Definition:

It is a combination of two terms cloud and computing.

Meaning of Cloud:

The cloud refers to servers that are accessed over the internet, and the software and databases that run on these servers.

Computing:

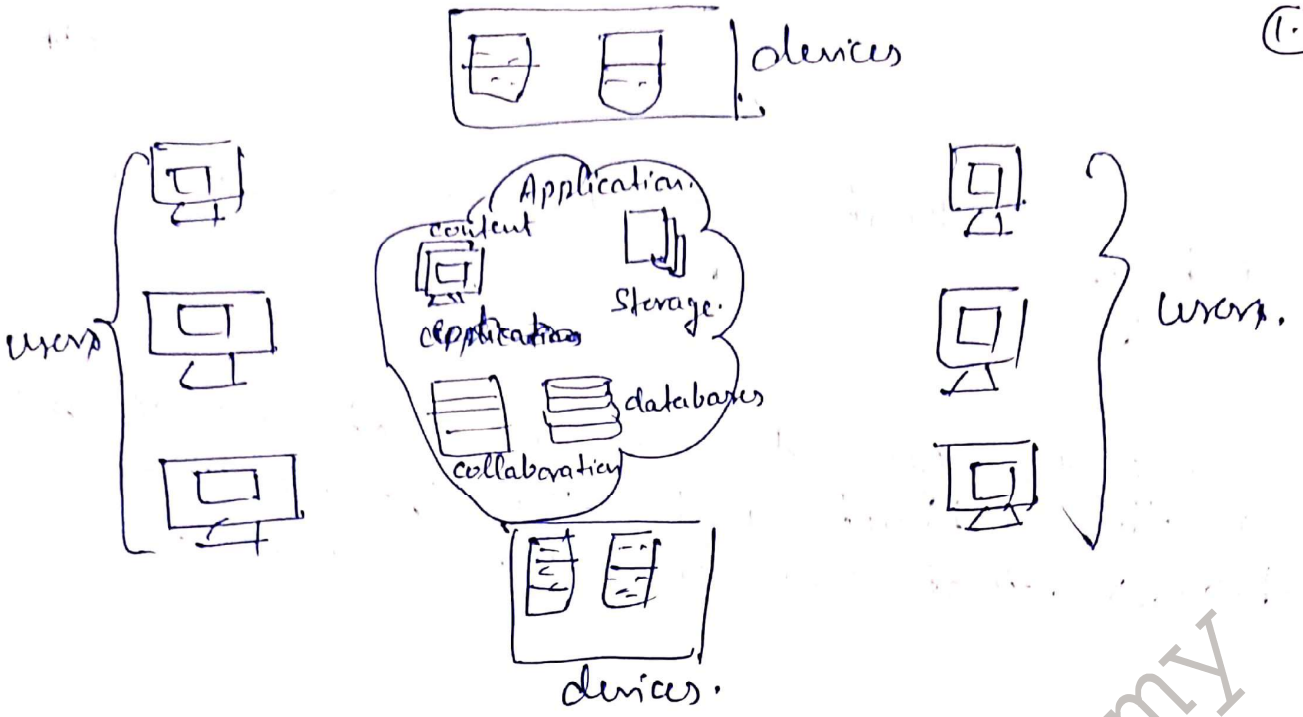
Any activity that uses computers to manage, process and communicate information.

Definition of Cloud Computing:

Cloud-Computing is the on-demand availability of computer system resources (data storage especially) and computing power without direct active management by the user.

Properties of Cloud Computing:

* It is generally used to describe the data centres available to many users over the internet. (on-demand self service.).
* It is a combination of both hardware and software computing resources delivered as network service.
* Broad network access.
* Resource pooling



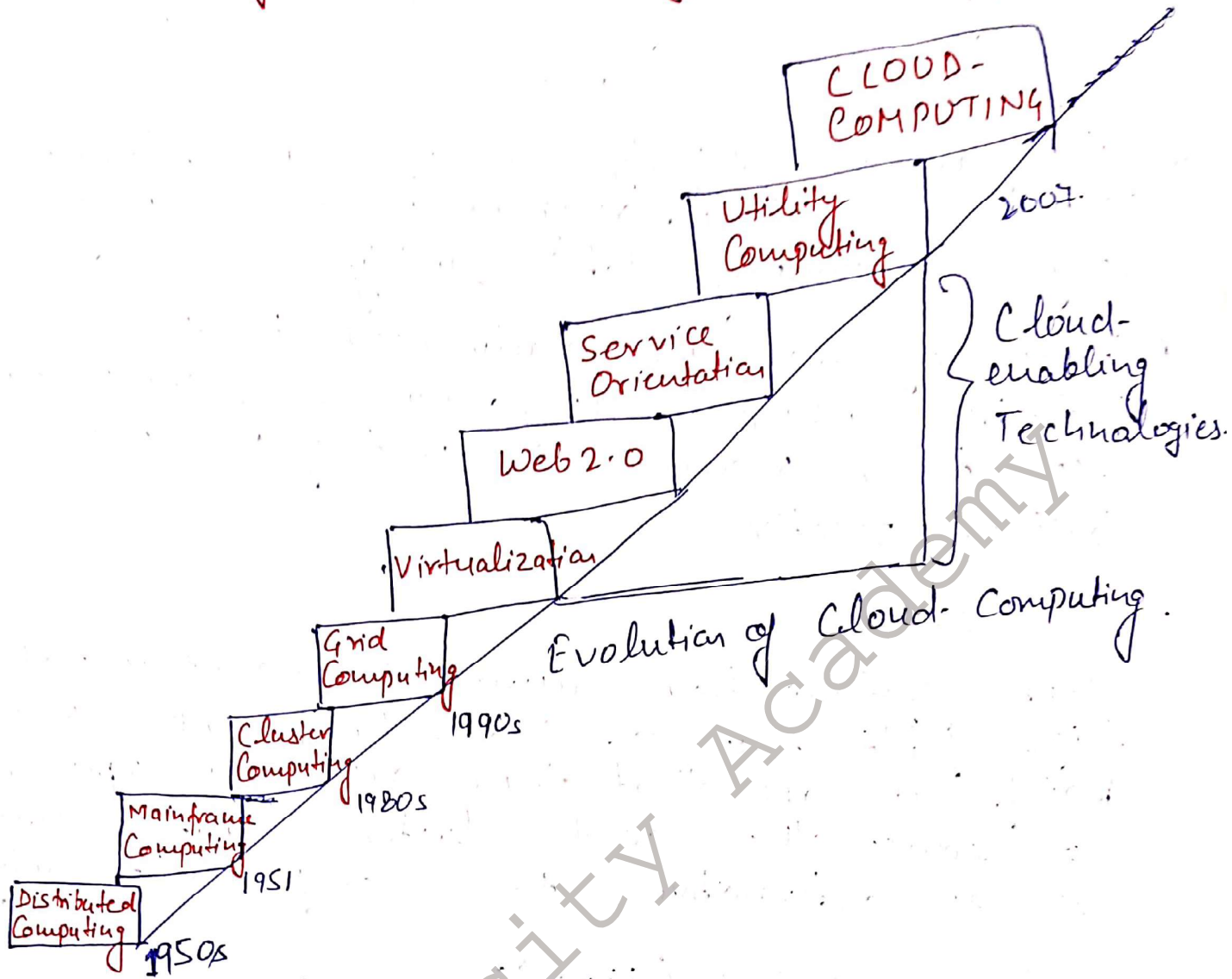
Advantages of Cloud Computing:

1) Cost Reduction
2) Security
3) Reliability
4) Improved performance
5) Instant Software Updates.
6) Universal document Access.
7) ~~Devide~~ Device independance.

Disadvantages:

1) Requires a constant Internet Connection.
2) Does not work well with low internet connection.

Evolution of Cloud - Computing :-



Evolution of Cloud- Computing.

Distributed Systems:

* It is a composition of multiple independent systems but all of them are depicted as a single entity to the users.
* The purpose of distributed system is to share resources and also use them effectively and efficiently.

Problem with Distributed Systems:

The main problem with this system was that it requires all the systems to be present at the same geographical location. To solve this problem it led to three more types of

computing — Mainframe Computing, cluster computing and grid computing.

Mainframe Computing :- (1951)

* Mainframes are highly powerful and reliable computing machines, designed to procers very large amount of data quickly.
* These systems are widely used in the industries where a large number of transactions need to be processed as part of routine business practices.

Drawback :-

These systems have almost no downtime with high fault tolerence. The only drawback with mainframes are that these are very expensive. To reduce the cost, cluster computing came as an alternative to manframe technology

Cluster Computing :- (1980s) :

Cluster computing refers that many of the computer connected on a network and they perform like a single entity.

These were way cheaper than the manframe systems, equally capable of high computations. Also new nodes could be easily added to the cluster if it was required.

Drawback :-

The problem of cost was solved to some extent, but the problem related to geographical restrictions still pertained. To solve this, the concept of grid computing was introduced.

Grid- Computing:

In 1990s, the concept of grid- computing was introduced as a solution to cluster computing.

In grid -computing different systems were placed at entirely different locations and these all were connected via the internet.

Problem:

Although it solved some problems but new problems emerged as the distance b/w the nodes increased.

The main problem which was encountered was the low availability of high bandwidth connectivity and other n/w issues also arised.

Cloud - Computing:

Cloud- computing is referred as "Successor of grid- computing.

Virtualization:

It refers to the process of creating a virtual layer over the h/w which allows the user to run multiple instances simultaneously on the h/w.

web 2.0:- It is the interface through which the cloud-computing services interact with the clients. It is because of web2.0 that we have interactive and dynamic web pages.

Service Orientation :-

It acts as a reference model for Cloud-computing.

Two important concepts were introduced in this computing model.

(i) Quality of service (QoS) ⇒ also includes SLA (service level agreement.

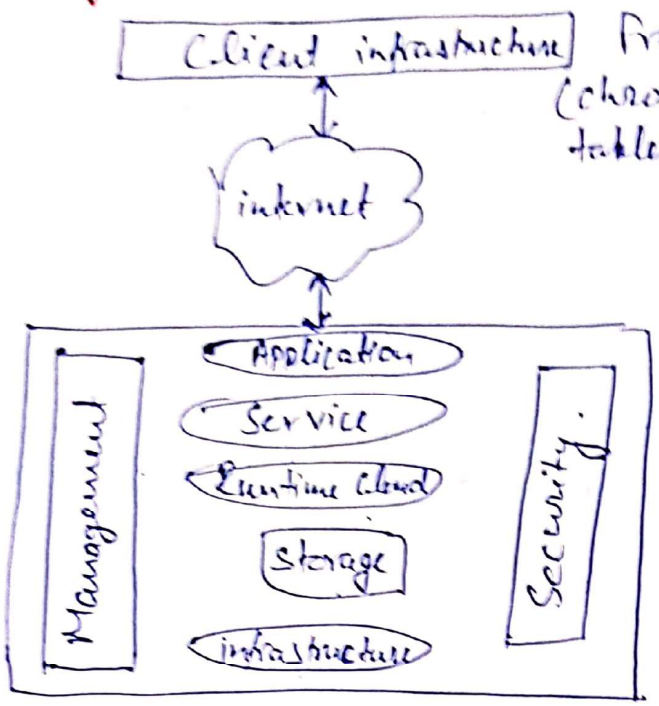
(ii) Software as a Service (SaaS).

Utility Computing :-

It is a computing model that defines service provisioning techniques for services such as compute services along with other major services such as storage, infrastructure etc which are provisioned on a pay-per-use basis.

Hence there are the technologies (virtualization, web 2.0, service orientation & utility computing) which contributed to the making of Cloud-computing.

Components of Cloud Computing: / Architecture of Cloud Computing



Front End:

* Front end is used by clients.
* It consists of client-side interfaces and applications that are required to access the cloud computing platforms.
* It includes web servers (including chrome, Firefox, internet explorer etc) tablets and mobile devices.

Back-End:

* Back-end is used by the service provider.
* It manages all the resources that are required to provide cloud computing services.
* It consists of huge amount of data storage, security mechanism, virtual machines, deploying models, servers, traffic control mechanism etc.

The various components can be given as

1) Client - Infrastructure :-

GI is the front end component. GI provides GUI (Graphical User Interface) to interact with cloud.

2) ~~Application~~

2) Internet :-

* It is the medium through which front end and back end can interact and communicate with each other.

3) Security :-

* GI is an in-built back-end component of cloud - computing.
* GI is decided by the cloud - service provider

4) Management :-

* GI is used to manage components such as application, service, storage, infrastructure and other security issues in the cloud.
* GI is used to establish coordination b/w all the components.

5) Infrastructure :-

GI provides services on host level, application level and network level.

GI includes both h/w and s/w components that are needed to support the cloud computing model.

Storage:

It provides a huge amount of storage capacity in the cloud to store and manage data.

Runtime Cloud:

It provides the execution and runtime environment to virtual machines.

Services:

It totally depends upon the client's requirement.

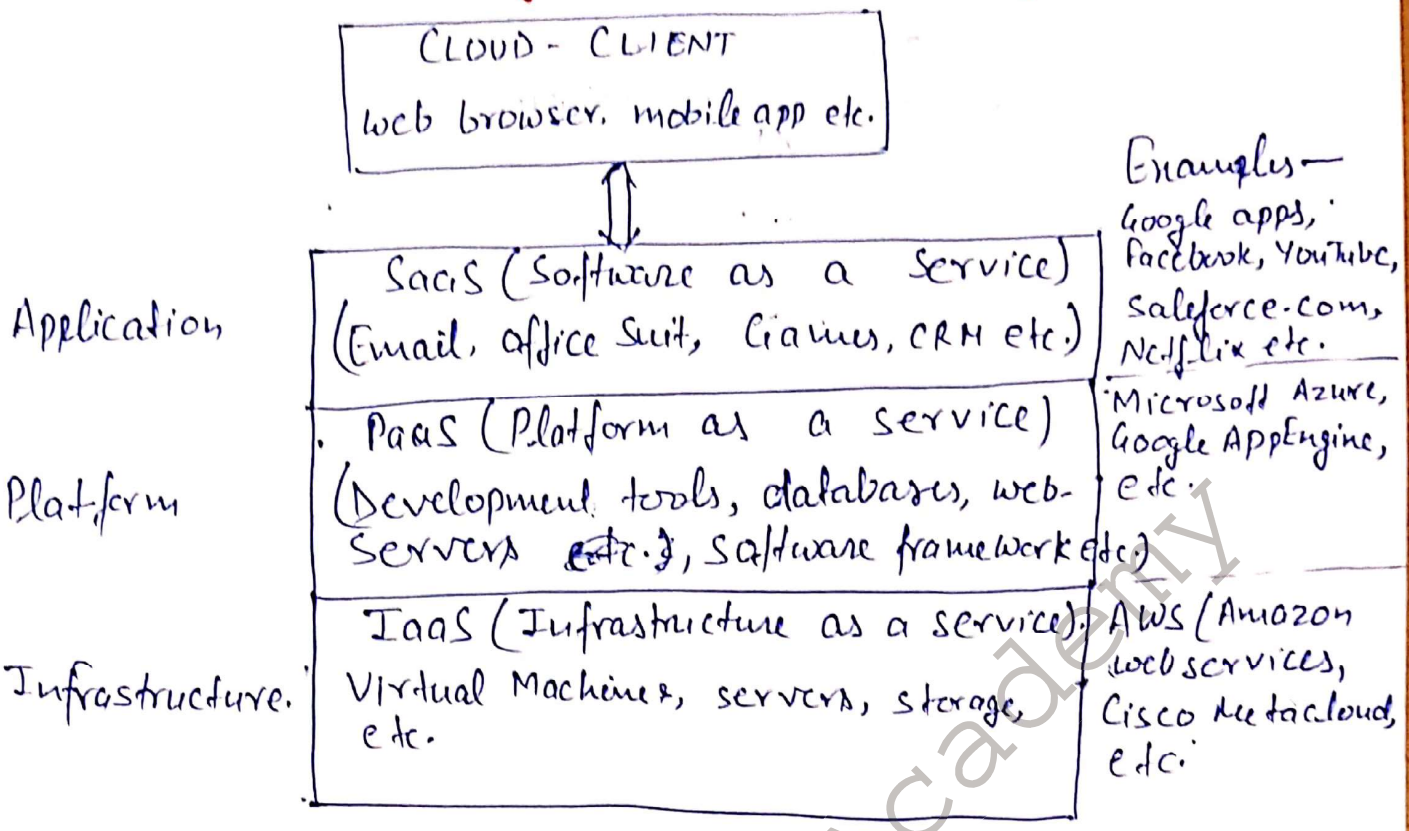
Cloud computing offers three types of services.

(i) Software as a Service (SaaS)
(ii) Plateform as a Service (PaaS)
(iii) Infrastructure as a service (IaaS).

Application:

It can be defined as any S/w or platform that client wants to access.

Service Models of Cloud - Computing :-



SaaS (Software as a service) :-

* It is also known as cloud application services. The service is purchased on a subscription basis.
* It is a software distribution model in which a third-party service provider hosts applications and makes them available to the customers over the internet.

Characteristics of SaaS :-

* Software managed from a central location.
* Web access to commercial softwares.
* Software delivered in a "one to many" model.
* User not required to handle software upgrades and patches.

Platform as a Service (PaaS):

* It is a cloud computing model in which cloud vendors provides developers with a platform for building apps.
* The developers basically rent everything they need to build an application. It depending upon cloud provider for development tools (compiler, debugger etc), databases, infrastructure etc.

Characteristic:

* Provides a variety of services to assist with the development, testing and deployment of apps.
* Resources can be easily scaled up or down as busines changes.
* Accessible to numerous users via the same development application.

Iaas: Infrastructure as a Service

It is a form of cloud computing that provides virtualized computing resources over the internet (storage, memory, infrastructure etc)

Characteristic:

Shared infrastructure
web access to resources.
Pay-as-per use.
On-demand scalability.

Difference b/w SaaS, PaaS and IaaS:

SaaS	PaaS	IaaS
1- It provides web software and apps to complete business tasks as well as personal uses.	It provides virtual platforms and tools to create, test and deploy the apps.	It provides a virtual infrastructure in which resources are provided to the users but not physically.
2- It provides software as a service to the end users.	It provides runtime environments and deployment tools for applications.	It provides access to resources such as virtual machines, virtual storage etc.
3- It is used by the end users.	It is used by developers.	It is used by network architects.
4- It provides infrastructure + Platform + Software	PaaS provides Infrastructure + Platform.	IaaS provides only Infrastructure
5. ex: Cisco WebEx, Google apps, Dropbox, ZenDesk etc.	ex: force.com, Magento commerce cloud, Openshift etc.	ex: AWS, Rackspace, Cisco Metacloud.

Underlying Principles of Parallel and distributed computing:

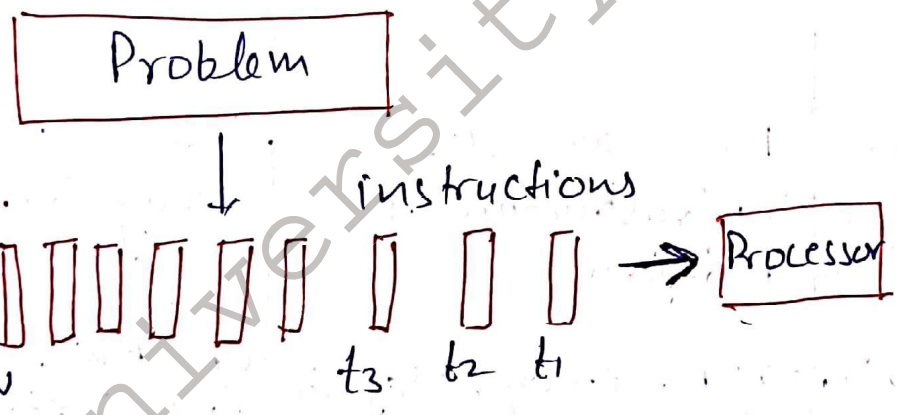
Before discussing parallel and distributed computing we need to discuss serial computation.

Serial Computation:

⇒ Initially S/w has been written for serial computations. i.e. to be run on a single computer having a single CPU.

⇒ In serial computation a problem is broken into a discrete series of instructions and instructions are executed one after another.

⇒ Only one instruction may execute at any moment in time.



Problem with Serial Computation:

⇒ Low transmission speed.

⇒ Limits to miniaturization

⇒ Only one instruction at a time can execute so it is a time taking process.

Requirements of Parallel Processing :

(To solve problems of serial computing.) (1-14)

⇒ Save time and/or money.

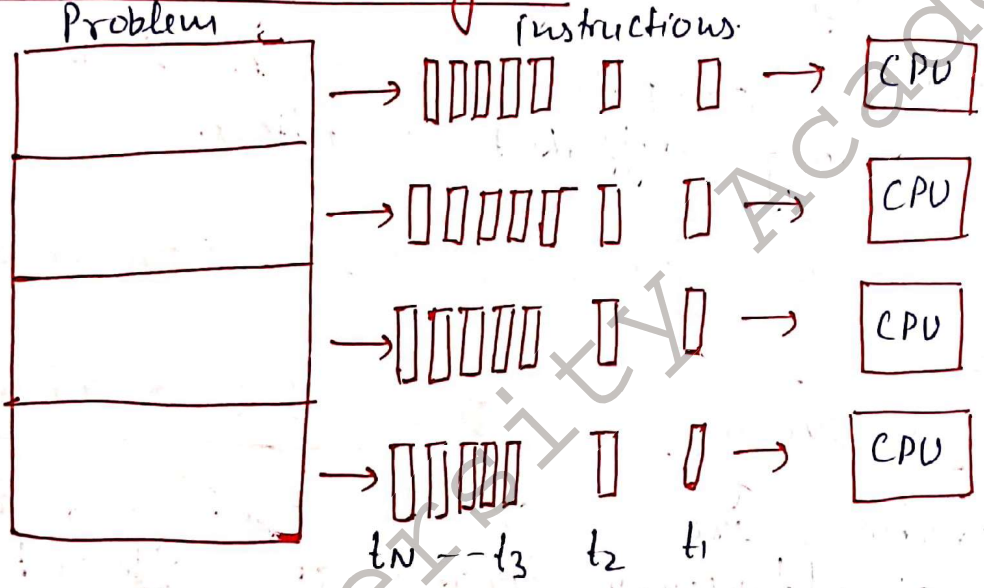
⇒ Solve larger/more complex problems.

⇒ Provides concurrency.

⇒ Takes advantages of non-local resources.

⇒ Makes better use of underlying parallel hardware.

Parallel - Computing :



Parallel computing involves the concurrent computation or simultaneous execution of process or threads at the same time.

Basically it consists of —

⇒ Decomposition of a problem into discrete parts that can be solved concurrently.

⇒ Decomposition of each parts into series of instructions.

⇒ Distributing the parts as tasks which are worked on by multiple processors simultaneously

⇒ Coordinating work and communications of those processors or cores.

Distributed Computing:

In distributed computing we have multiple autonomous computers which seems to the user a single system.

In distributed systems there is no shared memory and computers communicate with each other through message passing.

In distributed computing a single task is divided among different computers.

Difference b/w Parallel and Distributed Computing:

Parallel Computing	Distributed Computing
① Many operations are performed simultaneously	System components are located at different locations.
② Single computer is required	Uses multiple computers.
③ Multiple processors performs multiple operations.	Multiple computers performs multiple opr^{n}s.
④ It may have shared or distributed memory.	It have only distributed memory.

(5) Processors communicates with each other through bus.	Computers communicates with each other through message passing.
(6) Improves the system performance.	Improves system scalability, fault tolerance, and resource sharing capabilities.
7) Ex: weather forecasting, movie special effects etc.	Telecommunication networks, aircraft control systems etc.

Deployment Models of CLOUD-COMPUTING

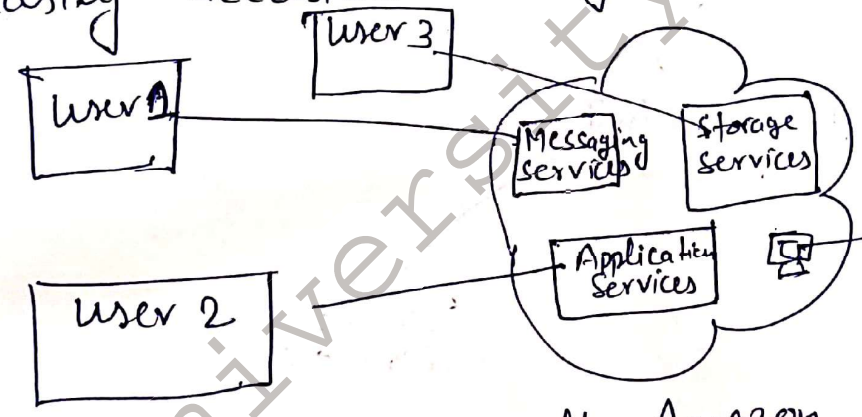
↳ In its general terms deployment is the process of making software also available and ready for use.

4 types of deployment models are available in cloud.

1) Public Cloud
2) Private Cloud
3) Hybrid Cloud
4) Community Cloud

1) Public Cloud Model :

* It allows systems and services to be easily accessible to general public.



Examples: Google, Microsoft, Amazon etc.

Advantages:

* Flexible
* Low Cost
* Place independence

Disadvantages

* Less secure.
* Less customization.

Examples: Google Cloud, IBM's Blue Cloud, Sun cloud etc.

2) Private Cloud Model :- (Internal Cloud)

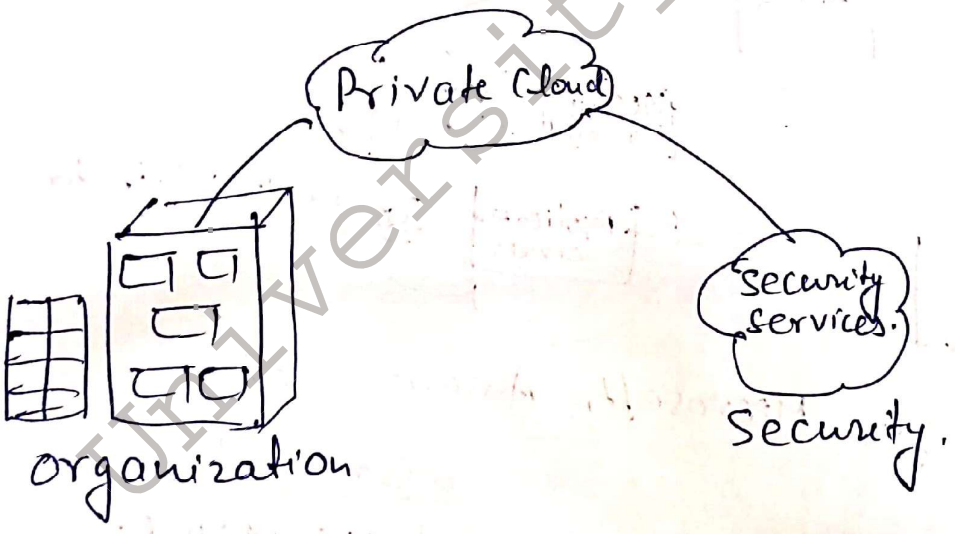
* It allows systems and services to be accessible within an organization.
* However, it may be managed internally by the organization itself or by third party.

Advantages :-

* Highly Private and Secured.
* Control oriented.

Disadvantages :-

* Costly.
* Restriction
* Pricing is inflexible i.e. purchasing new hardware for upgradation is more costly.
* restricted area of operation.
* Limited area of operation.



Examples :- HP data Centres, Microsoft, Elastra- private cloud etc.

3) Hybrid Cloud:

* It is a combination of public and private clouds.

> Hybrid cloud = public cloud + private cloud.

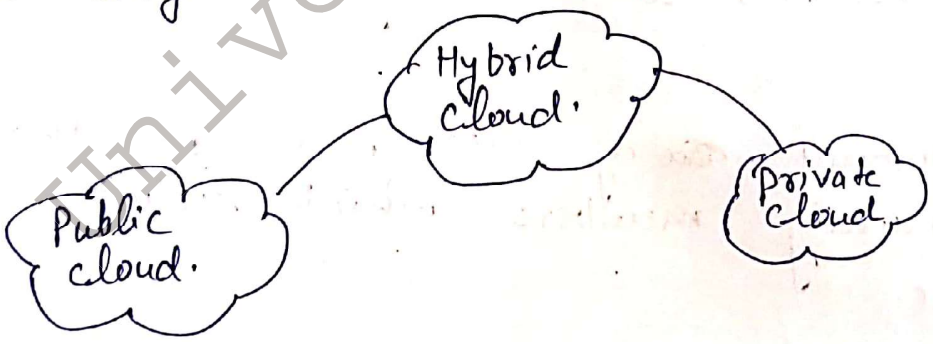
* In hybrid cloud, non critical activities are performed by public cloud and critical activities are performed by the private cloud.
* A hybrid cloud is an infrastructure that includes links between one cloud managed by user and at least one cloud managed by a third party (public cloud).

Advantages:

* Flexible and Secure
* Cost-effective
* Security.
* Risk-management.

Disadvantages

* Network-issues
* Infrastructure compatibility required.

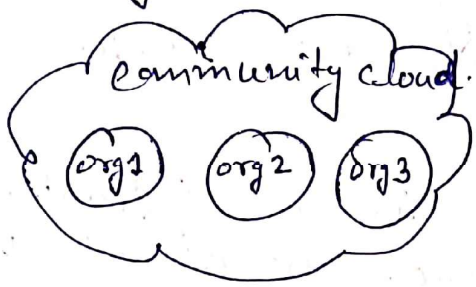


Examples: Amazon, Microsoft, Google, Cisco and NetApp are the various hybrid cloud provider companies.

4) Community Cloud:

* It is a cloud infrastructure that allows systems and services to be accessible by a group of several organizations to share the information.

* It is owned, managed and operated by one or more organizations in the community, a third party or a combination of them.



Advantages:

* Cost-effective
* Flexible and scalable.
* security
* sharing infrastructure

Disadvantages:

* Sharing resources within organization is little difficult.
* Fixed amount of resources are shared b/w community members which reduces performance.

Example: V.s based dedicated IBM SoftLayer cloud for federal agencies.

Technologies used in Cloud-Computing :-

The various technologies that are used in Cloud-Computing are given as follows —

* Virtualization
* SOA (Service Oriented Architecture).
* Grid Computing
* Utility Computing

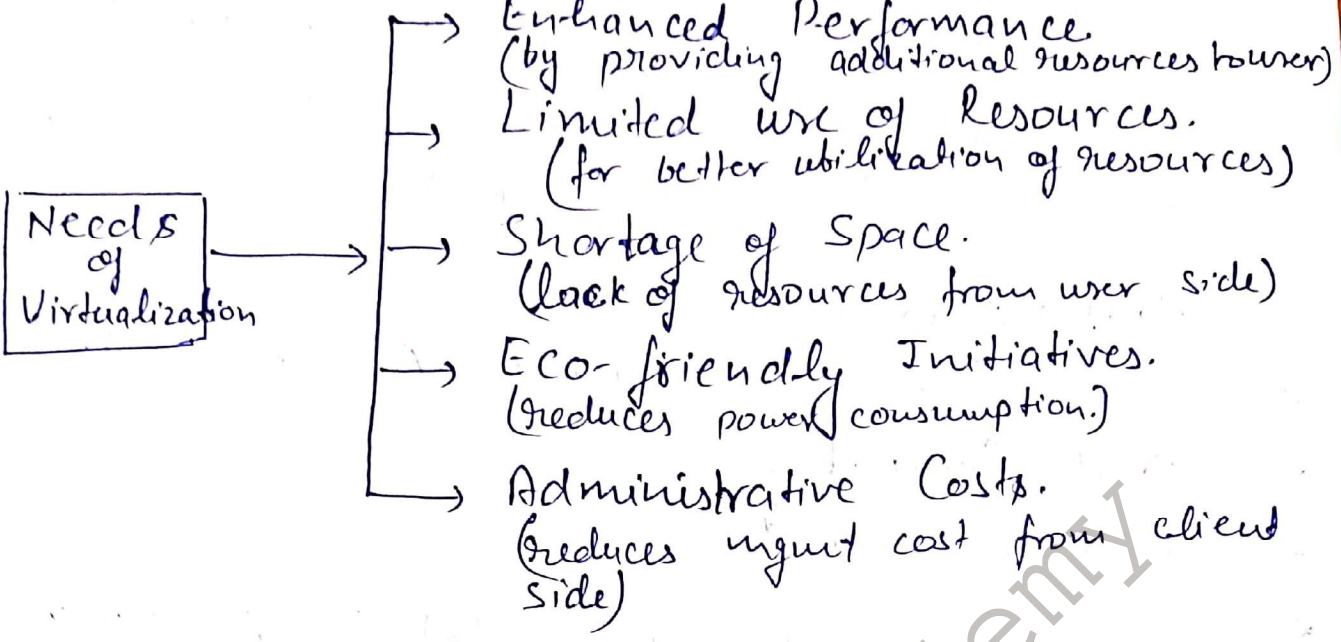
If we talk about the latest technologies, there are various trends in 2020. The various latest technologies are as follows.

* Serverless Computing.
* Omni-Cloud.
* Quantum Computing.
* Kubernetes
* Digital Natives

Virtualization :-

* It is the creation of virtual (version of something, such as server, a desktop, a storage device, an operating system or network resources. i.e resources are made available to the users but virtually not physically.
* It is a technique which allows sharing a single physical instance of resources to multiple users.

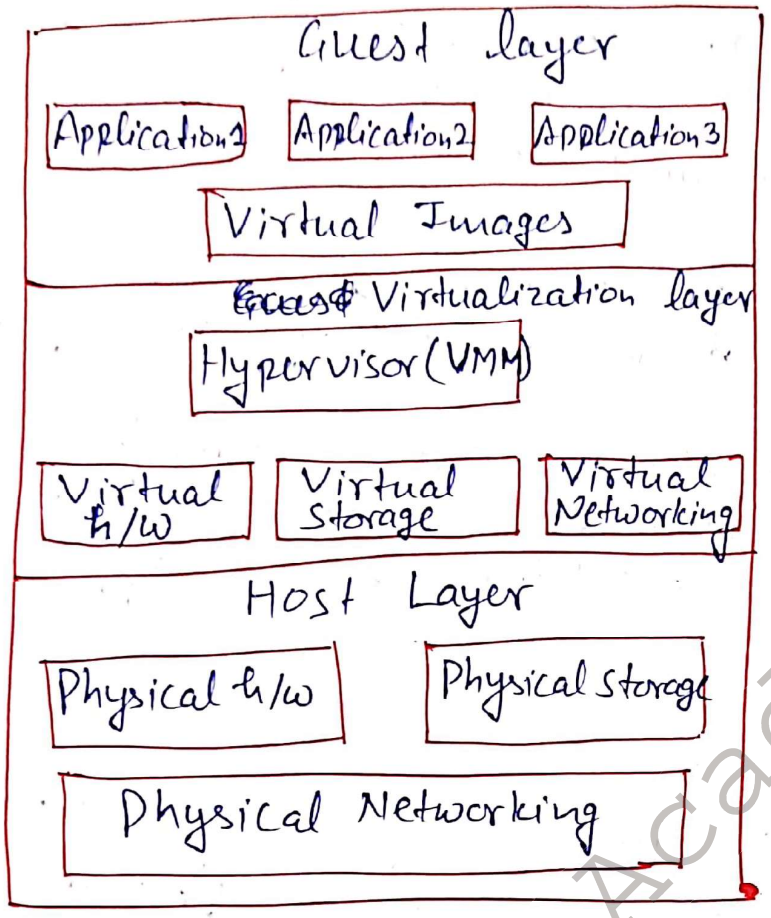
Need of Virtualization :-



Advantages of Virtualization :-

* Economical :- (Don't need to buy high capacity hardware and other resources.).
* Flexible Operations :- (You can access it from anywhere and customization can be done)
* Security :- Provided by cloud-service Provider.
* Eliminates the risk of system failure.
* Flexible transfer of data
* Faster provisioning of applications and resources.
* Greater business continuity and disaster recovery.
* Simplified data centre management.

Virtualization Reference Model:-



Four major components of Virtualization reference Model is available here.

i) Host Layer:-

⇒ The host layer represents the original environment where the guest is supposed to be managed.

⇒ All the physical resources and physical networking is present in this layer.

⇒ Each guest runs on the host machine using shared resources donated to it by the host.

⇒ The OS works as the host and manages the physical resources management and the device support.

Guest Layer:

⇒ The guest represents the system components that interacts with the virtualization layer rather than with the host.

⇒ Guest usually consists of one or more virtual disk files, and a VM definition file.

⇒ Virtually machines are centrally managed by a host application that sees and manages each virtual machine as a different application.

Virtualization Layer:

⇒ The virtualization layer is responsible for recreating the same or a different environment where the guest will operate.

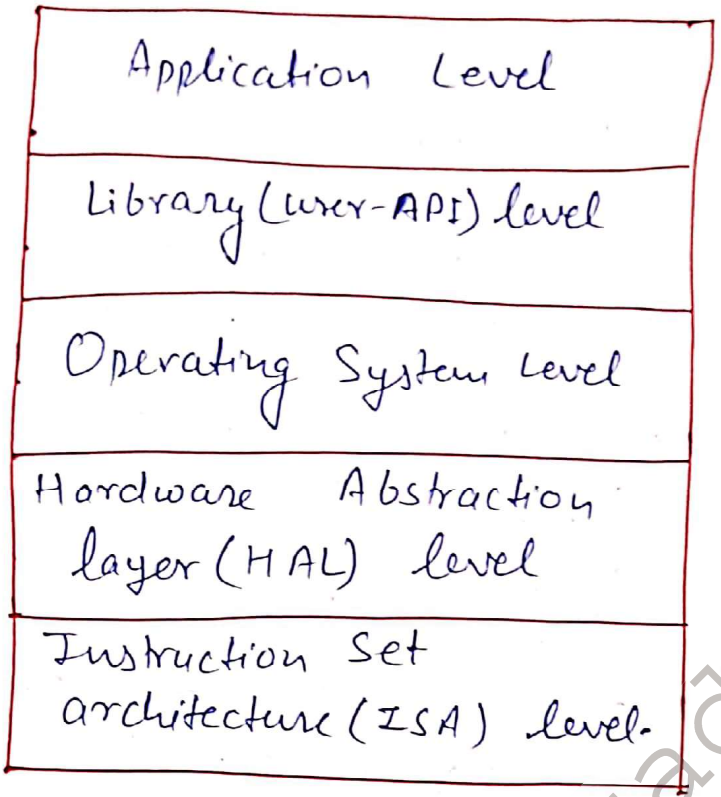
⇒ It is an additional abstraction ~~layer~~ layer between a network and a storage hardware, computing and the application running on it.

Hypervisor:

⇒ A hypervisor, also known as Virtual Machine Monitor (VMM), is a software that creates and runs virtual machines (VMs)

⇒ A hypervisor allows one host computer to support multiple guest VMs by virtually sharing its resources, such as memory and processing.

Implementation Levels of Virtualization:



Instruction Set Architecture (ISA) Level & Applications:

⇒ In ISA level implementation, every machine has an instruction set which is an interface b/w software and hardware.

⇒ An emulator is created which receives all the instructions from the virtual machines.

⇒ The emulator interprets what type of instruction it is and then map that instruction to the host machine's instruction and then that instruction will be carried out on host machine and the results will be passed to the emulator and emulator will return it to the virtual machine.

Problems in ISA level implementations:

Since every instruction has to be interpreted before mapping it, too much time is consumed and performance becomes poor.

Virtualization at HAL level:

⇒ To overcome the problems of ISA level implementation of virtualization, we have virtualization at HAL level.

⇒ On HAL level we map the virtual resources with physical resources.

⇒ we dont interpret every instruction (as of in ISA level), but we just check whether it is privileged or non-privileged.
(ex:- memory mgmt, scheduling etc)

⇒ If the instruction is not privileged we simply allow normal execution because already virtual and physical resources are mapped.

⇒ If the instruction is privileged, we pass the control to VMM and it deals with it accordingly.

Problems in HAL implementation:

⇒ even after many advancements still there are certain exceptions which cannot be caugh by this method.

⇒ Since, in this method each VM is build from scratch i.e by installing OS, application suites, networking systems etc., so if it is required to initialize more virtual machine at a single time, then it will take too much of time.

Virtualization at OS level:

⇒ To overcome the problems of HAL level implementation we can use OS level virtualization.

⇒ In this method each VM is not built from scratch rather we share operating system b/w virtual machine along with the h/w.

⇒ we keep the base OS same and install only the differences in each single virtual machine.

Problem with OS level implementation:

The major problem with this is that we can install only those OS in VMs whose base OS family is same like for example we can't install ubuntu on a VM whose base OS is windows.

Virtualization at library level or Programming language level:

⇒ In this type, we use library level interfaces to provide a different virtual environment (VE) for that application.

⇒ In short we provide user with an emulator with which user can run applications of different OSs.

Virtualization at Application Layer Level:

⇒ In this kind of virtualization virtual machine run as an application on the Host operating-system.

⇒ we create a virtualization layer which is present above the host OS and it encapsulates all the applications from the underlying OS.

⇒ While all the applications are loaded, Host OS provides them with a runtime-environment.

⇒ But virtualization layer replaces a part of this runtime environment and gives a virtual environment to the virtualized applications.

Types of Virtualization:

Desktop - Virtualization.	
Types → [Virtual desktop infrastructure, Hosted Virtual desktop]	ex: Citrix, Xen desktop
Data - Virtualization	
Types → Databases	ex: e-commerce websites, web-portals etc.
Software - Virtualization	
Types → [OS Level Virtualization, Application " , Service "]	ex: Virtual box, VMware etc.
Memory - Virtualization	
Types → [Software base, Hardware Assisted]	Memory virtualization in paging and segmentation.
Storage - Virtualization	
Types → Block & file Virtualization	ex: windows storage spaces.
N/w Virtualization	
Types → Internal & External	ex: Virtual LAN (VLAN)
Hardware - Virtualization	
Types → Full, Para, Partial	ex: Microsoft hyperV, Xen etc.

① Hardware Virtualization: (also known as Server Virtualization).

⇒ In h/w virtualization, multiple physical segments of hardware or physical servers are consolidated into one virtual server and provides services to the users.

⇒ The hardware resource allotment is done by the hypervisor.

Types:

Full Virtualization:

In this type, the complete simulation of the actual hardware takes place to allow the s/w to run an unmodified guest OS.

Para Virtualization:

In this type, s/w unmodified runs in modified OS as a separate system.

Partial Virtualization:

In this type of h/w virtualization, the s/w may need modification to run.

② Network Virtualization:

Network virtualization is a method of n/w, combining the available resources in a n/w, to consolidate multiple physical networks, divide the network into segments or create s/w networks b/w virtual machines (VMs).

Types: ~~Entered~~

Internal: Provide n/w like functionality to a single system.

External: Combine many networks or parts of n/ws into a virtual unit.

3) Storage Virtualization :

In this type of virtualization, multiple physical storage devices are grouped together, which then appear as a single storage device for easier and more efficient management of these resources.

Types of Storage Virtualization :

(i) Block Virtualization :

Multiple storage devices are consolidated into one.

(ii) File Virtualization :

storage system grants access to files that are stored over multiple hosts.

4) Memory Virtualization :

⇒ Physical memory across different servers is aggregated into a single virtualized memory pool.

⇒ It enhances performances by providing greater memory capacity without any addition to the main memory.

Types of Memory Virtualization :-

(i) S/w based memory Virtualization :

Guest's physical memory is virtualized by adding an extra level of address translation.

(ii) H/w Assisted Memory Virtualization : In this type Some CPUs such as AMD SVM-V and intel Xeon 5500 series, provides h/w support to memory virtualization by using different types (layers) of page tables.

5) Software Virtualization: (Application Virtualization)

⇒ It provides the ability to the main Computer to run and create one or more virtual environments.

⇒ One S/w is physical while others are virtual as it allows 2 or more OS using only one computer.

Types of S/w Virtualization:

(i) **Operating System Virtualization:**
In OS virtualization, the H/w is used which consists of software on which different OSs work.

(ii) **Application Virtualization:**
It is a S/w technology that encapsulate computer programs from the underlying operating system on which they are executed.

(iii) **Service Virtualization:**
Service virtualization is a method that helps us to emulate the behaviours of the component in heterogenous component based applications such as API-driven applications, cloud-based applications and Service Oriented architectures.

6) Data Virtualization:

Data Virtualization is the proces of retrieving data from various resources without knowing its type and physical location where it is stored.

⇒ It collects heterogenous data from different resources and allows data users across the organization to access this data according to their requirements. (2.12)

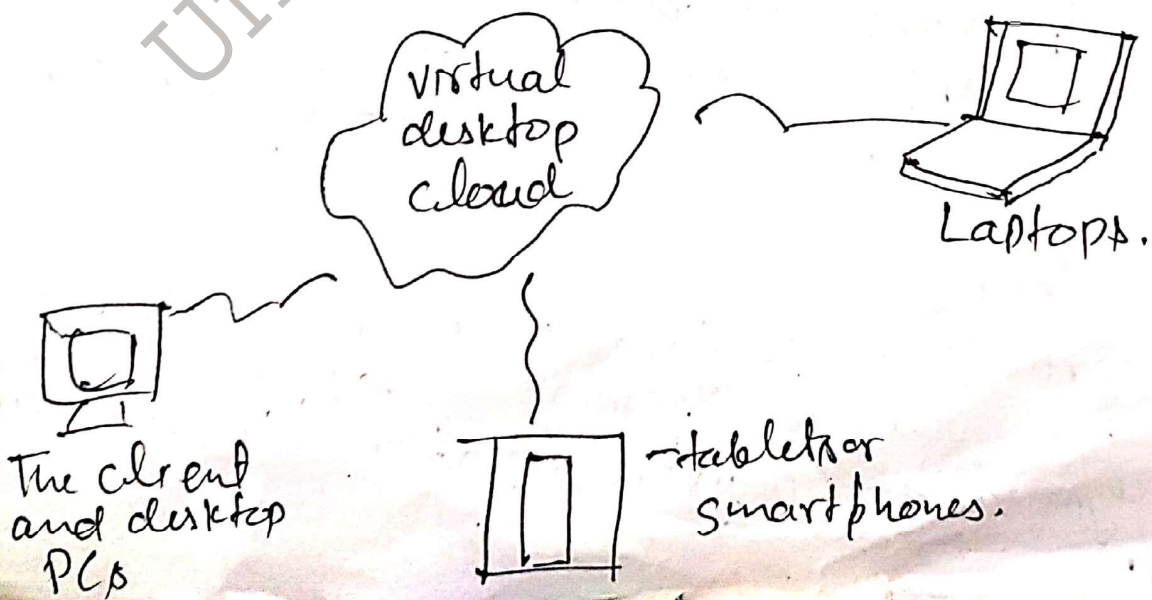
⇒ This heterogenous data can be accessed using any application such as web portals, web services, E-commerce, SaaS and mobile applications.

7) Desktop Virtualization :-

⇒ The user's desktop is stored on a remote server, which allows the user to access his desktop from any device or location.

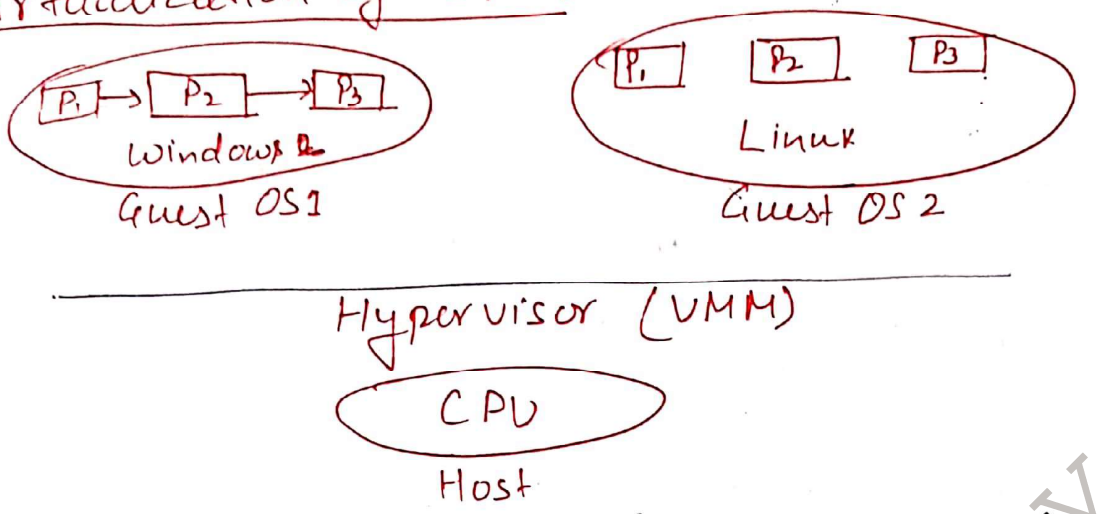
⇒ It provides work convinience and security.

⇒ It also protects confidential data from being lost or stolen by keeping it safe on central servers.



Virtualization of CPU, Memory & I/O devices

↳ Virtualization of CPU:-



⇒ CPU virtualization involves a single CPU acting as if it were multiple separate CPUs.

⇒ This allows an OS to more effectively & efficiently utilize the CPU power in the computer so that it runs faster.

⇒ All the programs and instructions are running through virtual machines giving the feeling like physical workstations

⇒ All the operations are handled by an emulator that controls software to run according to it.

Types:-

1) Software based CPU Virtualization:-

⇒ The CPU virtualization is S/W based where with the help of it, application code gets executed on the processor and the privileged code gets translated first and that translated code gets executed directly on the processor.

⇒ The translation process used here is h/a Binary Translation (BT). (2.14)

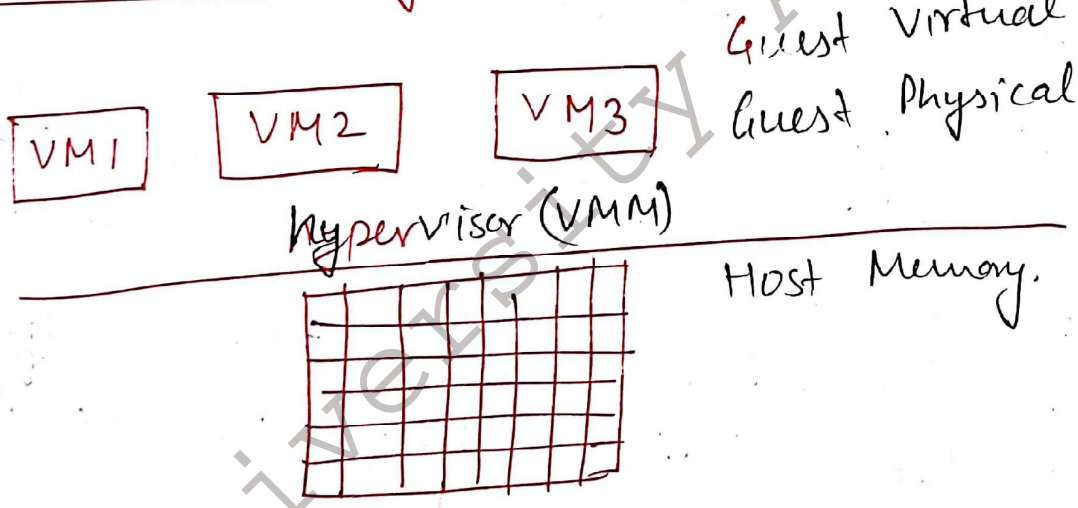
(ii) Hardware Assisted CPU Virtualization:

⇒ In h/w assisted CPU virtualization the h/w gets assistance from certain processors, but it also requires hypervisor for creating virtual machine.

⇒ In this method there is no requirement of translation.

⇒ The system calls runs faster than expected.

Virtualization of Memory:



Memory virtualization is the process of consolidating ~~the~~ random memory access resources from individual systems in the data centres, aggregates them and then provides them to the individual users with the help of virtualization using hypervisors.

Basically three layers of memory are present

(2-18)

1) Host Machine Memory:

Provides a contiguous memory space for use by the virtual machine.

2) Guest Operating System Physical Memory:

Presented to the VM (virtual Machine) by VMkernel.

3) Guest Operating System Virtual Memory:

Presented to applications by the guest Operating System.

Process of Memory Virtualization:

Two key concepts are used in the process of Memory Virtualization.

1) Mapping
2) Shadow Page Table

1) Mapping:

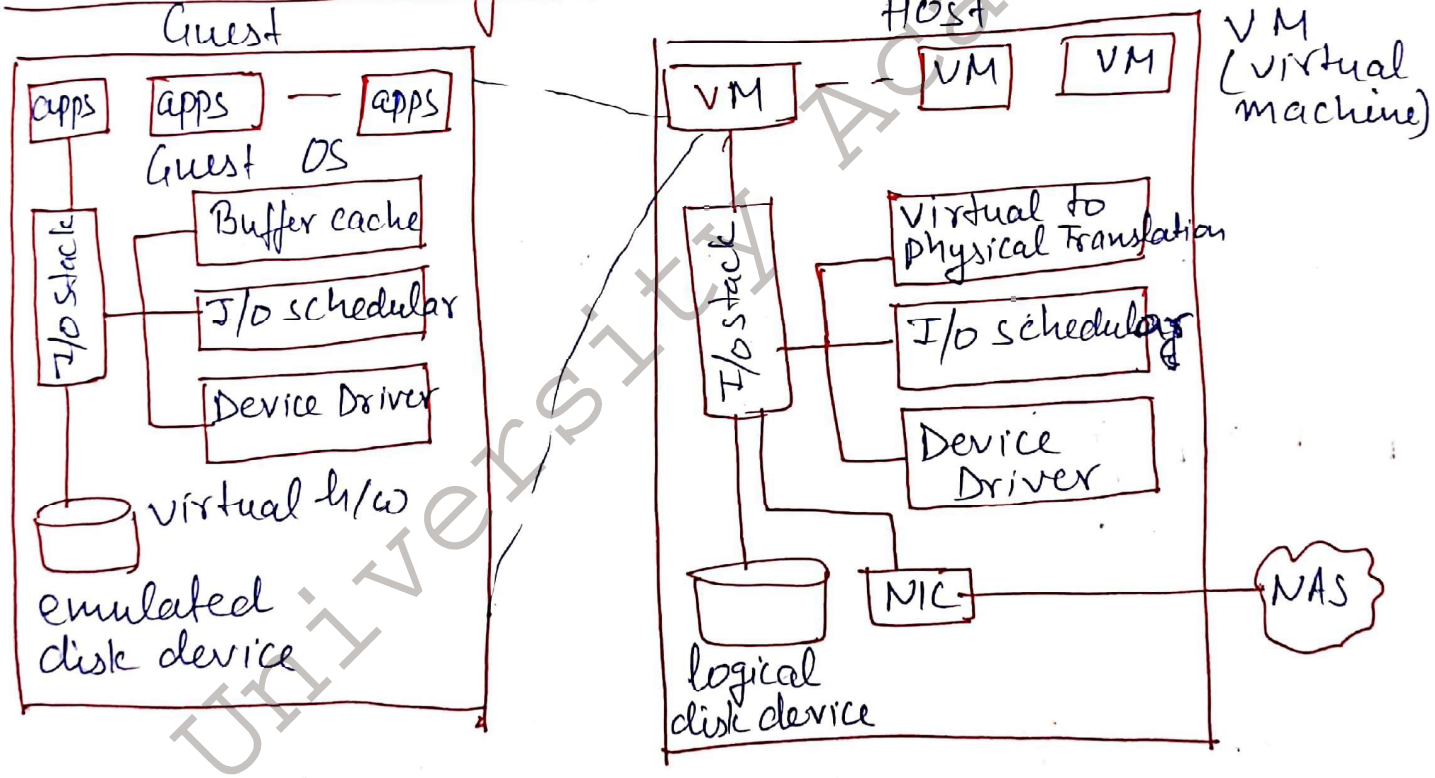
Mapping is required here for providing host's physical memory to the users with the help of virtualization. i.e. hypervisor creates different virtual copies of the same memory and provides them to the different users.

>) Shadow Page Tables:

* Shadow Page Tables are used by the hypervisors to keep track of the state in which the guest defines the allocations or gives the info about the allocation of resources.

* It provides the record of the resources allocated to the users i.e. how many virtual machines have been created actually.

Virtualization of I/O devices:

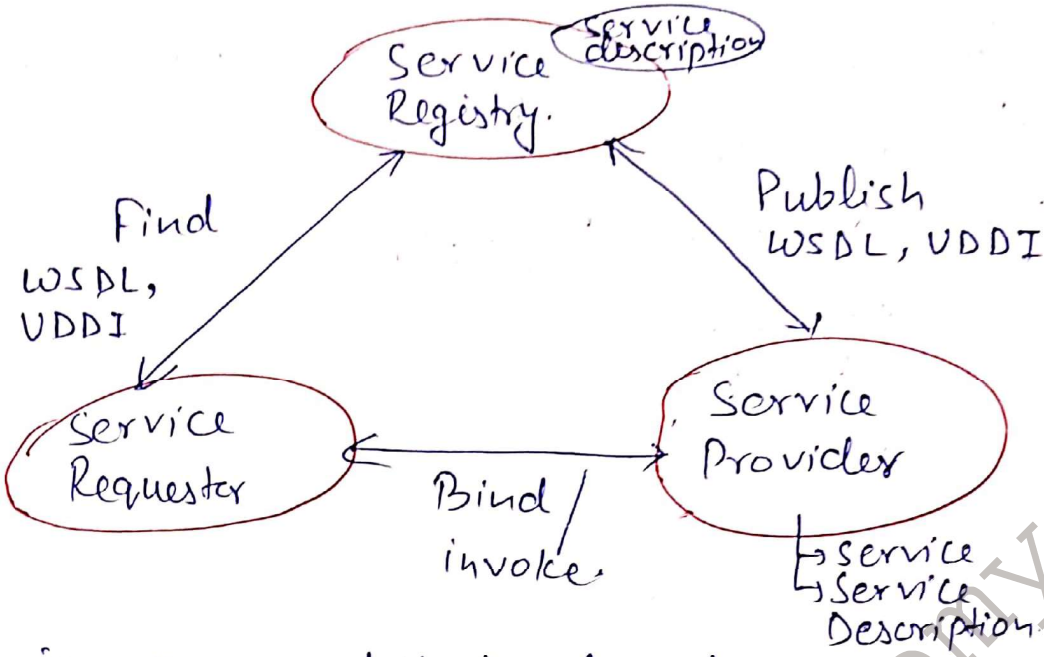


⇒ I/O device virtualization is the process of providing I/O devices (resources) ~~to the~~ from host to the user virtually. i.e. virtual machine of the I/O resources are created and provided to the user.

Process of I/O device Virtualization :-

1) User made a request for the I/O devices with the help of guest OS.
2) All the requests of the user are put into the I/O stack of the guest OS.
3) Guest OS provides various facilities like Buffur caching, I/O scheduling & also consists of device driver.
4) With the help of emulated disk device or emulator all the requests are sent to the Host i.e. to the virtual machine of the host.
5) All the requests are store in the I/O stack of Host and checked by the hypervisor.
6) Different virtualized copy of resources are created from the host side and stored.
7) If any request is made for any resource (i.e. for I/O device) then with the help of hypervisor different VM are created and provided to the different users.

SOA (Service Oriented Architecture):



⇒ SOA is an architectural frame-work in which different services provided by the service provider communicates with each other.

⇒ It describes a standard method for requesting services from distributed components and after that the result or outcome is managed.

⇒ SOA provides a translation and management layer within the cloud architecture that removes the barrier for cloud clients obtaining desired services.

ex:- Suppose if we are using any service over the cloud and we want to incorporate some other service with previous one then SOA can be used for the communication b/w those services.

ex ⇒ Online printing of credit card statements.
⇒ Putting some add-on services to google docs.
⇒ Using location services in some other applications. etc.

Components of SOA:

Basically it consists of 3- components.

1) Service Provider
2) Services Consumer (Requestor)
3) Service Registry

1) Service Provider:

* Service provider will create the services and provide them to the user.
* After creating the services provider will convert them in WSDL format and by using UDDI request for the service registry is made to the service directory.
* So basically it is the platform which will host the services.

2) Service Consumer:

* Service consumer is the entity who will actually use the services.
* Service consumer requests to the provider for invoking the services.
* The browser plays the requestors role driven by a consumer.
* services consumer serches within the service directory for finding the services of their need.

3) Service Registory :

Service requestors finds services and obtain binding info for services during development.

Operations used in SOA :

i) Publish : for publication of service descriptions
ii) Find : Finding of any service descriptions.
iii) Bind : Invoking of services based on service descriptions.

Benefits of SOA :

1) Greater Buisiness Agility.
2) Ability to leverage legacy functionality in new markets.
3) Improveed Collaboration b/w busines & IT.
4) Platform independent.
5) Availability
6) Reliability
7) Service Reusability
8) Scalability

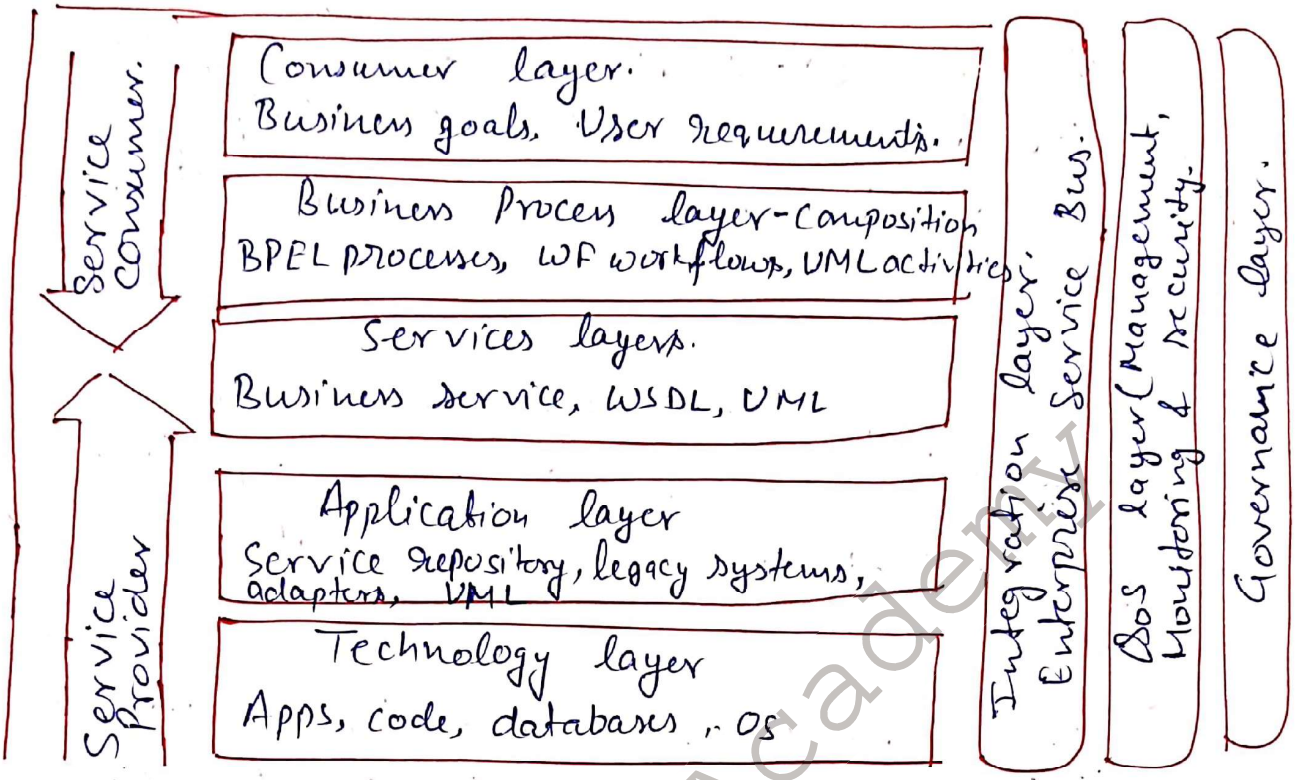
Guiding Principles of SOA:

1) Standardized Service Contract.
2) Loose - Coupling.
3) Abstraction
4) Reusability
5) Discoverability.
6) Composability.

Disadvantages:

1) High - Overhead.
2) High investment
3) Complex Service Management

SOA Reference Model & layered Architecture of SOA



⇒ The goal of SOA reference model is to provide a blueprint for creating or evaluating architecture.

⇒ It provides the insights, patterns and the building blocks for integrating fundamental elements of SOA into a solution or enterprize architecture.

SOA reference model consists of following layers.

* Technology layer
* Application layer
* Services layers
* Business Process Layer
* Consumer layer
* Integration layer
* QoS layer
* Governance Layer

Functions of Each layers :-

1) **Technology Layer :-** This layer consists of variety of application, databases, code and operating system with the help of which service provider can create their services.

2) **Application Layer :-**

⇒ This layer basically serves as the service-repository of service provider, where variety of services can be stored at a common place.

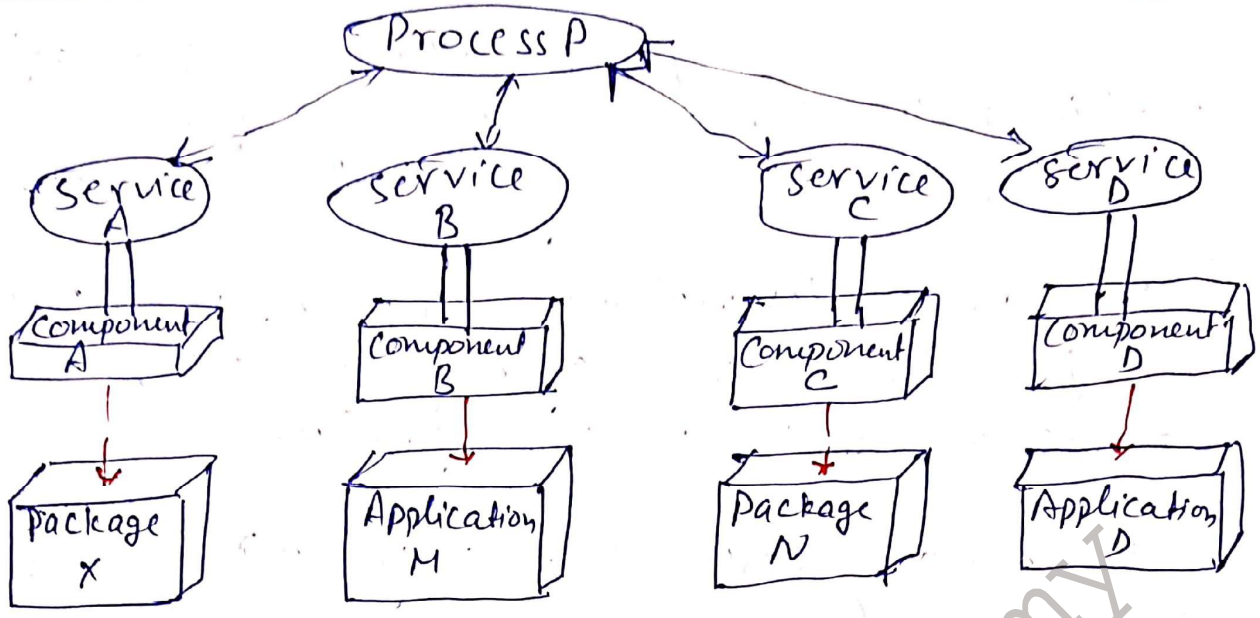
⇒ These services are ideally reusable ~~services~~ utility services which can be used by the service consumer.

⇒ Various service adapters are used here for integrating and transfering services to the next level. The various adapters that can be used here are as follows —

* FTP and File → For file exchange.
* JMS (Java Messaging Services)
* Message Queue. → For message exchange.
* Sockets → For Modeling standards.

⇒ UML can also be used in this layer for modeling of services which provide a standard way to visualize the design of the system.

Services Orchestration :



⇒ Service orchestration can be defined as the coordination and arrangement of multiple services exposed as a single service.

⇒ Service orchestration works through the exchange of messages in the domain layer of enterprise applications.

Consumer-Layer :

⇒ Consumer layer is the point where consumer interact with SOA.

⇒ It is the entry point for interactive consumers and services from external sources.

⇒ In this layer all the services are presented in such a form that user can view it and utilize it.

⇒ Backend integration is accomplished in this layer for integrating consumer layer with backend and legacy systems using SOAs so that users can use it according to their need.

Service Layer:

This layer consists of all the services defined within the SOA. Basically it defines the functional capabilities of all the services.

The service descriptions, contracts, and policies are given in this layer using predefined standards, and various formats.

The various responsibilities of service layer are as follows —

⇒ To identify and define services

⇒ To provide a container which houses the services.

⇒ To provide a registry that virtualizes runtime service access.

~~To provide a~~

Business Process Layer:

⇒ This layer supports and manages business processes and enables the SOA to orchestrate services to realize business processes.

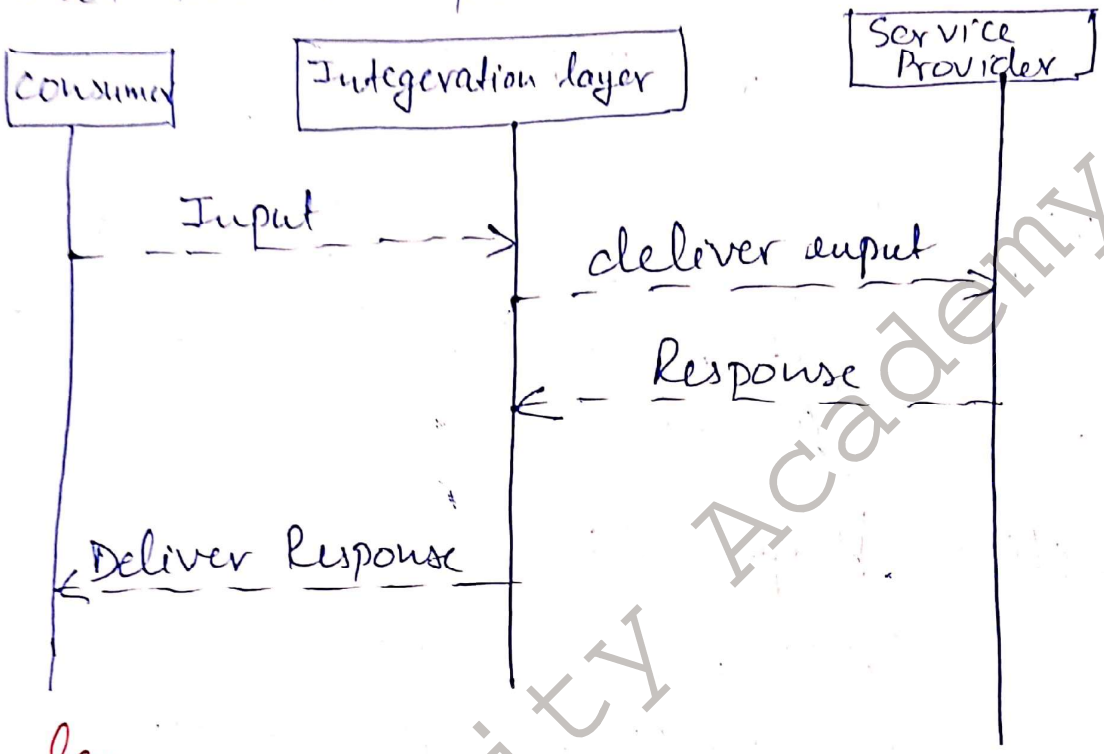
⇒ This layer covers process representation and composition and provides building blocks for aggregation.

⇒ This layer includes info exchange flow between participants (individual user or business entities), resources and processes.

⇒ BPEL and WF workflows supporting business processes are used for

Integration - Layer :

This layer provides the capability to mediate which includes transformation, routing and protocol conversions to transport service requests from the service requester to the correct service provider.



QoS layer:

This layer provides solution QoS mgmt of various aspects such as availability, reliability, security and safety as well as mechanism to support, track, monitor and manage solution QoS control.

Activities Performed in this layer:

1) Command and Control Management.
2) Security Management
3) IT system Monitoring & Management.
4) Application monitoring & Management.

5) Business Activity Monitoring & Management.
6) Event Management.
7) Policy Monitoring & Enforcement.

Governence Layer:

This layer ensures that the services and SOA solutions within an organization are adhering to the defined policies, guidelines and standards that are defined as a function of objective, strategies and regulations applied in the organization.

Activities Performed:

1) Defines Policies & compliance.
2) Monitors the health of SOA services.
3) Provides a consolidation point of business rules.

This layer includes both SOA governance as well as service governance.

Web Services:

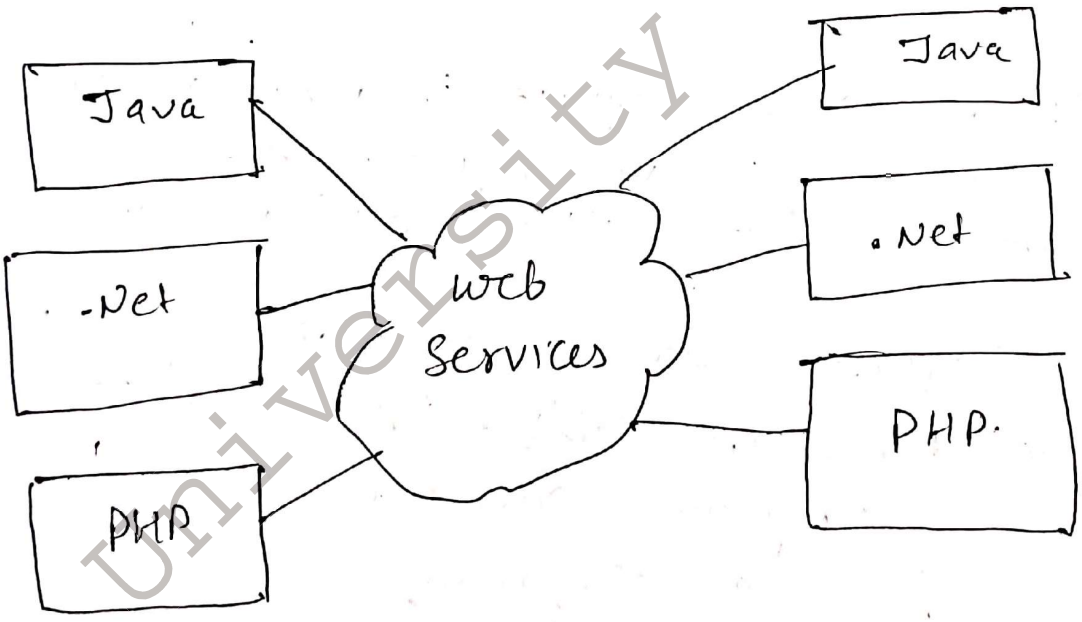
⇒ A web service is a collection of open protocols and standards used for exchanging data b/w applications or systems.

⇒ It is a technology to communicate one programming language with another.

ex:- java programming language can communicate with PHP and .Net by using web services.

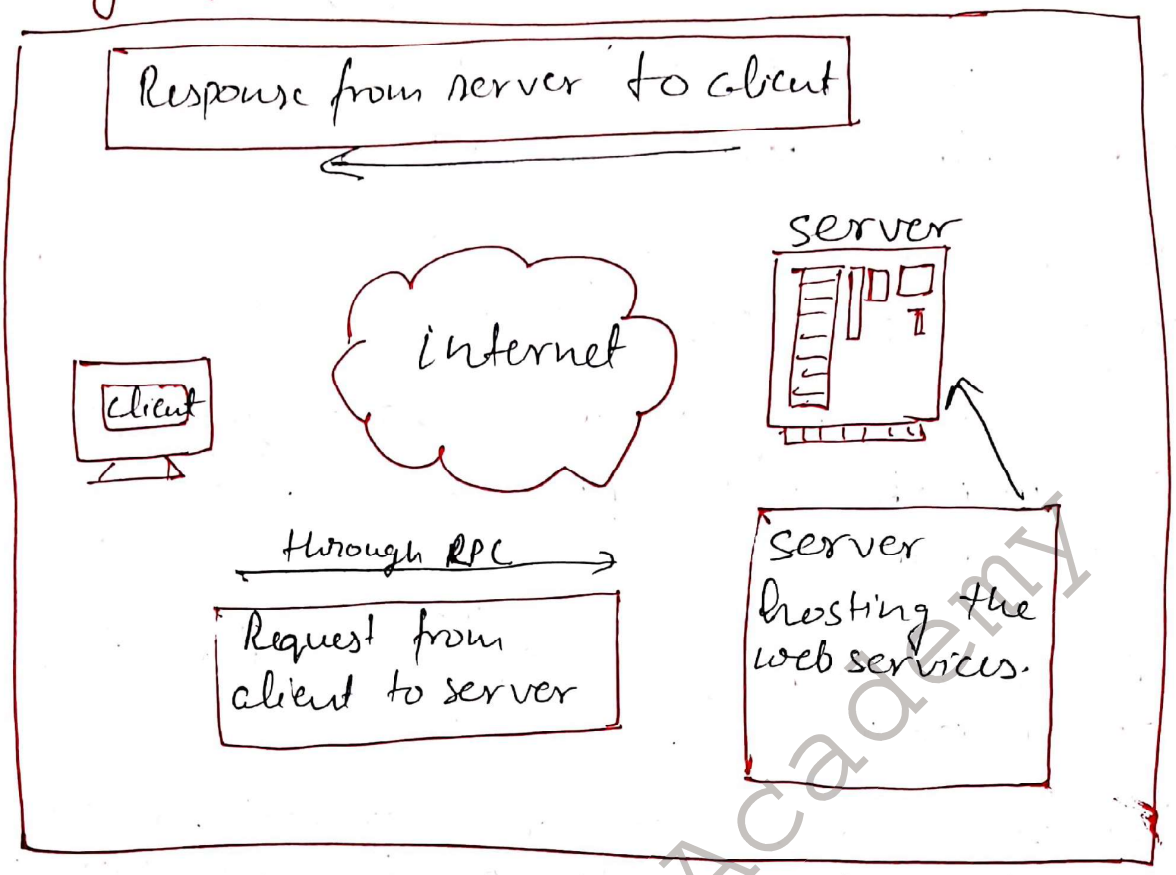
It is a s/w system for machine to machine interoperable communication.

⇒ The web services can be searched for over the internet and can also be invoked accordingly.



⇒ When invoked, the web services would be able to provide the functionality to the clients which invokes that web service.

Working of web-services: ~~Architecture~~



Steps:-

1) The client would request (invoke) a series of web service calls via requests to a server which would host the actual web service.

2) These requests are made through RPC (Remote Procedure Calls). RPC is a protocol that one program can use to request a service from a program.

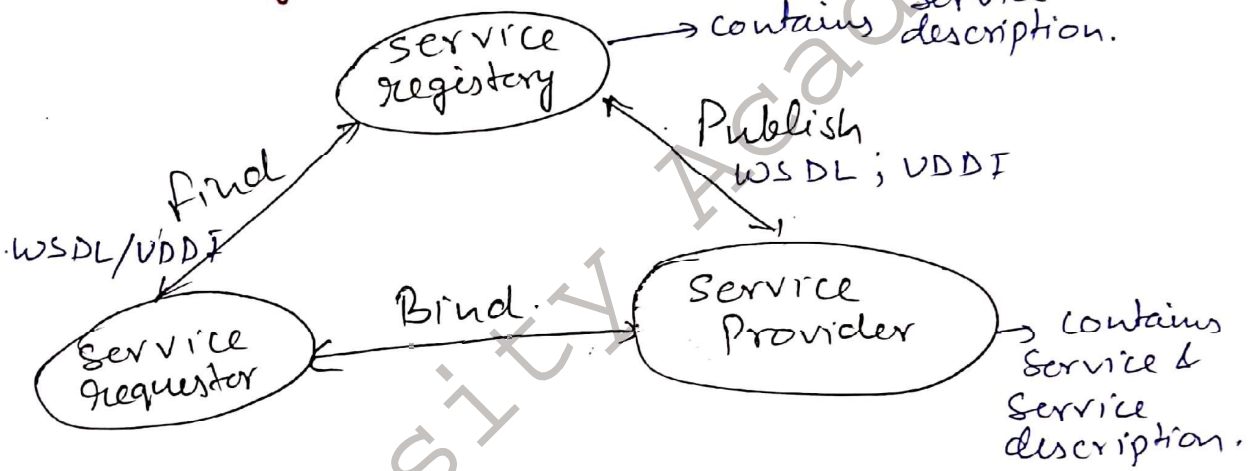
3) The data which is transferred b/w client and server is in XML, i.e the applications can talk to each other in XML.

4) Web services use SOAP protocol (Simple Object access Protocol) for sending the XML data b/w applications.

5) The data is sent over HTTP.

6) The data which is sent from the web service to the application is called SOAP message, which is actually an XML document.

Architecture of web services:-



Roles in web Service Architecture:

There are basically three roles in web service architecture.

i) **Service Provider:**

It is the platform that hosts the services.

(ii) **Service Requestor:**

* It is the application that is looking for and invoking or initiating an interaction with a service.
* The browser plays the requestor role, driven by a consumer.

(iii) Service Registry :-

Service requesters finds services and obtain binding info. for services during development

Operations in Web Service Architecture :-

(i) Publish :- for publication of service descriptions.

(ii) Find :- Finding of any service descriptions

(iii) Bind :- Invoking of service based on service descriptions.

REST (Representational State Transfer)

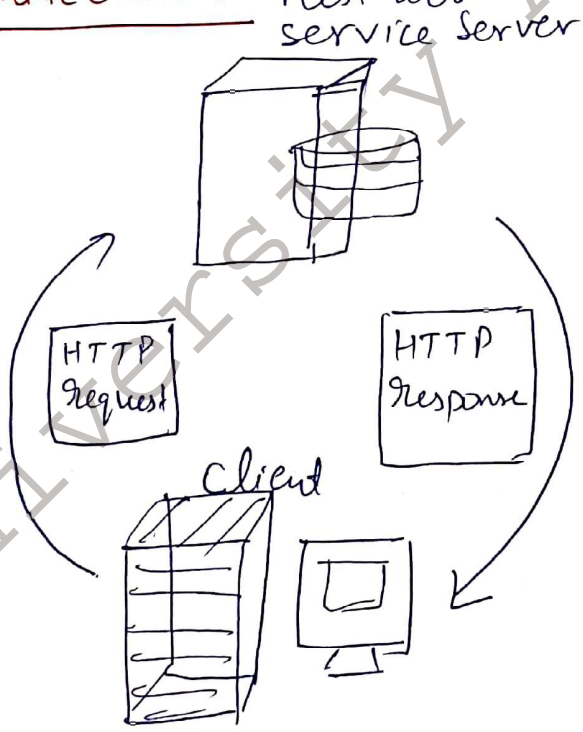
↳ a term coined by Roy Fielding in 2000.

It is an architectural style for designing loosely coupled applications over HTTP, that is often used in the development of web-services.

web services which follow the REST architectural style are known as RESTful web services.

Interaction in REST based system happen through ~~Hypertext~~ hypertext transfer Protocol (HTTP).

REST Architecture :



Basically it consists of :-

i) A client who request for the resources.

(ii) A Server who has the resources.

ex: Facebook, twitter, Google etc. exposes their functionality in the form of Restful web services

Architectural Constraints of RESTful API :-

There are six architectural constraints which can be used for implementing web services.

1) Uniform Interface :

It suggests that there should be an uniform way of interacting with a given server irrespective of device or type of application. (website, mobile app).

There are four guidelines principles of uniform interface are :-

a) Resource based :

Individual resources are identified in requests. ex :- API/users.

b) Manipulation of resources through representations :

Client contain enough infor to modify or delete the resource on the server, provided it has permission to do so.

c) Self descriptive Message :

Each message includes enough infor to describe how to process the message so that server can easily analyses the request.

d) Hypermedia as the Engine of Application State (HATEOAS) :

It needs to include links for each response so that client can discover other resources easily.

2. Stateless:

It means that the necessary state to handle the request is contained within the request itself and server would not store anything related to the session. i.e. client must include all the information.

3. Cacheable:

Every response should include whether the response is cacheable or not and for how much time response can be cached at the client side.

4. Client - Server:

REST API should have a client-server architecture.

Client can request for resources and not concerned with data storage.

Server holds the resources and are not concerned with user interface, or user state.

5. Layered System:

An application architecture needs to be composed of multiple layers. Each layer doesn't know anything about any other layer other than that of immediate layer.

There can be lot of intermediate servers b/w client and server.

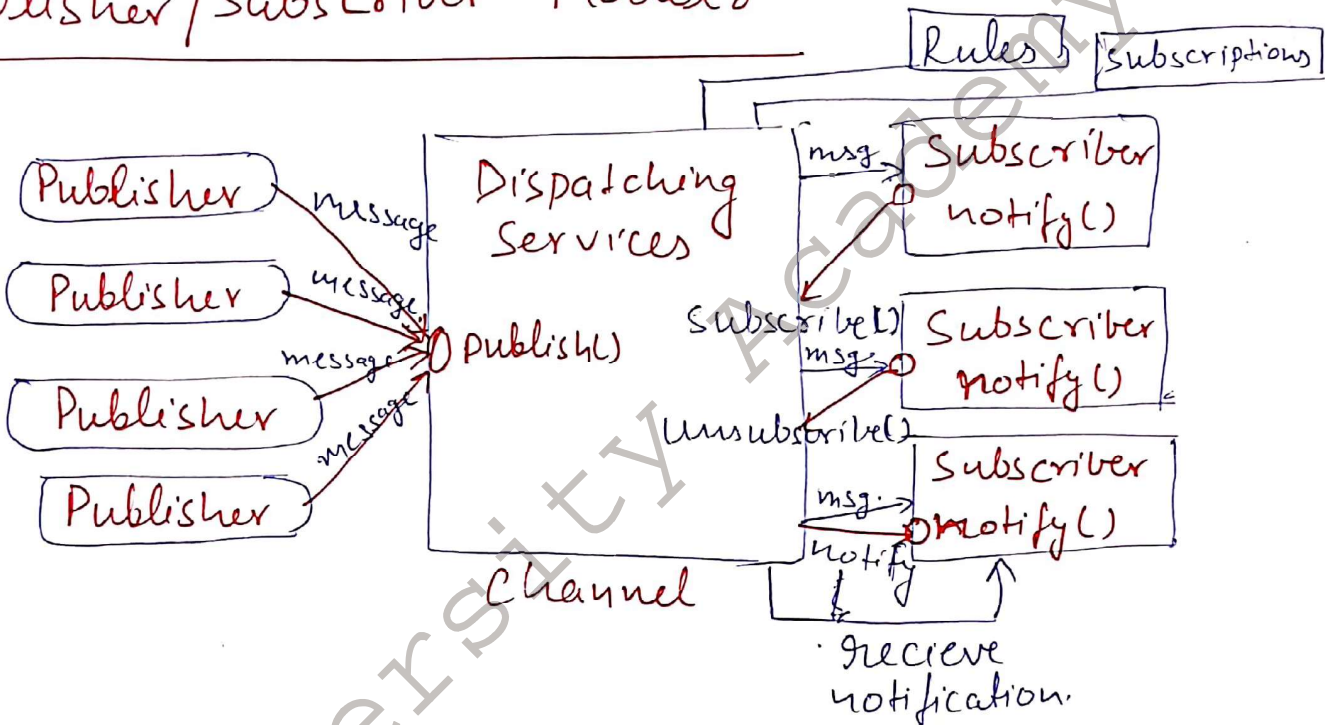
2.35

6- Code - on - demand:

It is optional feature.

Server can provide executable code to the client if demanded.

Publisher / Subscriber Model:



1- Publisher:

Publisher will publish the services i-e. post services or send messages to the channel.

2- Subscriber:

Subscribe to a category of messages.

3 - Channel:

Receives messages from publisher and maintain subscriber subscription.

Disadvantages of Publisher – Subscriber Models

1) Inflexibility of data sent by the publisher.
   ↳ i.e. changing the format of the message is not an easy task. It requires affirmation of all the publishers.

2) **Instability of Delivery:**
   i.e. Publisher does not have the perfect idea of the subscriber, sometimes unwanted or false subscribers can be there.

3) **Bottlenecks:**
   Sometimes load surges can slow down message sending, and subscriber gets a spike in the response time.

Process:-

* If publisher wants to publish any content using the channel, he sends the message to the channel using publish command.

* As soon as the content is published to the channel, all the subscribers gets a notification regarding the same and can check the content also.

* The activities that the subscriber can perform are :-
  (i) Subscriber can subscribe to the channel
  (ii) Subscriber can unsubscribe from the channel.

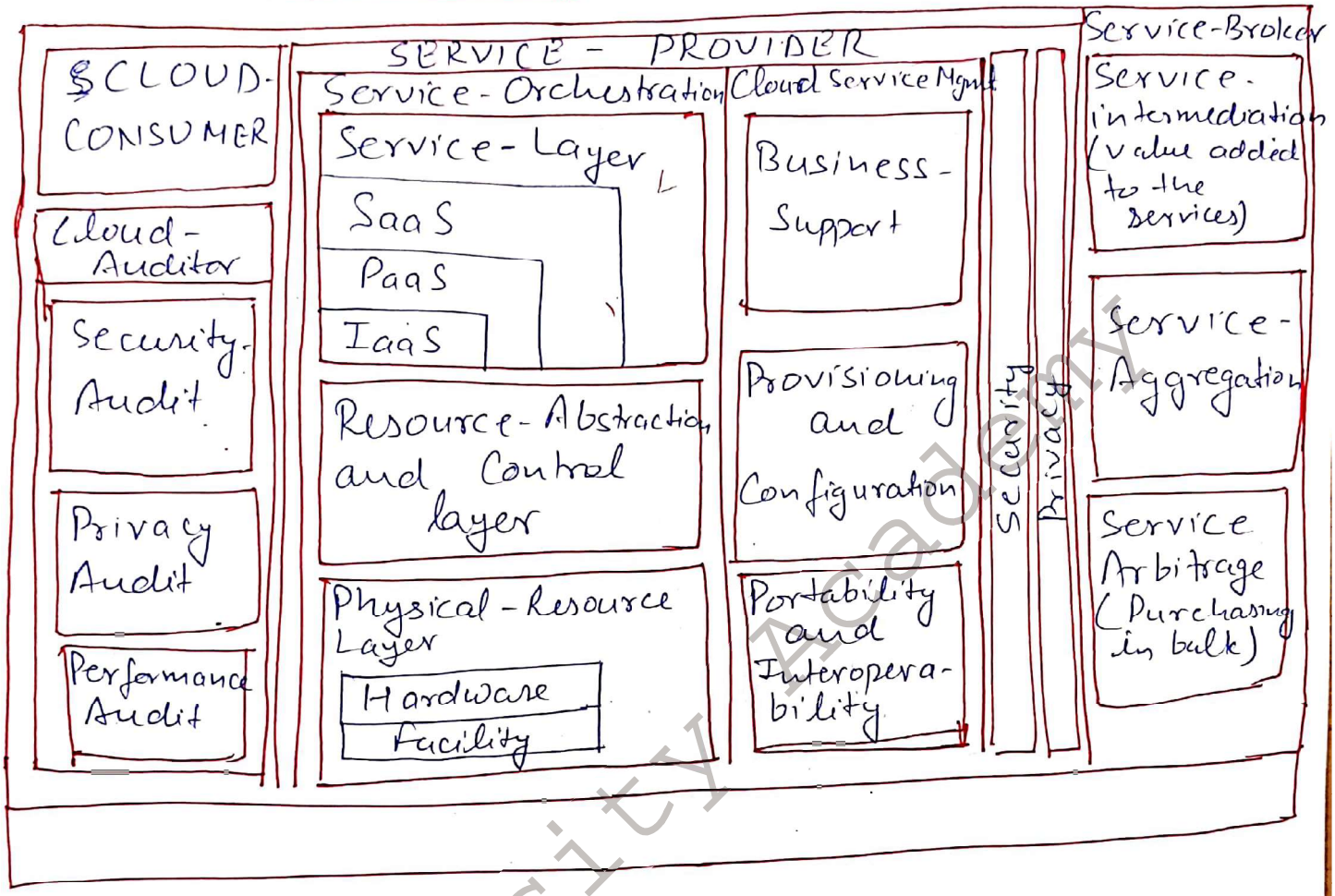
* Subscriber follows the rules & subscription methods provided by the channel.

* Advantages of Publisher - Subscriber Model :-

1) Low coupling on the publisher's end.
2) Reduced Cognitive load on the subscribers.
3) Separation of concerns
4) Improved testability
5) Improved security.

UNIT-3 Cloud Architecture, Services & Storage

Layered Architecture – NIST Cloud – Computing Reference Architecture (3.1)



1) Cloud Consumer :-

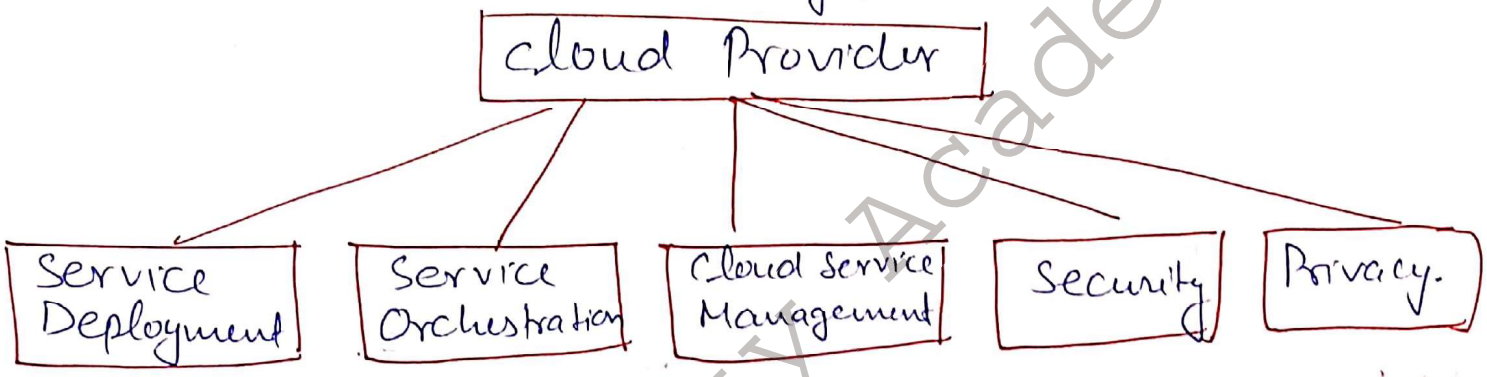
Cloud consumer is a client or user who has subscribed to the cloud services.

⇒ **Cloud Auditor :-** A party that can conduct independent check (assessment) of cloud services, information system operations, performance and security of the cloud computing implementation.

An entity that manages the delivery of cloud services & negotiates relationship b/w providers & consumers.

2) Service Provider :

- A cloud provider is a person, an organization.
- It is the entity responsible for making a service available to interested parties.
- A cloud provider acquires & manages the computing infrastructure required for providing the services, runs the cloud S/w that provides services and makes arrangements to deliver the cloud services to the cloud consumers through N/w access.



3) Service Broker :

- As cloud computing evolves the integration of cloud services that can be too complex for cloud consumers to manage.
- A cloud consumer can request services from the cloud broker.
- A cloud broker is an entity that manages the use, performance and delivery of cloud services & negotiates relationship b/w providers & consumers.

Software as a Service (SaaS):

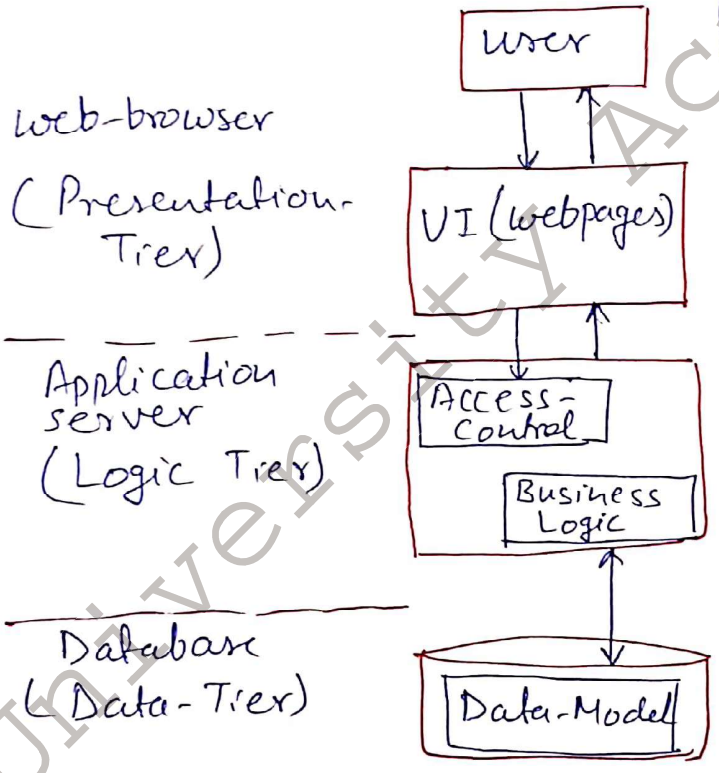
Features:

* Saas Model allows to provide software applications as a service to the users on subscription basis.

* It basically refers to a S/w that is deployed on a host server and is accessible via internet.

examples:- google apps, dropbox, Netflix etc.

Logical Architecture of SaaS:



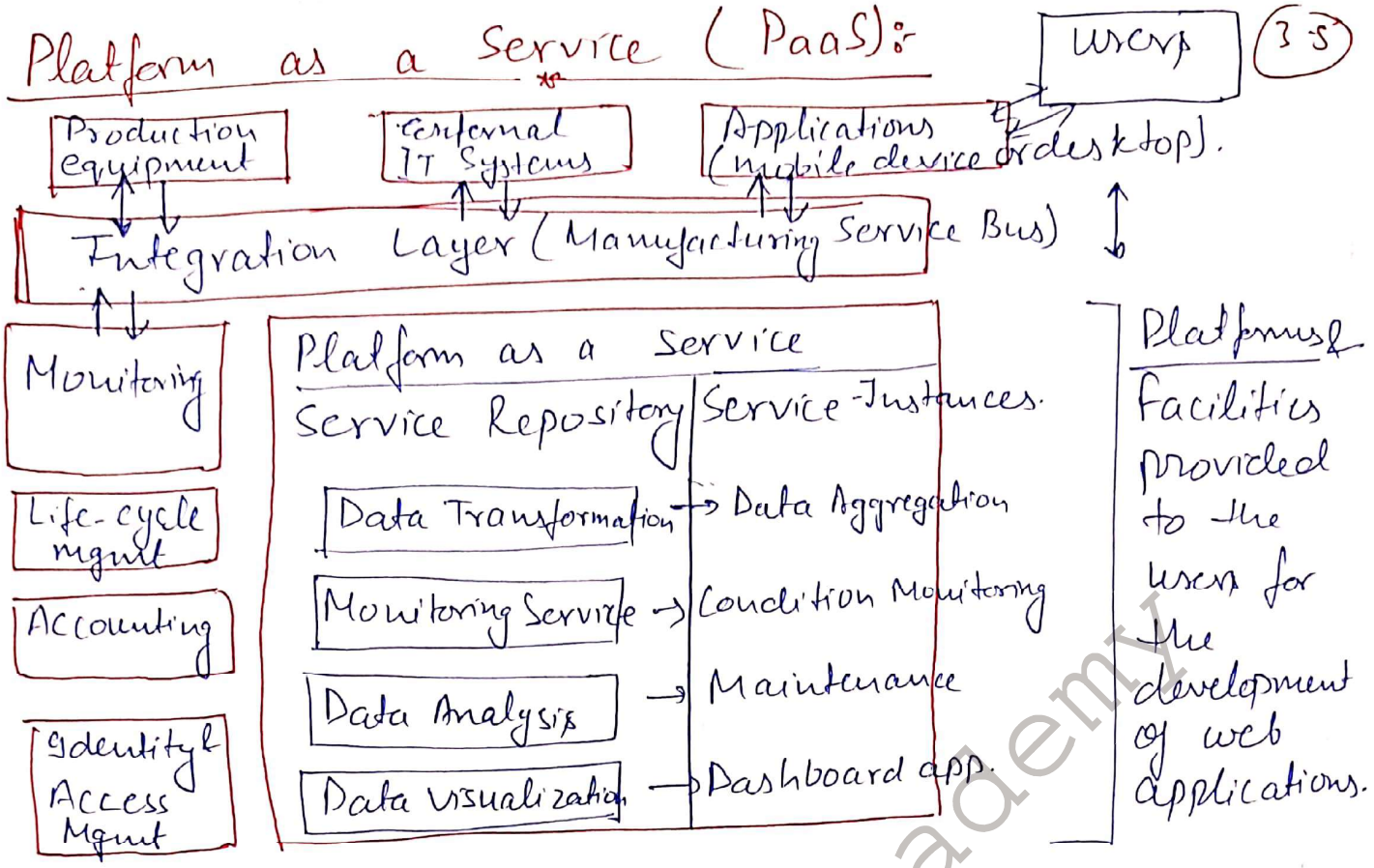
Advantages and Disadvantages of SaaS:

1) Lower up-front cost.
2) Quick setup and deployment.
3) Easy Updates.
4) Accessibility.

Disadvantages:

* Lack of Control
* Security & data Concerns.
* Limited range of applications.
* Connectivity requirement.

Platform as a Service (PaaS):



* Paas offers the runtime environment for applications. (browser based).

* It allows programmers to create, run and test, deploy web applications.

* It includes platform like middleware, development tools, database management systems, & business intelligence to support web application life-cycle.

* It provides built-in security, scalability & web services interfaces.

ex: Google app engine, Force.com, Azure.

In the above diagram it is show that how various services & Facilities (Platforms) are provided to the users for creation of web application.

Advantages and Disadvantages of PaaS:

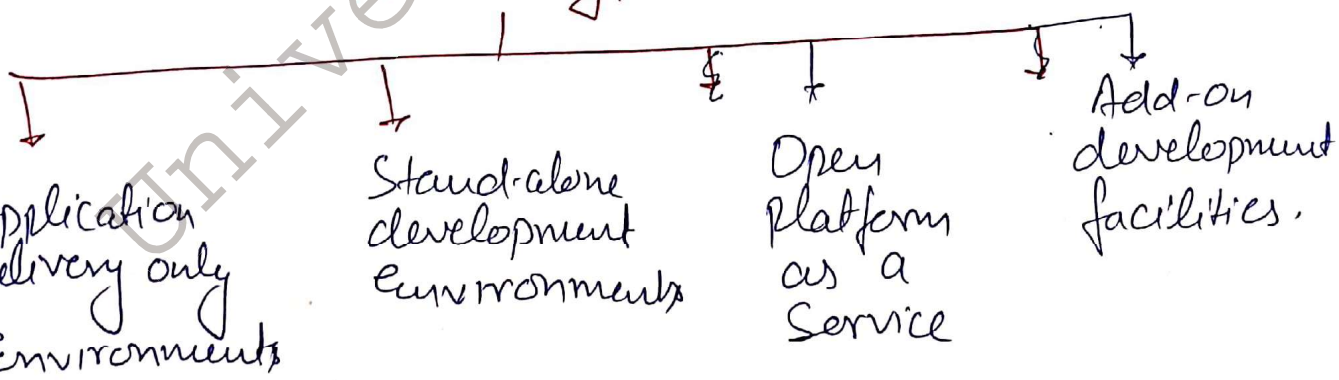
Advantages:

1) Simplified Development.
2) Lower Risk.
3) Prebuilt business functionality.
4) Scalability
5) Lower total cost of ownership.
6) More current system S/w.

Disadvantages:

1) Lack of portability. b/w PaaS Clouds.
2) Data Privacy.
3) Vendor lock-in

PaaS Types



Infrastructure as a Service:

Features:

An IaaS client is provided with infrastructures such as servers, networking, storage, virtual machines etc.

Customers access these resources on the internet using a pay-per-use model. via server virtualization.

Examples: AWS (Amazon web services).

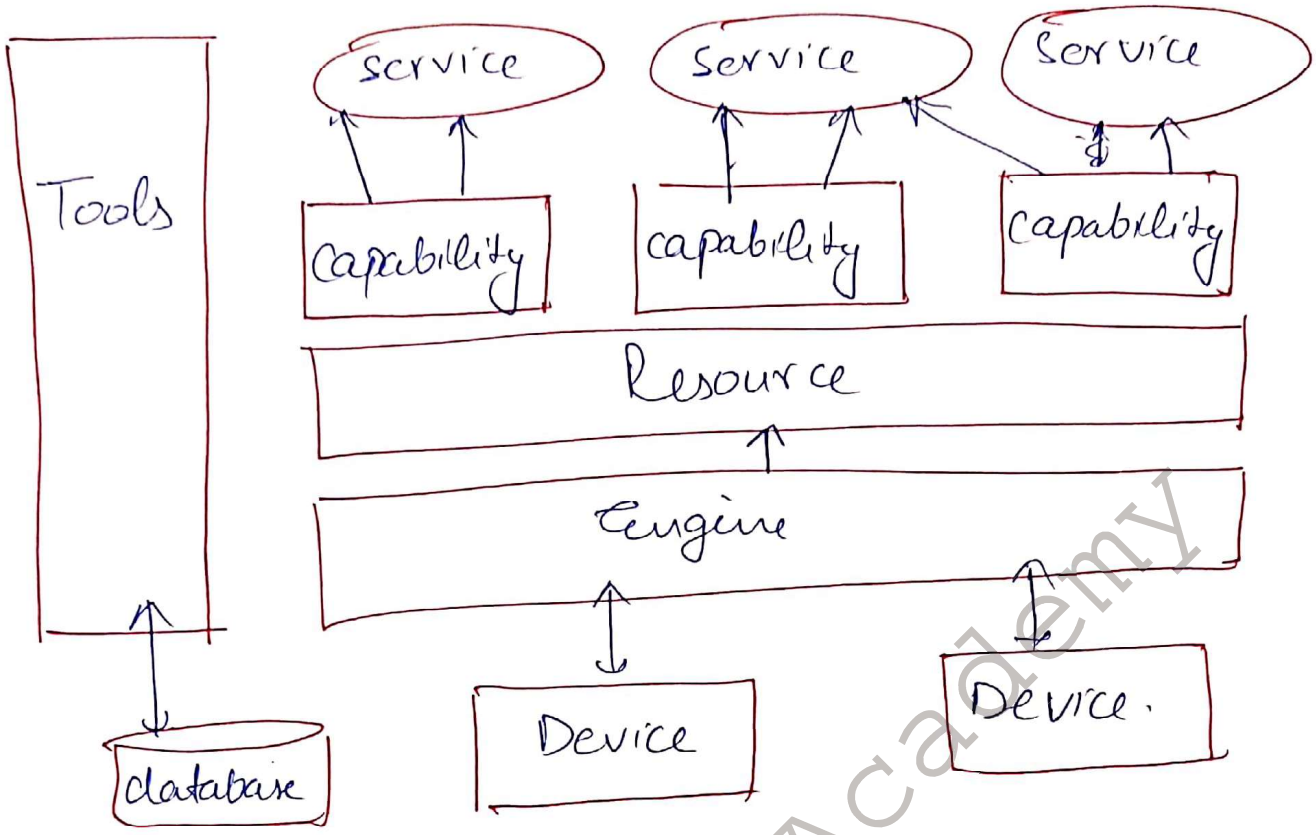
Advantages:

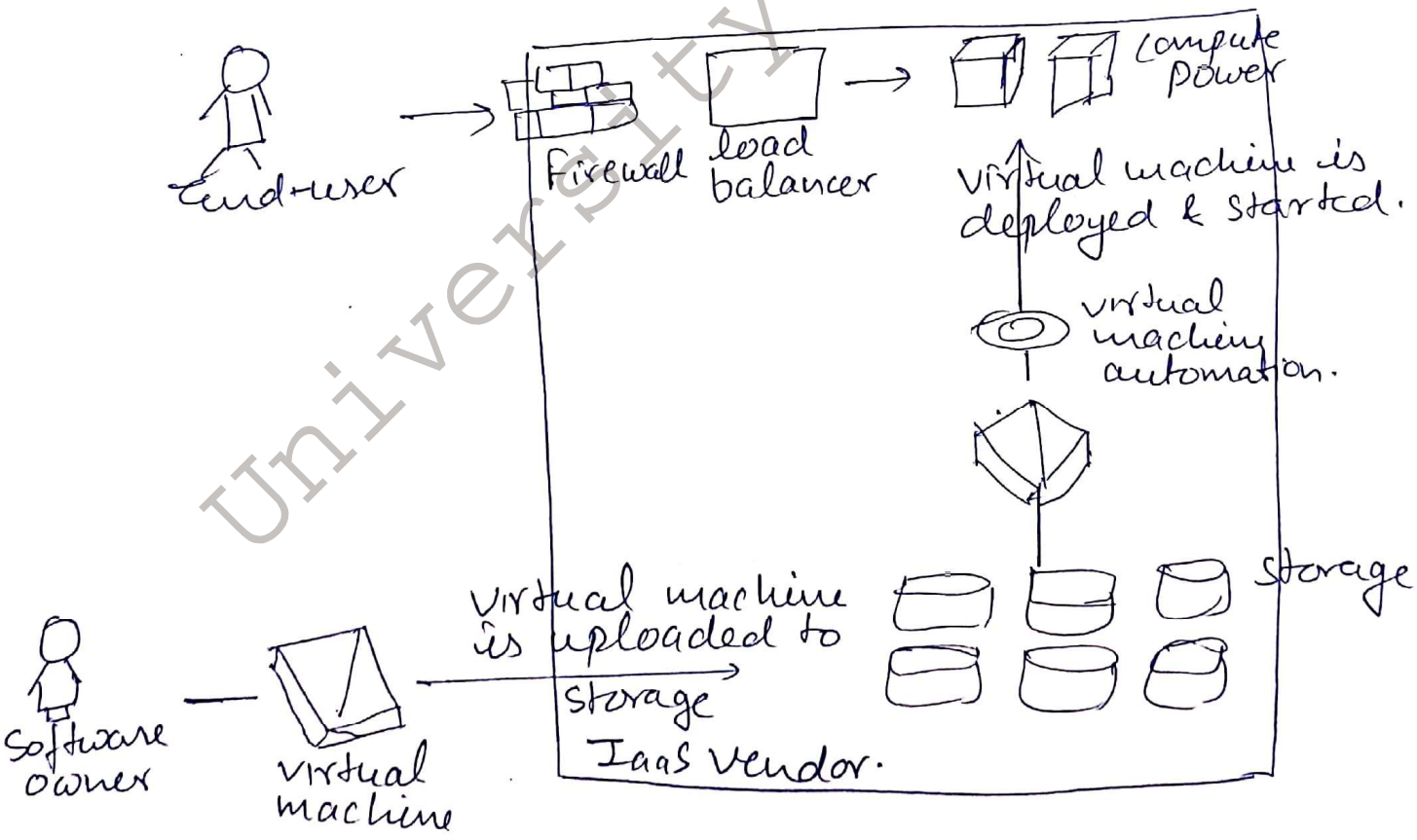
1) Shared infrastructure.
2) web-access to the resources.
3) Pay-as-per-use model.
4) On-demand scalability.
5) Focus on the core business.

Disadvantages:

1) Security Issues.
2) Interoperability issues.
3) Maintenance & Upgrade.

Infrastructure as a Service.





Cloud - Storage:

Cloud-storage is a service model in which data is transmitted and stored on remote storage systems, where it is maintained managed, backed up and made available to users over a network (internet).

Cloud storage is based on virtualized infrastructure with accessible interfaces.

Cloud based data is stored in logical pools across disparate, commodity server located on premises or in data centres managed by third party cloud-provider.

Using RESTful APIs, the various users are assigned an ID no.

When content needs to be retrieved, the user presents the ID to the system and the content is assembled with all its metadata, authentication & security.

Advantages:

1) Pay-for what is used.
2) Utility billing
   Global availability.
   Ease of use.
   offsite security
   Recovery, Security & accessibility.

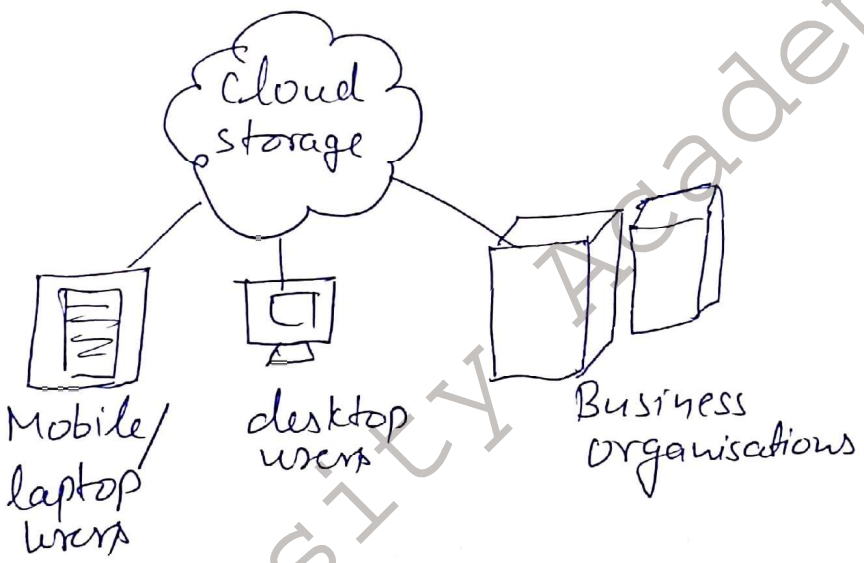
Disadvantages:

Backups may be slower.
Higher Internet Utilization.
Privacy concerns.

Storage as a Service (SaaS):-

* Storage as a service is a cloud business model in which a company rents its storage area (infrastructure) to another company or individuals to store data.

* The storage provider provides the client with the S/w required to access their stored data.



Advantages:-

1) Cost
2) Invisibility
3) Security
4) Automation
5) Accessibility
6) Syncing
7) Sharing
8) Collaboration
9) Data Protection
10) Dicaster Recovery

Cloud Storage Providers:

1) Amazon S3
2) iCloud
3) OpenDrive
4) Microsoft One Drive
5) Google Drive
6) Dropbox.
7) Amazon Cloud Drive
8) IDrive
9) IBackup
10) Livedrive
11) Polarbackup
12) Icedrive
13) Sync.Com
14) pCloud
15) Box

Amazon S3 :- (Amazon Simple Storage Service) :-

* This storage service will allow you to store and retrieve data in any amount from anywhere.
* It can be used by any sized business and by any industry.
* It is useful for storing the data of websites, mobile applications, IoT devices, enterprize applications, back up and big data analytics.

Features:

* Scalability
* Data availability
* Security
* Performance

OS Platform: web based

Price: Starting package starts at $0.023 Per GB.

website AmazonS3.

Public, Private and Hybrid Cloud: Comparison:

Difference	Private	Public	Hybrid
1) Tenancy	Single tenancy: there's only the data of a single organization stored in the Cloud.	Multi tenancy: the data of multiple organizations is stored in a shared environment	It consists of both single and multi-tenancy.
2) exposed to the public?	No, only the organization itself can use the private cloud services.	Yes, Anyone can use the public cloud services	Public cloud services are exposed while private cloud services are not.
3) Data Centre location.	Inside the organization's network	Anywhere on the internet where the cloud service provider's services are located.	For private inside the organisation while for public, anywhere on the internet

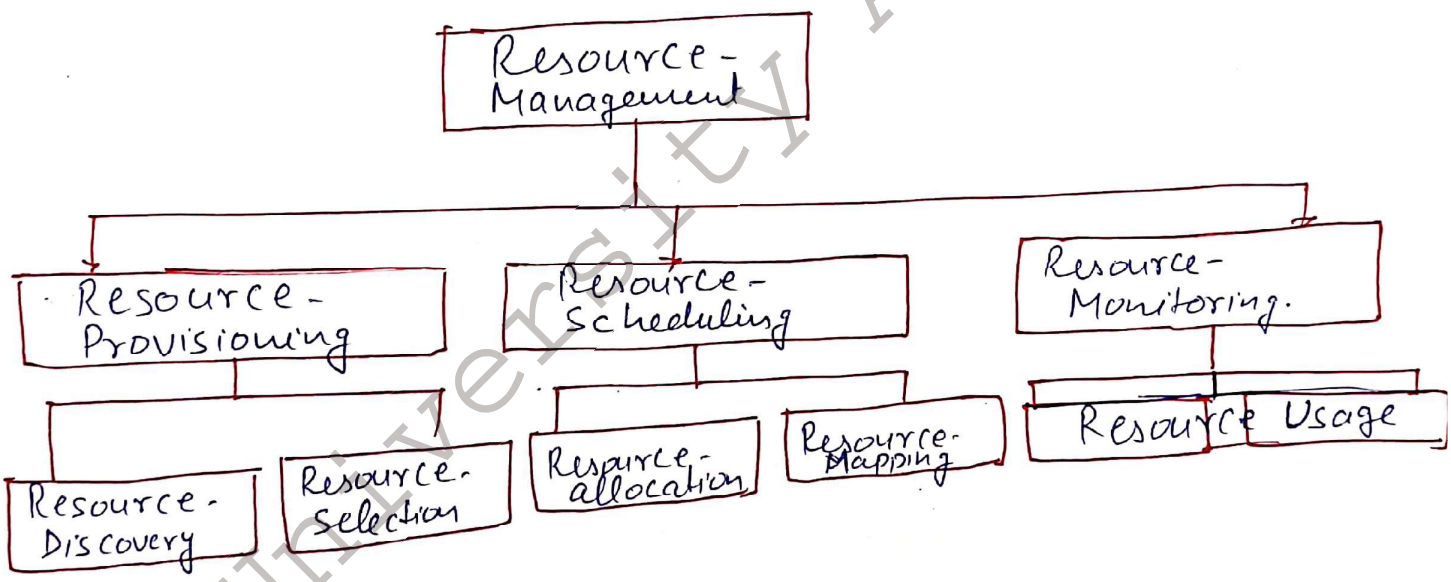
Difference	Private	Public	Hybrid.
4) Cloud-service Management	The organization must have their own administrators managing their private cloud services	The cloud service provider manages the services, where the organization merely uses them.	Private cloud services are managed by the organization itself while ~~public~~ ~~private~~ cloud services are managed by cloud service providers.
5) Hardware Components	Must be provided by the organization itself, which has to buy physical servers to build the private cloud	The cloud service provider provides all the hardware and ensures its working all the times.	For private, org will provide while for public cloud service provider will provide.
6) Expenses	Can be quite expensive, since the h/w, applications and networks have to be provided and managed by the organization itself.	Since, the cloud service provider has to be provide all the services so if we compare it with private cloud then it is less expensive as we can use these services by paying some amount only.	Less expensive as compare to private cloud model, because the public cloud model services costs less than private cloud model services.

Inter Cloud Resource Management:

The inter cloud resource management services are built to perform resource - discovery, match, select, composition, negotiate, schedule and monitor operations.

The S/W agents are built with decision-making and agent interaction features. to communicate with coordination, and cooperation.

Taxonomy of Inter-Cloud resource Mgmt: (Methods):



Resource Provisioning:

Resource Provisioning means selection, deployment and run-time management of the software (like database server management systems, load balancers) and hardware resources (like CPU, storage and network) for ensuring guaranteed performance of applications.

Types/Methods of Resource Provisioning:

1) Static Provisioning
2) Dynamic Provisioning.
3) User - Self Provisioning

1) Static Provisioning:

* For applications that have predictable and generally unchanging demands / workloads, static provisioning is used effectively.

* The customer contracts with the service provider for services and the provider prepares the appropriate resources in advance of start of service.

The customer is charged as flat fee or is billed on monthly basis.

2) Dynamic Provisioning:

* In cases where demand by applicants may change or vary, "dynamic provisioning" technique have been used.

* With dynamic provisioning, the provider allocates more resources as they are needed and removes them when they are not.

* The customer is used on a pay-per-use basis.

3) User Self-Provisioning:

With user self provisioning, the customer purchases resources from the cloud-provider through a web-form, creating a customer account and paying for resources with credit card.

Methods/Techniques of Resource-Provisioning:

1) Demand-Driven Method - provides static resources.
2) Event Driven Method - based on predicted workload by time.
3) Popularity driven Method - based on internet traffic monitored.

1) Demand Driven:

This method adds or removes computing instances based on the current utilization level of the allocated resources.

When a resource has surpassed a threshold for certain amount of time, this scheme increases the resources.

When a resource is below a threshold for a certain amount of time, that resource can be decreased accordingly.

2) Event Driven:

This scheme adds or removes machine instances based on a specific time event.

This scheme works better for seasonal or predicted events.

During these events, the no. of users grow before the event period and then decreases during the event period.

This scheme anticipates peak traffic before it happens.

The method results in a minimal loss of QoS, if the event is predicted correctly.

3) Popularity Driven:

In this method the internet searches for popularity of certain applications and creates the instances by popularity demand.

The scheme anticipates increased traffic with popularity.

The scheme has minimal loss of QoS if the predicted popularity is correct.

Resources may be wasted if traffic does not occur as expected.

Global Exchange of Cloud Resources:

Limitations of Present Service Providers:

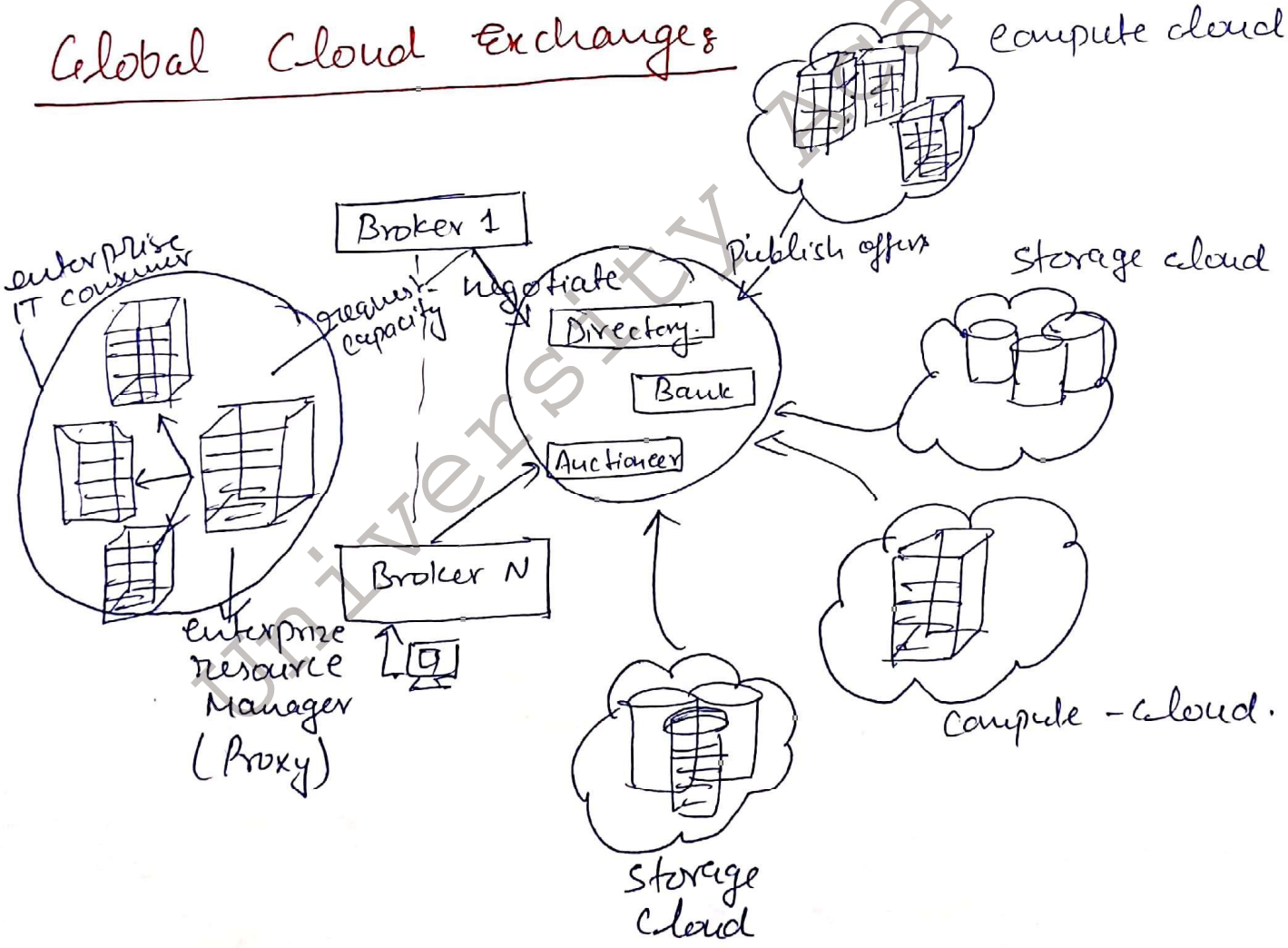
Inflexible Pricing

Consumers are restricted to offering from a single provider at a time.

Unable to swap from one provider to other.

No standard interface.

Global Cloud Exchange:



Entities of Global Cloud Exchanges

Market Directory.
Banking System
Brokers
Price Setting Mechanism
Admission Control Mechanism.
Resource Management System.
Consumers Utility functions.
Resource Management Proxy.
Enterprise IT consumer.

Cloud - Security - Overview

Definition:

⇒ Cloud security consists of set of policies, controls, procedures and technologies that work together to protect cloud based-systems, data and infrastructure

⇒ These security measures are configured to protect cloud data, support regulatory compliance and protect customers privacy as well as setting authentication rules for individual users and devices.

⇒ The way cloud security is delivered will depend upon the individual cloud provider or the cloud security solution in place.

Cloud Security challenges / Issues:

1-> Data loss

2- Hacked Interfaces and Insecure APIs.

3- Data breach: It is the process in which confidential data is viewed, accessed and/or stolen by the third party without any authorization, so organization's data is hacked by the hackers.

4) Vendor-lock-in:

Organization may face problems when transferring their services from one vendor to another. As different vendor provide different platforms, that can cause difficulty moving one cloud to another.

5) Denial of Service attack:

=) Denial of service (DoS) occurs when the system recieves too much traffic to buffer the server.

=) A DoS attack prevents the users from accessing a service by overwhelming either its physical resources or network connections.

=) The attack essentially floods the service with so much traffic or data that no one else can use it until the malicious flow has been handled.

6 Account Hijacking.

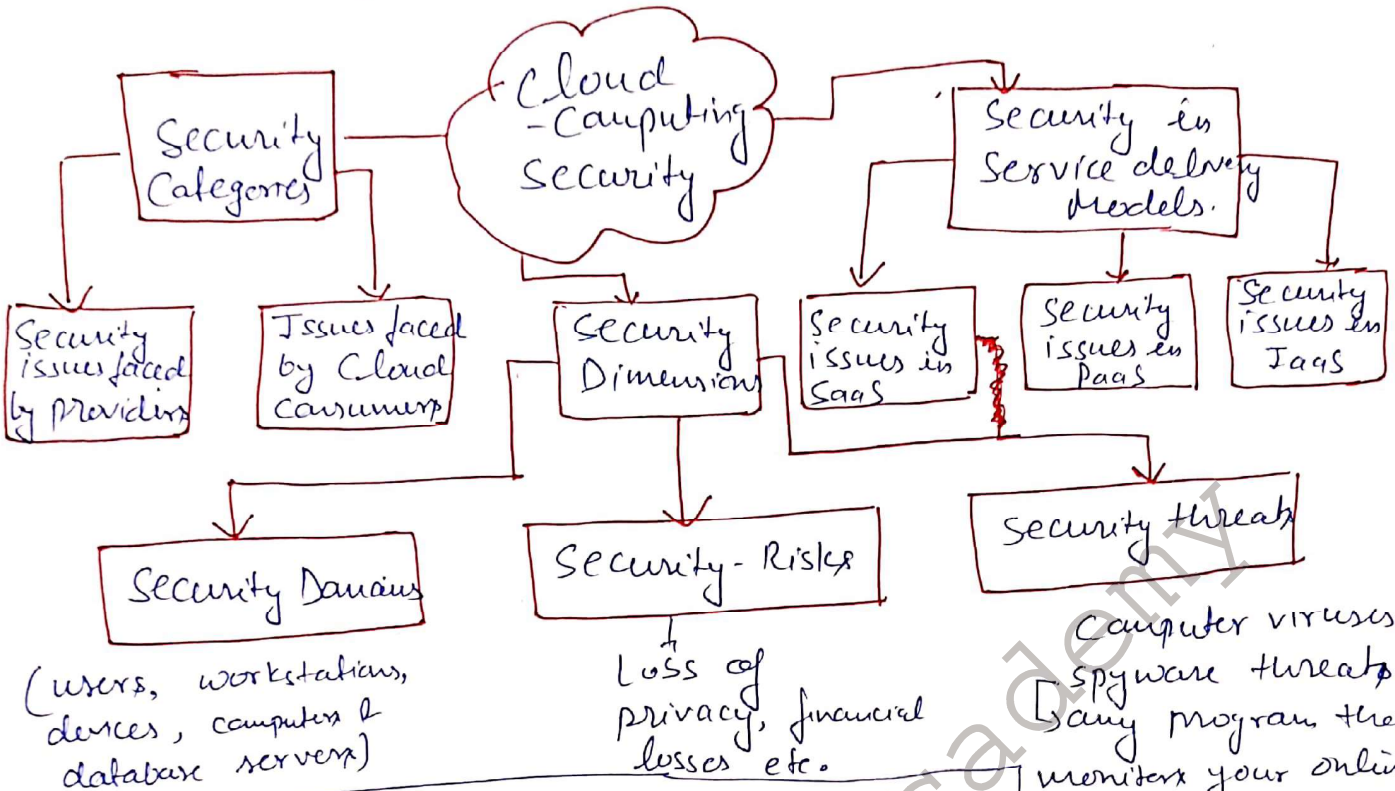
7 Misconfiguration

8 Accidental exposure of Credentials.

9 Cyberattacks

10 Data Privacy & Confidentiality.

Categories of Cloud-Computing Security:



Cloud Computing security refers to a broad set of policies, technologies and controls deployed to protect data, applications and associated infrastructure of cloud computing.

⇒ Cloud Computing security can be classified as follows:

1- Security Categories
2- Security Dimensions
3- Security in Service Delivery Models.

1) Security Categories:

It can be classified into two parts.

a) Security issues faced by providers → resource security, computer system security

b) Security issues faced by cloud-consumers.
- attack on authenticity
- " " privacy
- loss of data.

2- Security Dimensions :-

Security Dimensions can be categorized as follows :-

a- Security Domains
b)- Security Risks
c) Security threats.

a) Security Domains :-

Security domain includes various users, workstations, devices, computers and database servers.

b) Security Risks :-

Data loss is the most common security risk of cloud computing

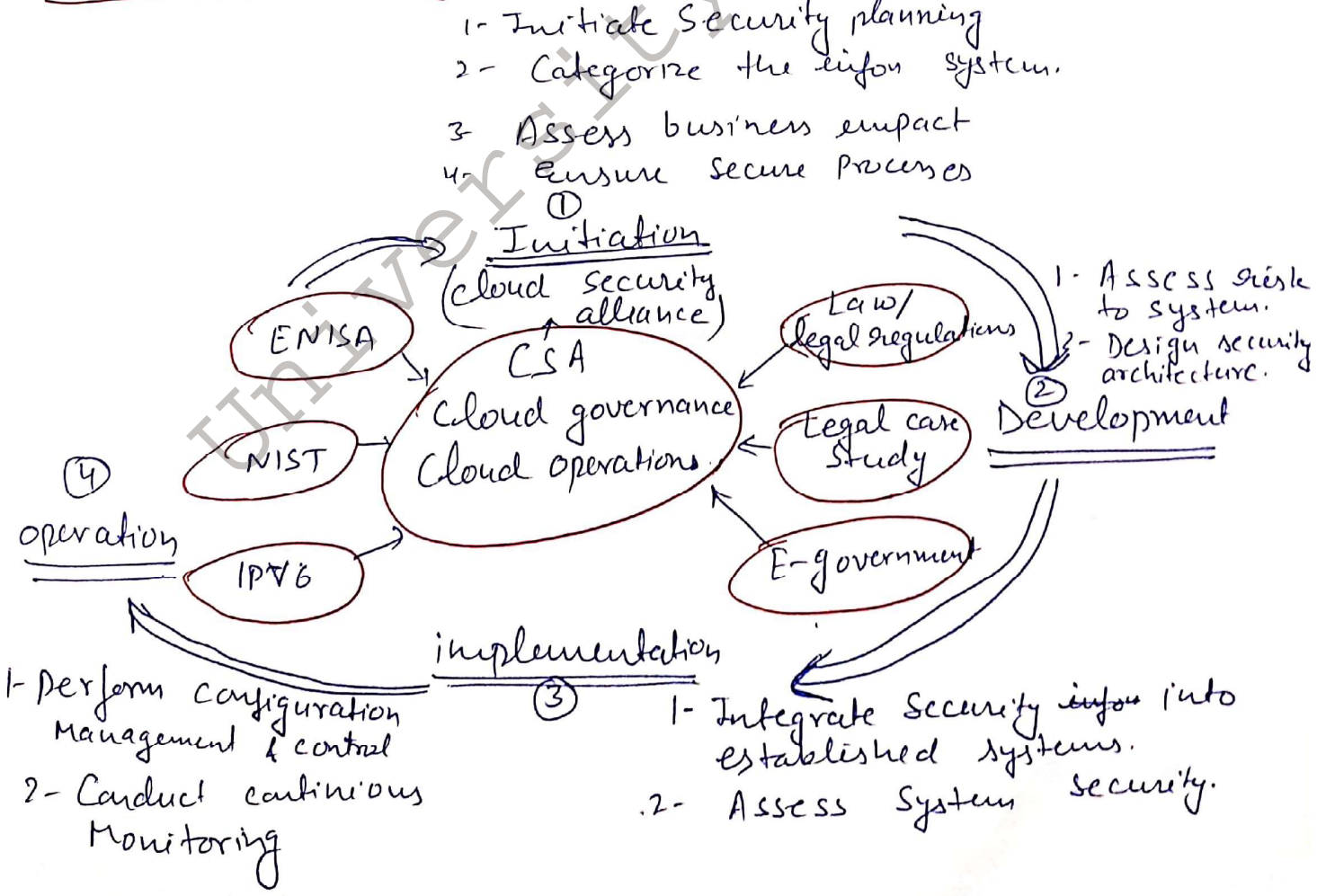
Security Governance :-

Cloud security governance refers to the management model that facilitates effective and efficient security management and operations in the cloud environment to achieve business targets.

This model incorporates a hierarchy of :-

⇒ executive mandates
⇒ Performance expectation
⇒ Operational Practices
⇒ Structure and metrices for optimization.

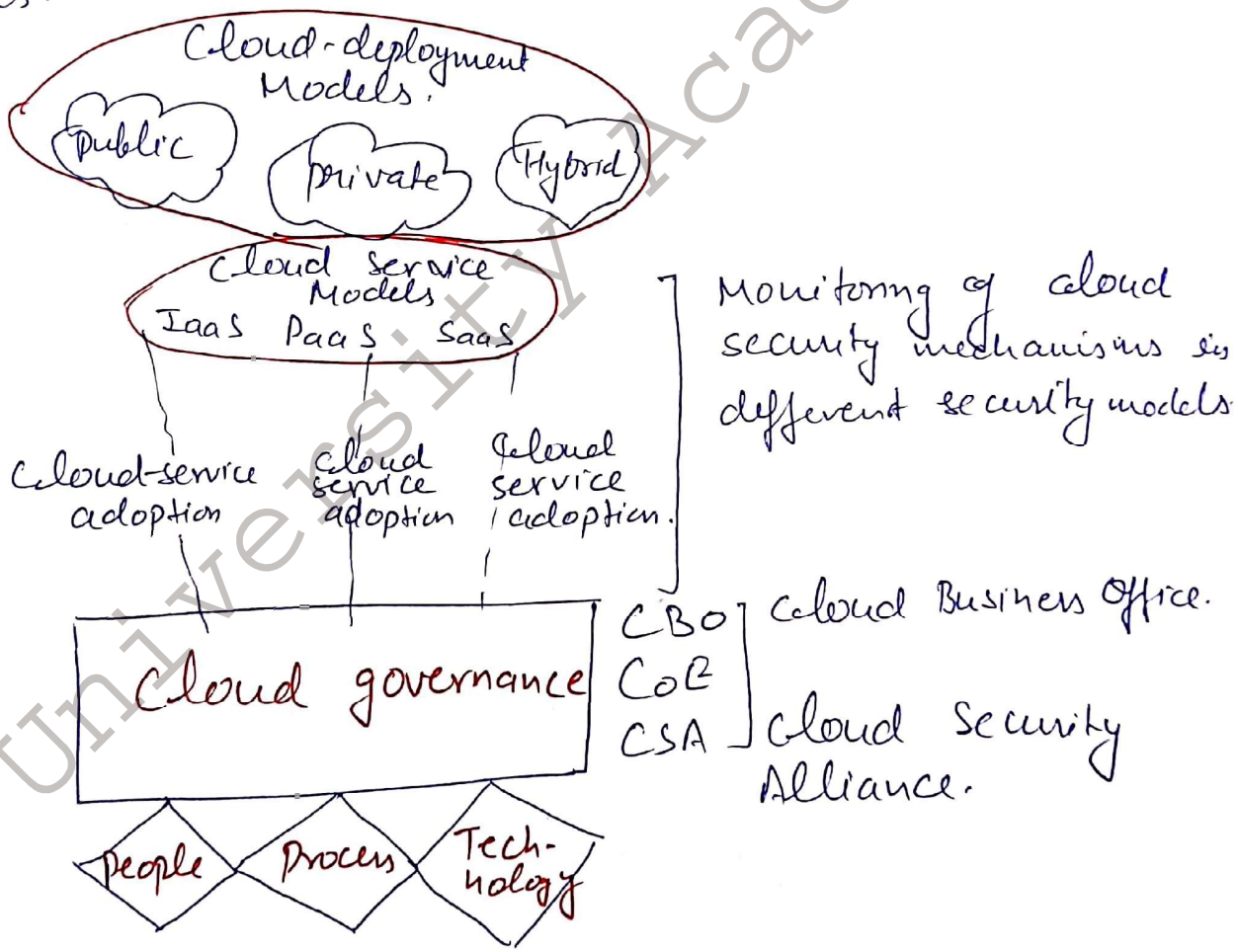
Cloud Security Governance Deployment framework :-



Cloud governance is a framework to govern the use of cloud services.

It encompasses people, processes & technology while ensuring security cost management & deployment acceleration.

It helps in regulating and controlling the use of cloud services by defining processes, standards & policies to be followed in planning, on boarding and managing cloud services.



(9) Elements of Cloud Governance Security Model:

* Cloud Business office (CBO) for ensuring that governance is enforced across the enterprise.
* Cloud CoE, a cross functional team that defines processes, regulates and standardizes cloud adoption, migration & operation across the enterprise.
* Cloud governance organization structure.
* Cloud governance process around the cloud service lifecycle.
* Cloud foundational components like cloud reference architecture, standards, templates, guidelines, best practices & policies.
* CSA → which is a nonprofit organization that describes the best practices for securing cloud computing.
  → (Cloud security Alliance)

Virtual Machine Security in Cloud-Computing :-

(4-14)

Since virtual machine is composed of many entities and resources, so for ensuring security within virtual machine, we need to secure all the resources, softwares and hardware to which virtual machine is composed off. So it includes the security of following resources.

1- Hypervisor Security

2- VM identity security

3- VM server security

4- Securing host resources

5- Virtualization sw security.

It is the responsibility of CSP (cloud-service Provider) to manage all these security issues that can arise during the cloud-computing process.

IAM Security Mechanism & Standards :-

(Identity and Access Management)

IAM is about defining and managing the roles and access priviledges of individual users and circumstances in which users are granted those priviledges.

The core objective of IAM systems is one digital identity per individual, and when this identity is created, it must be maintained, modified and monitored throughout the each users "access life-cycle".

Components of IAM :-

1) **Authentication :-**
   - username + password
   - Digital signatures
   - Digital certificates
   - Biometric

2) **Authorization :-** It basically deals with access control. i.e. user is authorized to access which resources.

User → R_1 (authorized)
User → R_2 (not authorized)

3- User Management (Administrative) :- The main functions of this component are :-

→ Creating new user

→ Adding user to required access group.

→ Maintaining Password Policies, privileges.

4) Credential Management :- Access control rules for defined user accounts.

⇒ Establishes identities and access control rules for users.

IAM Standards :-

1) LDAP (Lightweight Directory Access Protocol)

2) MFA (Multifactor authentication)

together with user name and password it requires authentication to a user system.

3) Risk based Authentication (RBA) :-

Dynamic adjustment of user's requirement- based on the user's situation.

4) Single - Sign on :-

with single credential multiple systems can be accessed.

5) User behaviour Analytics :-

examining the pattern of user behaviour.

Hadoop:

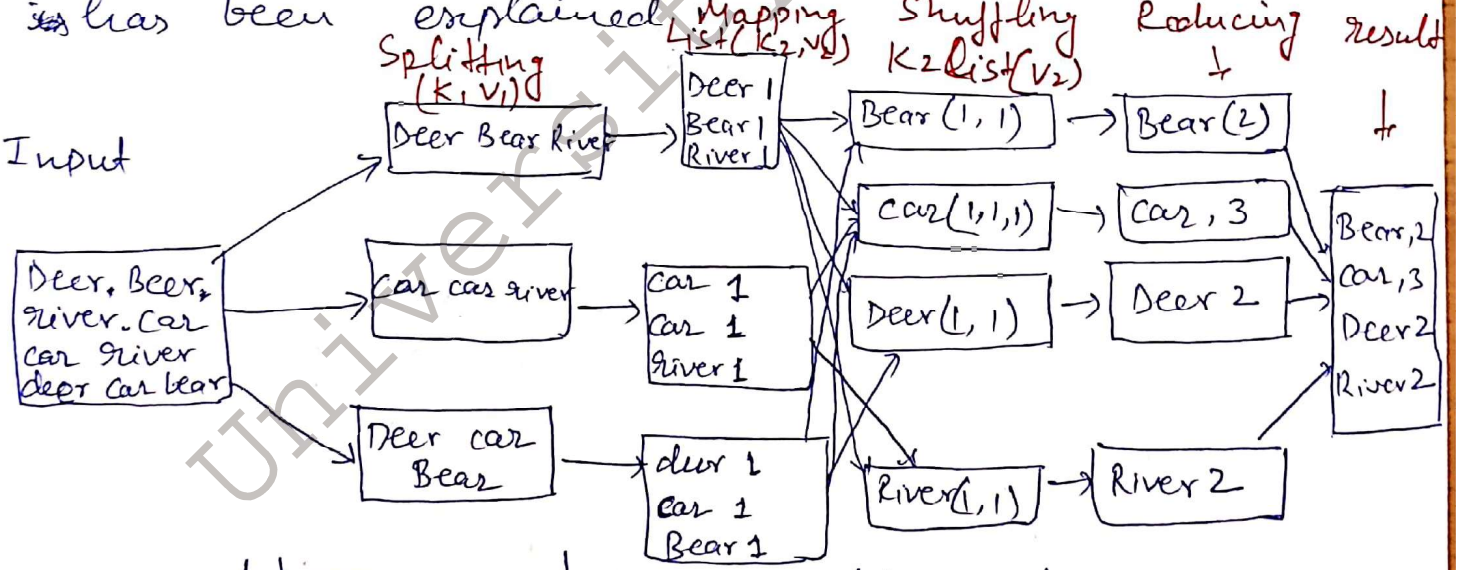
MapReduce:

* A MapReduce is a data processing tool which is used to procss the data parallely in a distributed form.

* In this we design some algorithms which divides the task into small parts and assigns them to many computers and collects the result from them, which when integrated generates data sets.

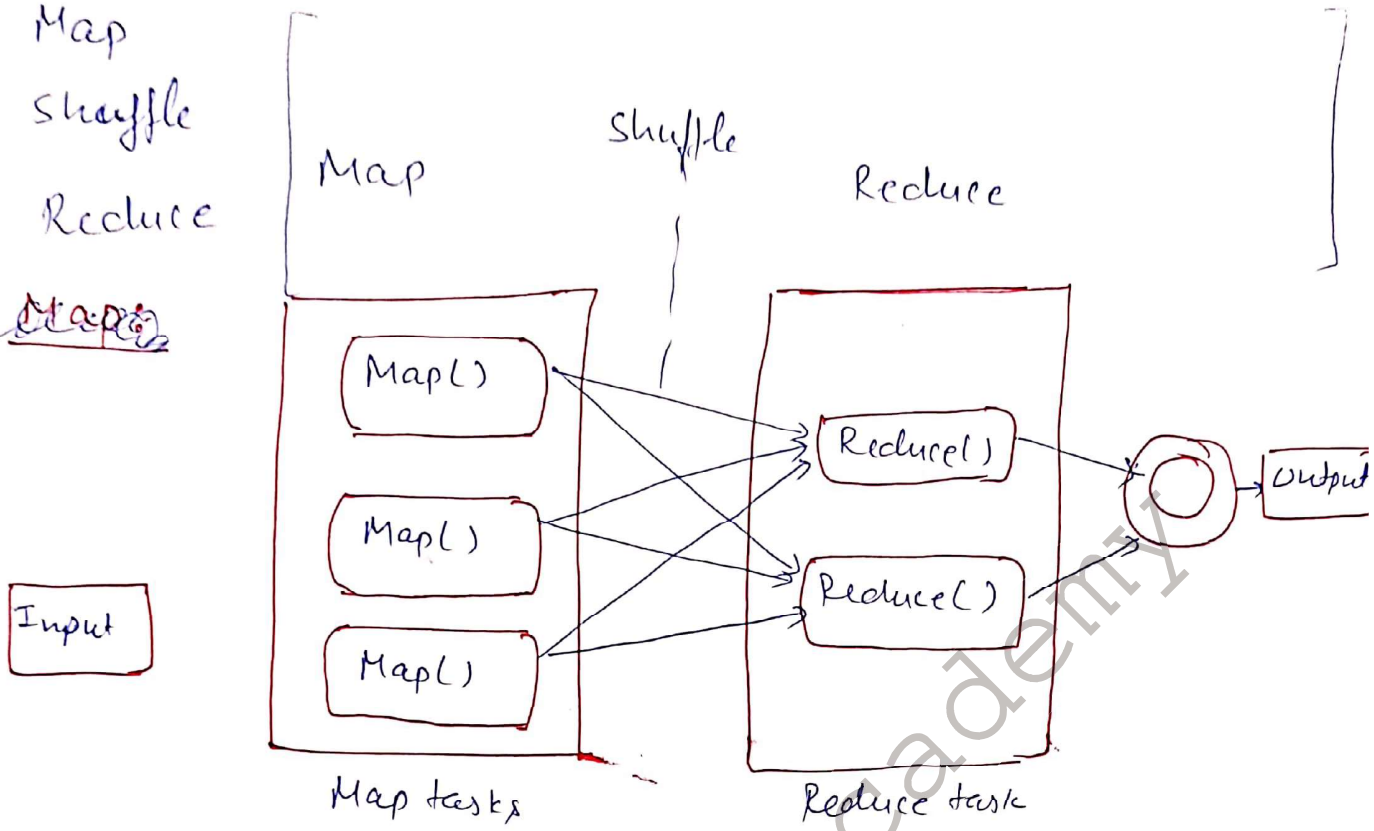
Working of Map reduce:

⇒ By taking one example we can understand this process. Here the example for word count has been explained.



Steps in MapReduce:

1. Map
2. Shuffle
3. Reduce



1. Map:

The map takes the data in form of pairs and returns a list of <key, value> pairs. The keys will not be unique in this case.

2. Shuffle:

Using the output of map, sort and shuffle are applied. This sort and shuffle acts on these list of <key, value> pairs and sends out unique keys and a list of values associated with this unique key <key, list(values)>.

3. Reduce:

An output of sort and shuffle sent to the reducer phase. The reducer performs a defined function on a list of values for unique keys, and final output <key, value> will be stored/displayed.

Hadoop:-

Hadoop is an open source, java based framework used for storing and processing big data.

Big data:

It is a term that describes the large volume of data which is yet growing exponentially with time.

ex:- social media sites, stock exchange etc.

Benifits of Hadoop:

1- **Resilience:**

Data stored in any node is also replicated in other nodes of the cluster.

2- **Scalability:**

Hadoop is scalable because it operates in distributed environment. As need arises setup can be easily expanded.

3- **Low Cost:**

As Hadoop is an open source framework, with no license to be procured, the costs are relatively lower compared to ~~traditional~~ relational database systems.

4- **Speed:**

Very fast.

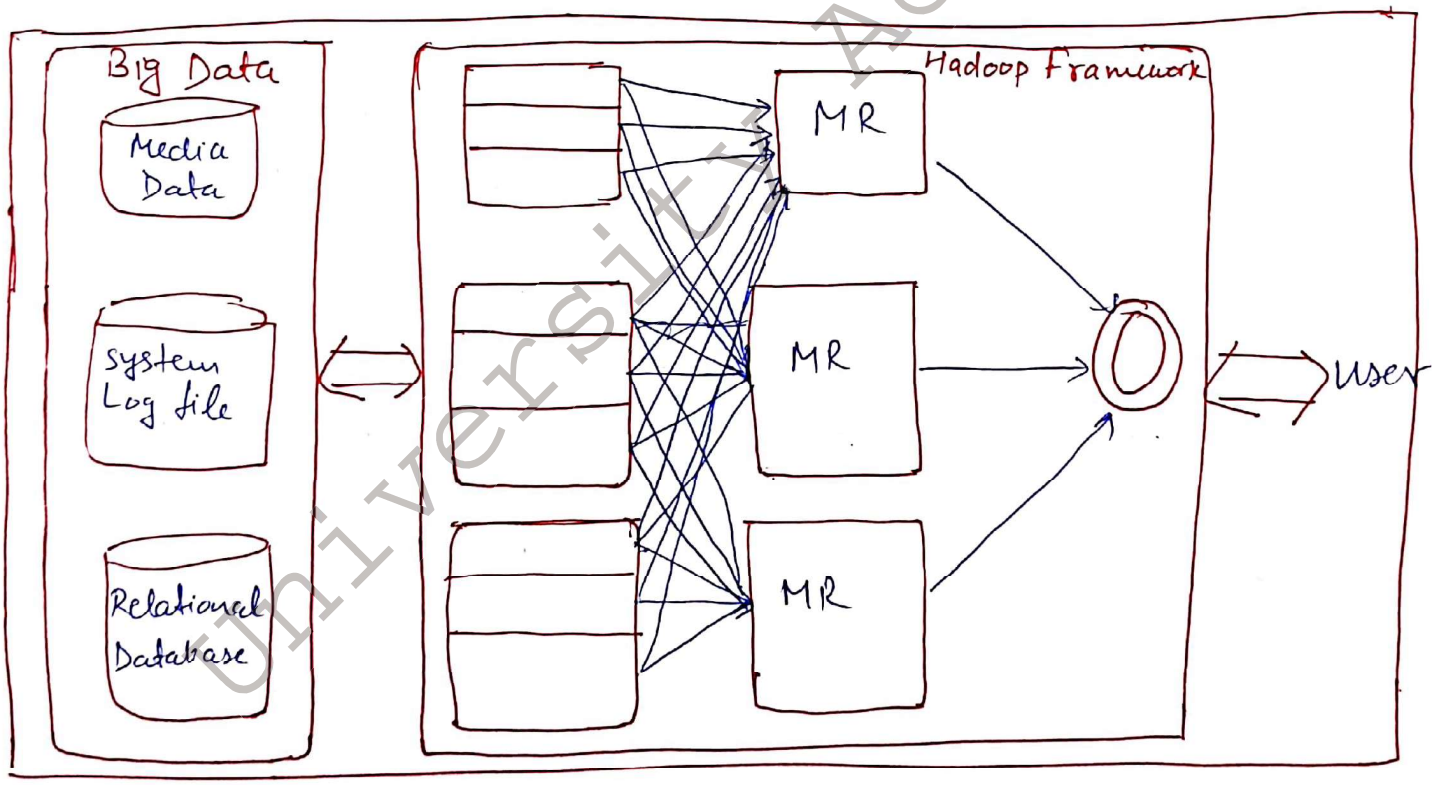
5 & Data Diversity :-

HDFS (Hadoop Distributed file System) has the capability to store different data formats such as unstructured, semi structured and structured.

MapReduce :- (Develop in 2004).

A MapReduce is a data processing tool which is used to process the data parallely in a distributed form.

Working of Hadoop :-



⇒ Hadoop runs applications using the MapReduce algorithm, where the data is processed in parallel with others.

⇒ So all the steps of MapReduce process is followed here for generating the data sets.

Virtual Box:-

* VirtualBox is a general purpose virtualization tool for X86 and X86-64 hardware, targeted at server, desktop and embedded use, that allows users and administrators to easily run multiple guest operating systems on a single host.
* It is open source software for virtualizing the X86 architecture.
* The OS where virtual box runs is called "host" OS. The OS running in the VM is called the "guest" OS.
* Virtual box supports Windows, Linux or macOS as its host OS.
* Supported guest OSs are :-
  - Windows 10, 8, 7, XP, Vista, 2000 NT and 98.
  - Solaris and Opensolaris.
  - MS-DOS
  - OS/2
  - QNX
  - BeOS R5.
  - Haiku
  - ReactOS

Google App Engine:

Google App Engine is a Platform as a service and cloud-computing platform for developing and hosting web-applications in Google-managed data centres.

Applications are sandboxed and run across multiple servers.

Advantages:

* Readily available servers with no configuration requirement.
* Power scaling function all the way down to "free" when resource usage is minimal.
* Automated cloud-computing tools.

Openstack:

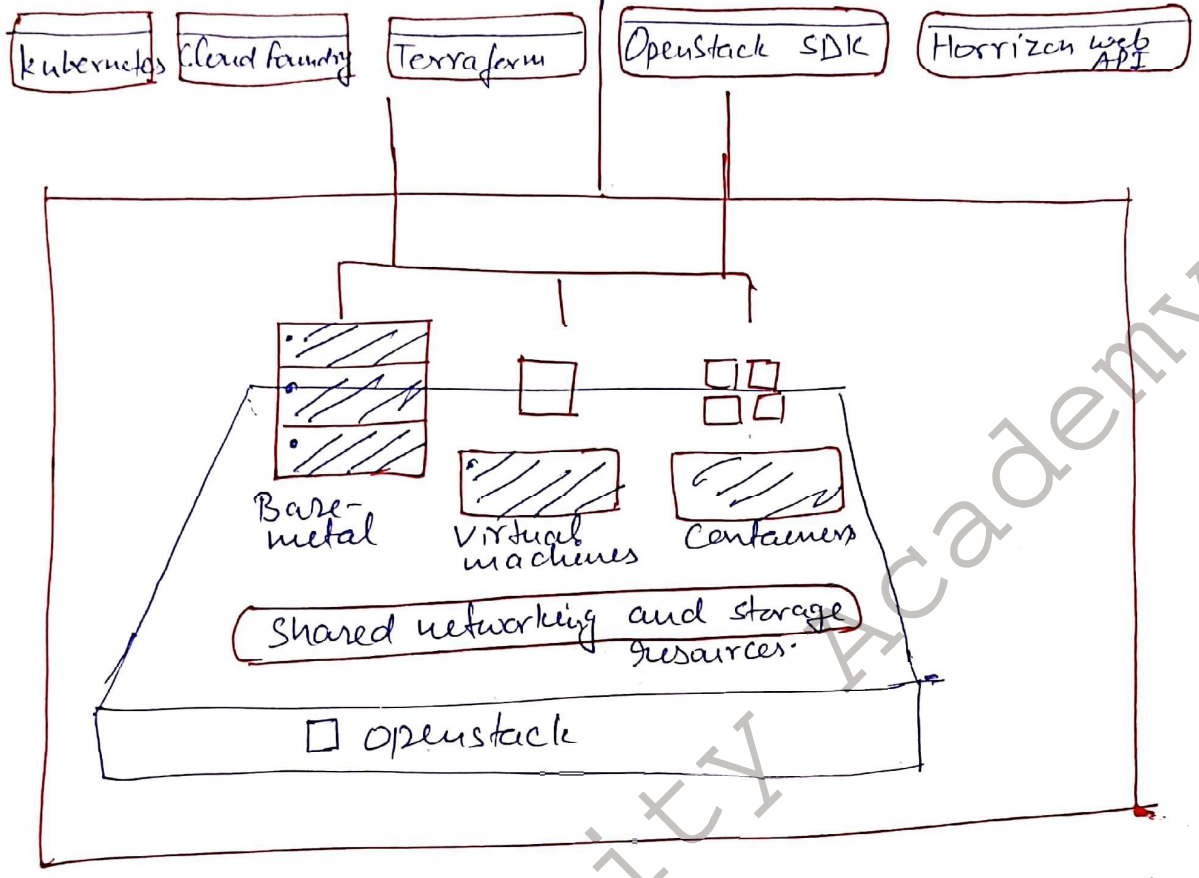
Openstack is a cloud operating system that controls large pool of compute, storage and networking resources throughout a datacenter, all managed and provisioned through APIs with common authentication mechanism.

Basically it is deployed as Infrastructure as a service in both public and private clouds where virtual servers and other

resources are made available to the users.

Architecture :

Deploy third party service such as — or use built in tools.



- A dashboard is available giving administrators control while empowering their users to provision resources through a web interface.

- Beyond standard IaaS functionality, additional components provides orchestration, fault management and service management amongst other services to ensure high availability of user applications.

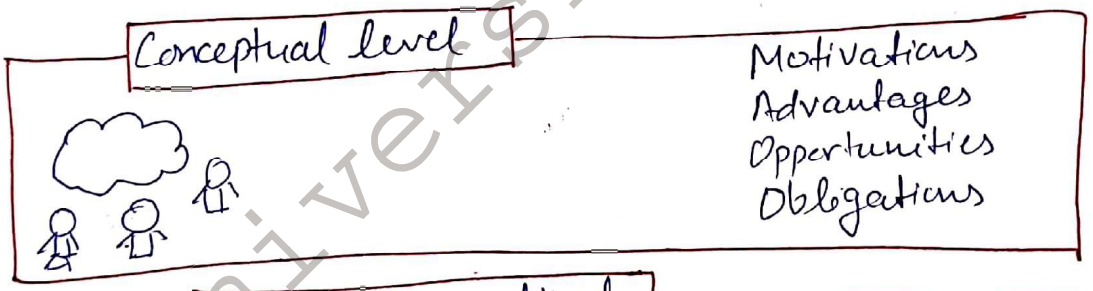
Cloud - Federation:

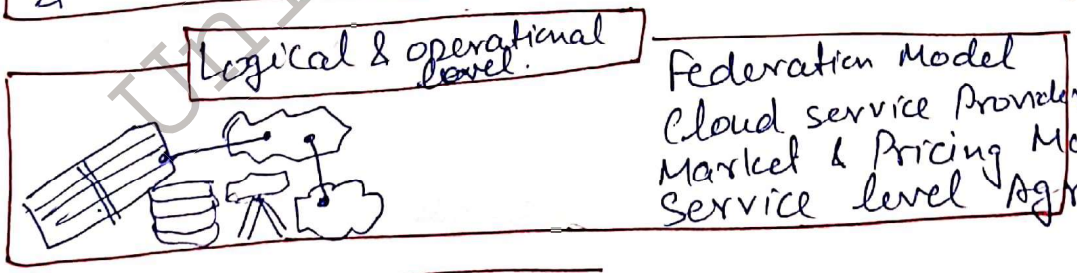
* Cloud - federation is the practice of interconnecting the cloud computing environments of two or more cloud service providers for the purpose of load-balancing and providing services to the users.

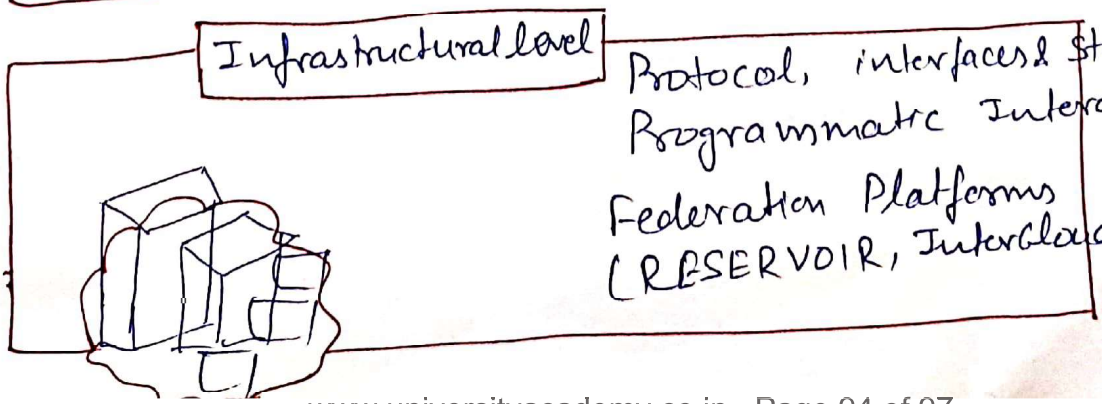
* Cloud federation requires one provider to wholesale or rent computing resources to another cloud provider.

* Those resources became a temporary or permanent extension of the buyer's cloud computing environment, depending upon the specific federation agreement b/w providers.

Levels of federation in cloud:







Each cloud federation level presents a different challenges and operates at different layers of the IT stack.

Conceptual Level: This layer consists of following elements

* Motivations for cloud-providers to join a federation.
* Motivations for service consumers to leverage a federation.
* Advantages for providers in leasing their services to other providers.
* Obligations of providers once they have joined the federation.
* Trust agreement b/w providers.
* Transparency b/w consumers.

Logical & Operational Level:

* At this level, policies and rules for interoperation are defined.
* This is the layer at which decisions are made as to how and when to lease a service to- or to leverage a service from - another providers.

Challenges at this level: Following challenges needs to be addressed.

* How should a federation be presented.
* How should we model and represent a cloud service, a cloud provider or an agreement.
* How should we define the rules & policies that allow providers to join federation.
* What are providers responsibility.
* When should providers & consumers take advantage of the federation.
* Which kind of services are more likely to be leased or bought.

Infrastructure Level:

This level addresses the technical challenges involved in enabling heterogenous cloud computing systems to interoperate seamlessly.

Issues to be addressed at this level:

* What kind of standards should be used.
* How should design interfaces and protocols be designed for interoperations.
* Which are the technology used for interoperation.

Future of federation: Following are the benifits that could be achieved in near future.

1- Additive benifits can be provided to the user by using cloud federation.

2- Risk can be minimized by using federated cloud as it will follow the security solutions provided by each service providers.

3- Integrity could be improved