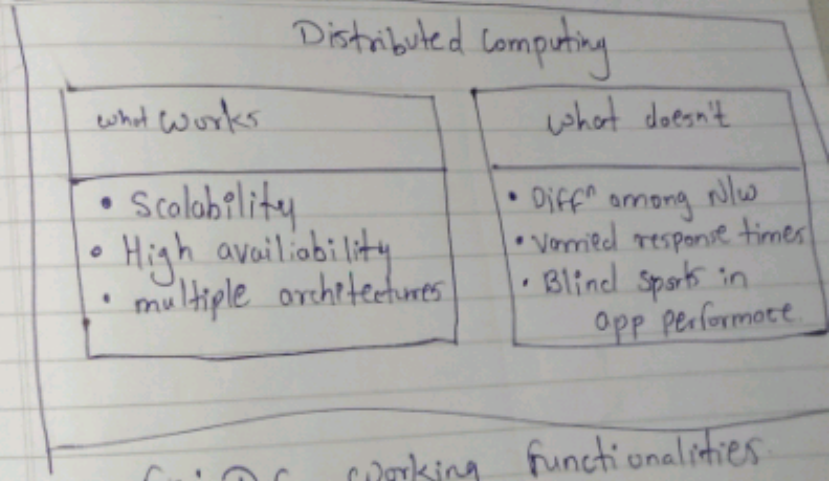


fig: D.C working functionalities

5) Actuators
6) Control systems
7) Connectivity
8) Data Analytics

(Q2) Explain the IIOT Architecture ?

↳

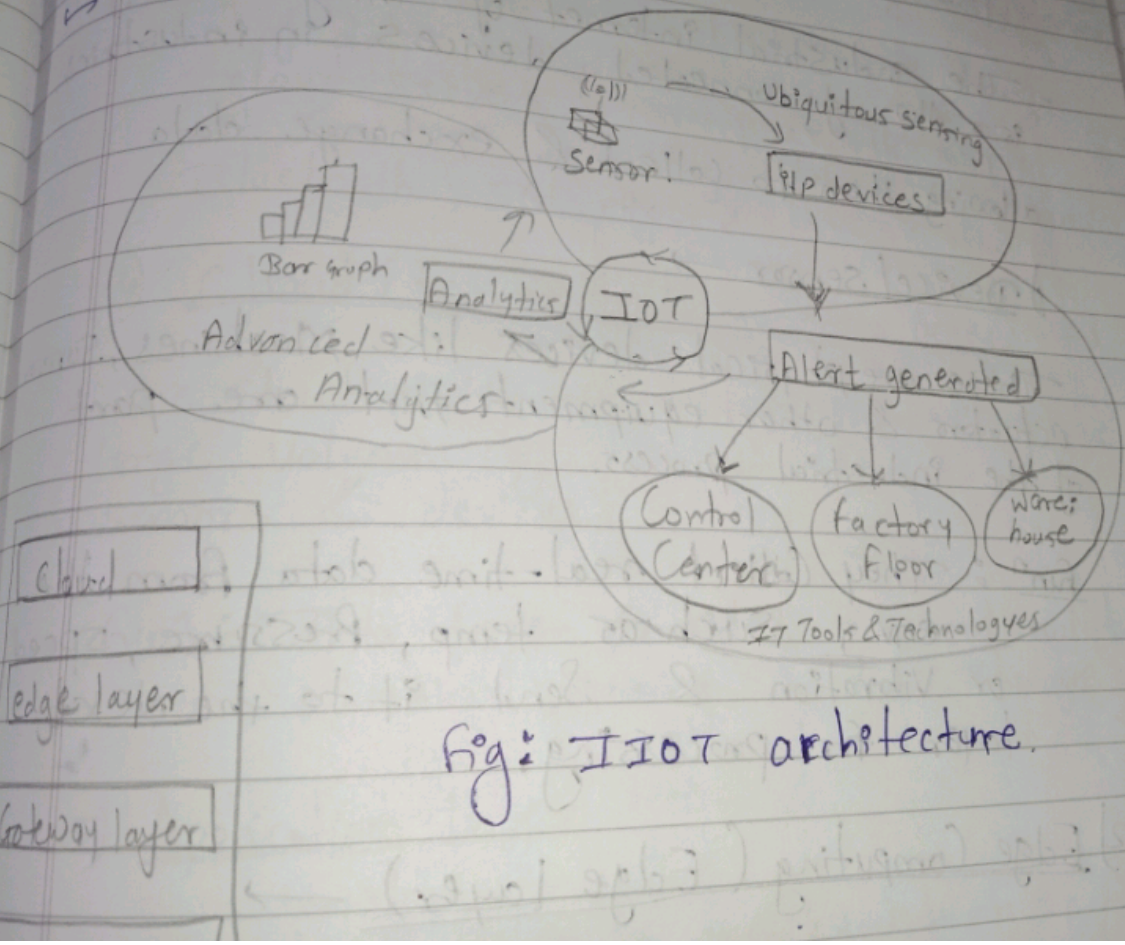


fig: IIOT architecture.

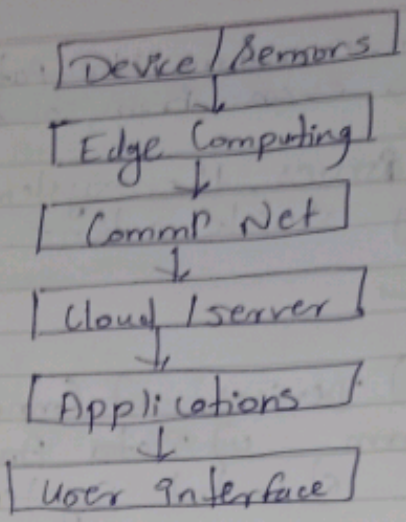


fig: Simple Architecture Diagram

- The Industrial Internet of Things (IIoT) is a Nw of connected devices in industries, allowing them to collect & exchange data

1) Device/Sensor →

These are physical devices like Machines, Sensors actuators & other equipment that are part of the Industrial process.

Fun^n : They Collect real-time data from the env, such as temp, Pressure, speed or Vibration & Send it to the Next layer for processing.

2) Edge Computing (Edge layer) →

Some data processing is done locally, closer to the source of the data, using edge devices like gateways.

fun°: it reduces latency by processing some data locally, filtering out unnecessary information & sending only imp data to the cloud.

3) Comm° Nlw (Connectivity layer) →

- The Comm° layer includes Nlw (wired or wireless) that connect all the devices & systems together

fun°: This layer ensures the smooth transfer of data betn devices, edge system & cloud servers
It can use technologies like Wifi, ethernet, Bluetooth, 5G, etc.

4) Cloud / server (Data processing layer) →

The cloud platform servers store & analyze large volumes of data collected from various sensors & devices.

fun°: This layer provides advanced analytics, Machine learning & data storage.

5) Application layer →

~~This~~ where data is used by human or system to control operations.