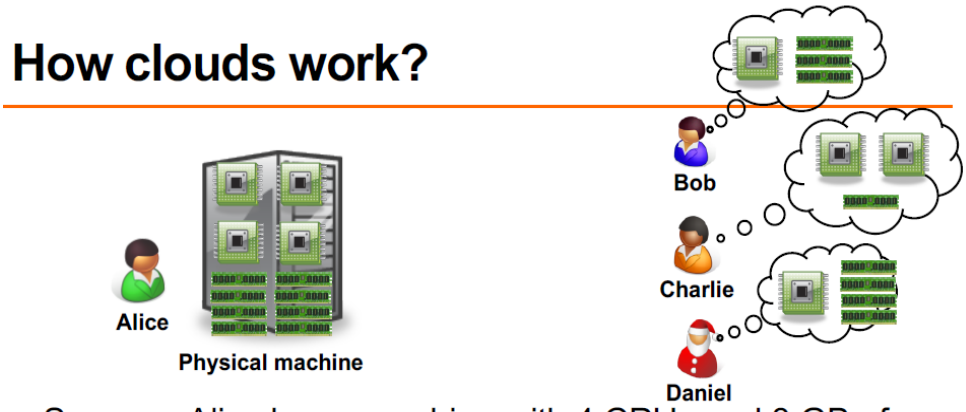
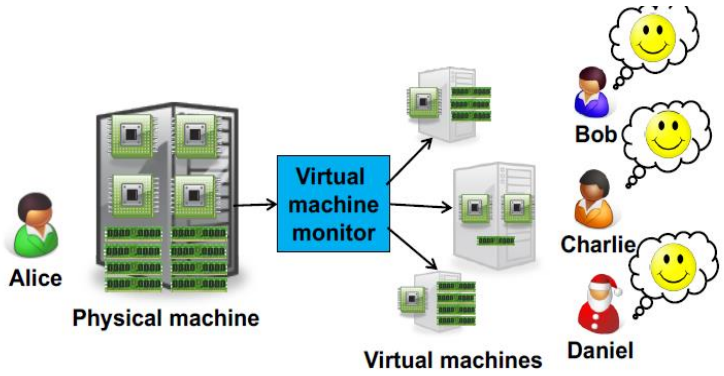
Unit 4 - Virtualization Concepts

Overview of Virtualization, Types of Virtualization, Benefits of Virtualization, Hypervisors

1. Overview of Virtualization

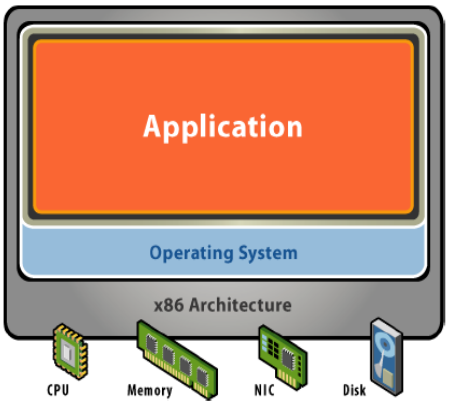


- Suppose Alice has a machine with 4 CPUs and 8 GB of memory, and three customers:
  - Bob wants a machine with 1 CPU and 3GB of memory
  - Charlie wants 2 CPUs and 1GB of memory
  - Daniel wants 1 CPU and 4GB of memory
- What should Alice do?



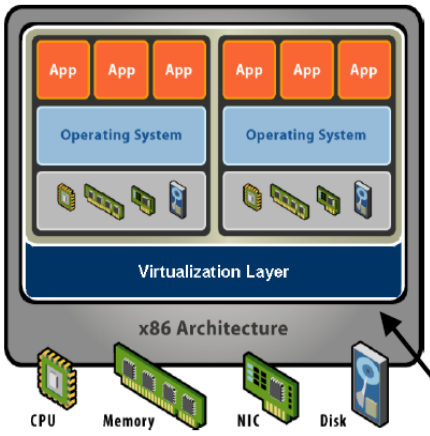
- Alice can sell each customer a virtual machine (VM) with the requested resources
  - From each customer's perspective, it appears as if they had a physical machine all by themselves (isolation)

Starting Point: A Physical Machine



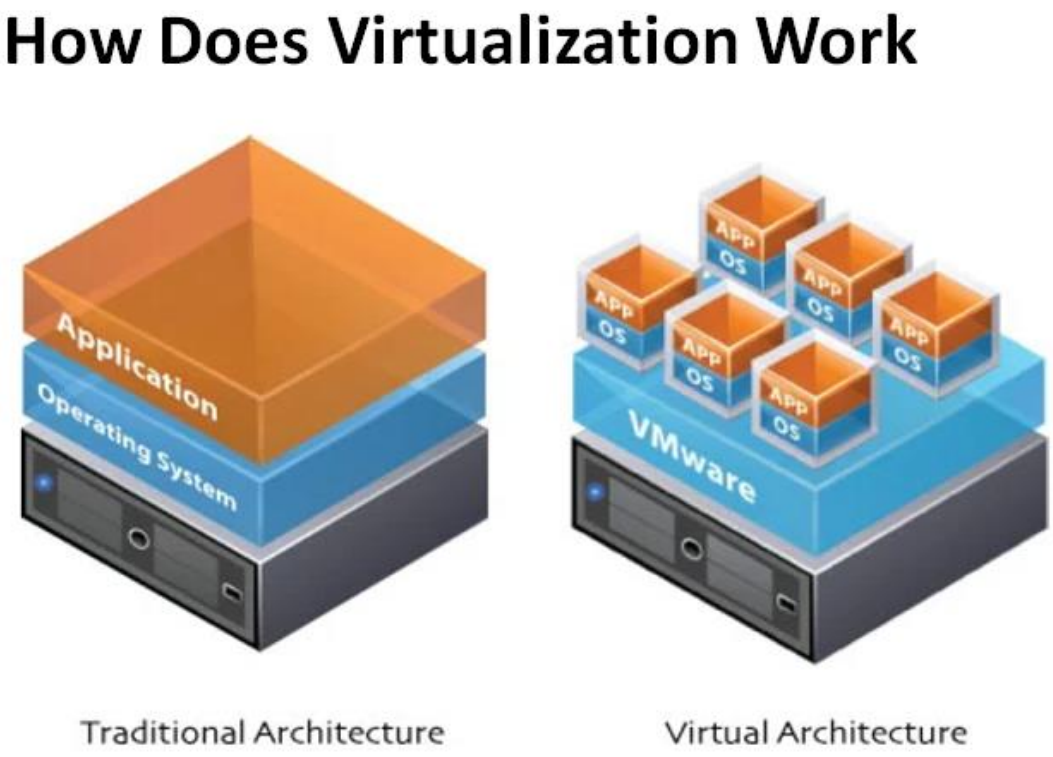
- Physical Hardware
  - Processors, memory, chipset, I/O devices, etc.
  - Resources often grossly underutilized
- Software
  - Tightly coupled to physical hardware
  - Single active OS instance
  - OS controls hardware

What is a Virtual Machine?



- Software Abstraction
  - Behaves like hardware
  - Encapsulates all OS and application state
- Virtualization Layer
  - Extra level of indirection
  - Decouples hardware, OS
  - Enforces isolation
  - Multiplexes physical hardware across VMs

Virtual Machine Monitor or Hypervisor



- A technique for hiding the physical characteristics of computing resources from the way in which other systems, applications, or end users interact with those resources.
- This includes making a single physical resource appear to function as multiple logical resources; or it can include making multiple physical resources appear as a single logical resource.
- Virtualization is the process of creating a virtual environment on an existing server to run your desired program, without interfering with any of the other services provided by the server or host platform to other users.

2. Types of Virtualization

- **Hardware Virtualization**
- **Software Virtualization**
- **Memory Virtualization**
- **Storage Virtualization**
- **Network Virtualization**
- **Data Virtualization**
- **Desktop Virtualization**

Hardware Virtualization

- Also known as server virtualization
- When the virtual machine software or virtual machine manager (VMM) is directly installed on the hardware system is known as hardware virtualization.
- The hardware resource allotment is done by the hypervisor.
- The main advantages include increased processing power as a result of maximized hardware utilization.

Subtypes

- Full Virtualization – Guest software does not require any modifications since the underlying hardware is fully simulated.
- Emulation Virtualization – The virtual machine simulates the hardware and becomes independent of it. The guest operating system does not require any modifications.
- Para Virtualization – the hardware is not simulated and the guest software run their own isolated domains

Software Virtualization

- Software Virtualization involves the creation of an operation of multiple virtual environments on the host machine.
- It creates a computer system complete with hardware that lets the guest operating system to run.
- For example, it lets you run Android OS on a host machine natively using a Microsoft Windows OS, utilizing the same hardware as the host machine does.

Memory Virtualization

- Physical memory across different servers is aggregated into a single virtualized memory pool. It provides the benefit of an enlarged contiguous working memory.
- You may already be familiar with this, as some operating systems such as Microsoft Windows allows a portion of your storage disk to serve as an extension of your RAM.

Subtypes

- **Application-level control** – Applications access the memory pool directly
- **Operating system level control** – Access to the memory pool is provided through an operating system

Storage Virtualization

- Multiple physical storage devices are grouped together, which then appear as a single storage device.
- This provides various advantages such as homogenization of storage across storage devices of multiple capacity and speeds.
- Partitioning your hard drive into multiple partitions is an example of virtualization.

Subtypes

- **Block Virtualization** – Multiple storage devices are consolidated into one.
- **File Virtualization** – Storage system grants access to files that are stored over multiple hosts.

Network Virtualization

- In network virtualization, multiple sub-networks can be created on the same physical network, which may or may not is authorized to communicate with each other.
- This enables restriction of file movement across networks and enhances security, and allows better monitoring and identification of data usage which lets the network administrator's scale up the network appropriately.
- It also increases reliability as a disruption in one network doesn't affect other networks, and the diagnosis is easier.

Subtypes

- **Internal network:** Enables a single system to function like a network
- **External network:** Consolidation of multiple networks into a single one, or segregation of a single network into multiple ones

Data Virtualization

- It lets you easily manipulate data, as the data is presented as an abstract layer completely independent of data structure and database systems. Decreases data input and formatting errors.

Desktop Virtualization

- This is perhaps the most common form of virtualization for any regular IT employee.
- The user's desktop is stored on a remote server, allowing the user to access his desktop from any device or location.
- Employees can work conveniently from the comfort of their home. Since the data transfer takes place over secure protocols, any risk of data theft is minimized

3. Benefits of Virtualization

- **Increase efficiency and productivity**
  - With fewer servers, your IT teams will be able to spend less time maintaining the physical hardware. You'll be able to install, update, and maintain the environment across all the virtual machines on the server instead of going through the laborious and tedious process of applying the updates server-by-server.
- **Smoother IT Operations**
  - Virtual networks help IT professionals become efficient and agile at work. These networks are easy to operate and process faster, reducing the effort and time required to work on them. Before virtual networks were introduced in the digital world, it would take days and weeks for technical workers to maintain and install devices and software on physical servers.
- **Hassle-free Transfer of Data**
  - You can easily transfer data from a physical storage to a virtual server, and vice versa. Administrators don't have to waste time digging out hard drives to find data. With a

dedicated server and storage, it's quite easy to locate the required files and transfer them within no time.

- **Security**
  - During the process of virtualization security is one of the important concerns. The security can be provided with the help of firewalls, which will help to prevent unauthorized access and will keep the data confidential.
- **Protection from System Failures**
  - While performing some task there are chances that the system might crash down at the wrong time. This failure can cause damage to the company but the virtualizations help you to perform the same task in multiple devices at the same time.
- **Cost-Effective**
  - saves the cost for a physical system such as hardware and servers. It stores all the data in the virtual server, which are quite economical.

4. Hypervisor

- A hypervisor is software that creates and runs virtual machines (VMs).
- Also known as a virtual machine monitor or VMM
- A hypervisor allows one host computer to support multiple guest VMs by virtually sharing its resources, such as memory and processing.

Why use a hypervisor?

- Hypervisors make it possible to use more of a system's available resources and provide greater IT mobility since the guest VMs are independent of the host hardware. This means they can be easily moved between different servers. Because multiple virtual machines can run off of one physical server with a hypervisor, a hypervisor reduces:
- Space
- Energy
- Maintenance requirements

5. Types of Hypervisors

There are two main hypervisor types

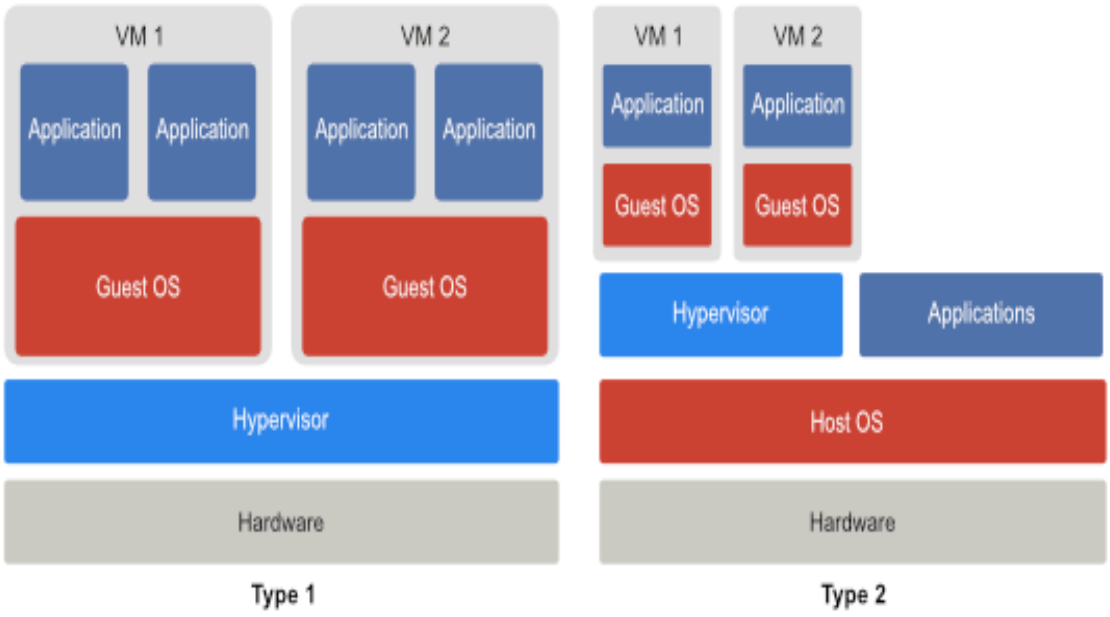
- Type 1 or bare-metal
- Type 2 or hosted

Type 1 Hypervisor

- Hypervisor runs directly on underlying host system.
- It is also known as “Native Hypervisor” or “Bare metal hypervisor”.
- It dose not require any base server operating system.
- It has direct access to hardware resources.
- Examples of Type 1 hypervisors include VMware ESXi, Citrix XenServer and Microsoft Hyper-V hypervisor.

Type 2 Hypervisor

- A Host operating system runs on underlying host system.
- Also known as Hosted Hypervisor.
- Basically a software installed on an operating system.
- Hypervisor asks operating system to make hardware calls.
- Example of Type 2 hypervisor include VMware Player or Parallels Desktop. Hosted hypervisors are often found on endpoints like PCs.



6. Benefits of Hypervisors

- **Speed**
  - Hypervisors allow virtual machines to be created instantly

- **Efficiency**
  - Hypervisors that run several virtual machines on one physical machine's resources also allow for more efficient utilization of one physical server. It is more cost- and energy-efficient to run several virtual machines on one physical machine than to run multiple underutilized physical machines for the same task.
- **Flexibility**
  - Bare-metal hypervisors allow operating systems and their associated applications to run on a variety of hardware types because the hypervisor separates the OS from the underlying hardware, so the software no longer relies on specific hardware devices or drivers.
- **Portability**
  - Since virtual machines are independent from the physical machine, they are portable.

Unit - 5 Cloud Security

Infrastructure Security, Data Security & Privacy Issues, Legal Issues in Cloud Computing

1. Overview of Cloud Security

Here are the most critical security questions to ask the Cloud provider: (only for understanding the topic)

- What is the cloud provider's security architecture and policy?
- Does the cloud provider use a third party to assess its own security risks?
- Does the cloud provider understand its responsibilities for governance issues (such as cross-border data transfers)?
- How comprehensive is the service level agreement between you and the cloud provider?
- Where does your data physically live? Do you have the cloud provider's assurance that it will remain private?
- Does your cloud provider separate (partition) your data, applications, and/or management tools from other users of its cloud services?
- Are there clear penalties for a data or system breach?
- Are you allowed to inspect the cloud facility?
- Does the cloud provider have application level firewalls and other tools that help keep your application or code safe?
- Does the cloud provider provide encryption and key management?
- Does the cloud provider have a well-defined, well-executed identity and access management architecture?

---

2. Cloud security is the set of control-based security measures and technology protection, designed to protect online stored resources from theft and data loss.

- Protection encompasses cloud infrastructure, applications, and data from threats.
- Topics that fall under the umbrella of security in the cloud include:
  - Datacenter Security
  - Access control
  - Threat prevention
  - Threat detection

- Threat mitigation
- Legal compliance
- Security policy

Planning of security

- In security planning, before deploying a particular resource to cloud there is a need to analyze different aspects of the resources which are as follow:
  - Select resource which requires to move to the cloud and examine its sensitivity risk.
  - The cloud service models i.e. IaaS, PaaS and SaaS are necessary to be considered for security at different level of services.
  - The cloud types, i.e. public, private, community, hybrid also need to be considered.
  - The risk in a cloud deployment generally depends on the types of cloud and service models

Risks and Security Concerns (Top Threats)

- Abuse of Cloud Computing;
- Insecure Application Programming Interfaces;
- Malicious Insiders;
- Shared Technology Vulnerabilities; (असुरक्षित, कमजोर, दोषपूर्ण)
- Data Loss and Leakage;
- Account, Service and Traffic Hijacking;

3. Infrastructure security

- The foundational infrastructure for a cloud must be inherently secure whether it is a private or public cloud or whether the service is SAAS, PAAS or IAAS.
- The infrastructure security can be viewed, assessed and implemented according its building levels
  - Network level security
  - Host level security
  - Application level security

Network level security

- Ensuring the confidentiality and integrity of organization's data-in-transit to and from a public cloud provider
- Ensuring proper access control (authentication, authorization, and auditing) to whatever resources are used at the public cloud provider
- Ensuring the availability of the resources in a public cloud that are being used by an organization

Host level security

- When reviewing host security, the context of cloud services delivery models (SaaS, PaaS, and IaaS) and deployment models (public, private, and hybrid) should be considered
- The host security responsibilities in SaaS and PaaS services are transferred to the provider of cloud services.
- IaaS customers are primarily responsible for securing the hosts provisioned in the cloud:
  - Virtualization software security
  - Customer guest OS
  - Virtual server security (a cloud server is a virtual server in cloud computing)

Application level security

- Application or software security should be a critical element of a security program.
- The application security spectrum ranges from standalone single-user applications to sophisticated multiuser e-commerce applications used by many users.

This level is responsible for managing:

- Application-level security threats;
- End user security;
- SaaS application security;
- PaaS application security;
- Customer-deployed application security;
- IaaS application security;
- Public cloud security limitations;

4. Data Security and Privacy

- Data security has consistently been a major issue in information technology.
- In the cloud computing environment, it becomes particularly serious because the data is located in different places even in the entire globe.
- Data security and privacy protection are the two main factors of user's concerns about the cloud technology.
- Securing data sent to, received from, and stored in the cloud is the single largest security concern that most organizations should have with cloud computing.
- You must assume that any data can be intercepted and modified. That's why, traffic to a cloud service provider and stored off-premises is encrypted.
- Following are the key mechanisms for protecting data mechanisms:
    - Access control
    - Auditing
    - Authentication
    - Authorization

5. Data Security and Privacy Issues

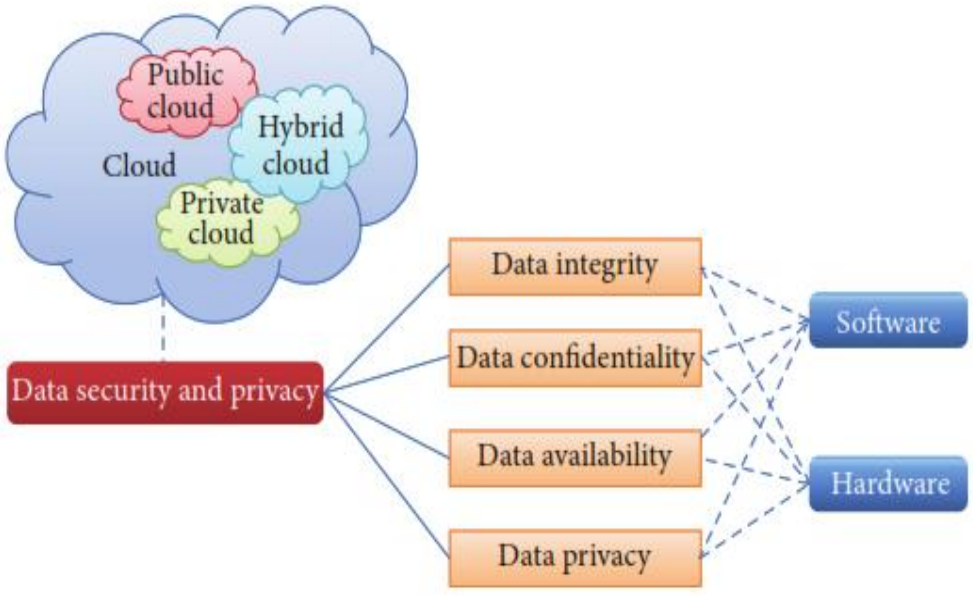


FIGURE 1: Organization of data security and privacy in cloud computing.

- **Data integrity**
  - It is one of the most critical elements in any information system.
  - Generally, data integrity means protecting data from unauthorized deletion, modification, or fabrication.
- **Data confidentiality**
  - It is important for users to store their private or confidential data in the cloud.
  - Authentication and access control strategies are used to ensure data confidentiality.
  - The data confidentiality, authentication, and access control issues in cloud computing could be addressed by increasing the cloud reliability and trustworthiness.
- **Data availability**
  - Data availability is a term used to describe products and services that ensure that data continues to be available, at a required level of performance, in situations ranging from normal to disastrous.
- **Data Privacy**
  - It is the ability of an individual or group to isolate themselves or information about themselves and thereby reveal them selectively.

6. Legal Issues in Cloud Computing

- Liability
- Regulatory Compliance
- Control Over Physical Location of Data
- Trade Secret Protection
- Hacking of Cloud Provider
- Financial Liability of Cloud Vendor
- Jurisdiction & Court of Law

Cross border legal issue

- Cloud located in different countries creates issues related to conflict of laws & jurisdiction.
- Cross - border data flow – potentially causes conflict of regulations

Involvement of multiple parties

- Cloud services usually involve multiple parties which makes responsibility/ liability shift on one another

- Contractual privity lacks between the parties which make it difficult for the client to bind a provider for a breach
- Agreements should include liability of providers for act of subcontractor
- Right to conduct due diligence & to understand the model of delivery of services should be given to the customers

Privacy & Security

- Multi-tenant architecture
- Data from different users are usually stored on a single virtual server
- Multi virtual server run on a single physical server
- Data security depends upon the integrity of virtualization

Issues with service level agreement

- Standard mass market contracting terms are used
- Generally, non - negotiable agreements
- Little opportunity to conduct the due diligence
- Strong limits on liability (including direct liability)
- Terms often subject to change without notice
- Risk is generally shifted to user through provider friendly agreements.

Audit trail

- As data is on continuous move & flow in the cloud services, client should have the right to know where & by whom its data is stored , accessed , transferred & altered .
- Confirm whether the vender provides the audit trail rightsor not .

IPR & ownership issues

- Trade secret protection - as third parties might have access to data , which can be detrimental to trade secret of a company
- Company should have non - disclosure agreements with the vendors
- Ensure that no rights in IPR(intellectual property rights) are transferred to the vendor

Exit issues

- In case a user has to change provider in the future the options for portability and interoperability are critical issues to be considered
- In case of exit, can the records be successfully accessed?
- Can data be extracted from the cloud?
- Obligations of each party in case of exit

Hacking of cloud vendor

- In the event the cloud vendor system is hacked, does the owner ion the data has the right to move against for claiming lost profits.

Jurisdictional issues

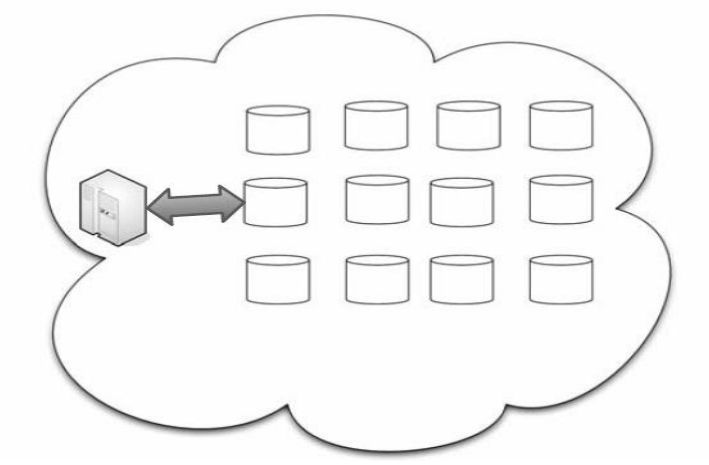
- In cloud services, location of data is usually uncertain. The owner of data is not aware of the country where the data is stored. The physical location of data raises the question of law to be governed and jurisdiction. It is important to be aware of the prevailing law in that particular nation.
- What if the dispute arises, what will be the place of jurisdiction. The owner of the data should be aware of the countries' court system which will govern the conflict arose between the parties.

Unit 6 - Cloud Storage

Overview, Storage as a Service, Benefits and Challenges, Storage Area Networks (SANs).

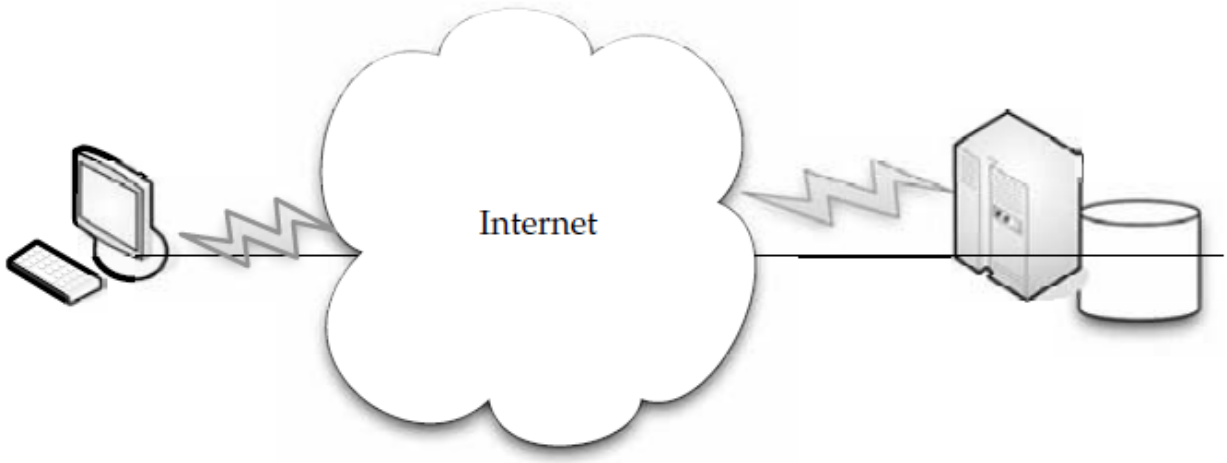
1. Overview of Cloud Storage

- Google Drive, DropBox, OneDrive etc
- Storing your data with a cloud service provider rather than on a local system.
- As with other cloud services, you access the data stored on the cloud via Internet link.
- Cloud storage has a number of advantages over traditional data storage.
- If you store your data on a cloud, you can get it from any location that has Internet access.
- Cloud storage system just needs one data server connected to the Internet. A subscriber copies files to the server over the Internet, which then records the data. When a client wants to retrieve the data, he or she accesses the data server with a web-based interface, and the server then either sends the files back to the client or allows the client to access and manipulate the data itself. However, cloud storage systems utilize dozens or hundreds of data servers.
- Because servers require maintenance or repair, it is necessary to store the saved data on multiple machines, providing redundancy.
- Without that redundancy, cloud storage systems couldn't assure clients that they could access their information at any given time.
- Many clients use cloud storage not because they've run out of room locally, but for safety. If something happens to their building, then they haven't lost all their data.



2. Storage as a Service

- Storage as a service (STaaS/SaaS) is a cloud business model in which a company leases or rents its storage infrastructure to another company or individuals to store data.
- It is also ideal when technical personnel are not available or have inadequate knowledge to implement and maintain that storage infrastructure.
- The biggest advantage of STaaS/SaaS is cost savings.
- Storage is rented from the provider using a cost-per-gigabyte-stored or cost-per-data-transferred model.
- The end user doesn't have to pay for infrastructure; they simply pay for how much they transfer and save on the provider's servers.



Clients rent storage capacity from cloud storage vendors.

- There are hundreds of cloud storage providers on the Web, and more seem to be added each day. Not only are there general-purpose storage providers, but there are some that are very specialized in what they store.

Some examples of cloud storage providers:

- **YouTube** hosts millions of user-uploaded video files.
- **Facebook, Twitter and Instagram** are social networking sites and allow members to post pictures and other content. That content is stored on the company's servers.
- **Google Docs** allows users to upload documents, spreadsheets, and presentations to Google's data servers.

- Web email providers like **Gmail, Hotmail, and Yahoo! Mail** store email messages on their own servers.
- **Flickr and Picasa** host millions of digital photographs. Users can create their own online photo albums.
- **Hostmonster and GoDaddy** store files and data for many client web sites.

3. Benefits of Cloud Storage

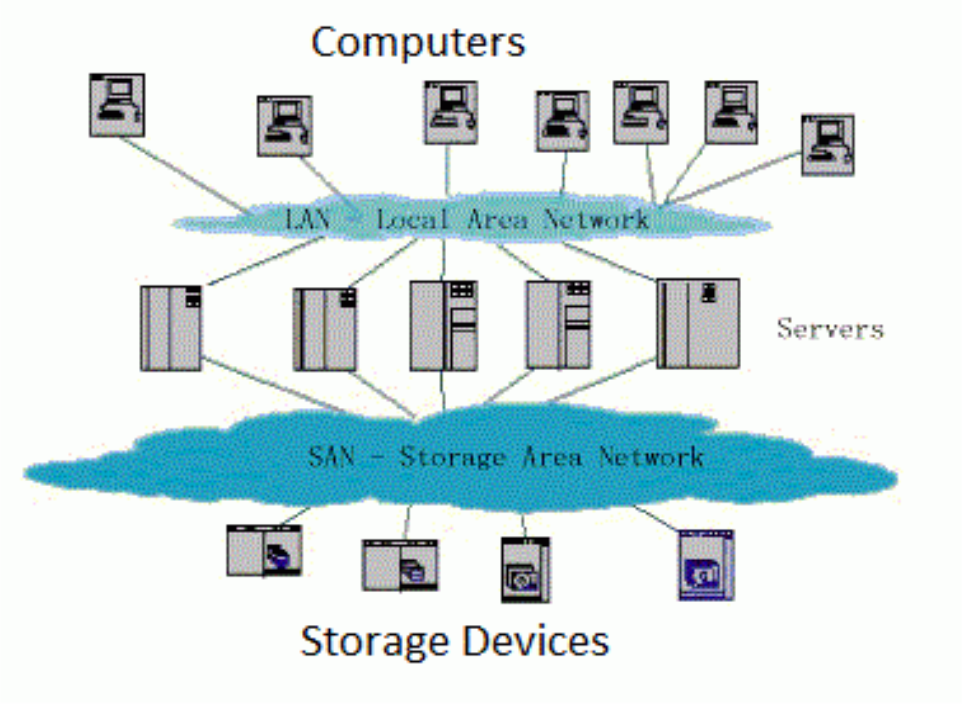
- **Storage costs**
  - Personnel, hardware and physical storage space expenses are reduced.
- **Disaster recovery**
  - Having multiple copies of data stored in different locations can better enable disaster recovery measures.
- **Scalability**
  - With most public cloud services, users only pay for the resources that they use.
- **Syncing**
  - Files can be automatically synced across multiple devices.
- **Sharing**
  - Online storage services allow the users to easily share data with just a few clicks
- **Security**
  - Data is encrypted both during transmission and while at rest, ensuring no unauthorized user access to files
- **Automation**
  - Storage as a service makes the tedious process of backing up easy to accomplish through automation. Users can simply select what and when they want to backup, and the service does all the rest.
- **Accessibility**
  - By going for storage as a service, users can access data from smart phones, laptops to desktops and so on.

4. Challenges of Cloud Storage

- **Security**
  - Users may end up transferring business-sensitive or mission-critical data to the cloud, which makes it important to choose a service provider that's reliable.
- **Downtimes**
  - Vendors may go through periods of downtime where the service is not available, which can be trouble for mission-critical data.
- **Limited customization**
  - Since the cloud infrastructure is owned and managed by the service provider, it is less customizable.
- **Vendor lock-in**
  - It may be difficult to migrate from one service to another.
- **Performance**
  - Concerns about application performance if the application storage is in the cloud.
- **Bandwidth limitations**
  - Bandwidth is a limiting factor when accessing a public storage cloud, as they are accessed over the Internet.
- **Latency constraints**
  - Latency is the silent killer of application performance, both in terms of response time and throughput.

5. Storage Area Networks (SANs)

- SAN is an abbreviation of the Storage Area Network.
- Storage Area Network is a dedicated, specialized, and high-speed network which provides block-level data storage. It delivers the shared pool of storage devices to more than one server.
- Storage Area Network (SAN) is basically a combination of computers and storage devices connected in a network.
- A SAN presents storage devices to a host such that the storage appears to be locally attached.



- The main aim of SAN is to transfer the data between the server and storage device. It also allows for transferring the data between the storage systems.

6. Applications of SANs

- SANs are primarily used to make storage devices, such as **disk arrays, tape libraries** accessible to servers so that the devices appear like locally attached devices to the operating system.

7. Two principal **types** of networking technologies and interfaces in SANs:

- **Fibre Channel**
  - FC is a high-speed network noted for its high throughput and low latency when optical fibre cabling and interfaces are used. This kind of dedicated network potentially enables block level storage to be consolidated in one location, while servers can be distributed across campus buildings or a city.
- **iSCSI** (Internet Small Computing System Interface)
  - Commonly used in small and medium sized organizations as a less expensive alternative to FC
  - iSCSI storage networks use the same cabling, network adapters, switches and other network components used in any Ethernet network

8. Advantages/ Disadvantages of SANs

Advantages

- Greater performance
- Backup and Online Recovery
- Increased disk utilization
- Increased I/O performance
- Less Number of Servers are required
- Storage Virtualization

Disadvantages

- If there is a lot of traffic in the storage area network, then operations will be **extremely slow**. So it is better not to use storage area networks for data extensive applications.
- The storage area network operates in a shared environment. So there is a chance that **data may be leaked** for sensitive operations.

Unit 7 - Scheduling in Cloud

Overview of Scheduling problem, Different types of scheduling, Scheduling for independent and dependent tasks, Static vs. dynamic scheduling

1. Overview

- Cloud computing gives the illusion of infinite (virtual) resources. Actually there is a finite amount of (physical) resources.
- We would like to efficiently share those resources. Therefore, we should be able to plan ahead computations.
- To efficiently increase the working of cloud computing environments, scheduling is performed in order to gain maximum profit.
- The concept of scheduling in cloud computing refers to the technique of mapping a set of jobs to a set of virtual machines (VMs) or allocating VMs to run on the available resources in order to fulfill users' demands.
- The aim of using scheduling techniques in cloud environment is to improve system throughput and load balance, maximize the resource utilization, save energy, reduce costs, and minimize the total processing time.
- The need for scheduling arises because efficiency of scheduling algorithm directly affects the performance of the system with respect to delivered QoS, resource utilization.

Task:

- Represents a computational unit to run on a node. A task is considered as an indivisible schedulable unit. Tasks could be independent (or loosely coupled) or there could be dependencies.

Job:

- A job is a computational activity made up of several tasks that could require different processing capabilities and could have different resource requirements (CPU, memory, etc.).

Resource:

- A resource is something that is required to carry out an operation, for example: a processor for data processing, a data storage device, or a network link for data transporting.

Resources in cloud computing are scheduled at two levels - **VM-level and Host-level**.

- **VM-level**
  - At the VM-level, tasks are mapped for execution to the allocated VMs using a task/job scheduler. It is called Task Scheduling.
- **Host-level**
  - At the host-level, a VM scheduler is used to allocate the VMs into physical hardware. This type is usually called VM Scheduling.

2. Types of Scheduling

Scheduling is generally categorized as:

- **Centralized/ decentralized**
- **Static/ Dynamic**
- **Immediate Mode/ Batch Mode**
- **Heuristic/ Metaheuristic**
- **Preemptive/ Non-Preemptive**

Centralized / decentralized scheduling

- **Centralized scheduling**
  - When scheduling is centralized, decisions are made in a central node.
  - It ensures efficiency and ease of monitoring resources. However, it lacks scalability and fault tolerance.
- **Decentralized scheduling**
  - Decentralized or distributed scheduling is more applied in real cloud environment although it lacks efficiency.

Static / Dynamic scheduling

- **Static scheduling**
  - All timing information about tasks is available before, so the execution schedule of each task is computed before executing any task.
  - It is effective for applications that have fixed demands.

- **Dynamic scheduling**
  - Timing information about the tasks is not known at runtime. So the execution schedule of task may change as per the user demand.
  - Dynamic scheduling incurs runtime overhead compared to static scheduling.

Preemptive/ Non-Preemptive scheduling

- **Preemptive scheduling**
  - Allows interrupting each task during the execution and migrating the task to another resource.
  - For example, when a task has a higher priority than another task and need to be executed although it is running in the virtual machine.
- **Non-preemptive scheduling**
  - The virtual machine cannot be taken away until the task running on it completes.
  - It does not allow the task to be interrupted while it is executing.

Immediate mode / Batch mode scheduling

- **Immediate mode**
  - Also called online mode, tasks are scheduled to resources immediately without any delay.
  - Tasks are scheduled only once and cannot be changed.
- **Batch mode**
  - Also called as offline mode, it collects tasks into a set and are examined for mapping at prescheduled times.

Heuristic / Metaheuristic scheduling

- Heuristic scheduling techniques are problem dependent that can solve specific problems.
- Metaheuristic techniques are high level problem-independent techniques that provide master strategies to solve general problems and can be applied to a wide range of problems.

Note - In addition to above categorization, Scheduling is sometime also categorized in following manner:

- First Come First Serve
- Round Robin
- Min-min
- Max-min

- Priority Queue Scheduling
- Shortest Job First
- Multi Level Feedback Queue

First Come First Serve (FCFS)

- This type of scheduling is based on first job come and first job serve.
- The basic scheduling technique is FCFS which is used in cloud computing.
- Cloud computing use FCFS to send data in packets form as it is received by router at sender end and received on other end of router .

Round Robin scheduling

- The Round Robin Scheduling was designed based on the CPU time distribution among the tasks of schedule.
- All tasks are in queue list and each task get small unit of CPU time that is known as quantum that range between 10 to 100 ms.

Min-min scheduling

- The min-min scheduling mechanism works on determining the minimum completion time for each job submitted for execution.
- All jobs go through two steps:
  - In the first step, it sees for a set of job with minimum completion time.
  - Second step allocates the job selected in the previous step to the right resource.

Max-min scheduling

- The Max-min algorithm is commonly used in distributed environment which begins with a set of unscheduled tasks.
- Calculate the expected execution matrix and expected completion time of each task on the available resources.
- Next, choose the task with overall maximum expected completion time and assign it to the resource with minimum overall execution time.
- Finally recently scheduled task is removed from the meta tasks set, update all calculated times, then repeat until meta-tasks set become empty

Priority Queue Scheduling

- Priority is assigned to process on the basis of their requirement by user.
- User assigns priority to processes and highest priority process executes first and the lowest priority process execute in the last

Shortest Job First Scheduling

- Shortest Job First (SJF) scheduling is best where small size process needs to execute first.
- This scheduling method is best forever to execute processes but as the scheduling depends on the basis of user requirement somewhere it is not suitable.

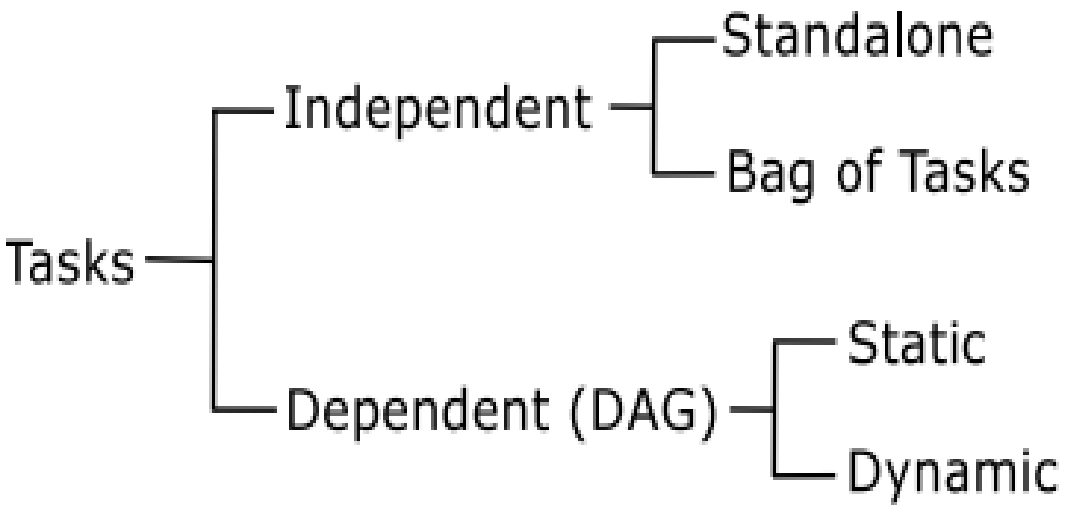
Multi Level Feedback Queue Scheduling

- Uses multiple queues to transmit data in the first queue and it uses RR with a time quantum assigned to particular queue.
- Each process first enters in this queue and execute according to RR and quantum. Then process enter in second queue if it did not complete in first queue, and if completed then came out of queue.
- Second queue also execute process in the same way as in first queue. If process did not complete in second queue then it enters in third queue and the processing continues in same manner.

3. Scheduling for Independent and Dependent tasks

- Task scheduling is very important issue.
- It is used to schedule tasks for better utilization of resources by allocating certain tasks to particular resources in particular time.
- Main aim of task scheduling is to improve the performance and quality of service and also maintaining the efficiency among the tasks and reduce the cost.

Tasks can be classified as dependent or independent.



Independent Tasks

- Independent tasks perform no communication among them.
- The independent tasks have no dependencies with other tasks and no priority order need to be followed during scheduling process.

- Independent tasks can be either **standalone** or **bag of tasks (BoT)**.
- While a standalone task has no relation to other tasks arriving to the scheduler, tasks within a bag of tasks have similarities among them.
- An example of a class of BoT is the parameter sweep applications, where the same task is executed many times with different input parameters.

Dependent tasks

- Dependent tasks present communication dependencies among them.
- The dependent tasks have precedence order based on dependencies among the tasks and need to be followed during the scheduling process.
- Dependent tasks can be modeled as directed acyclic graphs (DAGs), in which nodes represent tasks and arcs represent communication dependencies among tasks.
- In our classification we separate DAGs into two classes: static DAGs and dynamic DAGs.
- Static DAGs have all their tasks run during their execution.
- On the other hand, dynamic DAGs may change during the execution.

4. Static/ Dynamic scheduling

- **Static scheduling**
  - All timing information about tasks is available in advance, so the execution schedule of each task is computed before executing any task.
  - It is effective for applications that have fixed demands.
  - In this type of scheduling, the consumer makes agreement with the cloud provider for services and the cloud provider prepares the required resources before the start of required service
- **Dynamic scheduling**
  - Timing information about the tasks is not known at runtime. So the execution schedule of task may change as per the user demand.
  - Dynamic scheduling incurs runtime overhead compared to static scheduling.
  - In this type of scheduling, the cloud provider cannot plan required resources before usage. It allocates and removes resources as per need.

5. Static Vs dynamic scheduling

- In static scheduling, the prior information regarding the incoming tasks and the number of resources available for them is known.
- The static scheduling can be applied only when we know the information about the tasks in advance whereas dynamic scheduling is used for executing tasks in an instant.

- Although the performance of dynamic scheduling is better than static, overhead of static algorithms is less since in dynamic algorithms there is a need of change in system's information instantaneously.