# UNIT III

# CHAPTER 3

# Virtualization

**University Prescribed Syllabus**

Introduction to Virtualization, Difference between Cloud Computing and Virtualization Types of Virtualization: Hardware, Software, Operating system, Server, Storage, Methods of implementing storage Virtualization, Network Virtualization Types, Advantages, Disadvantages, Virtualization Architecture and Software, Virtual Clustering, Applications of Virtualization.

## 3.1 INTRODUCTION TO VIRTUALIZATION

**GQ.** Define Virtualization. State the characteristics of virtualization.

- In cloud computing, **virtualization** refers to preparing a virtual version of a server, a desktop, a storage device, an operating system, or network resources.
- This approach allows a single physical instance of an application or resource to be shared among multiple organizations or customers.
- It does by assigning a logical name to a physical storage and providing a pointer to that physical resource when demanded.
- It helps to separate the service from its physical delivery.
- As a result of this technique, multiple operating systems and applications can be run on the same machine and hardware at the same time.
- The machine on which the virtual machine is built is called the Host Machine and the virtual machine is known as the Guest Machine.
- This virtual machine is managed by a software or firmware, which is known as **hypervisor.**

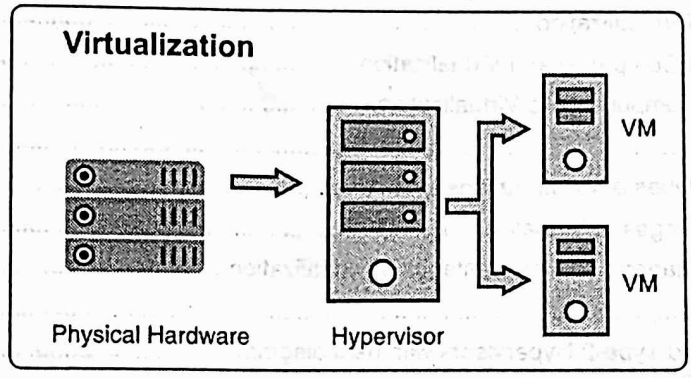


**Fig. 3.1.1 : Virtualization**

### 3.1.1 Characteristics of Virtualization

Following are the characteristics of virtualization :

(1) **Resource Sharing :** Virtualization allows its users to create different computing environments on one host machine, which could be a single computer or a network of servers that are all connected to each other. This allows user limit the number of servers that are active, use less power, and manage resources.

(2) **Isolation :** The self-contained VMs that come with virtualization software give guest users (a term that includes not only people but also applications, operating systems, and devices) a separate online environment. This separation keeps private information safe while allowing guests stay connected.

(3) **Availability :** Virtualization software offers various characteristics not available with physical servers that boost uptime, availability, fault tolerance, and more, hence assisting users in avoiding downtime that impedes user productivity and raises security risks.

(4) **Aggregation :** Virtualization allows multiple devices to share a single machine's resources, but it can also be used to integrate multiple devices into a single, powerful host. Aggregation necessitates cluster management software, which connects a number of identical computers or servers to form a unified resource center.

(5) **Reliability :** Currently, virtualization technologies provide continuous uptime by automated load balancing, which runs multiple servers on distinct host machines to prevent disruptions. Consequently, hardware failures are a minor inconvenience. If downtime is a prime concern, you may need to invest in backup hardware.

## 3.2 DIFFERENCE BETWEEN CLOUD COMPUTING AND VIRTUALIZATION

**GQ.** Compare Cloud Computing and Virtualization.

In this section, we will discuss about the difference between Cloud computing and Virtualization.

| Sr. No. | Cloud Computing | Virtualization |
|---|---|---|
| 1. | Cloud computing is used to provide pools and automated resources that can be accessed on-demand. | Virtualization is used to make various simulated environments through a physical hardware system. |
| 2. | Cloud computing setup is tedious, complicated. | Virtualization setup is simple. |
| 3. | Cloud computing is high scalable. | Virtualization is low scalable i.e., Virtual machine configuration limits its scalability. |
| 4. | Cloud computing is Very flexible. | Virtualization is less flexible. |
| 5. | In the condition of disaster recovery, cloud computing relies on multiple machines. | In the condition of disaster recovery, virtualization relies on single peripheral device. |
| 6. | In cloud computing, the workload is stateless. | In virtualization, the workload is stateful. |
| 7. | The total cost of cloud computing is higher than virtualization. | The total cost of virtualization is lower than cloud computing. |
| 8. | Cloud computing requires many dedicated hardware. | In virtualization, single dedicated hardware can do a great job in it. |
| 9. | Cloud computing provides unlimited storage space. | Storage space depends on physical server capacity in virtualization. |

| Sr. No. | Cloud Computing | Virtualization |
|---|---|---|
| 10. | Cloud computing is of two types : Public cloud and Private cloud. | Virtualization is of two types : Hardware virtualization and Application virtualization. |
| 11. | In Cloud Computing, Configuration is image based. | In Virtualization, Configuration is template based. |
| 12. | In cloud computing, we utilize the entire server capacity and the entire servers are consolidated. | In Virtualization, the entire servers are on-demand. |
| 13. | In cloud computing, the pricing pay as you go model, and consumption is the metric on which billing is done. | In Virtualization, the pricing is totally dependent on infrastructure costs. |
| 14. | Easy to integrate with existing solutions, many providers support integrations and APIs. May require a data integration solution to prevent data silos. | Easily integrate with public and private clouds, IoT devices, and databases. If integrating with legacy equipment, integration software to unify data is needed |
| 15. | Cloud computing deliver variable resources to groups of users for a variety of purposes | Virtualization deliver packaged resources to specific users for a specific purpose |

## 3.3 TYPES OF VIRTUALIZATIONS

**GQ.** Explain different types of virtualizations.

In this section, we will discuss about different types of virtualizations.

### 1. Hardware Virtualization

- It is the abstraction of computing resources from the software that uses cloud resources.
- It involves embedding virtual machine software into the server's hardware components.
- That software is called the hypervisor. The hypervisor manages the shared physical hardware resources between the guest OS & the host OS.
- The abstracted hardware is represented as actual hardware.
- Virtualization means abstraction & hardware virtualization is achieved by abstracting the physical hardware part using Virtual Machine Monitor (VMM) or hypervisor.
- The term hardware virtualization is used when VMM or virtual machine software or any hypervisor gets directly installed on the hardware system.
- The primary task of the hypervisor is to process monitoring, memory & hardware controlling.

- After hardware virtualization is done, different operating systems can be installed, and various applications can run on it.
- Hardware virtualization, when done for server platforms, is also called server virtualization.
- Hardware virtualization is of three kinds:
  (i) **Full Virtualization :** Here, the hardware architecture is completely simulated. Guest software doesn't need any modification to run any applications.
  (ii) **Emulation Virtualization :** Here, the virtual machine simulates the hardware & is independent. Furthermore, the guest OS doesn't require any modification.
  (iii) **Para-Virtualization :** Here, the hardware is not simulated; instead, the guest software runs its isolated system.

**2. Software Virtualization**

- Software virtualization is a technique that allows one computer server to work with more than one virtual system.
- The primary function of software virtualization is to develop virtual Software and make the work easier.
- It is capable of abstracting the software installation procedure and building virtual software installations.
- Software virtualization will build a virtual environment and allows the user to use more than one Operating System.
- Software virtualization is of three kinds :
  (i) **OS Virtualization :** In OS Virtualization, more than the Operating system wants to work individually to complete the task without affecting others. Thus, a particular Operating system can perform its specified job.
  (ii) **Application Virtualization :** Application Virtualization is the second Virtualization method where users can remotely access their applications on the central server. It helps to run multiple applications at the same time by building a virtual environment.
  (iii) **Service Virtualization :** Service Virtualization is a technique to simulate the Behaviors of components in the form of combination component-based applications.

**3. Operating System Virtualization**

- The OS virtualization allows you to virtualize physical servers on the operating system (kernel) layer.
- The OS virtualization layer ensures isolation and security of resources between different containers.
- The virtualization layer makes each container appear as a standalone server.
- Finally, the container itself houses its own applications and workload.

- OS virtualization is streamlined for the best performance, management, and efficiency.
- OS virtualization is of two types:
  (i) **Linux Operating System Virtualization :** VMware Workstation software is widely used in virtualizing Linux Systems. If the users want to install any of the other software with the help of Virtualization, then the user will require to install the VMware Software at the beginning.
  (ii) **Windows Operating System Virtualization :** Windows Operating System Virtualization is also the same as Linux Operating System Virtualization. And if the user wishes to install any software, they must install the VMware Software first.

**4. Server Virtualization**

- In this type of virtualization, we aim to virtualize the server that we use, that is we will be running multiple VM's (virtual machines) in a single physical server.
- Here the resource form this physical server will be shared among all the virtual servers that are being used.
- Some of the resources which are being shared majorly are CPU, Storage, ROM, and RAM, etc. and we will be sharing them on the hypervisor (a layer of software between the base hardware and the virtual machines).
- These virtual machines are isolated and independent of each other, and they are completely capable of running the different OS in different machines.
- Some of the competitive vendors that are available in the market who do this server virtualization are vSphere (VMware), Xenserver (Citrix) and Hyper-V (Microsoft), etc.

**5. Storage Virtualization**

- Storage virtualization basically combines/pools the storage that is available in various devices and keeps it as single storage.
- Identification of the available storage is done by leveraging the software and aggregates them to use it in a virtual system/environment.
- The software actually constantly monitors the various I/O requests from any virtual/physical system, and it intercepts them and sends it to the appropriate location where the combined storages are maintained in a virtual environment.
- This technique of storage virtualization helps the administrator for any recovery or backup or archival of data in an effective and efficient manner by taking comparatively less time than the usual.

☞ **Methods to implement storage virtualization**

**(a) File-based Storage Virtualization**

- This type of virtualization is used for a specific purpose and can apply to network-attached storage (NAS) system.

- File-based storage virtualization in Cloud Computing utilizes server message block or network file system protocols and with its help of it breaks the dependency in a normal network attached storage array.
- This is done between the data being accessed and the location of the physical memory.
- It also provides a benefit of better handling file migration in the background which improves the performance.

**(b) Block-based Virtual Storage**

- The Block based virtual storage is more widely used than the virtual storage system as the virtual storage system is sometimes used for a specific purpose.
- The block-based virtual storage system uses logical storage such as drive partition from the physical memory in a storage device.
- It also abstracts the logical storage such as a hard disk drive or any solid-state memory device.
- This also allows the virtualization management software to get familiar with the capacity of the available device and split them into shared resources to assign.

**6. Network virtualization**

- Here we will be using software to decouple the virtual network form the baseline and it will perform the functionality of a network.
- After we have started using this network virtualization then we will be using the physical network for the sole purpose to forward the packets and we will be doing the management work using the software.
- We basically collect the entire network and with the help of the routing table we will manage it in real-time and they are also independent of each other.
- One example of network virtualization is VPN i.e., virtual private network. With the help of this anybody can create a network for them virtually on the internet.
- If we are providing network virtualization (NV) to one system, we will call it internal NV and if we are combining them in a virtual network, we call it as external NV.

## 3.4 ADVANTAGES AND DISADVANTAGES OF VIRTUALIZATION

**GQ.** Explain the advantages and disadvantages of virtualization.

☞ **Advantages :** Following are the advantages of virtualization:

1. **Uses Hardware Efficiently :** The majority of businesses invest a substantial amount of money in setting up their systems and servers, but only utilize a small portion of that investment successfully. If they choose virtualization, however, they can build multiple instances on the same hardware and maximize its value. This allows them to save money on hardware expenditures and achieve a high degree of efficiency.

2. **Available at all Times :** One of the best things about virtualization is that it has advanced features that make virtual instances always available. The best thing about this is that the virtual instance can be moved from one server location to another. It can be done without having to stop the processes that are already running and start them up again. It also makes sure that you don't lose any of your data while moving. So, even if there are unplanned downtimes, your instance will always be online and running. Because of this, virtualization service providers today offer 99.999 percent uptime for the same reason.

3. **Recovery is Easy :** With virtual instances on remote servers, duplication, backup, and recovery are also easier. With new tools available that provide near real-time data backup and mirroring, one can be sure of zero data loss at any point in time. In case of downtime or a crash, they can simply pick up from the last saved position mirrored on another virtual instance and run with it. This ensures business continuity at all times. Organizations can attain the highest efficiency with this.

4. **Quick and Easy Setup :** Setting up physical equipment and servers requires considerable time. You must submit a purchase order and await its processing. Wait for the products to be supplied and installed, which can take hours. After ensuring that all connections are correct, you must then install the necessary operating system and software, which takes additional time. The full procedure of installation requires days or even weeks of waiting. In contrast, with virtualization, you can have a productive setup up and running within minutes.

5. **Cloud Migration is Easier :** Many organizations are using old school methodologies even today. They have been doing so because they had made a substantial investment back in the day to ensure their IT systems were always up and running. With the current digital transformation wave, organizations are looking to move to the cloud for various advantages. The challenge here is the migration of such a large amount of data available on-premise. Virtualization would have made the task much easier because most of the data would already be available on a server. Hence, migrating all of it to the cloud would be easier.

### ☞ Disadvantages

The following are the disadvantages of virtualization:

1. **High Initial Investment :** As helpful virtualization is, it does have some flaws, and the high initial investment is one of the major one. Virtualization indeed helps the business reduce operational costs. But the initial setup cost of servers and storage is higher than a regular setup. Hence, companies need years before they break even and then realize savings and higher profitability with virtualization. It is a bad bet for companies opting for a large set up at the beginning. They could instead opt for a regular desktop setup and then gradually make a move to desktop virtualization.

2. **Data can be at Risk :** Working on virtual instances on shared hardware resources entails your data is hosted on a third-party resource. It can leave your data vulnerable to attacks or unauthorized access. This is a challenge if your service provider does not have proper security solutions to safeguard your virtual instance and data. It is true, specifically in the case of storage virtualization.

3. **Quick Scalability is a Problem :** Scaling on virtualization is a breeze, but not so much if it has to be done in a short period of time. In case of physical setup, one can quickly set up new hardware and scale, even if it entails some initial setting up complications. With virtualization, having to ensure all the requisite software, security, enough storage, and resource availability can be a tedious task. It consumes more time than one might expect since a third-party provider is involved. Moreover, the additional cost involved in increased resource use is another challenge to manage.
4. **Performance Witnesses a Dip :** It is true that virtualization allows the optimum use of all resources. However, it is also a challenge when you need that additional boost sometimes, but it is not available. Resources in virtualization are shared. The same resources that a single user might have consumed are now shared among three or four users. The overall available resources might not be shared equally or may be shared in some ratio depending upon the tasks being run. As the complexity of tasks increases, so does the need for performance from the system. It results in a substantially higher time required to complete the task.
5. **Unintended Server Sprawl :** Unintended server sprawl is a major cause of concern for many server admins and users alike. Many of the issues that service desk persons raise is of server sprawls. Setting up a physical server consumes time and resources, whereas a virtual server can be created in a matter of minutes. Every time, instead of reusing the same virtual server, users tend to create new servers since it allows them the chance to make a fresh start. The server administrator who should be handling five or six servers has to handle over 20 virtual servers. This can cause a major complication in the smooth operations, and forced termination of certain servers can also cause loss of data.

## 3.5 VIRTUALIZATION ARCHITECTURE

**GQ.** Explain Type-1 and Type-2 Hypervisors with neat diagram.
**GQ.** Explain the implementation levels of virtualization.

- Virtualization enables or allows multiple applications or operations to gain access to the hardware resources/software resources of the host machine.
- Virtualization is a layer between the hardware and the operating system, and it also provides access transparency.
- The hypervisors also known as the Virtual Machine Monitor (VMM), manages the applications and the operating system in general.
- There's a path created by the VMM which allows multiple of the same operating system to run on the host machine as well with the hypervisor managing the resources among the various operating system hardware requirement.
- The hypervisor plays a key role in Cloud hosting because it is a type of virtualization software that divides and allocates resources among a variety of hardware devices.
- Hypervisors are hardware virtualization techniques that allow multiple guest operating systems (OS) to run on a single host.

- A hypervisor is sometimes also called a virtual machine manager(VMM).
- There are two types of virtualization architectures: Bare metal virtualization and Hosted Virtualization.

### 3.5.1 Bare Metal Virtualization/ TYPE-1 Hypervisor

- The hypervisor runs directly on the underlying host system.
- It is also known as a "Native Hypervisor" or "Bare metal hypervisor".
- It does 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.

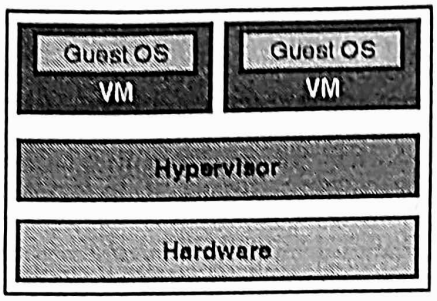


Fig. 3.5.1 : Type 1 Hypervisor

### 3.5.2 Hosted Virtualization/ TYPE-2 Hypervisor

- A Host operating system runs on the underlying host system.
- It is also known as 'Hosted Hypervisor".
- Such kind of hypervisors doesn't run directly over the underlying hardware rather they run as an application in a Host system (physical machine).
- Basically, the software is installed on an operating system. Hypervisor asks the operating system to make hardware calls.
- Containers, KVM, Microsoft Hyper V, VMWare Fusion, Virtual Server 2005 R2, Windows Virtual PC and VMWare workstation 6.0 are examples of Type 2 hypervisor.

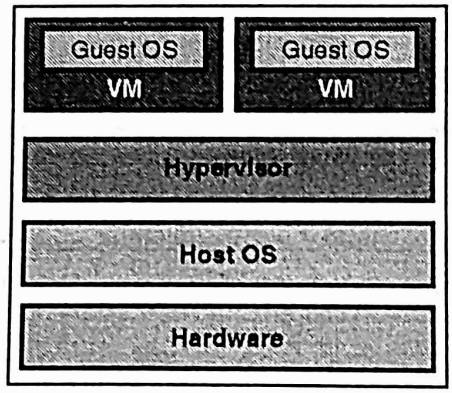


Fig. 3.5.2 : Type 2 Hypervisor

### 3.5.3 Implementation Levels of Virtualization

- Virtualization is not that easy to implement. A computer runs an OS that is configured to that particular hardware. Running a different OS on the same hardware is not exactly feasible.
- To tackle this, there exists a hypervisor. What hypervisor does is, it acts as a bridge between virtual OS and hardware to enable its smooth functioning of the instance. There are five levels of virtualizations available that are most commonly used in the industry. Fig. 3.5.3 below shows the five implementation levels of virtualization.

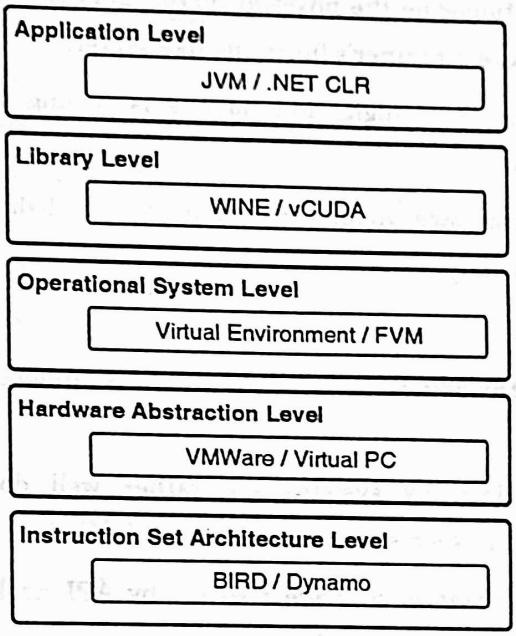


Fig. 3.5.3 : Implementation Levels of Virtualization

**1. Instruction Set Architecture Level (ISA)**

- In ISA, virtualization works through an ISA emulation. This is helpful to run heaps of legacy code which was originally written for different hardware configurations.
- These codes can be run on the virtual machine through an ISA.
- A binary code that might need additional layers to run can now run on an x86 machine or with some tweaking, even on x64 machines. ISA helps make this a hardware-agnostic virtual machine.
- The basic emulation, though, requires an interpreter. This interpreter interprets the source code and converts it to a hardware readable format for processing.

**2. Hardware Abstraction Level (HAL)**

- As the name suggests, this level helps perform virtualization at the hardware level. It uses a bare hypervisor for its functioning.
- This level helps form the virtual machine and manages the hardware through virtualization.
- It enables virtualization of each hardware component such as I/O devices, processors, memory, etc.
- This way multiple users can use the same hardware with numerous instances of virtualization at the same time.

- IBM had first implemented this on the IBM VM/370 back in 1960. It is more usable for cloud-based infrastructure. Xen hypervisors are using HAL to run Linux and other OS on x86 based machines.

### 3. Operating System Level

- At the operating system level, the virtualization model creates an abstract layer between the applications and the OS.
- It is like an isolated container on the physical server and operating system that utilizes hardware and software. Each of these container's functions like servers.
- When the number of users is high, and no one is willing to share hardware, this level of virtualization comes in handy.
- Here, every user gets their own virtual environment with dedicated virtual hardware resources. This way, no conflicts arise.

### 4. Library Level

- OS system calls are lengthy and cumbersome. Due to this, applications opt for APIs from user-level libraries.
- Most of the APIs provided by systems are rather well documented. Hence, library level virtualization is preferred in such scenarios.
- Library interfacing virtualization is made possible by API hooks. These API hooks control the communication link from the system to the applications.
- Some tools available today, such as vCUDA and WINE, have successfully demonstrated this technique.

### 5. Application Level

- Application-level virtualization comes handy when you wish to virtualize only an application. It does not virtualize an entire platform or environment.
- On an operating system, applications work as one process. Hence it is also known as process-level virtualization.
- It is generally useful when running virtual machines with high-level languages. Here, the application sits on top of the virtualization layer, which is above the application program.
- The application program is, in turn, residing in the operating system.
- Programs written in high-level languages and compiled for an application-level virtual machine can run fluently here.

## 3.6 VIRTUALIZATION SOFTWARE

**GQ.** Define virtualization software. Explain features of any two virtualizations software.

Virtualization software can be defined as a kind of a computer program which helps in achieving IT abstraction, to make it clear it can be said as it helps in hiding or masking the physical resources from the end-user.

### 3.6.1 Benefits of Using Virtualization Software

1. One can use multiple operating systems in a single computer.
2. One can share the components of the single operating system hosted centrally on multiple computer systems located at a different geographical location.
3. With the use of virtualization software, one can utilize the full capacity of the computer system as this helps improves the performance in terms of speed and functionality.
4. Virtualization software also provides security options that help to keep the data as well as the resources that are shared among different users safe. There is a feature known as a snapshot in the virtualization where one can take a backup of a current working system and restore that when the system runs into trouble.

### 3.6.2 Different Virtualization Softwares

Now let's discuss the different Virtualization Softwares which are available in the market to do virtualization:

**1. SolarWinds Virtualization Manager**

- This is kind of management software for all the virtual machines, this software helps in tracking the performance and fixing if there are any performance issues such as memory and storage.
- It provides complete visibility for all the virtual machines attached to the system.
- The tool has the functionality to manually fix all the performance issues and trigger if any issues are reported.
- This tool is also useful in maintaining the cloud platforms and the check on their usage or performance of it.
- There are triggers and automatic indications present in the tool which helps the user to monitor everything properly.

**2. VMware Fusion**

- This software is for Mac users where one can run Windows, Linux, Unix and any other operating system on their Mac using this software.
- VMware Fusion also supports cloud-based platforms for virtualization.

- The VMware fusion pro version provides the facility of integration of different development tools with it.
- This software is very simple to use and can support real-time demonstration for different software's and applications.
- It also has a rollback point where can save the last proper working versions of the OS and can go back to it whenever required.
- The only drawback as of now for this tool is that the drag and drop functionality is not proper and needs improvement.

**3. Parallels Desktop**

- This software is also for the Mac users to use windows and another operating system.
- This supports windows 10 and Mac OS High Sierra
- They provide lots of different tools which are very useful for daily day to day tasks.
- The view for this software is very good and it requires no reboot while installation.
- The performance for the application inside the virtual OS is also very fast and easily usable without any lag.

**4. Virtual Box**

- This virtual box comes from Oracle and the best part of them is its very user friendly.
- This software is used in windows to run different operating systems.
- At a time, it can host up to 4 operating system.
- It supports drag and drops feature and the window can be minimized and resized.

**5. VMware Workstation**

- This is the most popular and widely used virtualization software.
- It supports multiple operating systems especially windows and Linux.
- It's made for the developers and IT professionals who generally work on different OS.
- This can be integrated with multiple applications.
- This software also supports cloud applications.

**6. QEMU**

- This software is used for hardware virtualization.
- This is also an open-source free software.
- There is no restriction for the host OS that means this software can run in mac as well as a windows system.
- But the only con in this is it's not at all user-friendly.

**7. Windows Virtual PC**

- This software comes with the windows operating system.
- This is only for windows users and it is very much user-friendly.
- One can use the print option from inside the virtual box and can run multiple virtual machines simultaneously.
- The only drawback for this one is that it doesn't support any other OS apart from the windows.

**8. Microsoft Hyper V**

- This software comes bundled with Microsoft windows server 2008 and later.
- It provides hardware virtualization.
- This software supports the running of multiple virtual machines.
- This supports cloud as well such as Microsoft Azure.
- This supports multiple versions of the Linux operating system.

**9. RedHat Virtualization**

- This virtualization software comes from the RedHat family.
- This software is written in java and as promised by the RedHat software company it provides very good performance for the application which are running inside the virtual machine.
- It's an open-source system so any user can tweak the code and make it work for his own use and application.
- It's free software and the installation for this is very easy.

## 3.7 VIRTUAL CLUSTERING

**GQ.** Explain virtual clustering. Compare it with physical clustering.

- Virtual cluster is a many-to-one virtualization technology, which can form a routing system from multiple common devices connected through a switching network, while performing the same as a single logical router to all external appearances.
- In cloud computing, a virtual cluster is a group of virtual machines (VMs) that are deployed as a single logical unit. They share the same virtualization software and hardware, and they appear as a single unit to the end-user.
- Virtual clusters provide the ability to scale operations easily. You can add or remove VMs to meet changing demands, and you can move VMs to optimize the use of hardware. You can leverage a virtual clustering solution to reduce data center costs, increase efficiency, and increase scalability.
- Clusters provide the computational power through the use of parallel programming, a technique for coordinating the use of many processors for a single problem.

- A cluster of virtual servers will be used to host the services to support high availability and resource utilization.
- Virtual clusters also provide flexibility in adding more services in the future, with minimal code and configuration changes. An additional standby virtual cluster is also used.
- Virtual clusters work by enhancing the server utilization.
- Virtual machine clusters work by protecting the physical machine from any hardware and software failures. When a physical node fails, the virtual machine can access another node, with no time lag. And thus, virtual machine clustering provides a dynamic backup process.

### 3.7.1 Comparison of Physical Cluster and Virtual Cluster

**Table 3.7.1 : Physical Cluster Vs Virtual Cluster**

| Sr. No. | Physical Cluster | Virtual Cluster |
|---|---|---|
| 1. | A physical cluster is a group of server units (servers or computer systems) that are deployed physically together in one location or multiple locations, connected with a physical network. | A virtual cluster is a group of virtual machines (VMs) deployed as a single logical unit in a single data center or in multiple data centers connected with a virtual network. |
| 2. | Physical clusters are connected by network cables and are managed with a single system console. | Virtual clusters are connected by a virtual network and are managed with multiple user consoles. |
| 3. | Physical clusters are created on different systems, and they have different hardware. | Virtual clusters are created on a single system, and they share the same virtualization software and hardware. |

### 3.7.2 Benefits of Virtual Clusters

- Even though physical clusters are more reliable than virtual ones, VMs are more secure because they are not linked to the hardware. Data security is an important issue for virtual clusters, and there are several ways to secure data.
- Virtual clusters are highly scalable, so you can add or remove VMs to meet changing demands, and you can move VMs to optimize the use of hardware.
- Virtual clusters are easy to manage and provide a higher level of flexibility.
- Virtual clusters minimize dependencies on hardware and are more reliable during failover and failback operations.

## 3.8 APPLICATIONS OF VIRTUALIZATION

**GQ.** Enlist the applications of virtualization.

In this section, we will discuss few of the application areas of virtualization.

1. **Server Consolidation**
   - Virtual machines are used to consolidate many physical servers into fewer servers.
   - Each physical server is reflected as a virtual machine "guest". They reside on a virtual machine host system.
   - This is also known as "Physical-to-Virtual" or 'P2V' transformation.
2. **Disaster Recovery**
   - Virtual machines can be used as "hot standby" environments for physical production servers.
   - Virtual storage can be replicated and transferred to another location. Virtualization is very useful in planning for disaster recovery.
3. **Testing and Training**
   - Virtualization can give root access to a virtual machine.
   - This can be very useful such as in kernel development and operating system courses.
4. **Portable Applications**
   - Portable applications are needed when running an application from a removable drive, without installing it on the system's main disk drive.
   - Virtualization can be used to store temporary files, windows registry entries and other information in the application's installation directory and not within the system's permanent file system.
5. **Portable Workspaces**

   Recent technologies have used virtualization to create portable workspaces on devices like iPods and USB memory sticks.

## 3.9 DESCRIPTIVE QUESTIONS

**Q. 1** Define virtualization. State the characteristics of virtualization.
**Q. 2** Differentiate between cloud computing and virtualization.
**Q. 3** Explain different architectures of virtualization. Also explain implementation levels of virtualization.
**Q. 4** Differentiate between hardware virtualization and software virtualization.
**Q. 5** Explain server virtualization and network virtualization.
**Q. 6** What is storage virtualization ? Explain the methods to implement storage virtualization.
**Q. 7** Write a note on : Virtual Clusters
**Q. 8** State the advantages and disadvantages of virtualization. State the applications of virtualization.
**Q. 9** State the features of any two virtualization softwares.

*Chapter Ends*

□□□

# UNIT IV

# CHAPTER 4

# Service Oriented Architecture and Cloud Security

**University Prescribed Syllabus**

**Cloud Computing Architecture (COA) :** Design principles, Cloud computing life cycle (CCLC), Cloud computing reference architecture, Service Oriented Architecture (SOA) characteristics and fundamental components.

**Cloud Security :** Cloud CIA security model (Confidentiality, Integrity and Availability), Cloud computing security architecture, Service provider security issues, Cloud Security Issues and challenges, Security issues in virtualization, Host Security, Data Security, Firewalls

## 4.1 DESIGN PRINCIPLES OF CLOUD COMPUTING ARCHITECTURE (COA)

**GQ.** Explain in detail Design Principles of COA.

- Cloud Computing, which is one of the demanding technologies of the current time and which is giving a new shape to every organization by providing on demand virtualized services.
- Starting from small to medium and medium to large, every organization use cloud computing services for storing information and accessing it from anywhere and anytime only with the help of internet.
- The cloud computing technology is used by both small and large organizations to store the information in cloud and access it from anywhere at any time using the internet connection.
- Cloud computing architecture is a combination of service-oriented architecture and event-driven architecture.
- Transparency, scalability, security and intelligent monitoring are some of the most important constraints which every cloud infrastructure should experience.
- Current research on other important constraints is helping cloud computing system to come up with new features and strategies with a great capability of providing more advanced cloud solutions.
- Cloud computing architecture is divided into the following two parts -
  - Front End
  - Back End

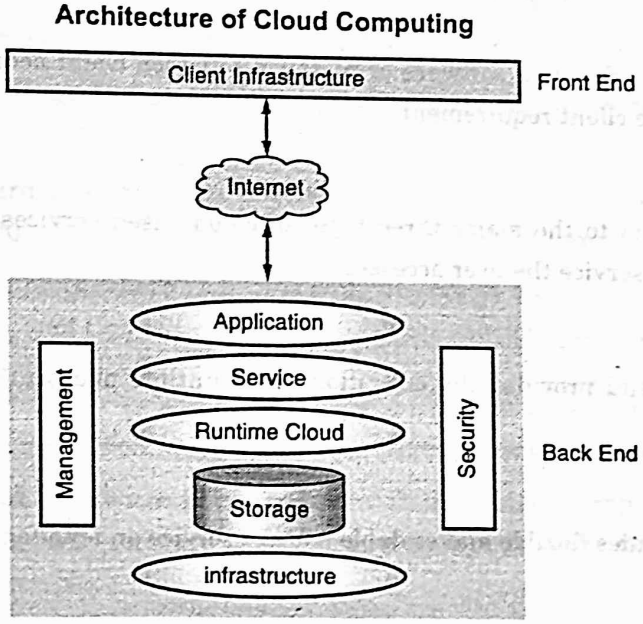


**Fig. 4.1.1 : Architecture of cloud computing**

- Architecture of cloud computing is the combination of both SOA (Service Oriented Architecture) and EDA (Event Driven Architecture).

- Client infrastructure, application, service, runtime cloud, storage, infrastructure, management and security all these are the components of cloud computing architecture.

**1. Frontend**

- Frontend of the cloud architecture refers to the client side of cloud computing system. Means it contains all the user interfaces and applications which are used by the client to access the cloud computing services/resources. For example, use of a web browser to access the cloud platform. It contains client-side interfaces and applications that are required to access the cloud computing platforms.
- The front end includes web servers (including Chrome, Firefox, internet explorer, etc.), thin & fat clients, tablets, and mobile devices.
- Client Infrastructure – Client Infrastructure is a part of the frontend component. It contains the applications and user interfaces which are required to access the cloud platform.
- In other words, it provides a GUI (Graphical User Interface) to interact with the cloud.

**2. Backend**

- Backend refers to the cloud itself which is used by the service provider. It contains the resources as well as manages the resources and provides security mechanisms.
- Along with this, it includes huge storage, virtual applications, virtual machines, traffic control mechanisms, deployment models, etc.

**Application**

Application in backend refers to a software or platform to which client accesses. Means it provides the service in backend as per the client requirement.

**Service**

Service in backend refers to the major three types of cloud-based services like SaaS, PaaS and IaaS. Also manages which type of service the user accesses.

**Runtime Cloud**

Runtime cloud in backend provides the execution and Runtime platform/environment to the Virtual machine.

**Storage**

Storage in backend provides flexible and scalable storage service and management of stored data.

**Infrastructure**

Cloud Infrastructure in backend refers to the hardware and software components of cloud like i includes servers, storage, network devices, virtualization software etc.

**Management**

Management in backend refers to management of backend components like application, service, runtime cloud, storage, infrastructure, and other security mechanisms etc.

**Security**

Security in backend refers to implementation of different security mechanisms in the backend for secure cloud resources, systems, files, and infrastructure to end-users.

**Internet**

Internet connection acts as the medium or a bridge between frontend and backend and establishes the interaction and communication between frontend and backend.

- Benefits of Cloud Computing Architecture:
- Makes overall cloud computing system simpler.
- Improves data processing requirements.
- Helps in providing high security.
- Makes it more modularized.
- Results in better disaster recovery.
- Gives good user accessibility.
- Reduces IT operating costs.

## 4.2 CLOUD COMPUTING LIFE CYCLE (CCLC)

- Cloud Computing is the booming industry of the present time and will continue to grow by many folds in the near future.
- Nowadays, it's really hard to find a safe, secure, and yet cost-effective place to store your data and business-critical ideas. But, with the rise of cloud computing, this problem is vanishing exponentially.
- Cloud provides us with a place where your data can not only be stored but can also be accessed easily over the internet. Using Cloud Computing you can also host and manage your applications.

**GQ.** Why we need Cloud Computing Solution ?

By using Cloud Computing Solution, we get various benefits, some of which are as follows

- **Improved software and hardware performance :** Through cloud computing solution one can easily make out what will be the best software and hardware specification for the better performance of the application running on the cloud.
- **Flexibility and affordability :** Cloud Computing provides its users with a wide variety of deployment models and functions through which they can choose the best options for their applications. Cloud services are much more affordable.

- **Increased uptime and availability :** It is highly available and has a great uptime which help's in managing more amount of traffic at a particular time.
- Better collaboration with real-time sharing – cloud computing has great real-time sharing.

### 4.2.1 Life Cycle of Cloud Computing Solution

To create such a cloud platform, it takes a long number of steps and dedicated time. Let's now look at the steps involved or the lifecycle of cloud computing solutions.

**Step 1 : Define the Purpose**

The first and foremost step is to define the purpose for which you want to create a cloud. For this, you have first to understand your business requirement and what type of application you want to run on the cloud. After this, you have to decide whether you want your cloud to be public, private, or hybrid.

**Step 2 : Define the Hardware**

Deciding what type of hardware, you will need is the most thought after the process. One needs to be very precise in making the decision. For this, you will have to choose the compute service that will provide the right support when you resize your compute capacity to maintain your application running.

**Step 3 : Define the Storage**

Every application needs a good amount of storage where it's data can be stored safely. For any application storage type that should be chosen carefully for this one should choose the storage service where they can back up and archive their data over the internet.

**Step 4 : Define the Network**

Networking is the key that will deliver your data to the end-users. So, the network must be configured sincerely and should be flawless so that intruders cannot break into the network. One should define the network that securely delivers data, videos, and applications with low latency and high transfer speed.

**Step 5 : Define the Security**

Security is a key aspect of any application. Set up your security service which enables services for user authentication or limiting access to a certain set of users on your resources.

**Step 6 : Define the Management Process and Tools**

The developer should have complete control over there resource and to configure these you should define some management tools which monitor your cloud environment, resources used, and the customer application running on it.

**Step 7 : Testing the Process**

Testing is yet another important thing in the life cycle of deploying any application. All the faults can figure out only through the testing process involved in it. During testing, you should verify your application using various developer tools where you build, test, and deploy your code quickly.

**Step 8 : Analytics**

Finally, analyse and visualize data using analytics service where you can start querying data instantly and get results then and there only. Once analysing is done complete, your application becomes ready you deploying.

☞ **Advantages**

- **Cost Saving :** It helps you to save substantial capital costs as it does not need any physical hardware investments.
- **High Speed :** Cloud computing allows you to deploy your service quickly in fewer clicks.
- **Backup and restore of data :** Back up and restore of data is easy in cloud computing.
- **Reliability :** It is highly reliable to use cloud computing solutions.

☞ **Disadvantages**

- **Performance can vary :** Its performance depends on the speed and quality of the internet
- **Downtime :** Cloud Computing Solutions has a great span of downtime.

## 4.3 SERVICE ORIENTED ARCHITECTURE (SOA)

A Service-Oriented Architecture or SOA is a design pattern which is designed to build distributed systems that deliver services to other applications through the protocol. It is only a concept and not limited to any programming language or platform.

**GQ.** What is Service Oriented Architecture ?

- A service is a well-defined, self-contained function that represents a unit of functionality.
- A service can exchange information from another service. It is not dependent on the state of another service. It uses a loosely coupled, message-based communication model to communicate with applications and other services.

☞ **Service Connections**

- The figure given below illustrates the service-oriented architecture.
- Service consumer sends a service request to the service provider, and the service provider sends the service response to the service consumer.
- The service connection is understandable to both the service consumer and service provider.

### 4.3.1 Service Oriented Architecture (SOA)

- Service-Oriented Terminologies
- Let's see some important service-oriented terminologies
- Service-Oriented Architecture (SOA) is a stage in the evolution of application development and/or integration. It defines a way to make software components reusable using the interfaces.

- Formally, SOA is an architectural approach in which applications make use of services available in the network. In this architecture, services are provided to form applications, through a network call over the internet. It uses common communication standards to speed up and streamline the service integrations in applications.
- Each service in SOA is a complete business function in itself. The services are published in such a way that it makes it easy for the developers to assemble their apps using those services. Note that SOA is different from microservice architecture.
- SOA allows users to combine a large number of facilities from existing services to form applications.
- SOA encompasses a set of design principles that structure system development and provide means for integrating components into a coherent and decentralized system.
- SOA-based computing packages functionalities into a set of interoperable services, which can be integrated into different software systems belonging to separate business domains.
- There are two major roles within Service-oriented Architecture :
  1. **Service provider :** The service provider is the maintainer of the service and the organization that makes available one or more services for others to use. To advertise services, the provider can publish them in a registry, together with a service contract that specifies the nature of the service, how to use it, the requirements for the service, and the fees charged.
  2. **Service consumer :** The service consumer can locate the service metadata in the registry and develop the required client components to bind and use the service.
- Services might aggregate information and data retrieved from other services or create workflows of services to satisfy the request of a given service consumer. This practice is known as service orchestration.
- Another important interaction pattern is service choreography, which is the coordinated interaction of services without a single point of control.

### 4.3.2 Guiding Principles of SOA

- **Standardized service contract :** Specified through one or more service description documents.
- **Loose coupling :** Services are designed as self-contained components, maintain relationships that minimize dependencies on other services.
- **Abstraction :** A service is completely defined by service contracts and description documents. They hide their logic, which is encapsulated within their implementation.
- **Reusability :** Designed as components, services can be reused more effectively, thus reducing development time and the associated costs.
- **Autonomy :** Services have control over the logic they encapsulate and, from a service consumer point of view, there is no need to know about their implementation.
- **Discoverability :** Services are defined by description documents that constitute supplemental metadata through which they can be effectively discovered. Service discovery provides an effective means for utilizing third-party resources.

- **Composability :** Using services as building blocks, sophisticated and complex operations can be implemented. Service orchestration and choreography provide a solid support for composing services and achieving business goals.

### ☞ Advantages of SOA

1. **Service reusability :** In SOA, applications are made from existing services. Thus, services can be reused to make many applications.
2. **Easy maintenance :** As services are independent of each other they can be updated and modified easily without affecting other services.
3. **Platform independent :** SOA allows making a complex application by combining services picked from different sources, independent of the platform.
4. **Availability :** SOA facilities are easily available to anyone on request
5. **Reliability :** SOA applications are more reliable because it is easy to debug small services rather than huge codes
6. **Scalability :** Services can run on different servers within an environment, this increases scalability

### ☞ Disadvantages of SOA

1. **High overhead :** A validation of input parameters of services is done whenever services interact this decreases performance as it increases load and response time.
2. **High investment :** A huge initial investment is required for SOA.

- Complex service management : When services interact, they exchange messages to tasks. the number of messages may go in millions. It becomes a cumbersome task to handle a large number of messages.
- Practical applications of SOA : SOA is used in many ways around us whether it is mentioned or not.
- SOA infrastructure is used by many armies and air forces to deploy situational awareness systems.

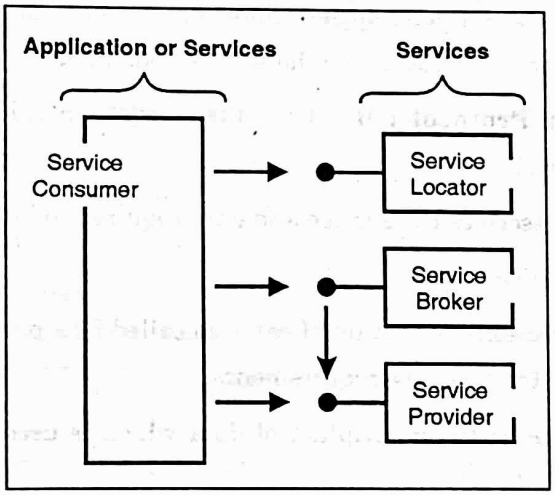


**Fig. 4.3.1 : Service oriented Architecture**

- **Services :** The services are the logical entities defined by one or more published interfaces.
- **Service provider :** It is a software entity that implements a service specification.
- **Service consumer :** It can be called as a requestor or client that calls a service provider. A service consumer can be another service or an end-user application.
- **Service locator :** It is a service provider that acts as a registry. It is responsible for examining service provider interfaces and service locations.
- **Service broker :** It is a service provider that pass service requests to one or more additional service providers.

### 4.3.3 Characteristics of SOA

The services have the following characteristics :

- They are loosely coupled.
- They support interoperability.
- They are location-transparent
- They are self-contained.

**Components of service-oriented architecture**

The service-oriented architecture stack can be categorized into two parts - functional aspects and quality of service aspects.

- Service Oriented Architecture (SOA)
- Functional aspects

**The functional aspect contains**

- **Transport :** It transports the service requests from the service consumer to the service provider and service responses from the service provider to the service consumer.
- **Service Communication Protocol :** It allows the service provider and the service consumer to communicate with each other.
- **Service Description :** It describes the service and data required to invoke it.
- **Service :** It is an actual service.
- **Business Process :** It represents the group of services called in a particular sequence associated with the particular rules to meet the business requirements.
- **Service Registry :** It contains the description of data which is used by service providers to publish their services.

Quality of Service aspects

☞ **The quality of service aspects contains**

- **Policy :** It represents the set of protocols according to which a service provider make and provide the services to consumers.
- **Security :** It represents the set of protocols required for identification and authorization.
- **Transaction :** It provides the surety of consistent result. This means, if we use the group of services to complete a business function, either all must complete or none of the complete.
- **Management :** It defines the set of attributes used to manage the services.

☞ **Advantages of SOA in terms of quality**

SOA has the following advantages :

1. **Easy to integrate :** In a service-oriented architecture, the integration is a service specification that provides implementation transparency.
2. **Manage Complexity :** Due to service specification, the complexities get isolated, and integration becomes more manageable.
3. **Platform Independence :** The services are platform-independent as they can communicate with other applications through a common language.
4. **Loose coupling :** It facilitates to implement services without impacting other applications or services.
5. **Parallel Development :** As SOA follows layer-based architecture, it provides parallel development.
6. **Available :** The SOA services are easily available to any requester.
7. **Reliable :** As services are small in size, it is easier to test and debug them.

SOA is used to improve healthcare delivery.

- Nowadays many apps are games and they use inbuilt functions to run. For example, an app might need GPS so it uses the inbuilt GPS functions of the device. This is SOA in mobile solutions.

## 4.4 CLOUD SECURITY

Cloud CIA security model (Confidentiality, Integrity and Availability)

**GQ.** What is Cloud Security ?

- Confidentiality, integrity and availability, also known as the CIA triad, is a model designed to guide policies for information security within an organization.
- The model is also sometimes referred to as the AIC triad (availability, integrity and confidentiality) to avoid confusion with the Central Intelligence Agency. Although elements of the triad are three of the most foundational and crucial cyber security needs, experts believe the CIA triad needs an upgrade to stay effective.
- In this context, confidentiality is a set of rules that limits access to information, integrity is the assurance that the information is trustworthy and accurate, and availability is a guarantee of reliable access to the information by authorized people.

Confidentiality, integrity, availability

The following is a breakdown of the three key concepts that form the CIA triad :

- Confidentiality is roughly equivalent to privacy. Confidentiality measures are designed to prevent sensitive information from unauthorized access attempts. It is common for data to be categorized according to the amount and type of damage that could be done if it fell into the wrong hands.
- More or less stringent measures can then be implemented according to those categories.
- Integrity involves maintaining the consistency, accuracy and trustworthiness of data over its entire lifecycle.
- Data must not be changed in transit, and steps must be taken to ensure data cannot be altered by unauthorized people (for example, in a breach of confidentiality).
- Availability means information should be consistently and readily accessible for authorized parties. This involves properly maintaining hardware and technical infrastructure and systems that hold and display the information.
- Diagram of CIA triad
- The three CIA triad principles

**GQ.** Why is the CIA important ?

- With each letter representing a foundational principle in cyber security, the importance of the CIA triad security model speaks for itself.
- Confidentiality, integrity and availability together are considered the three most important concepts within information security.
- Considering these three principles together within the framework of the "triad" can help guide the development of security policies for organizations. When evaluating needs and use cases for potential new products and technologies, the triad helps organizations ask focused questions about how value is being provided in those three key areas.
- Thinking of the CIA triad's three concepts together as an interconnected system, rather than as independent concepts, can help organizations understand the relationships between the three.

**GQ.** What are examples of the CIA t ?

Here are examples of the various management practices and technologies that comprise the CIA triad. While many CIA triad cyber security strategies implement these technologies and practices, this list is by no means exhaustive.

### ☞ Confidentiality

- Sometimes safeguarding data confidentiality involves special training for those privy to sensitive documents. Training can help familiarize authorized people with risk factors and how to guard against them.
- Further aspects of training may include strong passwords and password-related best practices and information about social engineering methods to prevent users from bending data-handling rules with good intentions and potentially disastrous results.

- A good example of methods used to ensure confidentiality is requiring an account number or routing number when banking online.
- Data encryption is another common method of ensuring confidentiality. User IDs and passwords constitute a standard procedure; two-factor authentication (2FA) is becoming the norm. Other options include Biometric verification and security tokens, key fobs or soft tokens.
- In addition, users can take precautions to minimize the number of places where information appears and the number of times it is actually transmitted to complete a required transaction.
- Extra measures might be taken in the case of extremely sensitive documents, such as storing only on air-gapped computers, disconnected storage devices or, for highly sensitive information, in hard-copy form only.

☞ **Integrity**

- These measures include file permissions and user access controls. Version control may be used to prevent erroneous changes or accidental deletion by authorized users from becoming a problem.
- In addition, organizations must put in some means to detect any changes in data that might occur as a result of non-human-caused events such as an electromagnetic pulse (EMP) or server crash.
- Data might include checksums, even cryptographic checksums, for verification of integrity. Backups or redundancies must be available to restore the affected data to its correct state.
- Furthermore, digital signatures can be used to provide effective no repudiation measures, meaning evidence of logins, messages sent, electronic document viewing and sending cannot be denied.

☞ **Availability**

- This is best ensured by rigorously maintaining all hardware, performing hardware repairs immediately when needed and maintaining a properly functioning operating system (OS) environment that is free of software conflicts. It's also important to keep current with all necessary system upgrades.
- Providing adequate communication bandwidth and preventing the occurrence of bottlenecks are equally important tactics. Redundancy, failover, RAID -- even high-availability clusters -- can mitigate serious consequences when hardware issues do occur.
- Fast and adaptive disaster recovery is essential for the worst-case scenarios; that capacity relies on the existence of a comprehensive DR plan.
- Safeguards against data loss or interruptions in connections must include unpredictable events such as natural disasters and fire. To prevent data loss from such occurrences, a backup copy may be stored in a geographically isolated location, perhaps even in a fireproof, waterproof safe.
- Extra security equipment or software such as firewalls and proxy servers can guard against downtime and unreachable data blocked by malicious denial-of-service (DoS) attacks and network intrusions.

### 4.4.1 Special Challenges for the CIA Triad

- Big data poses challenges to the CIA paradigm because of the sheer volume of information that organizations need safeguarded, the multiplicity of sources that data comes from and the variety of formats in which it exists.
- Duplicate data sets and disaster recovery plans can multiply the already-high costs. Furthermore, because the main concern of big data is collecting and making some kind of useful interpretation of all this information, responsible data oversight is often lacking.
- Whistle-blower Edward Snowden brought that problem to the public forum when he reported on the National Security Agency's collection of massive volumes of American citizens' personal data.
- Internet of things privacy protects the information of individuals from exposure in an IoT environment. Almost any physical or logical entity or object can be given a unique identifier and the ability to communicate autonomously over the internet or a similar network.
- The data transmitted by a given endpoint might not cause any privacy issues on its own. However, when even fragmented data from multiple endpoints is gathered, collated and analysed, it can yield sensitive information.
- Internet of things security is also challenging because IoT consists of so many internet-enabled devices other than computers, which often go unpatched and are often configured with default or weak passwords.
- Unless adequately protected, IoT could be used as a separate attack vector or part of a thinghood. As more and more products are developed with the capacity to be networked, it's important to routinely consider security in product development.

### 4.4.2 Best practices for Implementing the CIA Triad

In implementing the CIA triad, an organization should follow a general set of best practices. Some best practices, divided by each of the three subjects, include:

**Confidentiality**

1. Data should be handled based on the organization's required privacy.
2. Data should be encrypted using 2FA.
3. Keep access control lists and other file permissions up to date.
4. Integrity
5. Ensure employees are knowledgeable about compliance and regulatory requirements to minimize human error.
6. Use backup and recovery software.
7. To ensure integrity, use version control, access control, security control, data logs and checksums.

☞ **Availability**

1. Use preventive measures such as redundancy, failover and RAID. Ensure systems and applications stay updated.
2. Use network or server monitoring systems.
3. Ensure a data recovery and business continuity (BC) plan is in place in case of data loss.

## 4.5 CLOUD COMPUTING SECURITY ARCHITECTURE

**GQ.** Explain in detail Cloud Computing Security Architecture.

- Security in cloud computing is a major concern.
- Proxy and brokerage services should be employed to restrict a client from accessing the shared data directly.
- Data in the cloud should be stored in encrypted form.

☞ **Security Planning**

Before deploying a particular resource to the cloud, one should need to analyze several aspects of the resource, such as :

- A select resource needs to move to the cloud and analyze its sensitivity to risk. Consider cloud service models such as IaaS, PaaS, and These models require the customer to be responsible for Security at different service levels.
- Consider the cloud type, such as public, private, community, or Understand the cloud service provider's system regarding data storage and its transfer into and out of the cloud.
- The risk in cloud deployment mainly depends upon the service models and cloud types.

### 4.5.1 Understanding Security of Cloud

☞ **Security Boundaries**

- The Cloud Security Alliance (CSA) stack model defines the boundaries between each service model and shows how different functional units relate.
- A particular service model defines the boundary between the service provider's responsibilities and the customer.

- The following diagram shows the CSA stack model :

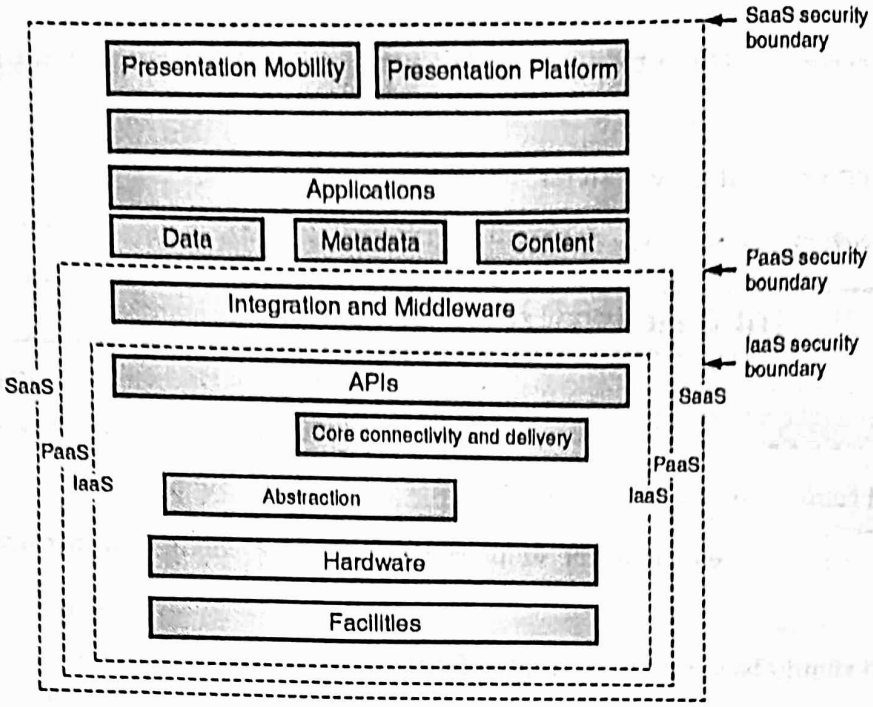


**Fig. 4.5.1 : Cloud Computing Security Architecture**

### 4.5.2 Key Points to CSA Model

- IaaS is the most basic level of service, with PaaS and SaaS next two above levels of services. Moving upwards, each service inherits the capabilities and security concerns of the model beneath.
- IaaS provides the infrastructure, PaaS provides the platform development environment, and SaaS provides the operating environment.
- IaaS has the lowest integrated functionality and security level, while SaaS has the highest. This model describes the security boundaries at which cloud service providers' responsibilities end and customers' responsibilities begin.
- Any protection mechanism below the security limit must be built into the system and maintained by the customer. Although each service model has a security mechanism, security requirements also depend on where these services are located, private, public, hybrid, or community cloud.

**Understanding data security**

- Since all data is transferred using the Internet, data security in the cloud is a major concern. Here are the key mechanisms to protect the data.
  - access control
  - audit trail
  - certification
  - authority
- The service model should include security mechanisms working in all of the above areas.

### 4.5.3 Separate Access to Data

- Since the data stored in the cloud can be accessed from anywhere, we need to have a mechanism to isolate the data and protect it from the client's direct access.
- Broker cloud storage is a way of separating storage in the Access Cloud. In this approach, two services are created :
  - A broker has full access to the storage but does not have access to the client.
  - A proxy does not have access to storage but has access to both the client and the broker.
  - Working on a Brocade cloud storage access system
  - When the client issues a request to access data:
  - The client data request goes to the external service interface of the proxy.
  - The proxy forwards the request to the broker.
  - The broker requests the data from the cloud storage system.
  - The cloud storage system returns the data to the broker.
  - The broker returns the data to the proxy.
  - Finally, the proxy sends the data to the client.

**All the above steps are shown in the following diagram**

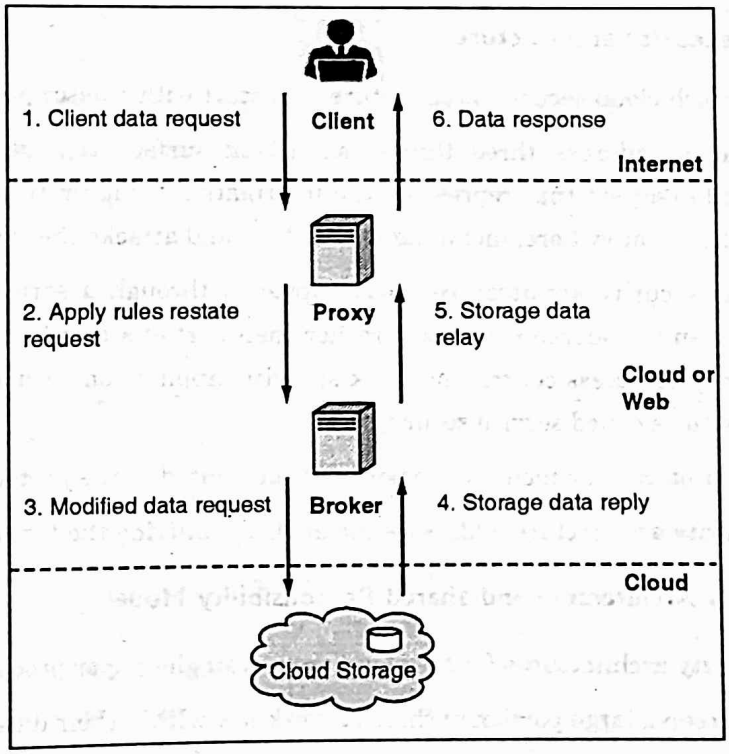


**Fig. 4.5.2 : Steps for Cloud Storage Access**

### ☞ Encoding

- Encryption helps to protect the data from being hacked. It protects the data being transferred and the data stored in the cloud.
- Although encryption helps protect data from unauthorized access, it does not prevent data loss.

**GQ.** Why is cloud security architecture important ?

- The difference between "cloud security" and "cloud security architecture" is that the former is built from problem-specific measures while the latter is built from threats.
- A cloud security architecture can reduce or eliminate the holes in Security that point-of-solution approaches are almost certainly about to leave.
- It does this by building down - defining threats starting with the users, moving to the cloud environment and service provider, and then to the applications.
- Cloud security architectures can also reduce redundancy in security measures, which will contribute to threat mitigation and increase both capital and operating costs.
- The cloud security architecture also organizes security measures, making them more consistent and easier to implement, particularly during cloud deployments and redeployments.
- Security is often destroyed because it is illogical or complex, and these flaws can be identified with the proper cloud security architecture.

### ☞ Elements of cloud security architecture

- The best way to approach cloud security architecture is to start with a description of the goals.
- The architecture has to address three things: an attack surface represented by external access interfaces, a protected asset set that represents the information being protected, and vectors designed to perform indirect attacks anywhere, including in the cloud and attacks the system.
- The goal of the cloud security architecture is accomplished through a series of functional elements. These elements are often considered separately rather than part of a coordinated architectural plan. It includes access security or access control, network security, application security, contractual Security, and monitoring, sometimes called service security.
- Finally, there is data protection, which are measures implemented at the protected-asset level.
- A complete cloud security architecture addresses the goals by unifying the functional elements.

## 4.5.4 Cloud Security Architecture and Shared Responsibility Model

- The security and security architectures for the cloud are not single-player processes.
- Most enterprises will keep a large portion of their IT workflow within their data centres, local networks, and VPNs.
- The cloud adds additional players, so the cloud security architecture should be part of a broader shared responsibility model.

- A shared responsibility model is an architecture diagram and a contract form. It exists formally between a cloud user and each cloud provider and network service provider if they are contracted separately.
- Each will divide the components of a cloud application into layers, with the top layer being the responsibility of the customer and the lower layer being the responsibility of the cloud provider.
- Each separate function or component of the application is mapped to the appropriate layer depending on who provides it. The contract form then describes how each party responds.

## 4.6 SERVICE PROVIDER SECURITY ISSUES

- In addition to the general security concerns that affect anyone who uses IT technology or connects to the Internet, the community of service providers has its own set of security-related issues to deal with.

**GQ.** What are the security issues in cloud service providers ?

The most important security issues that service providers face is the following :

- Denial of service (DoS) and distributed denial of service (DDoS) attacks are aimed at disabling access to various Internet services for legitimate users.
- Excessive traffic and resource depletion caused by infected machines can generate problems for service providers.
- Attacking Border Gateway Protocol (BGP) routing and injecting faulty BGP routes for traffic redirection is one technique that attackers are using to obtain the "interesting" traffic.
- Domain Name System (DNS) information is sometimes used to redirect Internet traffic to serve the needs of people with criminal intent.
- Device compromise means breaking into vital components of the infrastructure and modifying their configuration.

These threats are correlated with the following factors specific to service provider networks :

- The size of the network. Service providers must be able to rapidly implement security measures against a large number of parties that may be involved in the attack, and deploy these tools and techniques on a large number of devices, usually network entry points.
- In the enterprise world, the number of devices to take care of is typically considerably smaller than in the service provider space. (Although some enterprises have huge networks, this is still an exception). Size is one of the significant differences between the service provider and enterprise security paradigm.
- The number of possible targets of and entry points for an attack is also higher in the service provider space than it is in the enterprise world, where typically a smaller number of clearly identified assets frequently enjoy the highest level of protection possible.
- Accordingly, service providers must be able to defend multiple targets from multiple parallel attacks.
- Securing the transit paths and the infrastructure carrying them and not necessarily securing the endpoints brings its own set of challenges.

- Many of the standard edge-security measures that are applicable in the enterprise world are not applicable in the service provider security paradigm.
- A primary difference is that firewalls and intrusion detection and prevention system (IDS/IPS) devices cannot be applied on transit paths in service provider networks.
- Service providers cannot afford to provide granular access control - one of the main functions of a firewall - for transit traffic.
- Moreover, they cannot afford focused monitoring of transit traffic to detect indications of exploitation attempts in the way that IDSs/IPSs usually do.
- Finally, the whole set of security measures available for hardening endpoints, like host IPSs and antivirus software, is not of much interest in the service provider world.
- Managed security service providers (MSSPs) - a subset of service providers - manage the security components of their customers' networks. MSSPs care about security primarily from the standpoint of enterprises. MSSP operation is not within the scope of this white paper.
- Service providers are also interested in the endpoint security measures with clearly identified security zones; they use these mechanisms to secure their own back-end systems and certain host-based services, like DNS infrastructure, web servers, mail servers, and CPE devices. This paper does not discuss this aspect of securing service provider networks. Instead, this paper focuses on only those aspects that are specific to service providers and their backbone networks.

## 4.7 CLOUD SECURITY ISSUES AND CHALLENGES

**GQ.** What are security Issues in Cloud Computing ?

Cloud Computing is a type of technology that provides remote services on the internet to manage, access, and store data rather than storing it on Servers or local drives. This technology is also known as Serverless technology. Here the data can be anything like Image, Audio, video, documents, files, etc.

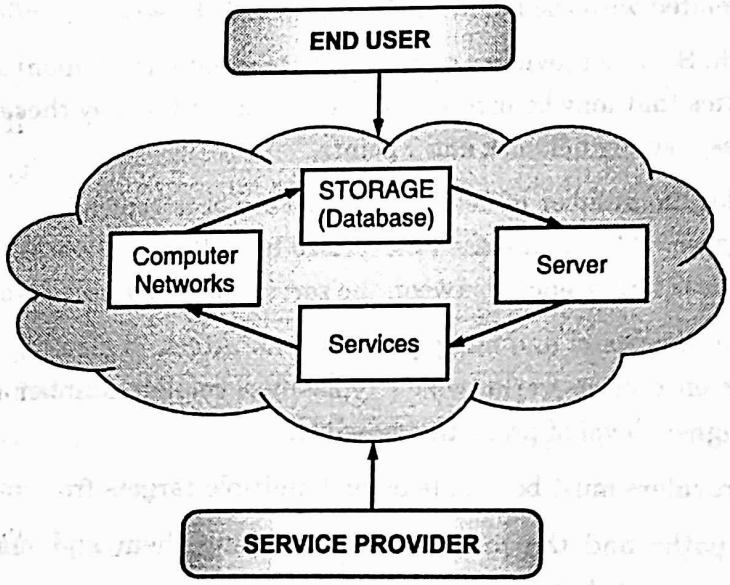


**Fig. 4.7.1 : Cloud Security Issues**

### 4.7.1 Need of Cloud Computing

- Before using Cloud Computing, most of the large as well as small IT companies use traditional methods i.e. they store data in Server, and they need a separate Server room for that.
- In that Server Room, there should be a database server, mail server, firewalls, routers, modems, high net speed devices, etc. For that IT companies have to spend lots of money.
- In order to reduce all the problems with cost Cloud computing come into existence and most companies shift to this technology.

### 4.7.2 Security Issues in Cloud Computing

There is no doubt that Cloud Computing provides various Advantages but there are also some security issues in cloud computing. Below are some following Security Issues in Cloud Computing as follows.

#### Data Loss

Data Loss is one of the issues faced in Cloud Computing. This is also known as Data Leakage. As we know that our sensitive data is in the hands of Somebody else, and we don't have full control over our database. So, if the security of cloud service is to break by hackers then it may be possible that hackers will get access to our sensitive data or personal files.

#### Interference of Hackers and Insecure API's

- As we know if we are talking about the cloud and its services it means we are talking about the Internet. Also, we know that the easiest way to communicate with Cloud is using API. So, it is important to protect the Interface's and API's which are used by an external user. But also, in cloud computing, few services are available in the public domain.
- An is the vulnerable part of Cloud Computing because it may be possible that these services are accessed by some third parties. So, it may be possible that with the help of these services hackers can easily hack or harm our data.

#### User Account Hijacking

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

#### Changing Service Provider

- Vendor lock In is also an important Security issue in Cloud Computing.
- Many organizations will face different problems while shifting from one vendor to another. For example, An Organization wants to shift from AWS Cloud to Google Cloud Services then they ace various problem's like shifting of all data, also both cloud services have different techniques and functions, so they also face problems regarding that. Also, it may be possible that the charges of AWS are different from Google Cloud, etc.

**Lack of Skill**

While working, shifting o another service provider, need an extra feature, how to use a feature, etc. are the main problems caused in IT Company who doesn't have skilled Employee. So it requires a skilled person to work with cloud Computing.

**Denial of Service (DoS) attack**

- This type of attack occurs when the system receives too much traffic.
- Mostly DoS attacks occur in large organizations such as the banking sector, government sector, etc. When a DoS attack occurs, data is lost. So in order to recover data, it requires a great amount of money as well as time to handle it.

## 4.8 SECURITY ISSUES IN VIRTUALIZATION

**GQ.** What are Security issues in virtualization ?

- Virtualization-based technologies have become ubiquitous in computing. While they provide an easy-to-implement platform for scalable, high-availability services, they also introduce new security issues.
- Traditionally, discussions on security vulnerabilities in server platforms have been focused on stand-alone (i.e., non-virtualized) environments. For cloud and virtualized platforms, the discussion focuses on the shared usage of resources and the lack of control over the infrastructure.
- However, the impact virtualization technologies can have on exploit mitigation mechanisms of host machines is often neglected.
- Therefore, this survey discusses the following issues: first, the security issues and challenges that are introduced by the migration from stand-alone solutions to virtualized environments special attention is given to the Virtual Machine Monitor, since it is a core component in a virtualized solution; second, the impact (sometimes negative) that these new technologies have on existing security strategies for hosts; third, how virtualization technologies can be leveraged to provide new security mechanisms not previously available.; and, finally, how virtualization technologies can be used for malicious purposes.
- Virtualization, the process of allowing efficient utilization of physical computer hardware, is the core of many new technologies. With this comes the importance of understanding the related security aspects to avoid the compromise of underlying resources and services.
- In this paper, we provide an overview on the two main virtualization architectures and the different types of virtualization approaches related to those architectures.
- We also review the literature for virtualization security requirements and security attacks. We highlight the latest security techniques proposed in the literature.
- Due to the growth of cloud computing in the industry, we also discuss virtualization security in the industry. As a result, we have found that the gap between academia and industry has become very small in this field, and more importance should be given to client and service provider responsibility awareness.

- Lack of visibility: Post virtualization, organizations struggle to visualize their virtual assets to perform effective monitoring and management.
- Visualization of virtual assets means establishing visibility on the virtual layer of IT architecture i.e. separating the guest and host environment, positioning the virtual servers and desktops within the physical IT asset environment etc.
- Mixing of traffic : If no due diligence is carried out to understand the changes network will undergo due to virtualization, then the traffic of physical IT assets and virtualized environment get mixed with each other.
- The mixing of traffic results in ineffective monitoring of virtualized assets from both an IT and a security perspective.
- Traffic data exposures: In a virtualized IT environment it is an arduous task to scan data files resident on virtual machines.
- Organizations are implementing security capabilities that can discover and classify sensitive information hosted on virtual machine thus reducing the number of data leakage scenarios.
- By swiftly identifying sensitive data exposures, these security capabilities reduce the risks of non-compliance, such as reputational damage due to data leakage incidents.
- Some of the other security challenges are insecure provisioning in which device and user-based provisioning becomes difficult to implement because of elevated access given to provide flexibility in operations and business demanding deployment of varied mobile devices to enhance productivity of the workforce in a virtualized environment.

## 4.9 HOST-SECURITY

**GQ.** What is Host Security ?

- Host security describes how your server is set up for the following tasks :
  1. Preventing attacks.
  2. Minimizing the impact of a successful attack on the overall system.
  3. Responding to attacks when they occur.
- It always helps to have software with no security holes. Good luck with that! In the real world, the best approach for preventing attacks is to assume your software has security holes. As I noted earlier in this chapter, each service you run on a host presents a distinct attack vector into the host.
- The more attack vectors, the more likely an attacker will find one with a security exploit. You must therefore minimize the different kinds of software running on a server.
- Given the assumption that your services are vulnerable, your most significant tool in preventing attackers from exploiting a vulnerability once it becomes known is the rapid rollout of security patches. Here's where the dynamic nature of the cloud really alters what you can do from a security perspective.

- In a traditional data center, rolling out security patches across an entire infrastructure is time-consuming and risky.
- In the cloud, rolling out a patch across the infrastructure takes three simple steps :
  1. Patch your AMI with the new security fixes.
  2. Test the results.
  3. Relaunch your virtual servers.

## 4.10 DATA SECURITY

**GQ. What is Data Security ?**

Data, a word which is now spoken every time one or the other way, people are working in corporate throughout the day with small scale figures keeping in my find that our company data should not be leaked by any chance or by any external force but they haven't thought of their data being in-secured.

**☞ Why our data is not secured ?**

We feel free while using apps especially social media apps like Facebook, WhatsApp which is not normal because we logins on different devices which is not a favorable condition in terms of our personal data and also of the people linked through it.

**☞ Here is a flowchart for better understanding**

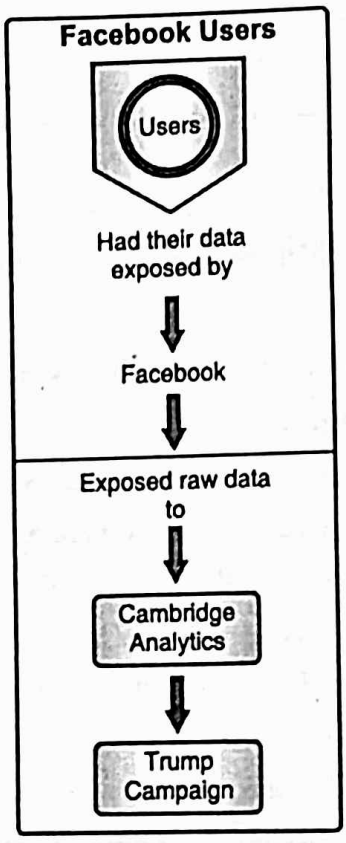


**Fig. 4.10.1 : Flowchart of Data Security**

- Data being the asset on the planet, it is very crucial to handle and secure in these days as data breaching is not difficult, hackers are hacking profiles and selling it, data selling is a new way of earning.
- Data security is the most vital part for online workers on which there should be no compromise at all but still it happens and it will be happening as there is no way getting rid of data being stolen but it can be controlled to an extent by many means.

**How data will be secured ?**

- Use firewalls.
- Use encrypted systems.
- Use VPN.
- Never give authorization to external parties.
- Use strong passwords and change them often.
- Public networks should be avoided as much as we can like WiFi on metros, airports.
- Do make trust issues while logging in another devices.
- From the above we came to know how far we are from all of this which wouldn't have been taken so easy at least in terms of our own personal data which is yours and only yours.
- There are laws being made for right to ask for the data if you think someone is having and making use of it. So, it solely depends on the individuals how they take this into the account.

### 4.10.1 Types of Data Security

**Access Controls**

This type of data security measures includes limiting both physical and digital access to critical systems and data. This includes making sure all computers and devices are protected with mandatory login entry, and that physical spaces can only be entered by authorized personnel.

**Authentication**

Similar to access controls, authentication refers specifically to accurately identifying users before they have access to data. This usually includes things like passwords, PIN numbers, security tokens, swipe cards, or biometrics.

**Backups and Recovery**

- Good data security means you have a plan to securely access data in the event of system failure, disaster, data corruption, or breach.
- You'll need a backup data copy, stored on a separate format such as a physical disk, local network, or cloud to recover if needed.

☞ **Data Erasure**

- You'll want to dispose of data properly and on a regular basis.
- Data erasure employs software to completely overwrite data on any storage device and is more secure than standard data wiping. Data erasure verifies that the data is unrecoverable and therefore won't fall into the wrong hands.

☞ **Data Masking**

- By using data masking software, information is hidden by obscuring letters and numbers with proxy characters. This effectively masks key information even if an unauthorized party gains access to it.
- The data changes back to its original form only when an authorized user receives it.

☞ **Data Resiliency**

- Comprehensive data security means that your systems can endure or recover from failures.
- Building resiliency into your hardware and software means that events like power outages or natural disasters won't compromise security.

☞ **Encryption**

- A computer algorithm transforms text characters into an unreadable format via encryption keys.
- Only authorized users with the proper corresponding keys can unlock and access the information.
- Everything from files and a database to email communications can - and should - be encrypted to some extent.

☞ **Main Elements of Data Security**

- There are three core elements to data security that all organizations should adhere to: Confidentiality, Integrity, and Availability. These concepts are also referred to as the CIA Triad, functioning as a security model and framework for top-notch data security. Here's what each core element means in terms of keeping your sensitive data protected from unauthorized access and data exfiltration.
- Confidentiality. Ensures that data is accessed only by authorized users with the proper credentials.
- Integrity. Ensure that all data stored is reliable, accurate, and not subject to unwarranted changes.
- Availability. Ensures that data is readily - and safely - accessible and available for ongoing business needs.

### 4.10.2 Data Security Regulations

- Data security is a critical element to regulatory compliance, no matter what industry or sector your organization operates in.
- Most - if not all - regulatory frameworks make data security a key aspect of compliance. Therefore, you'll need to take data security seriously and work with an experienced compliance partner to ensure you're employing all the right measures.

## 4.11 FIREWALLS

- Nowadays, it is a big challenge to protect our sensitive data from unwanted and unauthorized sources. There are various tools and devices that can provide different security levels and help keep our private data secure.
- One such tool is a 'firewall' that prevents unauthorized access and keeps our computers and data safe and secure.
- In this article, we have talked about firewalls as well as other related topics, such as why we need firewalls, functions of firewalls, limitations of firewalls, working of firewalls, etc.

GQ. What is a Firewall ?

- A firewall can be defined as a special type of network security device or a software program that monitors and filters incoming and outgoing network traffic based on a defined set of security rules. It acts as a barrier between internal private networks and external sources (such as the public Internet).
- The primary purpose of a firewall is to allow non-threatening traffic and prevent malicious or unwanted data traffic for protecting the computer from viruses and attacks.
- A firewall is a cyber security tool that filters network traffic and helps users block malicious software from accessing the Internet in infected computers.

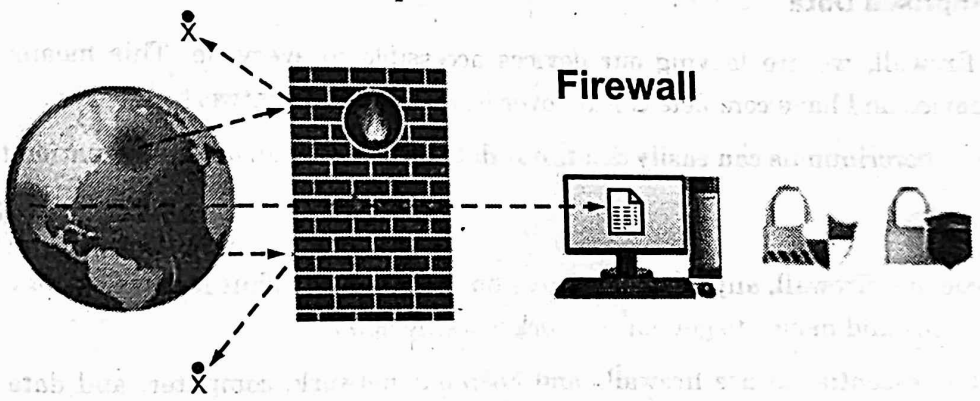


Fig. 4.11.1 : Firewall Architecture

### 4.11.1 Firewall : Hardware or Software

- This is one of the most problematic questions whether a firewall is a hardware or software. As stated above, a firewall can be a network security device or a software program on a computer. This means that the firewall comes at both levels, i.e., hardware and software, though it's best to have both.
- Each format (a firewall implemented as hardware or software) has different functionality but the same purpose. A hardware firewall is a physical device that attaches between a computer network and a gateway. For example, a broadband router.
- On the other hand, a software firewall is a simple program installed on a computer that works through port numbers and other installed software. Apart from that, there are cloud-based firewalls. They are commonly referred to as FaaS (firewall as a service).

- A primary advantage of using cloud-based firewalls is that they can be managed centrally. Like hardware firewalls, cloud-based firewalls are best known for providing perimeter security.

**GQ.** Why we need Firewall ?

- Firewalls are primarily used to prevent malware and network-based attacks. Additionally, they can help in blocking application-layer attacks. These firewalls act as a gatekeeper or a barrier. They monitor every attempt between our computer and another network. They do not allow data packets to be transferred through them unless the data is coming or going from a user-specified trusted source.
- Firewalls are designed in such a way that they can react quickly to detect and counter-attacks throughout the network. They can work with rules configured to protect the network and perform quick assessments to find any suspicious activity. In short, we can point to the firewall as a traffic controller.

Some of the important risks of not having a firewall are:

☞ **Open Access**

- If a computer is running without a firewall, it is giving open access to other networks. This means that it is accepting every kind of connection that comes through someone.
- In this case, it is not possible to detect threats or attacks coming through our network. Without a firewall, we make our devices vulnerable to malicious users and other unwanted sources.

☞ **Lost or Comprised Data**

- Without a firewall, we are leaving our devices accessible to everyone. This means that anyone can access our device and have complete control over it, including the network.
- In this case, cybercriminals can easily delete our data or use our personal information for their benefit.

☞ **Network Crashes**

- In the absence of a firewall, anyone could access our network and shut it down. It may lead us to invest our valuable time and money to get our network working again.
- Therefore, it is essential to use firewalls and keep our network, computer, and data safe and secure from unwanted sources.

### 4.11.2 Brief History of Firewall

- Firewalls have been the first and most reliable component of defense in network security for over 30 years. Firewalls first came into existence in the late 1980s. They were initially designed as packet filters. These packet filters were nothing but a setup of networks between computers.
- The primary function of these packet filtering firewalls was to check for packets or bytes transferred between different computers.
- Firewalls have become more advanced due to continuous development, although such packet filtering firewalls are still in use in legacy systems.
- As the technology emerged, Gil Shwed from Check Point Technologies introduced the first stateful inspection firewall in 1993. It was named as FireWall-1.

- Back in 2000, Netscreen came up with its purpose-built firewall 'Appliance'. It gained popularity and fast adoption within enterprises because of increased internet speed, less latency, and high throughput at a lower cost. The turn of the century saw a new approach to firewall implementation during the mid-2010.
- The 'Next-Generation Firewalls' were introduced by the Palo Alto Networks. These firewalls came up with a variety of built-in functions and capabilities, such as Hybrid Cloud Support, Network Threat Prevention, Application and Identity-Based Control, and Scalable Performance, etc.
- Firewalls are still getting new features as part of continuous development. They are considered the first line of defense when it comes to network security.

### How does a firewall work ?

- A firewall system analyzes network traffic based on pre-defined rules. It then filters the traffic and prevents any such traffic coming from unreliable or suspicious sources. It only allows incoming traffic that is configured to accept.
- Typically, firewalls intercept network traffic at a computer's entry point, known as a port.
- Firewalls perform this task by allowing or blocking specific data packets (units of communication transferred over a digital network) based on pre-defined security rules.
- Incoming traffic is allowed only through trusted IP addresses, or sources.

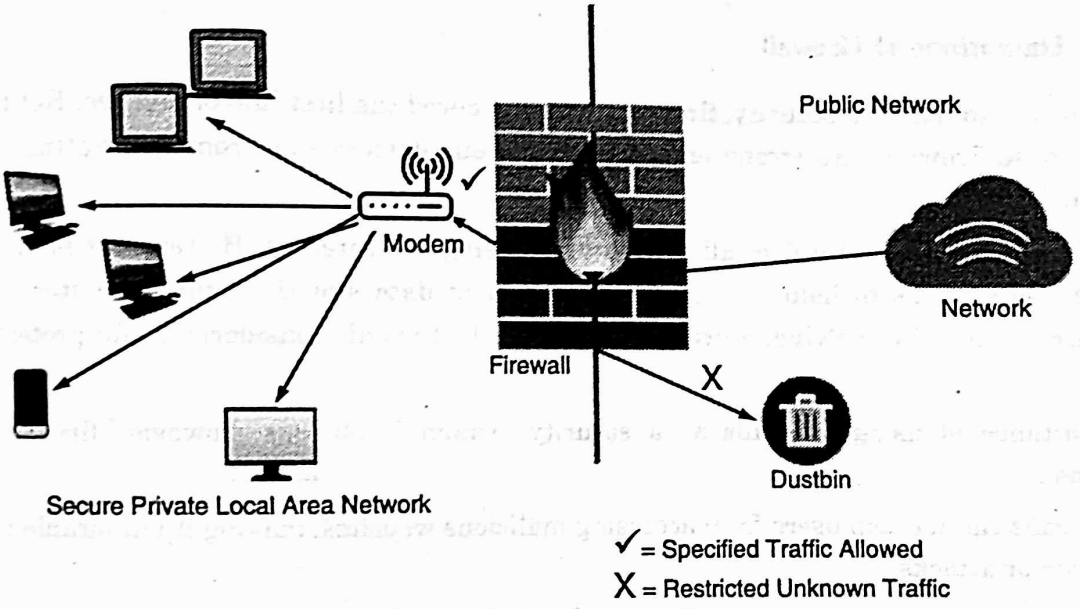


**Fig. 4.11.2 : Working of Firewall**

## 4.11.3 Functions of Firewall

GQ. What are the different function of firewall ?

- As stated above, the firewall works as a gatekeeper. It analyzes every attempt coming to gain access to our operating system and prevents traffic from unwanted or non-recognized sources.

- Since the firewall acts as a barrier or filter between the computer system and other networks (i.e., the public Internet), we can consider it as a traffic controller.
- Therefore, a firewall's primary function is to secure our network and information by controlling network traffic, preventing unwanted incoming network traffic, and validating access by assessing network traffic for malicious things such as hackers and malware.
- Generally, most operating systems (for example - Windows OS) and security software come with built-in firewall support. Therefore, it is a good idea to ensure that those options are turned on.
- Additionally, we can configure the security settings of the system to be automatically updated whenever available.
- Firewalls have become so powerful, and include a variety of functions and capabilities with built-in features :
  - Network Threat Prevention
  - Application and Identity-Based Control
  - Hybrid Cloud Support
  - Scalable Performance
  - Network Traffic Management and Control
  - Access Validation
  - Record and Report on Events

### 4.11.4 Limitations of Firewall

- When it comes to network security, firewalls are considered the first line of defense. But the question is whether these firewalls are strong enough to make our devices safe from cyber-attacks. The answer may be "no".
- The best practice is to use a firewall system when using the Internet. However, it is important to use other defense systems to help protect the network and data stored on the computer. Because cyber threats are continually evolving, a firewall should not be the only consideration for protecting the home network.
- The importance of using firewalls as a security system is obvious; however, firewalls have some limitations :
  - Firewalls cannot stop users from accessing malicious websites, making it vulnerable to internal threats or attacks.
  - Firewalls cannot protect against the transfer of virus-infected files or software.
  - Firewalls cannot prevent misuse of passwords.
  - Firewalls cannot protect if security rules are misconfigured.
  - Firewalls cannot protect against non-technical security risks, such as social engineering.
  - Firewalls cannot stop or prevent attackers with modems from dialing in to or out of the internal network.
  - Firewalls cannot secure the system which is already infected.

Therefore, it is recommended to keep all Internet-enabled devices updated. This includes the latest operating systems, web browsers, applications, and other security software (such as anti-virus). Besides, the security of wireless routers should be another practice.

The process of protecting a router may include options such as repeatedly changing the router's name and password, reviewing security settings, and creating a guest network for visitors.

### 4.11.5 Types of Firewall

GQ. Enlist Different types of Firewall ?

Depending on their structure and functionality, there are different types of firewalls.

The following is a list of some common types of firewalls :

- Proxy Firewall
- Packet-filtering firewalls
- Stateful Multi-layer Inspection (SMLI) Firewall
- Unified threat management (UTM) firewall
- Next-generation firewall (NGFW)
- Network address translation (NAT) firewalls.

*Chapter Ends*

□□□

UNIT V

CHAPTER 5

# Cloud Environment and Application Development

**University Prescribed Syllabus**

**Cloud Platforms :** Google App Engine, Compute Services, Storage Services, Communication Services, Amazon Web Services Architecture and core concepts, Application Lifecycle, Cost Model, Microsoft Azure Cloud services Azure core concepts, Windows Azure Platform Appliance.

## 5.1 CLOUD PLATFORMS

- Cloud computing applications develops by leveraging platforms and frameworks.
- Various types of services are provided from the bare metal infrastructure to customize-able applications serving specific purposes.

**GQ.** What are the Cloud Platforms Explain any 3 platforms ?

### 1. Amazon Web Services (AWS)

- AWS provides different wide-ranging clouds IaaS services, which ranges from virtual compute, storage, and networking to complete computing stacks.
- AWS is well known for its storage and compute on demand services, named as Elastic Compute Cloud (EC2) and Simple Storage Service (S3).
- EC2 offers customizable virtual hardware to the end user which can be utilize as the base infrastructure for deploying computing systems on the cloud. It is likely to choose from a large variety of virtual hardware configurations including GPU and cluster instances.
- Either the AWS console, which is a wide-ranged Web portal for retrieving AWS services, or the web services API available for several programming language is used to deploy the EC2 instances.
- EC2 also offers the capability of saving an explicit running instance as image, thus allowing users to create their own templates for deploying system.
- S3 stores these templates and delivers persistent storage on demand. S3 is well ordered into buckets which contains objects that are stored in binary form and can be grow with attributes. End users can store objects of any size, from basic file to full disk images and have them retrieval from anywhere.
- In addition, EC2 and S3, a wide range of services can be leveraged to build virtual computing system including: networking support, caching system, DNS, database support, and others.

### 2. Google App-Engine

- Google App-Engine is a scalable runtime environment frequently dedicated to executing web applications. These utilize benefits of the large computing infrastructure of Google to dynamically scale as per the demand.
- App-Engine offers both a secure execution environment and a collection of which simplifies the development if scalable and high-performance Web applications. These services include: in-memory caching, scalable data store, job queues, messaging, and corn tasks.
- Developers and Engineers can build and test applications on their own systems by using the App-Engine SDK, which replicates the production runtime environment, and helps test and profile applications.

- On completion of development, Developers can easily move their applications to App-Engine, set quotas to containing the cost generated, and make it available to the world. Currently, the supported programming languages are Python, Java, and Go.

### 3. Microsoft Azure

- Microsoft Azure is a Cloud operating system and a platform in which user can develop the applications in the cloud. Generally, a scalable runtime environment for web applications and distributed applications is provided.
- Application in Azure are organized around the fact of roles, which identify a distribution unit for applications and express the application's logic.
- Azure provides a set of additional services that complement application execution such as support for storage, networking, caching, content delivery, and others.

### 4. Hadoop

- Apache Hadoop is an open source framework that is appropriate for processing large data sets on commodity hardware.
- Hadoop is an implementation of MapReduce, an application programming model which is developed by Google. This model provides two fundamental operations for data processing: map and reduce.
- Yahoo! Is the sponsor of the Apache Hadoop project, and has put considerable effort in transforming the project to an enterprise-ready cloud computing platform for data processing.
- Hadoop is an integral part of the Yahoo! Cloud infrastructure and it supports many business processes of the corporates.
- Currently, Yahoo! Manges the world's largest Hadoop cluster, which is also available to academic institutions.

### 5. Force.com and Salesforce.com

- Force.com is a Cloud computing platform at which user can develop social enterprise applications. The platform is the basis of SalesForce.com – a Software-as-a-Service solution for customer relationship management.
- Force.com allows creating applications by composing ready-to-use blocks: a complete set of components supporting all the activities of an enterprise are available. From the design of the data layout to the definition of business rules and user interface is provided by Force.com as a support. This platform is completely hostel in the Cloud, and provides complete access to its functionalities, and those implemented in the hosted applications through Web services technologies.

There are a ton of ways in which every individual can state the meaning of the cloud platform. But in the simplest way it can be stated as the operating system and hardware of a server in an Internet-based data center are referred to as a cloud platform. It enables remote and large-scale coexistence of software and hardware goods.

Compute facilities, such as servers, databases, storage, analytics, networking, applications, and intelligence, are rented by businesses. As a result, businesses do not need to invest in data centers or computing facilities. They actually pay for the services they offer.

### 5.1.1 Types of Cloud Platforms

**GQ.** Explain different type of cloud platform ?

- Cloud systems come in a range of shapes and sizes. None of them are suitable for all. To meet the varying needs of consumers, a range of models, forms, and services are available.
- They are as follows :
  1. **Public Cloud :** Third-party providers that distribute computing services over the Internet are known as public cloud platforms. A few good examples of trending and mostly used cloud platform are Google Cloud Platform, AWS (Amazon Web Services), Microsoft Azure, Alibaba and IBM Bluemix.
  2. **Private Cloud :** A private cloud is normally hosted by a third-party service provider or in an on-site data center. A private cloud platform is always dedicated to a single company and it is the key difference between the public and private cloud.

     Or we can say that a private cloud is a series of cloud computing services used primarily by one corporation or organization.
  3. **Hybrid Cloud :** The type of cloud architecture that combines both the public and private cloud systems is termed to as a Hybrid cloud platform. Data and programs are easily migrated from one to the other. This allows the company to be more flexible while still improving infrastructure, security, and enforcement.
- Organizations can use a cloud platform to develop cloud-native software, test and build them, and store, back up, and recover data.
- The major role of it is that will not only help the company to grow but also it helps to perform the data analysis with the help of different algorithms and the results can be a true deal breaker.
- Streaming video and audio, embedding information into activities, and providing applications on-demand on a global scale are all possibilities.
- Simply stated, cloud computing is the distribution of computing services over the Internet ("the cloud") in order to provide quicker innovation, more versatile resources, and economies of scale.
- We usually only pay for the cloud services that we use, which helps us to cut costs, operate our infrastructure more effectively, and scale as our company grows.

### 5.1.2 Top Benefits of Cloud Computing

Cloud computing represents a significant departure from how companies have traditionally seen IT services.

The following are seven of the most popular reasons why businesses are moving to cloud computing services :

1. **Cost**

Cloud storage reduces the upfront costs of purchasing hardware and software, as well as the costs of setting up and operating on-site datacenters-server racks, round-the-clock power and cooling, and IT professionals to manage the infrastructure. It quickly adds up.

2. **Global scale**

The ability to scale elastically is one of the advantages of cloud computing services. In other words, it simply means that we can decide the processing speed, location of the data center where data is to be stored, storage and even the bandwidth for our process and data.

3. **Performance**

The most popular cloud computing services are hosted on a global network of protected datacenters that are updated on a regular basis with the latest generation of fast and powerful computing hardware.

4. **Security**

Many cloud providers have a comprehensive collection of policies, technologies, and controls to help us to enhance our overall security posture and protect our data, applications, and infrastructure from threats.

5. **Speed**

It means that the huge amount of calculation and the huge data retrieval as in download and upload can happen just within the blink of an eye, obviously depending on the configuration.

6. **Reliability**

Since data can be replicated at several redundant locations on the cloud provider's network, cloud storage makes data backup, disaster recovery, and business continuity simpler and less costly.

## 5.2 GOOGLE APP ENGINE

**GQ. What is Google App Engine ?**

- Google App Engine is a fully managed serverless platform for developing and hosting web applications at a scale.
- Users can choose from several popular languages, libraries, and frameworks to develop their applications and then App Engine takes care of provisioning servers and scaling app instances based on demand. It is a PaaS for building scalable applications.

- Google Cloud provides 2 environments to use App Engine, one is a standard environment with constrained environments and support for languages such as Python, Go, node.js.
- The other one is the Flexible Environment where developers have more freedom such as running custom runtimes using docker, longer request & response timeout, and ability to install custom dependencies/software, and SSH into the virtual machine.

**1. Standard Environment**

It is based on the container which runs on the Google infrastructure. It provides users with the facility to easily build and deploy an application that runs under heavy load and a large amount of data. It supports the following languages : Python, JAVA, Node.js, Ruby, PHP, and Go.

**Features of Standard Environment**

- Persistent storage with queries, sorting, and transactions.
- Automatic scaling and load balancing.
- Asynchronous task queues for performing work outside the scope of a request.
- Scheduled tasks for triggering events at regular intervals or specific time intervals.
- Integration with other Google cloud services and APIs.

**2. Flexible Environment**

- App Engine Flexible Environment allows users to concentrate on writing code.
- Based on Google Compute Engine, it automatically scales the app up and down and along with it also balances the load. It allows users to customize their runtime and the operating system of their virtual machines using Docker files.

**Features of Flexible Environment**

- **Infrastructure Customization :** App Engine flexible environment instances are Compute Engine virtual machines, which implies that users can take advantage of custom libraries, use SSH for debugging, and deploy their own Docker containers.

  It is an open-source community.
- **Native feature support :** Features such as microservices, authorization, SQL and NoSQL databases, traffic splitting, logging, etc are natively supported.

  Performance : Users can take advantage of a wide array of CPU and memory configurations.

**Benefits of Google App Engine**

The main benefits of Google App Engine are :

- **Open and familiar languages and tools :** Users can build and deploy apps quickly using popular languages or bring their own language runtimes and frameworks, they can also manage resources from the command line, debug source code, and run API back ends easily.

- **Just add code :** App Engine protects from security threats using firewall capabilities, IAM rules, and managed SSL/ TLS certificates so that it helps users to write code without any underlying infrastructure.
- **Pay only for what you use :** It naturally scales relying upon the application traffic and expends resources just when the code is running.

### 5.2.1 Features of Google App Engine

GQ. Enlist features of Google App Engine

Some of the prominent features of Google App Engine include :

1. **Popular language :** Users can build the application using language runtimes such as Java, Python, C#, Ruby, PHP or build their own runtimes.
2. **Open and flexible :** Custom runtimes allow users to bring any library and framework to App Engine by supplying a Docker container.
3. **Fully managed :** It allows users to add your web application code to the platform while it manages the infrastructure. The engine ensures that web apps are secure and running and enables the firewall to save them from malware and threats.
4. **Powerful application diagnostics :** Google App engine uses cloud monitoring and cloud logging to monitor the health and performance of the app and to diagnose and fix bugs quickly it uses cloud debugger and error reporting.
5. **Application versioning :** It easily hosts different versions of the app, and create development, test, staging, and production environments.
6. **Application security :** Google App Engine helps safeguard the application by defining access rules with an App Engine firewall and leverage managed SSL/TLS certificates by default on the custom domain without incurring any additional cost.

## 5.3 COMPUTE SERVICES

GQ. Explain Compute Services ?

- In cloud computing, the term "compute" describes concepts and objects related to software computation. It is a generic term used to reference processing power, memory, networking, storage, and other resources required for the computational success of any program.
- For example, applications that run machine learning algorithms or 3D graphics rendering functions require many gigs of RAM and multiple CPUs to run successfully.
- In this case, the CPUs, RAM, and Graphic Processing Units required will be called compute resources, and the applications would be compute-intensive applications.

### ☞ What are compute services ?

- Compute services are also known as Infrastructure-as-a-Service (IaaS). Compute platforms, such as AWS Compute, supply a virtual server instance and storage and APIs that let users migrate workloads to a virtual machine.
- Users have allocated compute power and can start, stop, access, and configure their computer resources as desired.

### ☞ How to choose between different AWS Compute Services

- Choosing the best AWS infrastructure depends on your application requirements, lifecycle, code size, demand, and computing needs. Take a look at these three examples :
- If you want to deploy a selection of on-demand instances offering a wide array of different performance benefits within your AWS environment, you would use Amazon Elastic Compute Cloud (EC2).
- If you want to run Docker-enabled applications packaged as containers across a cluster of EC2 instances, you could use Amazon Elastic Container Service (Amazon ECS).
- If you want to run your own code using only milliseconds of compute resource in response to event-driven triggers in serverless environment, you could use AWS Lambda.

**GQ.** What are the benefits of AWS compute services ?

AWS Compute services offer the broadest and deepest functionality for compute. Key benefits of using AWS Compute include :

**(I) Right compute for your workloads**

- Amazon EC2 (Amazon Elastic Compute Cloud) offers granular control for managing application infrastructure with the choice of processors, storage, and networking.
- Amazon Elastic Container Services (Amazon ECS) offer choice and flexibility to run containers.

**(II) Built-in security**

- AWS offers significantly more security, compliance, and governance services, and key features than the next largest cloud provider.
- The AWS Nitro System has security built in at the chip level to continuously monitor, protect, and verify the instance hardware.

**(III) Cost optimization**

With AWS compute you pay only for the instance or resource you need, for as long as you use it, without requiring long-term contracts or complex licensing.

**(IV) Flexibility**

- AWS provides multiple ways to build, deploy, and get applications to market quickly.

- For example, Amazon LightSail is an easy-to-use service that offers you everything you need to build an application or website.
- To determine which AWS Compute service is best suited to grow your business, don't hesitate to Get in Touch with our team of experts or sign-up for a Free AWS Account today.

## 5.4 STORAGE SERVICES

Cloud Storage is a service that allows to save data on offsite storage system managed by third-party and is made accessible by a web services API.

Storage devices can be broadly classified into two categories :

1. Block Storage Devices
2. File Storage Devices

1. **Block Storage Devices :** The block storage devices offer raw storage to the clients. These raw storages are partitioned to create volumes.
2. **File Storage Devices :** The file Storage Devices offer storage to clients in the form of files, maintaining its own file system. This storage is in the form of Network Attached Storage (NAS).

### ☞ Cloud Storage Classes

Cloud storage can be broadly classified into two categories :

1. Unmanaged Cloud Storage
2. Managed Cloud Storage

1. **Unmanaged Cloud Storage**
   - Managed Cloud Storage
   - Unmanaged Cloud Storage
   - Unmanaged cloud storage means the storage is preconfigured for the customer. The customer can neither format, nor install his own file system or change drive properties.
2. **Managed Cloud Storage**
   - Managed cloud storage offers online storage space on-demand.
   - The managed cloud storage system appears to the user to be a raw disk that the user can partition and format.

### ☞ Creating Cloud Storage System

- The cloud storage system stores multiple copies of data on multiple servers, at multiple locations. If one system fails, then it is required only to change the pointer to the location, where the object is stored.

- To aggregate the storage assets into cloud storage systems, the cloud provider can use storage virtualization software known as Storage GRID. It creates a virtualization layer that fetches storage from different storage devices into a single management system. It can also manage data from CIFS and NFS file systems over the Internet.
- The following diagram shows how Storage GRID virtualizes the storage into storage clouds :

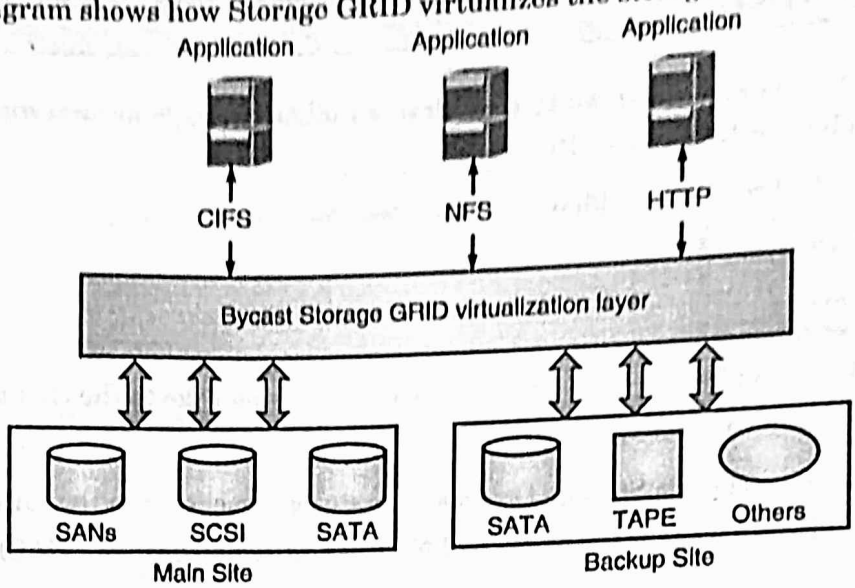


**Fig. 5.4.1 : Cloud Storage Services**

## 5.4.1 Cloud Computing Data Storage

**GQ.** What are Cloud Storage Services ?

### Virtual Storage Containers

- The virtual storage containers offer high performance cloud storage systems.
- Logical Unit Number (LUN) of device, files and other objects are created in virtual storage containers. Following diagram shows a virtual storage container, defining a cloud storage domain:

### Virtual Storage Containers

**Challenges**

- Storing the data in cloud is not that simple task.
- Apart from its flexibility and convenience, it also has several challenges faced by the customers.
- The customers must be able to :
  1. Get provision for additional storage on-demand.
  2. Know and restrict the physical location of the stored data.
  3. Verify how data was erased.
  4. Have access to a documented process for disposing of data storage hardware.
  5. Have administrator access control over data.

## 5.5 COMMUNICATION SERVICES

### What is Communication Service Provider (CSP)?

- CSP refers to the communication service providers. They provide us services in different means or in different fields of communication media.
- Communication service provider (CSP) is actually a generic term or is a category of service providers. As a communication service provider, lots of companies provide different services for different purposes.
- For example, ISP (Internet Service Provider) comes in the category of the communication service provider (CSP), their work is to provide service of internet data among people.
- ISP (Internet Service Provider) only provides internet data to the people also there are many companies across the world that are providing services to the people for better communication among people among countries.
- Telecommunication Service Provider (TSP) also comes under communication service provider (CSP). Their work is to provide landline connections or wireless connections, cable operators (companies), satellite transmission they all are known as Communication Service Provider.
- Nowadays, some mobile companies are also working as communication service providers.

### 5.5.1 Types of Communication Service Provider

There are many types of service providers, all the different service providers are listed below :

1. **Telecommunication services provide :** These are the service providers who are responsible for landline or wireless connections. this type of provider is having its different branches like cable providers, satellite transmission is included in this category of service providers. Also, mobile companies that provide devices to users and also internet service provider (ISP) comes to TSP.
2. **Entertainment service providers :** These providers help in TV transmissions like the different niches of channels which are running on the tv or theaters comes to the category of entertainment service provider music industries and video games industry also comes to this category.

   **For example :** motion pictures, theaters.
3. **Media/web services :** These providers provide services related to the web shows, media, series, movies on the internet over a web platform, known as media or web services.

   **For example :** Amazon prime video services, Netflix, etc.

### Advantages of Communication Service Provider (CSP)

1. Communication Service Providers play a vital role in communication across the world.
2. They do mass production through which a large number of people connect with each other.
3. CSP provides that today users can interact with the world.
4. They made people's life easier in terms of communication because now people can connect with anyone anywhere in the world.
5. CSP contributes to the world economy, last year their market cap was about 1.4 trillion dollars.

### ☞ Disadvantages of Communication Service Provider (CSP)

1. Companies collect user data and sell it to others.
2. There can be fraud in the means of providing services.
3. The user has no control over providers.
4. Some services cost too much that cannot be afforded.

## 5.5.2 Communication Services Functionalities

**GQ.** What are communication services ?

- A business organization must have constant contact with the outside world. There needs to be an exchange of information and ideas. This is why effective communication is the cornerstone of any successful company.
- A company must communicate with its employees, customers, buyers, suppliers, the government etc.
- For any communication service to be effective it must be fast and inexpensive.
- In the last few decades with the rapid technological advancements, communication has become highly effective now.
- In fact, the advancement of the internet (with its communication capabilities) is the reason we have a global economy.
- There are two main communication services in India that businesses generally rely on,
  1. **Postal Services :** The Indian Post Office is an important part of our society. They provide various types of mail and telegraph services pan-India. But did you know that post office also provides financial services similar to banks?
  2. **Telecom Services :** Telecommunication infrastructure is a very important part of a country's infrastructure and essential to its progress. These services include cellular services, internet services, DTH services etc.

### ☞ Transportation

- Transportation is concerned with the transport of goods and raw materials. However, transportation is not only the freight but all the auxiliary services associated with them.
- The main function of transportation is to overcome the barrier of place.
- The goods will be made available to the end consumer no matter where they are located in the world. They will be transported from their place of production to their place of consumption.
- To keep up with an expanding business, transportation services must also keep up. One main factor is the infrastructure of the country.
- Roads, railways, ports etc must be taken care of. It is both the responsibility of the industries and the government.

☞ **Warehousing**

- Communication Services, Transportation and Warehousing
- Once the goods are produced they also must be stored. There is generally a lag time between production and consumption. This systematic and scientific storage and maintenance of goods and raw materials is called warehousing.
- Warehousing isn't merely storing goods in a shed. It is a logistics center, which provides a variety of services. They are responsible for inventory management, which includes providing the production departments with the right quantity of goods at the correct time intervals.
- There are types of warehouses based on the ownership of them. Some of them are

1. **Private Warehouse :** Owned and operated by the company itself. Private warehousing requires huge capital investment but it provides the company with full and complete control. It is ideal for organizations that have a huge inventory and a high turnover like for example a chain retail store.
2. **Public Warehouses :** Here you use a warehousing facility in exchange for a fee. While the ownership will not be the company's it is a cost-effective method. The government will regulate such warehousing facilities. The owner of a public warehouse is expected to take reasonably good care of the goods.
3. **Bonded Warehouse :** These are warehouses for imported goods. The goods will be in storage at the facility till the importer pays his custom duty and other such taxes. So the goods are said to be in a bond.

## 5.6 AMAZON WEB SERVICES ARCHITECTURE AND CORE CONCEPTS

- This is the basic structure of AWS EC2, where EC2 stands for Elastic Compute Cloud. EC2 allow users to use virtual machines of different configurations as per their requirement. It allows various configuration options, mapping of individual server, various pricing options, etc.
- We will discuss these in detail in AWS Products section.
- Following is the diagrammatic representation of the architecture.

GQ. What is Amazon Web services with architecture ?

☞ **Amazon Web Services (AWS)**

- AWS consists of many cloud services that you can use in combinations tailored to your business or organizational needs. This section introduces the major AWS services by category.
- To access the services, you can use the AWS Management Console, the Command Line Interface, or Software Development Kits (SDKs).
- **AWS Management Console :** Access and manage Amazon Web Services through the AWS Management Console is a simple and intuitive user interface.

- **AWS Command Line Interface :** The AWS Command Line Interface (CLI) is a unified tool to manage your AWS services.11 With just one tool to download and configure, you can control multiple AWS services from the command line and automate them through scripts.
- **Software Development Kits :** Software Development Kits (SDKs) simplify using AWS services in your applications with an Application Program Interface (API) tailored to your programming language or platform.

☞ **Compute**

- Amazon EC2 : Amazon Elastic Compute Cloud (Amazon EC2) is a web service that provides secure, resizable compute capacity in the cloud. It is designed to make web-scale computing easier for developers.
- The Amazon EC2 simple web service interface allows you to obtain and configure capacity with minimal friction. It provides you with complete control of your computing resources and lets you run on Amazon's proven computing environment.
- Amazon EC2 Container Service : Amazon EC2 Container Service (ECS) is a highly scalable, high-performance container management service that supports Docker containers. It allows you to easily run applications on a managed cluster of Amazons EC2 instances.
- Amazon EC2 Container Registry : Amazon EC2 Container Registry (ECR) is a fully-managed Docker container registry that makes it easy for developers to store, manage, and deploy Docker container images.
- Amazon ECR is integrated with Amazon EC2 Container Service (ECS), simplifying your development to production workflow

☞ **Storage**

- **Amazon S3 :** Amazon Simple Storage Service (Amazon S3) is an object storage with a simple web service interface to store and retrieve any amount of data from anywhere on the web.
- **Amazon Elastic Block Store :** Amazon Elastic Block Store (Amazon EBS) provides persistent block storage volumes for use with Amazon EC2 instances in the AWS Cloud.
- **Amazon Elastic File System :** Amazon Elastic File System (Amazon EFS) provides simple, scalable file storage for use with Amazon EC2 instances in the AWS Cloud
- **Amazon Glacier :** Amazon Glacier is a secure, durable, and extremely low-cost storage service for data archiving and long-term backup

☞ **Database**

- **Amazon Aurora :** Amazon Aurora is a MySQL and PostgreSQL compatible relational database engine that combines the speed and availability of high-end commercial databases with the simplicity and cost-effectiveness of open source databases

- **Amazon RDS :** Amazon Relational Database Service (Amazon RDS) makes it easy to set up, operate, and scale a relational database in the cloud
- **Amazon DynamoDB :** Amazon DynamoDB is a fast and flexible NoSQL database service for all applications that need consistent, single-digit millisecond latency at any scale

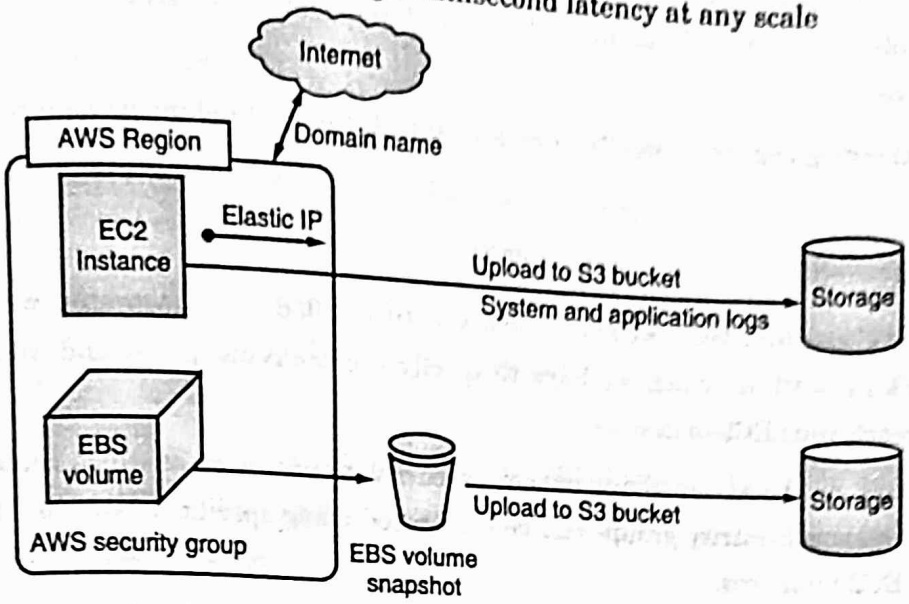


**Fig. 5.6.1 : AWS Architecture**

### ☞ Load Balancing

- Load balancing simply means to hardware or software load over web servers, that improver's the efficiency of the server as well as the application.
- Following is the diagrammatic representation of AWS architecture with load balancing.
- Hardware load balancer is a very common network appliance used in traditional web application architectures.
- AWS provides the Elastic Load Balancing service, it distributes the traffic to EC2 instances across multiple available sources, and dynamic addition and removal of Amazon EC2 hosts from the load-balancing rotation.
- Elastic Load Balancing can dynamically grow and shrink the load-balancing capacity to adjust to traffic demands and also support sticky sessions to address more advanced routing needs.

### ☞ Amazon Cloud-front

- It is responsible for content delivery, i.e. used to deliver website. It may contain dynamic, static, and streaming content using a global network of edge locations. Requests for content at the user's end are automatically routed to the nearest edge location, which improves the performance.
- Amazon Cloud-front is optimized to work with other Amazon Web Services, like Amazon S3 and Amazon EC2. It also works fine with any non-AWS origin server and stores the original files in a similar manner.
- In Amazon Web Services, there are no contracts or monthly commitments. We pay only for as much or as little content as we deliver through the service.

### ☞ Elastic Load Balancer

- It is used to spread the traffic to web servers, which improves performance.
- AWS provides the Elastic Load Balancing service, in which traffic is distributed to EC2 instances over multiple available zones, and dynamic addition and removal of Amazon EC2 hosts from the load-balancing rotation.
- Elastic Load Balancing can dynamically grow and shrink the load-balancing capacity as per the traffic conditions.

### ☞ Security Management

- Amazon's Elastic Compute Cloud (EC2) provides a feature called security groups, which is similar to an inbound network firewall, in which we have to specify the protocols, ports, and source IP ranges that are allowed to reach your EC2 instances.
- Each EC2 instance can be assigned one or more security groups, each of which routes the appropriate traffic to each instance. Security groups can be configured using specific subnets or IP addresses which limits access to EC2 instances.

### ☞ Elastic Caches

- Amazon Elastic Cache is a web service that manages the memory cache in the cloud.
- In memory management, cache has a very important role and helps to reduce the load on the services, improves the performance and scalability on the database tier by caching frequently used information.

### ☞ Amazon RDS

- Amazon RDS (Relational Database Service) provides a similar access as that of MySQL, Oracle, or Microsoft SQL Server database engine.
- The same queries, applications, and tools can be used with Amazon RDS.
- It automatically patches the database software and manages backups as per the user's instruction. It also supports point-in-time recovery. There are no up-front investments required, and we pay only for the resources we use.

### ☞ Hosting RDMS on EC2 Instances

- Amazon RDS allows users to install RDBMS (Relational Database Management System) of your choice like MySQL, Oracle, SQL Server, DB2, etc. on an EC2 instance and can manage as required.
- Amazon EC2 uses Amazon EBS (Elastic Block Storage) similar to network-attached storage.
- All data and logs running on EC2 instances should be placed on Amazon EBS volumes, which will be available even if the database host fails.
- Amazon EBS volumes automatically provide redundancy within the availability zone, which increases the availability of simple disks.

- Further if the volume is not sufficient for our databases needs, volume can be added to increase the performance for our database.
- Using Amazon RDS, the service provider manages the storage and we only focus on managing the data.

☞ **Storage and Backups**

- AWS cloud provides various options for storing, accessing, and backing up web application data and assets.
- The Amazon S3 (Simple Storage Service) provides a simple web-services interface that can be used to store and retrieve any amount of data, at any time, from anywhere on the web.
- Amazon S3 stores data as objects within resources called buckets. The user can store as many objects as per requirement within the bucket, and can read, write and delete objects from the bucket.
- Amazon EBS is effective for data that needs to be accessed as block storage and requires persistence beyond the life of the running instance, such as database partitions and application logs.
- Amazon EBS volumes can be maximized up to 1 TB, and these volumes can be striped for larger volumes and increased performance.
- Provisioned IOPS volumes are designed to meet the needs of database workloads that are sensitive to storage performance and consistency.
- Amazon EBS currently supports up to 1,000 IOPS per volume. We can stripe multiple volumes together to deliver thousands of IOPS per instance to an application.

☞ **Auto Scaling**

- The difference between AWS cloud architecture and the traditional hosting model is that AWS can dynamically scale the web application fleet on demand to handle changes in traffic.
- In the traditional hosting model, traffic forecasting models are generally used to provision hosts ahead of projected traffic.
- In AWS, instances can be provisioned on the fly according to a set of triggers for scaling the fleet out and back in.
- Amazon Auto Scaling can create capacity groups of servers that can grow or shrink on demand.

### 5.6.1 Key Considerations for Web Hosting in AWS

Following are some of the key considerations for web hosting –

☞ **No physical network devices needed**

- In AWS, network devices like firewalls, routers, and load-balancers for AWS applications no longer reside on physical devices and are replaced with software solutions.
- Multiple options are available to ensure quality software solutions. For load balancing choose Zeus, HAProxy, Nginx, Pound, etc. For establishing a VPN connection choose OpenVPN, OpenSwan, Vyatta, etc.

**No security concerns**

- AWS provides a more secured model, in which every host is locked down.
- In Amazon EC2, security groups are designed for each type of host in the architecture, and a large variety of simple and tiered security models can be created to enable minimum access among hosts within your architecture as per requirement.

**Availability of data centers**

EC2 instances are easily available at most of the availability zones in AWS region and provides model for deploying your application across data centers for both high availability and reliability.

## 5.7 APPLICATION LIFECYCLE

- Cloud Computing is the booming industry of the present time and will continue to grow by many folds in the near future.
- Nowadays, it's really hard to find a safe, secure, and yet cost-effective place to store your data and business-critical ideas. But, with the rise of cloud computing, this problem is vanishing exponentially.
- Cloud provides us with a place where your data can not only be stored but can also be accessed easily over the internet.
- Using Cloud Computing you can also host and manage your applications.

**GQ.** Explain Cloud Computing Application Lifecycle.

By using Cloud Computing Solution, we get various benefits, some of which are as follows -

- **Improved software and hardware performance :** Through cloud computing solution one can easily make out what will be the best software and hardware specification for the better performance of the application running on the cloud.
- **Flexibility and affordability :** Cloud Computing provides its users with a wide variety of deployment models and functions through which they can choose the best options for their applications. Cloud services are much more affordable.
- **Increased uptime and availability :** It is highly available and has a great uptime which help's in managing more amount of traffic at a particular time.
- **Better collaboration with real-time sharing :** Cloud computing has great real-time sharing.

Cloud Computing is available for every kind of users who want to deploy their applications onto the cloud service.

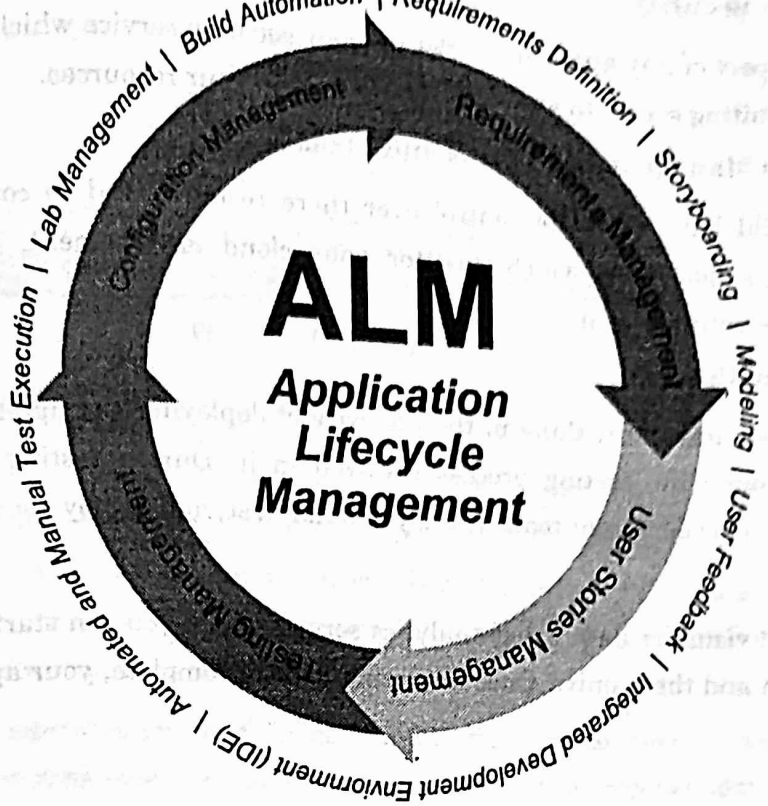


**Fig. 5.7.1 : Application Lifecycle Management**

## ☞ Life Cycle of Cloud Computing Solution

To create such a cloud platform, it takes a long number of steps and dedicated time. Let's now look at the steps involved or the lifecycle of cloud computing solutions.

- **Step 1 : Define the Purpose**

The first and foremost step is to define the purpose for which you want to create a cloud. For this, you have first to understand your business requirement and what type of application you want to run on the cloud. After this, you have to decide whether you want your cloud to be public, private, or hybrid.

- **Step 2 : Define the Hardware**

Deciding what type of hardware, you will need is the most thought after the process. One needs to be very precise in making the decision. For this, you will have to choose the compute service that will provide the right support when you resize your compute capacity to maintain your application running.

- **Step 3 : Define the Storage**

Every application needs a good amount of storage where it's data can be stored safely. For any application storage type that should be chosen carefully for this one should choose the storage service where they can back up and archive their data over the internet.

- **Step 4 : Define the Network**

Networking is the key that will deliver your data to the end-users. So, the network must be configured sincerely and should be flawless so that intruders can not break into the network. One should define the network that securely delivers data, videos, and applications with low latency and high transfer speed.

- **Step 5 : Define the Security**

  Security is a key aspect of any application. Set up your security service which enables services for user authentication or limiting access to a certain set of users on your resources.

- **Step 6 : Define the Management Process and Tools**

  The developer should have complete control over there resource and to configure these you should define some management tools which monitor your cloud environment, resources used, and the customer application running on it.

- **Step 7 : Testing the Process**

  Testing is yet another important thing in the life cycle of deploying any application. All the faults can figure out only through the testing process involved in it. During testing, you should verify your application using various developer tools where you build, test, and deploy your code quickly.

- **Step 8 : Analytics**

  Finally, analyze and visualize data using analytics service where you can start querying data instantly and get results then and there only. Once analyzing is done complete, your application becomes ready you deploying.

☞ **Advantages**

1. **Cost Saving :** It helps you to save substantial capital costs as it does not need any physical hardware investments.
2. **High Speed :** Cloud computing allows you to deploy your service quickly in fewer clicks.
3. **Backup and restore of data :** Backup and restore of data is easy in cloud computing.
4. **Reliability :** It is highly reliable to use cloud computing solutions.

☞ **Disadvantages**

1. **Performance can vary :** Its performance depends on the speed and quality of the internet
2. **Downtime :** Cloud Computing Solutions has a great span of downtime.

## 5.8 COST MODEL

**GQ.** What is Cost Model ?

- Cost estimation simply means a technique that is used to find out the cost estimates.
- The cost estimate is the financial spend that is done on the efforts to develop and test software in Software Engineering.
- Cost estimation models are some mathematical algorithms or parametric equations that are used to estimate the cost of a product or a project.

- Various techniques or models are available for cost estimation, also known as Cost Estimation Models as shown below :

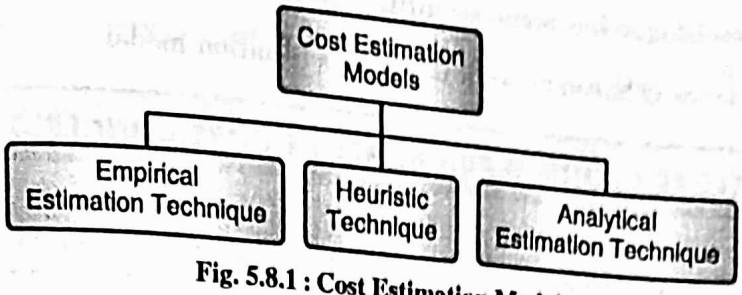


Fig. 5.8.1 : Cost Estimation Model

### ☞ Empirical Estimation Technique

- Empirical estimation is a technique or model in which empirically derived formulas are used for predicting the data that are a required and essential part of the software project planning step. These techniques are usually based on the data that is collected previously from a project and also based on some guesses, prior experience with the development of similar types of projects, and assumptions. It uses the size of the software to estimate the effort.
- In this technique, an educated guess of project parameters is made. Hence, these models are based on common sense. However, as there are many activities involved in empirical estimation techniques, this technique is formalized. For example Delphi technique and Expert Judgement technique.

### ☞ Heuristic Technique

- Heuristic word is derived from a Greek word that means "to discover".
- The heuristic technique is a technique or model that is used for solving problems, learning, or discovery in the practical methods which are used for achieving immediate goals. These techniques are flexible and simple for taking quick decisions through shortcuts and good enough calculations, most probably when working with complex data. But the decisions that are made using this technique are necessary to be optimal.
- In this technique, the relationship among different project parameters is expressed using mathematical equations.
- The popular heuristic technique is given by Constructive Cost Model (COCOMO). This technique is also used to increase or speed up the analysis and investment decisions.

### ☞ Analytical Estimation Technique

- Analytical estimation is a type of technique that is used to measure work. In this technique, firstly the task is divided or broken down into its basic component operations or elements for analyzing.
- Second, if the standard time is available from some other source, then these sources are applied to each element or component of work.
- Third, if there is no such time available, then the work is estimated based on the experience of the work.

- In this technique, results are derived by making certain basic assumptions about the project. Hence, the analytical estimation technique has some scientific basis.
- Halstead's software science is based on an analytical estimation model.

## 5.9 MICROSOFT AZURE CLOUD SERVICES AZURE CORE CONCEPTS

**GQ.** What is Microsoft Azure Cloud Services ?

- Microsoft Azure is a cloud computing platform that provides a wide variety of services that we can use without purchasing and arranging our hardware. It enables the fast development of solutions and provides the resources to complete tasks that may not be achievable in an on-premises environment.
- Azure Services like compute, storage, network, and application services allow us to put our effort into building great solutions without worrying about the assembly of physical infrastructure.
- This tutorial covers the fundamentals of Azure, which will provide us the idea about all the Azure key services that we are most likely required to know to start developing solutions. After completing this tutorial, we can crack job interviews or able to get different Microsoft Azure certifications.

### What is Azure

Microsoft Azure is a growing set of cloud computing services created by Microsoft that hosts your existing applications, streamline the development of a new application, and also enhances our on-premises applications. It helps the organizations in building, testing, deploying, and managing applications and services through Microsoft-managed data centers.

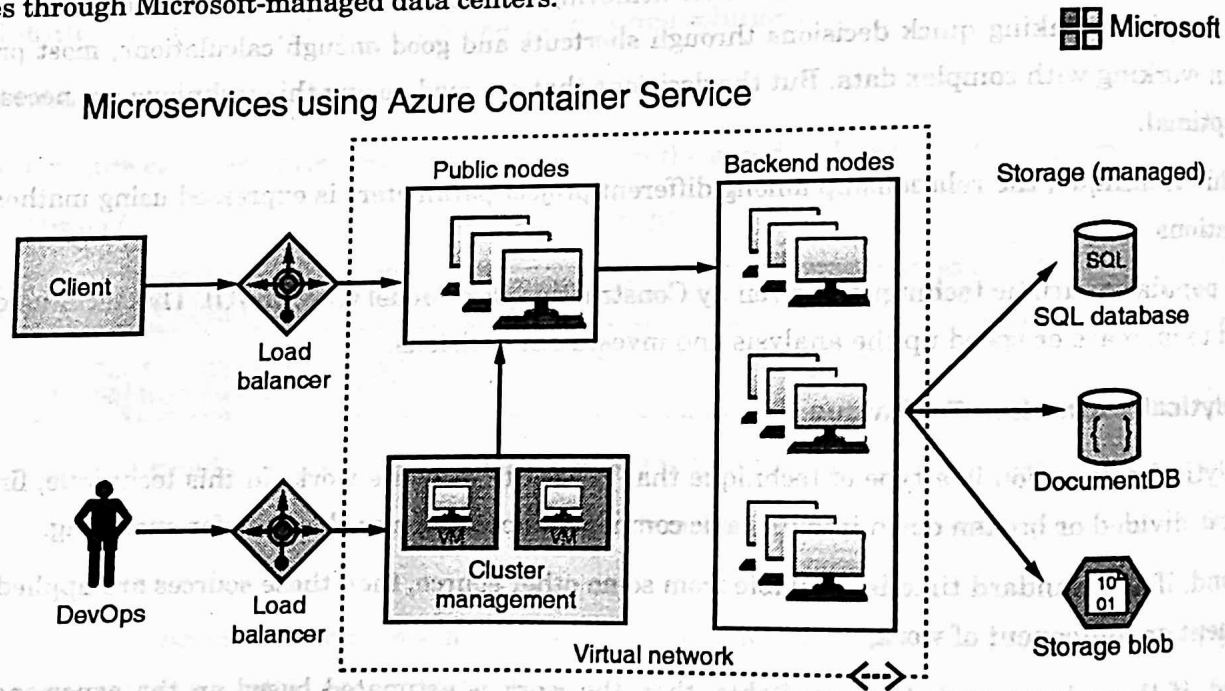


**Fig. 5.9.1 : Microsoft Azure**

### Azure Services

- **Compute services :** It includes the Microsoft Azure Cloud Services, Azure Virtual Machines, Azure Website, and Azure Mobile Services, which processes the data on the cloud with the help of powerful processors.
- **Data services :** This service is used to store data over the cloud that can be scaled according to the requirements. It includes Microsoft Azure Storage (Blob, Queue Table, and Azure File services), Azure SQL Database, and the Redis Cache.
- **Application services :** It includes services, which help us to build and operate our application, like the Azure Active Directory, Service Bus for connecting distributed systems, HDInsight for processing big data, the Azure Scheduler, and the Azure Media Services.
- **Network services :** It helps you to connect with the cloud and on-premises infrastructure, which includes Virtual Networks, Azure Content Delivery Network, and the Azure Traffic Manager.

### GQ. What is Azure Cloud ?

- Microsoft Azure is one of the biggest worldwide cloud computing platforms. It has the prestige and majesty that Microsoft products deserve.
- Azure, with a countless number of services, is really a great cloud platform that should be explored by any developer entering the cloud arena.
- From basic mobile app hosting to full virtualized networks and AI databases, Azure has a wide breadth of uses for development teams. It empowers organizations to meet current and future business challenges. For many, it bridges the gaps between what is possible in science fiction to the real world, bringing "smart" technology to businesses and software development firms.
- Microsoft Azure has so many features and use cases, that it can be difficult to fully discuss them in such a small forum, such as this article. However, this will not stop us from going ahead and trying to take a deep dive into Azure's countless technology oceans.
- Azure Cloud currently includes more than 100 services, most of which mainly fall in these services categories :
- **Compute Services :** Cloud computing with a special focus on Virtual Machines, Containers, and Serverless Computing that you can scale on-demand and on a pay-as-you-go basis
  - **Networking :** Private and public networks; connect on-prime networks with Azure. VPNs and load balance features.
  - **Storage :** Either by disks, file, Blob, or archive. Attach to VM and database. Also, expand and shrink per needs.
  - **Mobile Apps :** Create and deploy native mobile apps across Azure platforms with the help of cognitive and AI services.
  - **Databases :** Choice of various types of databases, including MySQL, MariaDB, PostgreSQL, and Cosmos DB. Developers can build a new database or migrate existing databases.

- **Cloud Web Hosting :** Create and deploy websites and web applications with additional special features.
- **Big Data :** If your enterprise has a huge amount of data, Azure helps you store and analyze that data for better decision-making.
- **App Hosting and DevOps :** Develop, run, and deploy applications on a managed platform including SAP and SQL.

- **AI and Machine Learning :** Throw prebuilt cognitive services and models and deploy distinct AI applications.
- **IoT :** Integrate sensors and smart devices and manage them with IoT Azure hubs to monitor all firm assets.
- **Integration :** Deploy logic apps and services, and connect with applications to orchestrate workflows for business. Also, try new software paradigms like Mixed Reality.
- **Security :** Included in the Azure infrastructure and services. Alongside Azure identity management for better control, including centralized account management.

## 5.10 WINDOWS AZURE PLATFORM APPLIANCE

**GQ.** What is Windows Azure Platform ?

- The Windows Azure platform can also be deployed as an appliance on third-party data centers and constitutes the cloud infrastructure governing the physical servers of the datacenter.
- The Windows Azure Platform Appliance includes Windows Azure, SQL Azure, and Microsoft-specified configuration of network, storage, and server hardware.
- The appliance is a solution that targets governments and service providers who want to have their own cloud computing infrastructure.

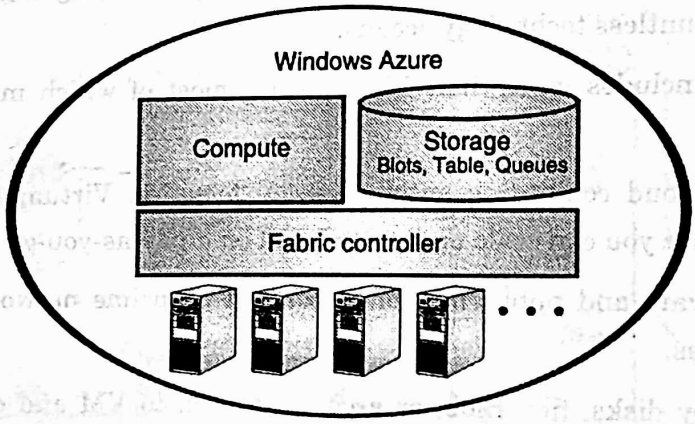


**Fig. 5.10.1 : Windows Azure**

- As introduced earlier, Azure already provides a development environment that allows building applications for Azure in their own premises.
- The local development environment is not intended to be production middleware, but it is designed for developing and testing the functionalities of applications that will eventually be deployed on Azure.

- The Azure appliance is instead a full-featured implementation of Windows Azure. Its goal is to replicate Azure on a third-party infrastructure and make available its services beyond the boundaries of the Microsoft Cloud.
- The appliance addresses two major scenarios: institutions that have very large computing needs (such as government agencies) and institutions that cannot afford to transfer their data outside their premises.
- Windows Azure provides data confidentiality via identity and access management, isolation, and encryption.
- The identity and access management mechanism adopt service management API (SMAPI) to provide web services via the Representational State Transfer (REST) protocol, which runs over SSL and is authenticated with a certificate and private key generated by the customer.
- Windows Azure does not grant customers with administrative access to their VMs. By default, customer software is restricted to running under an account with low privilege. By this, the level of attack will be reduced.
- Communication between Azure internal components are always protected with SSL and via mutual authentication.
- To assure data confidentiality, Azure provides isolation at different levels: hypervisor, root OS, guest VM, and fabric controller.
- Customer access infrastructure is also logically isolated from customer applications and storage.
- Critical internal stored or transmitted data can be encrypted with the .NET Cryptographic Service Providers (CSPs) provided by the Azure SDK. Azure's storage subsystem provides data deletion operations for customers. If the execution of a data delete operation is successful, all the references to that associated data item are removed and the data will not be accessible via the storage APIs.

*Chapter Ends*

□□□

UNIT VI

CHAPTER 6

# Distributed Computing and Internet of Things

**University Prescribed Syllabus**

**Distributed Computing :** Need, Distributed computing vs. Cloud computing, Enabling Technologies for the Internet of Things, Innovative Applications of the Internet of Things, Online Social and Professional Networking.

## 6.1 DISTRIBUTED COMPUTING

- A distributed system is a collection of multiple physically separated servers and data storage that reside in different systems worldwide. These components can collaborate, communicate, and work together to achieve the same objective, giving an illusion of being a single, unified system with powerful computing capabilities.
- A distributed computing server, databases, software applications, and file storage systems can all be considered distributed systems.

### Examples of Distributed Systems

- The internet (World Wide Web) itself.
- Telecommunication networks with multiple antennas, amplifiers, and other networking devices appear as a single system to end-users.

### 6.1.1 Distributed Computing Definition

**GQ.** What is Distributed Cloud ?

- In a distributed cloud, the public cloud infrastructure utilizes multiple locations and data centers to store and run the software applications and services. With this implementation, distributed clouds are more efficient and performance-driven.
- A distributed cloud computing architecture also called distributed computing architecture, is made up of distributed systems and clouds.

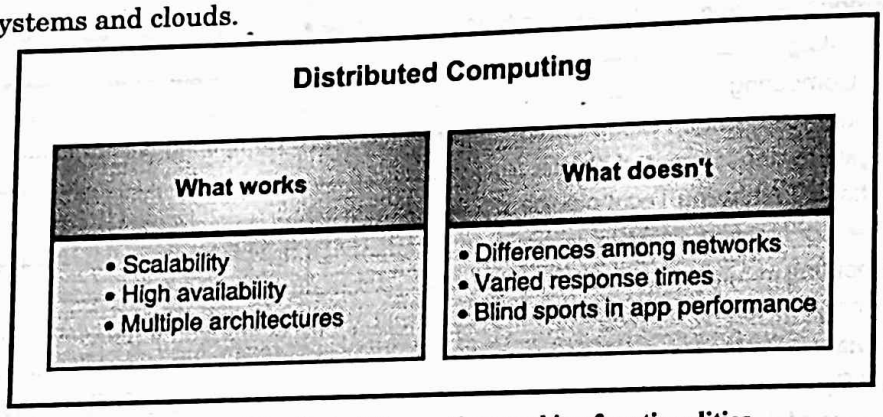


**Fig. 6.1.1 : Distributed Computing working functionalities**

### Examples of Distributed Computing

- Content Delivery Networks (CDNs) utilize geographically separated regions to store data locally in order to serve end-users faster.
- Ridge Edge Platform

## 6.1.2 How Does Distributed Computing Work ?

Distributed computing connects hardware and software resources to do many things, including :

- Work in collaboration to achieve a single goal through optional resource sharing;
- Manage access rights per the authority level of users;
- Keep resources, e.g., distributed computing software, open for further development;
- Achieve concurrency that lets multiple machines work on the same process;
- Ensure all computing resources are scalable and operate faster when multiple machines work together;
- Detect and handle errors in connected components of the distributed network so that the network doesn't fail and stays fault-tolerant.
- Advanced distributed systems have automated processes and APIs to help them perform better.
- From the customization perspective, distributed clouds are a boon for businesses.
- Cloud service providers can connect on-premises systems to the cloud computing stack so that enterprises can transform their entire IT infrastructure without discarding old setups. Instead, they can extend existing infrastructure through comparatively fewer modifications.
- The cloud service provider controls the application upgrades, security, reliability, adherence to standards, governance, and disaster recovery mechanism for the distributed infrastructure.

## 6.1.3 What Are the Advantages of Distributed Cloud Computing ?

- According to Gartner, distributed computing systems are becoming a primary service that all cloud services providers offer to their clients.
- Why? Because the advantages of distributed cloud computing are extraordinary. Here is a quick list:

### Ultimate Scalability

- All nodes or components of the distributed network are independent computers. Together, they form a distributed computing cluster.
- You can easily add or remove systems from the network without resource straining or downtime. Scaling with distributed computing services providers is easy.

### Improved Fault Tolerance

- Distributed systems form a unified network and communicate well. At the same time, the architecture allows any node to enter or exit at any time.
- As a result, fault-tolerant distributed systems have a higher degree of reliability.

### Boosted Performance and Agility

- Distributed clouds allow multiple machines to work on the same process, improving the performance of such systems by a factor of two or more.

- As a result of this load balancing, processing speed and cost-effectiveness of operations can improve with distributed systems.

☞ **Lower Latency**

- As resources are globally present, businesses can select cloud-based servers near end-users and speed up request processing.
- Companies reap the benefit of edge computing's low latency with the convenience of a unified public cloud.

☞ **Helpful in Compliance Implementation**

- Whether there is industry compliance or regional compliance, distributed cloud infrastructure helps businesses use local or country-based resources in different geographies. This way, they can easily comply with varying data privacy rules, such as GDPR in Europe or CCPA in California.
- If you want to learn more about the advantages of Distributed Computing, you should read our article on the benefits of Distributed Computing.

### 6.1.4 Four Types of Distributed Systems

- Under the umbrella of distributed systems, there are a few different architectures.
- Broadly, we can divide distributed cloud systems into four models :

☞ **Client-Server Model**

- In this model, the client fetches data from the server directly then formats the data and renders it for the end-user. To modify this data, end-users can directly submit their edits back to the server.
- For example, companies like Amazon that store customer information. When a customer updates their address or phone number, the client sends this to the server, where the server updates the information in the database.

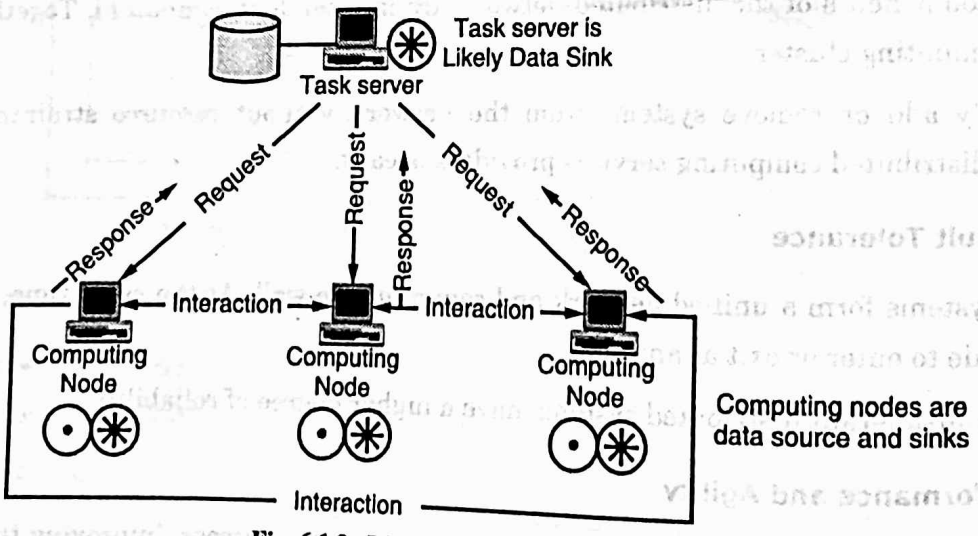


**Fig. 6.1.2 : Distributed Computing Nodes**

### Three-Tier Model

- The three-tier model introduces an additional tier between client and server - the agent tier.
- This middle tier holds the client data, releasing the client from the burden of managing its own information.
- The client can access its data through a web application, typically. Through this, the client application's and the user's work is reduced and automated easily.
- For example, a cloud storage space with the ability to store your files and a document editor.
- Such a storage solution can make your file available anywhere for you through the internet, saving you from managing data on your local machine.

### Multi-Tier Model

- Enterprises need business logic to interact with various backend data tiers and frontend presentation tiers. This logic sends requests to multiple enterprise network services easily. That's why large organizations prefer the n-tier or multi-tier distributed computing model.
- For example, an enterprise network with n-tiers that collaborate when a user publishes a social media post to multiple platforms. The post itself goes from data tier to presentation tier.

### Peer-to-Peer Model

- Unlike the hierarchical client and server model, this model comprises peers. Each peer can act as a client or server, depending upon the request it is processing. These peers share their computing power, decision-making power, and capabilities to work better in collaboration.
- For example, block chain nodes collaboratively work to make decisions regarding adding, deleting, and updating data in the network.

## 6.2 DIFFERENCE BETWEEN CLOUD COMPUTING AND DISTRIBUTED COMPUTING

GQ. State difference between Cloud and Distributed Computing.

### 6.2.1 Cloud Computing

- Cloud computing refers to providing on demand IT resources/services like server, storage, database, networking, analytics, software etc. over internet. It is a computing technique that delivers hosted services over the internet to its users/customers.
- Cloud computing provides services such as hardware, software, networking resources through internet.
- Some characteristics of cloud computing are providing shared pool of configurable computing resources, on-demand service, pay per use, provisioned by the Service Providers etc.
- It is classified into 4 different types such as
  1. Public Cloud
  2. Private Cloud
  3. Community Cloud
  4. Hybrid Cloud

### 6.2.2 Distributed Computing

- Distributed computing refers to solve a problem over distributed autonomous computers and they communicate between them over a network. It is a computing technique which allows to multiple computers to communicate and work to solve a single problem.
- Distributed computing helps to achieve computational tasks faster than using a single computer as it takes a lot of time.
- Some characteristics of distributed computing are distributing a single task among computers to progress the work at same time, Remote Procedure calls and Remote Method Invocation for distributed computations.
- It is classified into 3 different types such as
  1. Distributed Computing Systems
  2. Distributed Information Systems
  3. Distributed Pervasive Systems

### 6.2.3 Tabular Difference between Cloud Computing and Distributed Computing

| Sr. No. | Cloud computing | Distributed computing |
|---|---|---|
| 1. | Cloud computing refers to providing on demand IT resources/services like server, storage, database, networking, analytics, software etc. over internet. | Distributed computing refers to solve a problem over distributed autonomous computers and they communicate between them over a network. |
| 2. | In simple cloud computing can be said as a computing technique that delivers hosted services over the internet to its users/customers. | In simple distributed computing can be said as a computing technique which allows to multiple computers to communicate and work to solve a single problem. |
| 3. | It is classified into 4 different types such as Public Cloud, Private Cloud, Community Cloud and Hybrid Cloud. | It is classified into 3 different types such as Distributed Computing Systems, Distributed Information Systems and Distributed Pervasive Systems. |
| 4. | There are many benefits of cloud computing like cost effective, elasticity and reliable, economies of Scale, access to the global market etc. | There are many benefits of distributed computing like flexibility, reliability, improved performance etc. |
| 5. | Cloud computing provides services such as hardware, software networking resources through internet. | Distributed computing helps to achieve computational tasks more faster than using a single computer as it takes a lot of time. |

| Sr. No. | Cloud computing | Distributed computing |
|---|---|---|
| 6. | The goal of cloud computing is provide on demand computing services over internet on pay per use model. | The goal of distributed computing is to distribute a single task among multiple computers and to solve it quickly by maintain coordination between them. |
| 7. | Some characteristics of cloud computing are providing shared pool of configurable computing resources, on-demand service, pay per use, provisioned by the Service Providers etc. | Some characteristics of distributed computing are distributing a single task among computers to progress the work at same time, Remote Procedure calls and Remote Method Invocation for distributed computations. |
| 8. | Some disadvantage of cloud computing includes less control especially in the case of public clouds, restrictions on available services may be faced and cloud security. | Some disadvantage of cloud computing includes chances of failure of nodes, slow network may create problem in communication. |

| | Cloud Computing | Distributed Computing |
|---|---|---|
| Definition | Cloud computing defines a new way of computing based on the network technology. Cloud computing takes place over the common network like internet. It usually comprises of a collection of integrated and networked hardware, software and internet infrastructure resources. | Distributed computing contains multiple software components from multiple different computers which work together as a single system. Cloud computing can be referred as a virtualization achieved from distributed computing. |
| Goals | • Reduced Initial Investment and Proportional Costs<br>• Increased Scalability<br>• Increased Availability<br>• Increased Reliability | • Resource Sharing<br>• Openness<br>• Transparency<br>• Scalability |
| Types | • Public Clouds<br>• Private Clouds<br>• Community Clouds<br>• Hybrid Clouds | • Distributed Computing Systems<br>• Distributed Information Systems<br>• Distributed Pervasive Systems |

| | Cloud Computing | Distributed Computing |
|---|---|---|
| Characteristics | • It provides a shared pool of configurable computing resources.<br>• An on-demand network model is used to provide access<br>• The clouds are provisioned by the Service Providers.<br>• It provides broad network access. | • A task is distributed amongst different machines for the computation job at the same time.<br>• Technologies such as Remote Procedure calls and Remote Method Invocation are used to construct distributed computations. |
| Disadvantages | • More elasticity means less control especially in the case of public clouds.<br>• Restrictions on available services may be faced, as it depends upon the cloud provider. | • Higher level of failure of nodes than a dedicated parallel machine.<br>• Few of the algorithms are not able to match with slow networks.<br>• Nature of the computing job may present too much overhead. |

## 6.3 ENABLING TECHNOLOGIES FOR THE INTERNET OF THINGS

**GQ.** What are the IOT Enabling Technologies ?

- Internet of Things (IoT) is the concept of connecting devices to the internet and to each other.
- First coined in 1999, the term refers to the giant network of connected things and people, all of which share data amongst each other.
- Today, IoT objects have come to include smartphones to automobiles and everything in between.
- The innumerable data points that billions of IoT devices capture each day are processed into actionable insights with the help of analytics. While the reciprocity between AI and IoT is relatively well known, there are other technologies at play that enable the Internet of Things.
- IoT (internet of things) enabling technologies are
  1. Wireless Sensor Network
  2. Cloud Computing
  3. Big Data Analytics
  4. Communications Protocols
  5. Embedded System

### 6.3.1 Wireless Sensor Network (WSN)

- A WSN comprises distributed devices with sensors which are used to monitor the environmental and physical conditions.
- A wireless sensor network consists of end nodes, routers and coordinators. End nodes have several sensors attached to them where the data is passed to a coordinator with the help of routers.

- The coordinator also acts as the gateway that connects WSN to the internet.
- **Example :**
  - Weather monitoring system
  - Indoor air quality monitoring system
  - Soil moisture monitoring system
  - Surveillance system
  - Health monitoring system

## 6.3.2 Cloud Computing

- It provides us the means by which we can access applications as utilities over the internet. Cloud means something which is present in remote locations.
- With Cloud computing, users can access any resources from anywhere like databases, webservers, storage, any device, and any software over the internet.

### Characteristics

1. Broad network access
2. On demand self-services
3. Rapid scalability
4. Measured service
5. Pay-per-use

- Provides different services, such as – IaaS (Infrastructure as a service) Infrastructure as a service provides online services such as physical machines, virtual machines, servers, networking, storage and data center space on a pay per use basis.
- Major IaaS providers are Google Compute Engine, Amazon Web Services and Microsoft Azure etc.

  **Ex :** Web Hosting, Virtual Machine etc.
- PaaS (Platform as a service) Provides a cloud-based environment with a very thing required to support the complete life cycle of building and delivering West web based (cloud) applications – without the cost and complexity of buying and managing underlying hardware, software provisioning and hosting.
- Computing platforms such as hardware, operating systems and libraries etc. Basically, it provides a platform to develop applications.

  **Ex. :** App Cloud, Google app engine
- SaaS (Software as a service) It is a way of delivering applications over the internet as a service. Instead of installing and maintaining software, you simply access it via the internet, freeing yourself from complex software and hardware management.
- SaaS Applications are sometimes called web-based software on demand software or hosted software. SaaS applications run on a SaaS provider's service and they manage security availability and performance.

  **Ex. :** Google Docs, Gmail, office etc.

### 6.3.3 Big Data Analytics

- It refers to the method of studying massive volumes of data or big data.
- Collection of data whose volume, velocity or variety is simply too massive and tough to store, control, process and examine the data using traditional databases.
- Big data is gathered from a variety of sources including social network videos, digital images, sensors and sales transaction records.
- Several steps involved in analyzing big data :
  1. Data cleaning
  2. Munging
  3. Processing
  4. Visualization
- **Examples :**
  - Bank transactions
  - Data generated by IoT systems for location and tracking of vehicles
  - E-commerce and in Big-Basket
  - Health and fitness data generated by IoT system such as a fitness band

### 6.3.4 Communications Protocols

- They are the backbone of IoT systems and enable network connectivity and linking to applications. Communication protocols allow devices to exchange data over the network.
- Multiple protocols often describe different aspects of a single communication.
- A group of protocols designed to work together is known as a protocol suite; when implemented in software they are a protocol stack.
- They are used in
  - Data encoding
  - Addressing schemes

### 6.3.5 Embedded Systems

- It is a combination of hardware and software used to perform special tasks.
- It includes microcontroller and microprocessor memory, networking units (Ethernet Wi-Fi adapters), input output units (display keyword etc.) and storage devices (flash memory).
- It collects the data and sends it to the internet.
- Embedded systems used in Examples :
  - Digital camera
  - DVD player, music player
  - Industrial robots
  - Wireless Routers etc.

- **Sensors :** These are device that generate electronic signals from physical conditions or events. IoT devices have built in sensors to see, hear and touch the world around them, and hence, turn the physical information into digital data. Sensors are used to gauge variables like images, temperature, motion, proximity, pressure and so on.
- **Networks :** IoT devices are essentially networked devices. The mechanism for communicating the electronic signal can be through a variety of wireless connections such as WiFi, cellular, Bluetooth, near field communication (NFC), and satellite.
- **Standards :** These are the commonly accepted prohibitions or prescriptions for process framework. IoT devices follow uniform technical and regulatory standards that ensure network security, data protection, interoperability among different devices, and so on.
- **Augmented Intelligence :** These are the cognitive tools that provide the ability to describe, predict, and exploit relationships in database. Meaningful analysis of big data charts out the way for corrective future actions through technologies such as computer vision, natural language processing, speech recognition and so on.
- **Augmented Behavior :** This is the carrying out of prescribed action. Augmented behavior manifests in the form of machine-to-machine (M2M) interface and machine-to-human interface (M2H).

## 6.4 INNOVATIVE APPLICATIONS OF THE INTERNET OF THINGS

GQ. What are the different innovative application of IoT ?

- The Internet of Things (IoT) provides the ability to interconnect computing devices, mechanical machines, objects, animals or unique identifiers and people to transfer data across a network without the need for human-to-human or human-to-computer is a system of conversation. IoT applications bring a lot of value in our lives.

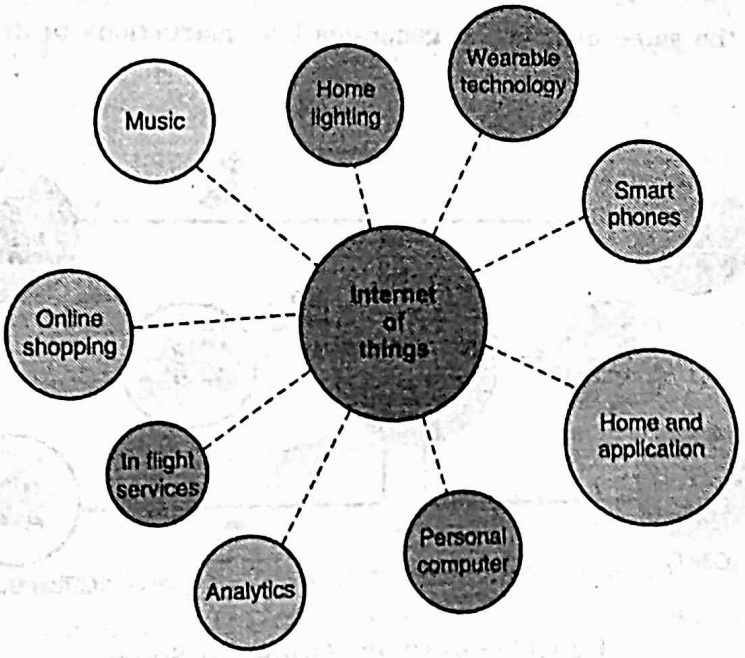


**Fig. 6.4.1 : Applications of IoT**

- The Internet of Things provides objects, computing devices, or unique identifiers and people's ability to transfer data across a network without the human-to-human or human-to-computer interaction.
- A traffic camera is an intelligent device. The camera monitors traffic congestion, accidents and weather conditions and can access it to a common entrance.
- This gateway receives data from such cameras and transmits information to the city's traffic monitoring system.

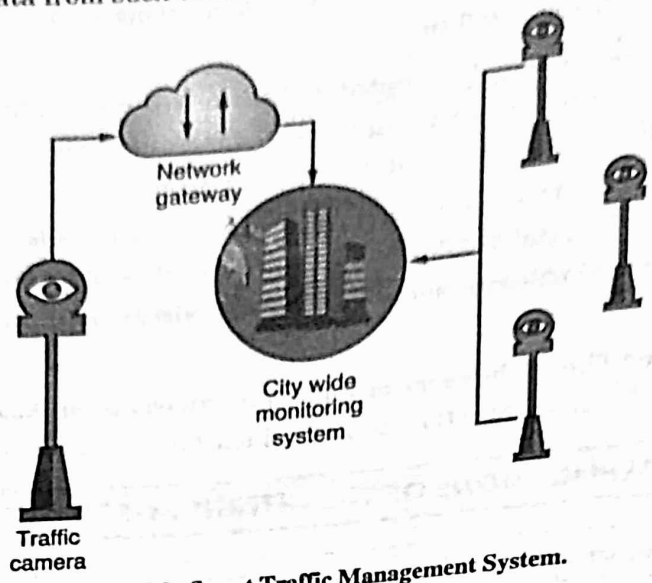


**Fig. 6.4.2 : Smart Traffic Management System.**

- For example, the municipal corporation has decided to repair a road that is connected to the national highway. It may cause traffic congestion to the national highway. The insight is sent to the traffic monitoring system
- The intelligent system analyzes the situation, estimate their impact, and relay information to other cities connected to the same highway. It generates live instructions to drivers by smart devices and radio channels.

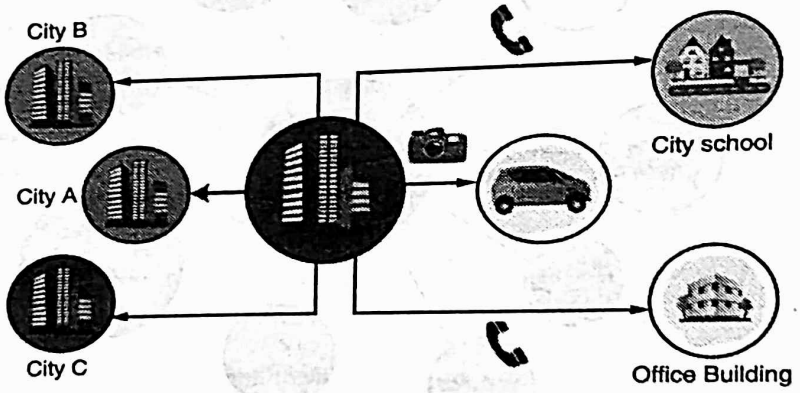


**Fig. 6.4.3 : Smart Traffic Management System.**

- It creates a network of self-dependent systems that take advantage of real-time control.

### 6.4.1 What is IoT ?

- IoT is a platform where embedded devices are connected to the Internet to collect and exchange data. It enables machines to interact, collaborate and learn from experiences like humans.
- IoT applications equipped billions of objects with connectivity and intelligence.

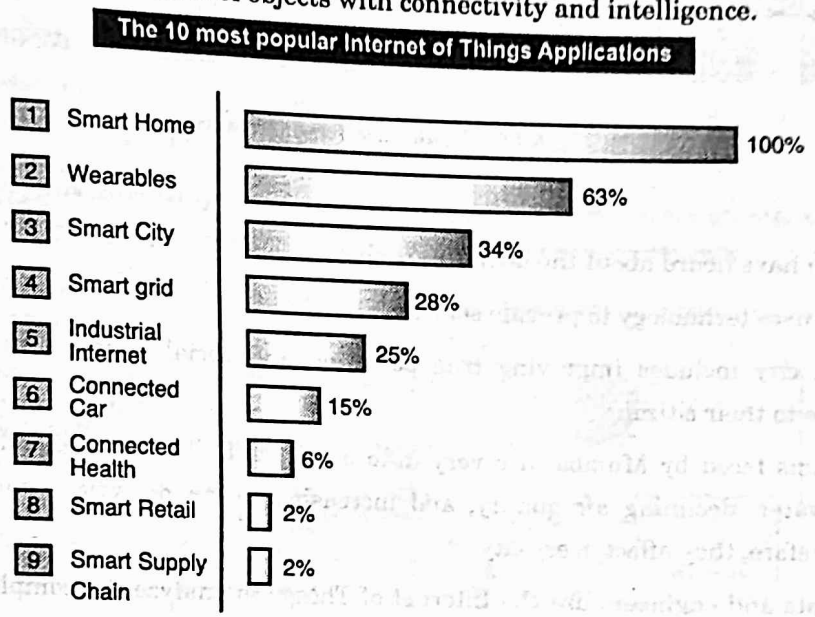


Fig. 6.4.4 : Internet of Things Applications

### 6.4.2 Innovative Applications of IoT

**1. Wearables**

- Wearable technology is the hallmark of IoT applications and one of the earliest industries to deploy IoT. We have fit bits, heart rate monitors and smartwatches these days.
- Guardian glucose monitoring device has been developed to help people with diabetes. It detects glucose levels in our body, uses a small electrode called the glucose sensor under the skin, and relates it to a radiofrequency monitoring device.

**2. Smart Home Applications**

- The smart home is probably the first thing when we talk about the IoT application.
- The example we see the AI home automation is employed by Mark Zuckerberg.
- Alan Pan's home automation system, where a string of musical notes uses in-house functions.

**3. Health care**

- IoT applications can transform reactive medical-based systems into active wellness-based systems. Resources that are used in current medical research lack important real-world information. It uses controlled environments, leftover data, and volunteers for clinical trials.

- The Internet of Things improves the device's power, precision and availability. IoT focuses on building systems rather than just tools. Here's how the IoT-enabled care device works.

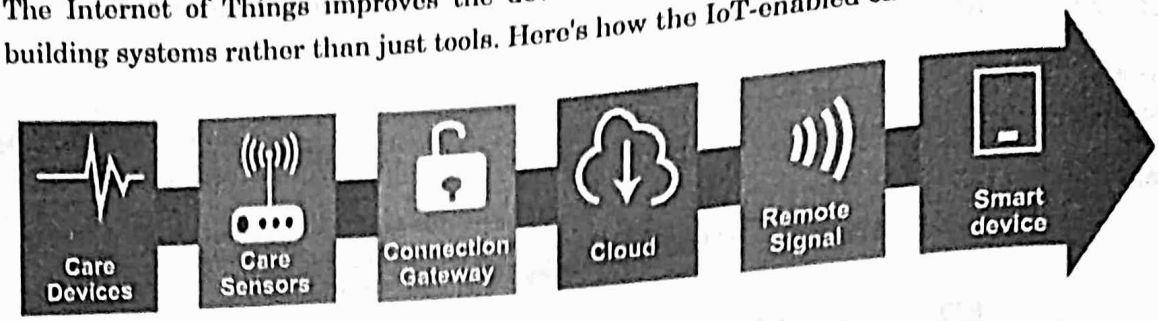


Fig. 6.4.5 : Health Care Sensor Network

**4. Smart Cities**

- Most of you have heard about the term smart city.
- Smart city uses technology to provide services.
- The smart city includes improving transportation and social services, promoting stability and giving voice to their citizens.
- The problems faced by Mumbai are very different from Delhi. Even global issues, such as clean drinking water, declining air quality, and increasing urban density, occur in varying intensity cities. Therefore, they affect every city.
- Governments and engineers use the Internet of Things to analyze the complex factors of town and each city. IoT applications help in the area of water management, waste control and emergencies.
- Example of a smart city - Palo Alto.

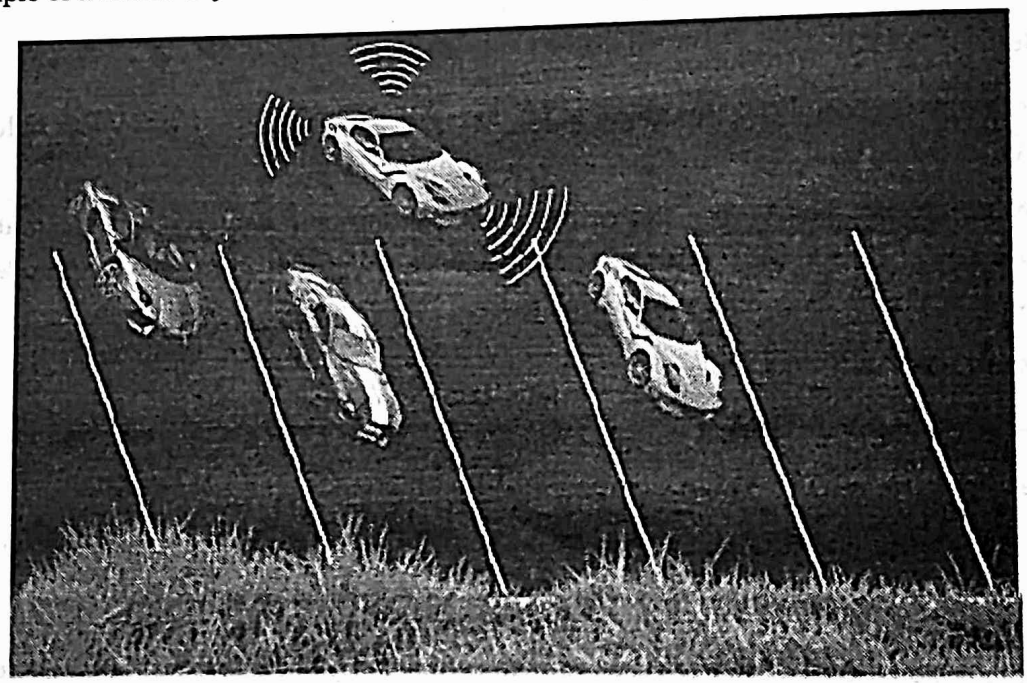

Fig. 6.4.6 : Smart Car System

- Palo Alto, San Francisco, is the first city to acquire the traffic approach. He realized that most cars roam around the same block on the streets in search of parking spots. It is the primary cause of traffic congestion in the city. Thus, the sensors were installed at all parking areas in the city. These sensors pass occupancy status to the cloud of each spot.
- This solution involves the use of sensor arrays that collects data and uses it for many purposes.

### 5. Agriculture

- By the year 2050, the world's growing population is estimated to have reached about 10 billion. To feed such a large population, agriculture needs to marry technology and get the best results. There are many possibilities in this area. One of them is Smart Greenhouse.
- Farming techniques grow crops by environmental parameters. However, manual handling results in production losses, energy losses and labor costs, making it less effective.
- The greenhouse makes it easy to monitor and enables to control the climate inside it.

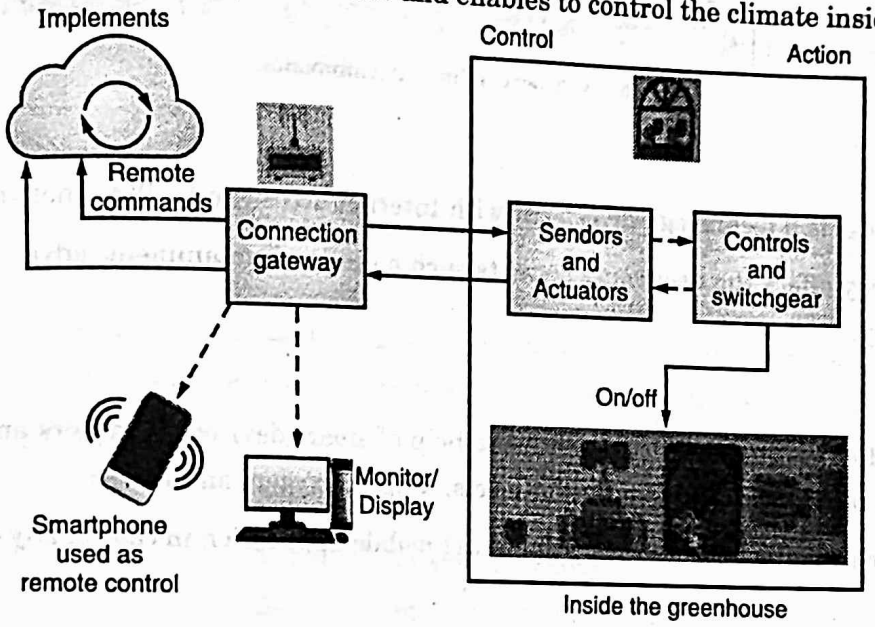


**Fig. 6.4.7 : Smart Agriculture System.**

### 6. Industrial Automation

- It is one of the areas where the quality of products is an essential factor for a more significant investment return.
- Anyone can re-engineer products and their packaging to provide superior performance in cost and customer experience with IoT applications. IoT will prove as a game-changer.
- In industrial automation, IoT is used in the following areas :
  - Product flow monitoring
  - Factory digitization
  - Inventory management
  - Safety and security

- Logistics and Supply Chain Optimization
- Quality control
- Packaging customization

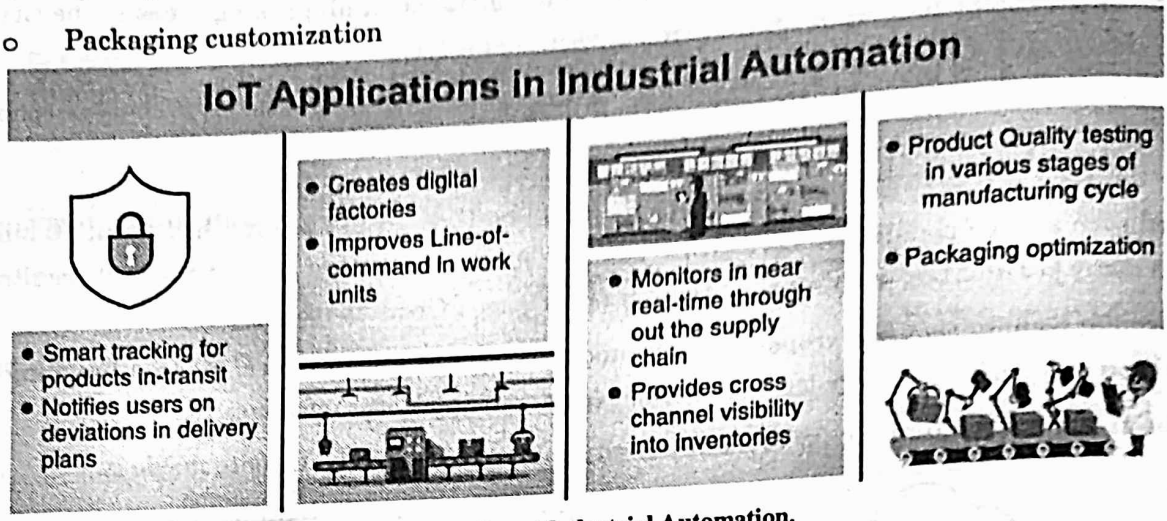


**Fig. 6.4.8 : Smart Industrial Automation.**

**7. Hacked Car**

- A connected car is a technology-driven car with Internet access and a WAN network.
- The technology offers the user some benefits such as in-car infotainment, advanced navigation and fuel efficiency.

**8. Healthcare**

- Healthcare do real-time monitoring with the help of smart devices. It gathers and transfers health data such as blood pressure, blood sugar levels, weight, oxygen, and ECG.
- The patient can contact the doctor by the smart mobile application in case of any emergency.

**9. Smart Retail**

- IoT applications in retail give shoppers a new experience.
- Customers do not have to stand in long queues as the checkout system can read the tags of the products and deduct the total amount from the customer's payment app with IoT applications' help.

**10. Smart Supply Chain**

Customers automate the delivery and shipping with a smart supply chain. It also provides details of real-time conditions and supply networks.

**11. Smart Farming**

- Farmers can minimize waste and increase productivity.
- The system allows the monitoring of fields with the help of sensors.
- Farmers can monitor the status of the area.

- Internet-connected devices go from 5 million to billions in just one year.
- Business Insider Intelligence estimates 24 billion IoT devices will install and generate more than 300 billion in revenue in the future.

## 6.5 ONLINE SOCIAL AND PROFESSIONAL NETWORKING

GQ. What is Online Social and Professional Networking ?

- Social networking, as shown by the massive user groups, has become an everyday part of the lives of many people.
- Some groups also surpass the population of large nations, with more than 400 million active users on Facebook, for example.
- Social networks offer a medium to promote user contact and sharing, thus modeling relationships in the real world. For example, there is a multitude of integrated applications and some organizations now use the Facebook credentials of a user for authentication rather than requiring their credentials. Social networking has now expanded beyond contact between friends.
- Via storing heavy multimedia content in cloud storage systems, social networks help improves Internet usability.
- The most popular material on social media is videos and images, which utilize the entire space available to them. For all of their resource needs, they have the potential to slow down applications and servers.
- Vendors of cloud computing, such as Salesforce and Amazon, currently provide numerous services, including Customer
- Relationship Management (CRM) and Enterprise Resource Planning (ERP). When they deliver these items through cloud storage, without buying standalone software or hardware, consumers can use the simplicity and scalability of the system.
- Social networks, in addition to storing heavy data, use cloud storage for data analytics. So, users can very easily obtain a lot of structured and non-structured knowledge.
- The new and improved analytics that Facebook shows for the benefit of its corporate users is a typical case.
- Backup costs and data recovery costs have been significantly reduced by cloud storage. When data is processed in one location, there is a high probability of losing the data in times of catastrophe. It becomes next to impossible to recover missing data. With cloud computing, however, the data is stored on remote servers and remains available throughout the world. This allows social networking websites to store their users' private information that they cannot afford to misplace under any circumstances.

### 6.5.1 The Social Network and Cloud Computing

- Some of the most controversially debated technologies in recent years include cloud computing and social networking sites.
- The potential for the use of powerful on-demand computing tools through the web is seen as a potential catalyst for the growth of the world economy.
- The cloud is a fact and will continue to be the most distinguished technical advancement, changing the way business is conducted.
- Social cloud computing is also referred to as peer-to-peer computing. It is a field of computer science that generalizes cloud computing to include the sharing, bartering, and leasing of computer resources through peers who are checked by a social network or reputation system to owners and operators. It extends cloud computing to include those interested in engaging in the sharing economy of cloud services outside the boundaries of formal commercial data centers run by cloud providers.
- In turn, this leads to more choices, higher economies of scale, while offering additional benefits for hosting information and computing resources closer to the edge where they might be most needed. There are many applications for cloud computing, and some of them are still being found, for example-
- Social networks can be hosted in a cloud environment, and scalable apps can be used. Via storing heavy multimedia content in cloud storage systems, social networks help improves Internet usability.
- Vendors of cloud computing, such as Salesforce and Amazon, currently provide numerous services, including Customer Relationship Management (CRM) and Enterprise Resource Planning (ERP). When they deliver these items through cloud storage, without buying standalone software or hardware, consumers can use the simplicity and scalability of the system.
- Cloud storage is useful in the event of a catastrophe by reducing the expense of data backup and recovery.
- Social networks and messaging applications such as Snapchat rely on anonymity and will potentially use these tools to provide their users with a more reliable and faster service. For data analytics, social networks use cloud computing.
- "Networking" has been a business buzzword since the 1970s, and it remains a fundamental element of the modern business world. However, what networking looks like has changed significantly since then.
- These days, you don't necessarily need to get in the room with people you want to connect with. You can build your network online instead.

### 6.5.2 The need for Professional Networking

- The benefits of business networking remain essentially the same. For starters, it allows you to access the expertise of others in your field. If you have a business relationship with your peers, you can consult with them about different issues and enrich your own understanding of your industry.

- Another advantage of a strong business network is that it empowers you to build your profile. You can become a well-known name in your field, someone who influences others and can make a real impact in their area of interest.
- When you know and are known by change-makers and powerful people in your industry, you're more likely to hear about exciting opportunities.
- You might be the first to be informed about a new position, or you may even be specifically approached to participate in a project.
- If the benefits are the same, what makes online networking different? Well, you can now make connections and access opportunities on an international level without leaving your own home.

☞ **The growth of online networking**

- Traditional business networking has evolved since the advent of the internet. In the early days of online networking, industries had their own dedicated message boards where people could exchange knowledge and build relationships with others in their field.
- Now there are social networks, such as LinkedIn, which are designed to replicate and improve upon the traditional in-person networking experience. These networks were especially useful during the 2020 pandemic. Because people couldn't leave their homes, many business events where networking would traditionally take place moved online.
- As normality gradually returns, it's natural to wonder whether traditional networking will make a comeback too. But will online networking continue to be a dominant force?

### 6.5.3 Where can I build my Network Online ?

- LinkedIn is the obvious choice for social media for business purposes; it was designed with networking in mind. However, there may be other options to explore. It's also possible to build a dedicated following on platforms such as Instagram and Tik-Tok Creative industries have especially flourished there.
- If you want to speak about specific issues, you might consider attending online conferences. We are more adept at using online conferencing software than ever, so don't assume that you'll just be listening to presentations. It's also possible to take part in "fireside discussions" with smaller groups of fellow participants.
- You can build deeper relations with a select group of people if you join an online mastermind. This involves meeting regularly to discuss pre-arranged topics over a set period of time.
- One purpose of a mastermind is to problem-solve collectively. You can ask others for their perspective on issues affecting your career.

### 6.5.4 What are the benefits of Online Networking over Traditional Networking ?

1. Although the recent online networking boom was driven by the necessities of the pandemic, there are reasons to prefer it over traditional marketing:
2. It's more convenient.
3. Rather than spend time traveling to conferences, you can stay at home and make the same connections. It's easier to pick and choose which parts of a conference are relevant to your business goals, too.
4. It's low-cost.
5. Events and conferences can be expensive. At these events, networking often takes place over dinner and drinks, which can incur additional costs. When you network online, you don't need to pay for this or for travel.
6. You can expand your range.
7. With traditional networking, you're usually limited to events in your immediate area. Online networking allows you to build connections all around the world. As business becomes more international, it makes sense that networking follows suit.
8. The internet is democratizing.
9. During traditional networking events, a hierarchy was often easily observable. For example, access to the most influential people in the room may have been restricted. However, everyone online has equal status, at least in theory.
10. It's less intimidating.
11. When you're a newcomer to your industry, the prospect of approaching seasoned professionals in person can be daunting. With online networking, you don't have to walk across the room, strike up a conversation, and introduce yourself in the same way. The dynamics can be very different.

### 6.5.5 Tips for Online Professional Networking

When networking online, bear the following tips in mind :

1. Be clear about your objectives.
2. What do you want to achieve with your online presence? Do you want to increase your influence, or gain access to specific opportunities? This knowledge will help you plan your contributions.
3. Be authentic but professional.
4. The only way to stand out online is to show your unique personality. However, you shouldn't say anything that could endanger your career. Be wary of using shock tactics to get attention.
5. Respond to other people's requests.

6. Remember, relationships have to be mutually beneficial. People will be less inclined to join your network if you're often asking for support but never offering it.

7. Connect your connections.

8. One way you can be helpful to those in your network is by introducing them to one another. Add people with similar interests into small groups to stimulate more focused conversations.

9. Respect boundaries and take it slow.

10. You may be desperate to add someone to your network, but desperation can be off-putting. Be attentive to other people's cues. If they're not responding right now, circle back in a while. Don't harass anyone or try to force relationships too quickly.

11. Deepen your online connections.

12. If you've been chatting via e-mail or direct messages for a long time, then you might want to suggest a Zoom or Skype call. An "online coffee morning" is a great way to informally emulate an in-person encounter.

13. Post about what matters to you.

14. The best way to build a following of like-minded people is by sharing content about your topics of interest. Keep your contributions relevant to your industry and your career goals.

*Chapter Ends*

□□□

# LAB Manual

## • Case Study 1 •
## Problem Statement : Data storage security in private cloud.

- Cloud Computing is a form of distributed computing wherein resources and application platforms are distributed over the Internet through on demand and pay on utilization basis.
- Data Storage is main feature that cloud data centres are provided to the companies/organizations to preserve huge data. But still few organizations are not ready to use cloud technology due to lack of security. Here we describe the different techniques along with few security challenges, advantages and also disadvantages. It also provides the analysis of data security issues and privacy protection affairs related to cloud computing by preventing data access from unauthorized users, managing sensitive data, providing accuracy and consistency of data stored.

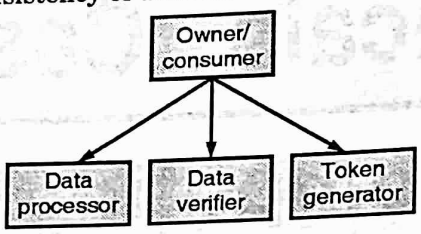


**Fig. 1**

- Cloud refers to the network that provides services to network through internet. It is a model that enables the characteristics like on demand self-service, pay-as-you-use-service. National
- Institute of Standards and Technology (NIST) defines cloud computing as a convenient, on-demand computing resources for storage services.
- Deployment models define purpose, applications and access to the cloud like public, private, hybrid and community.
- Service models are categorized into the three models like Infrastructure-as-Service (IaaS), Platform-as-a-Service (PaaS) and Software-as-Service (SaaS).
- Cloud is an enormous shared computing resource which includes Data Storage. It is managed by a cloud service provider on cloud data servers built on virtualization techniques known as utility storage.
- Most of the storage clouds run on the public internet cloud by well-known companies like Amazon, Dropbox and Google.
- A few bigger associations have discovered esteem in running private cloud inside their own data centres.
- Cloud storage is a utility where data is remotely maintained, managed and backed up in cloud environment and then the data is accessible to end users over internet. It permits the client to collect the files through online so that the client these files from anywhere via internet.

- Even though there are many advantages of cloud storage, few companies are still in dilemma to use the benefits of cloud computing technologies for not having proper security.
- The main objective of the cloud storage is to store the data safely in the free space and fetch the data whenever requested by the client.
- Security and Privacy are the distinguished methods used to secure the information from attackers. Third party is used as service providers to grasp the data sent by owner by offline mode in cloud environment.
- Sometimes cloud may reveal the data by accidentally for unauthorized purpose which strikes the results of privacy and confidentiality. When there is no direct link between clients and servers, master server comes into picture.
- Chunking operation is used for storing duplicate records to give data backup from improvements.
- Clients performs dynamic data operations to store data as tokens in master server and the records are filed in slave servers using token generation and merging algorithms.
- Cloud storage service often provides applications, services to users to access the storage capacity. It is hosted by Storage Service Provider (SSP) [along with the combination of Storage Servers. This SSP is plotted on storage virtualization architecture.
- SSP provides, manages the storage infrastructure to store the data of third party and is arranged as an online storage service provider, virtual storage service provider or cloud storage service provider.
- SSP has a facility that provides large storage infrastructure i.e., Storage Area Network (SAN) and it is distributed between the users/enterprises.
- A SSP provides a specific storage capacity that can be scaled depending upon user requirements. It may be used for various purposes such as data backup, data recovery, sharing and collaboration of various consumer/businesses well as with other applications.
- Multiple-Replica Provable Data Possession (MR-PDP) solves the assumption that multiple copies of data are stored instead of single copy.
- To overcome this assumption a protocol is used called a challenge-response protocol to verify the number of replicas of the file. MR-PDP is more efficient for storing replicas than a single replica PDP scheme.

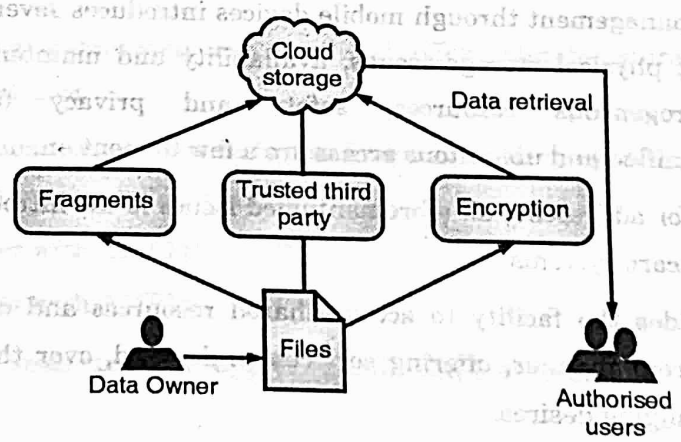


Fig. 2

## Case Study 2 • Problem Statement : Application of IoT / Ubiquitous based on cloud.

- The introduction of the pervasive healthcare paradigm has enabled the attention toward the independent residing of elderly people and the need for regular clinical supervision of continual patients or habitants at remote, isolated or underserved locations.
- In this context, advanced electronic healthcare services are required to be made available through a network anytime, wherever and to anybody.
- A medical assistive environment however concerns the utilization of pervasive and ubiquitous technologies for delivering the above services.
- Wireless technologies enable the real time transmission of data about a patient's circumstance to caregivers. numerous portable devices are available that can detect certain clinical conditions pulse rate, blood pressure, breath alcohol level, and so on from a user's stomach. But this improvement and deployment of health information management through mobile.
- Introduction The introduction of the pervasive healthcare paradigm has enabled the attention toward the independent residing of elderly people and the need for regular clinical supervision of continual patients or habitants at remote, isolated or underserved locations.
- In this context, advanced electronic healthcare services are required to be made available through a network anytime, wherever and to anybody.
- A medical assistive environment however concerns the utilization of pervasive and ubiquitous technologies for delivering the above services.
- Wireless technologies enable the real time transmission of data about a patient's circumstance to caregivers.
- Numerous portable devices are available that can detect certain clinical conditions pulse rate, blood pressure, breath alcohol level, and so on from a user's stomach. But this improvement and deployment of health information management through mobile devices introduces several challenges : data storage and management (e.g., physical storage issues, availability and maintenance), interoperability and availability of heterogeneous resources, safety and privacy (e.g., permission control, data anonymity, etc.), unified and ubiquitous access are a few to mention.
- One potential solution for addressing all aforementioned issues is the introduction of Cloud Computing concept in digital healthcare systems.
- Cloud Computing provides the facility to access shared resources and common infrastructure in a ubiquitous and transparent manner, offering services on-demand, over the network, and performing operations that meet changing desires.

- Similarly, the advance of machine to machine communication (M2M) permits the direct interaction of pervasive healthcare sensors with the internet and by extension with Cloud Computing systems. This communication with the internet has been recently introduced because the 'internet of things' (IoT).e devices introduces several challenges : data storage and management (e.g., physical storage issues, availability and maintenance), interoperability and availability of heterogeneous resources, safety and privacy (e.g., permission control, data anonymity, etc.), unified and ubiquitous access are a few to mention.
- One potential solution for addressing all aforementioned issues is the introduction of Cloud Computing concept in digital healthcare systems.
- Cloud Computing provides the facility to access shared resources and common infrastructure in a ubiquitous and transparent manner, offering services on-demand, over the network, and performing operations that meet changing desires.
- Similarly, the advance of machine to machine communication (M2M) permits the direct interaction of pervasive healthcare sensors with the internet and by extension with Cloud Computing systems. This communication with the internet has been recently introduced because the 'internet of things' (IoT).

## Case Study 3 •
## Problem Statement : Tools for building private cloud.

- Having cloud storage these days have become a requirement, and we are spoilt for choice with what is available out there to help backup our important data, e.g. Dropbox, Google Drive, Box etc. However, they all share one major drawback.
- They have limited storage space and at the end of the day, they are still a third party you have to trust with your (sometimes sensitive) data.
- Why compromise when there is an apparent solution? Thanks to a growing contingent of developers, we can now make our own cloud storage. These solutions forgo the use of a third-party server, ensuring that your data is for your eyes only.
- We have here five tools to create your own cloud – all offer unlimited storage, and a few other features third-party cloud storage lack.
- Do note that some of them require you to be familiar with setting up your own server. As you go down the list, the installation process will get trickier.
    - Set Up Local Server with AMPPS
    - Set Up Local Server with AMPPS
- MAMP is one of the most popular application in OSX to run local server; for Windows users, WAMP...Read more

### Bittorrent Sync

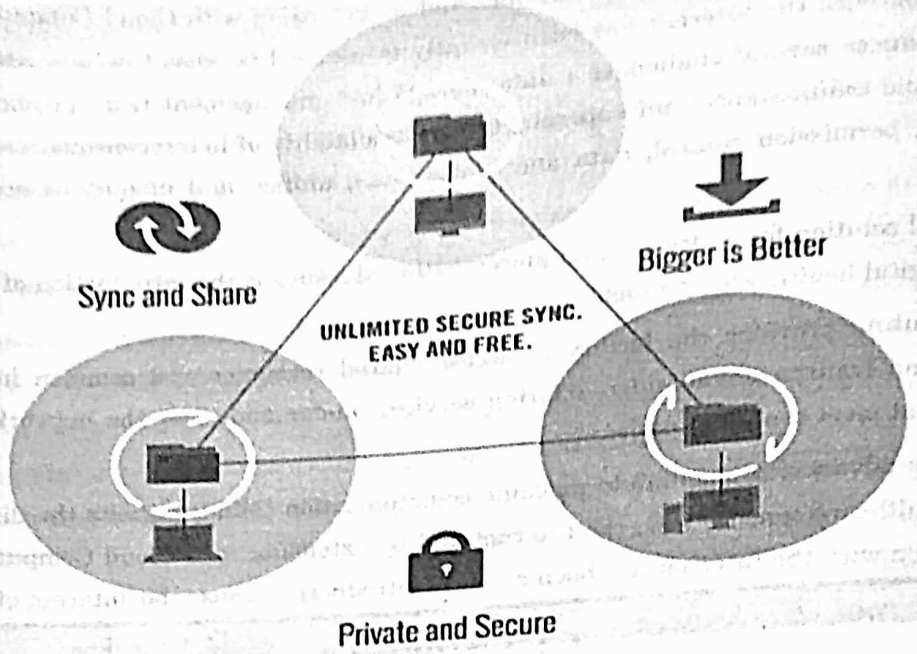


Fig. 3

- We've introduced Bittorrent Sync previously as a way to transfer large files anonymously but did you know that you can also use it to create your personal Cloud?
- All you need to do is configure a folder to act as a drop-off point so you can sync all your files on all your devices running Bittorrent Sync.
- Bittorrent Sync supports : Windows, macOS, Linux, FreeBSD, iOS, Android, Windows Phone, Kindle Fire.

### Own-Cloud

- An incredibly versatile tool, own-Cloud is a free, open source application that lets you build more than a Dropbox replacement to dump your data.
- Along with data storage, the app comes with a number of other features such as a way to manage your calendar, to-do lists, a document editing tool and many more.
- You can get Own-Cloud installed with the instructions found here.


Fig. 4

- **OwnCloud supports :** Clients available for Windows, macOS, Linux, iOS, Android. Server software installed using web installer.

☞ **Seafile**

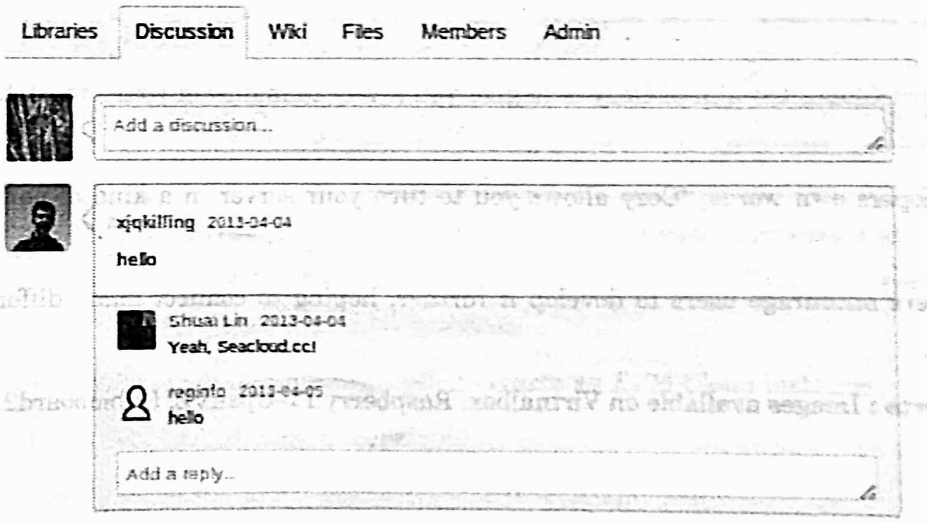


Fig. 5

- Seafile, another open source solution, sells itself as a file syncing and online collaboration tool.
- You have the option of using its cloud service, SeaCloud.cc or set up self-hosted servers. For the latter, there are two kinds: Open Source and Business ($25 per user per year). The application features a rich online file editor, version control, multi-platform file syncing and more.
- **Seafile supports :** Clients available for Windows, macOS, Linux, iOS, Android. Server software available for Windows, Linux, Raspberry Pi.

☞ **Cozy**

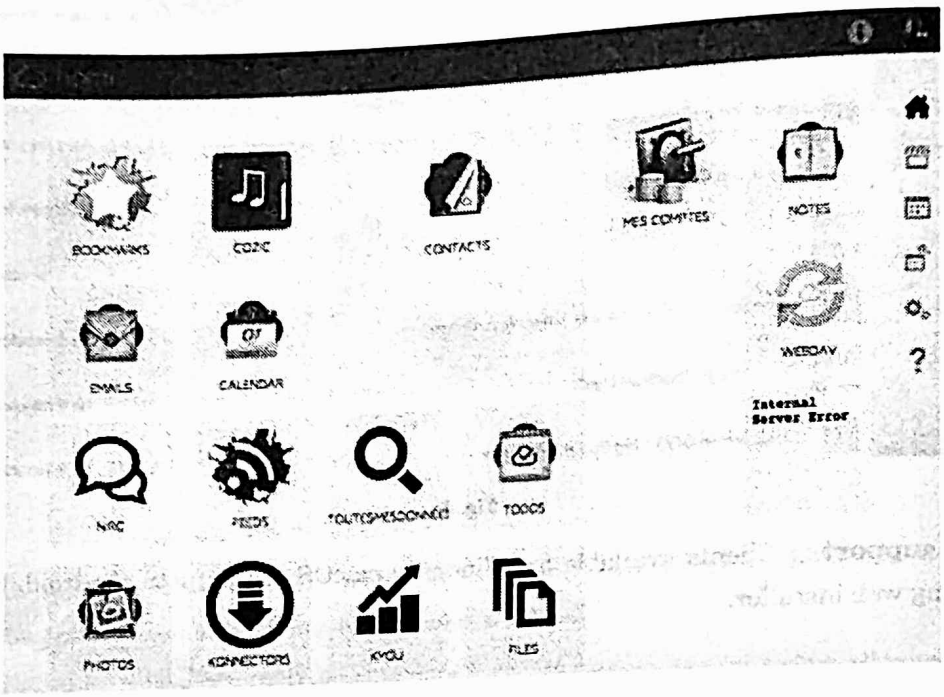


**Fig. 6**

- Similar to OwnCloud, the aim of Cozy is to give you a way to maintain your own data using your own web apps.
- In the developers own words, "Cozy allows you to turn your server in a kind of personal Google App Engine."
- The developers encourage users to develop it further, hoping to connect many different services and utilities to it.
- **Cozy supports :** Images available on Virtualbox, Raspberry Pi, OpenVZ, Cubieboard2, Cubietruck.

☞ **SparkleShare**

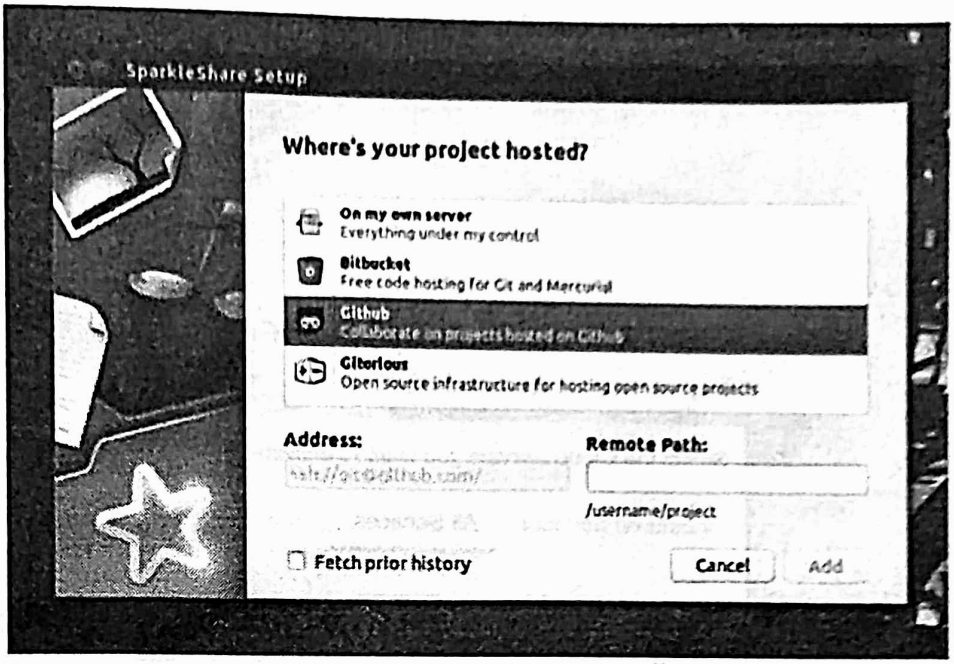


Fig. 7

- Sparkle Share uses git in order to maintain all your data. This means that you will get full version history of your files as well as the other good stuff that comes with git.
- This is an excellent solution if you have documents that require going through a lot of changes. It may not do so well with very large files though.
- **Sparkle Share supports :** Client available for Windows, macOS, Linux. Relies on a Git server for data storage.

## Case Study 4 ● Problem Statement : Creating an EPM Cloud Instance

- An Oracle Enterprise Performance Management Cloud subscription entitles you to one instance comprising two environments; one to host the test version of a business process and the other to host the production version. When you create an instance, Oracle Fusion Cloud Enterprise Performance Management automatically creates these environments.
- You require the Cloud Account Administrator role to create an EPM Cloud instance.
- To create an instance there are flowing 8 steps.

1. Complete a step:
2. Click Create Instance(s) in the email that you received after activating the service and sign in.

Access My Services (OCI). See Accessing My Services (OCI).

3. Click Create Instance.

   In Create Instance, click Create in the EPM tile.

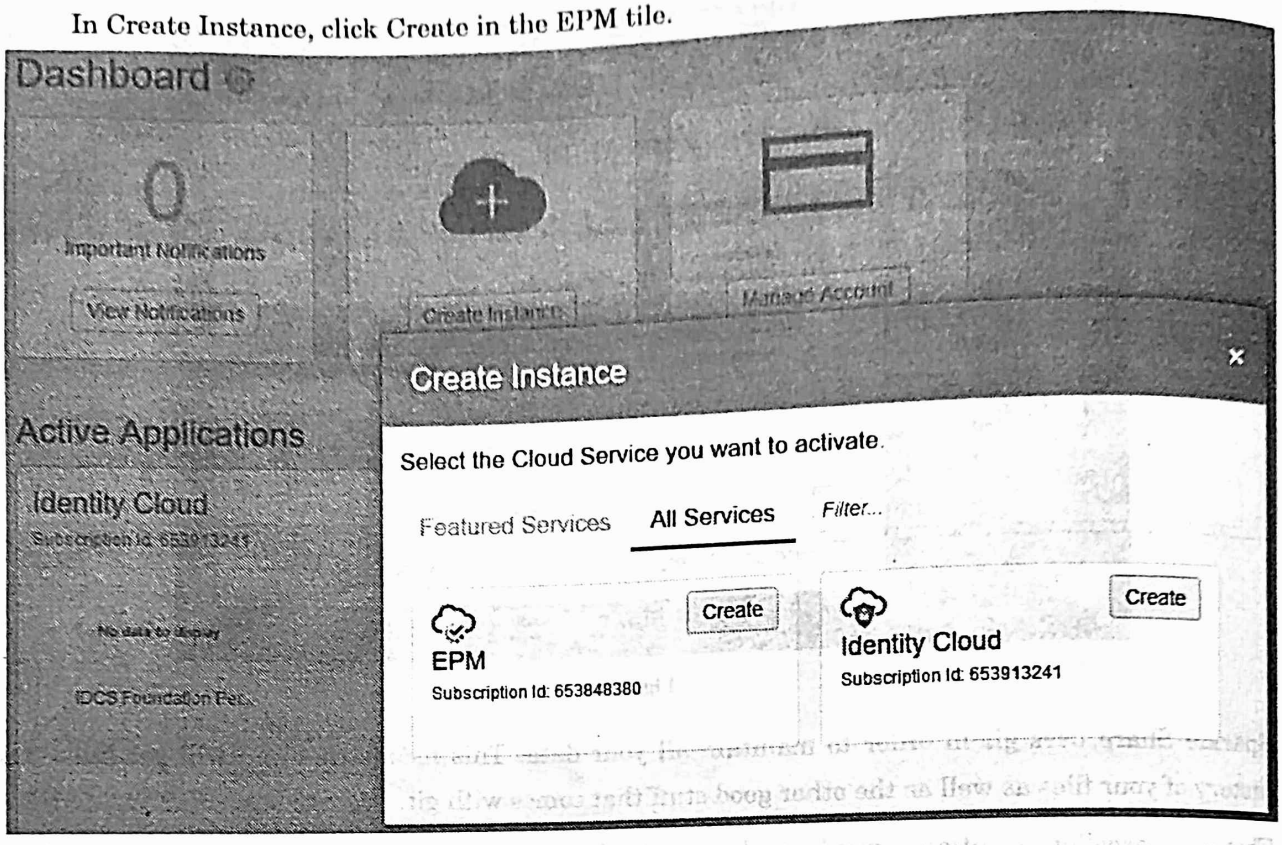


**Fig. 8**

Create Instance Screen

4. Click Configuration.
5. In Data Center, select a data center close to the majority of your users.
6. In Name, enter a name for this environment using only lowercase letters and numbers.

   This name forms a part of the URL to access your environments and should be easily identifiable to users; for example, an abbreviated form of your organization's name. See OCI (Gen 2) URLs for more information.

7. Click Review.
8. Click Complete to submit the request to create the environment.

- This process may take a few minutes to complete after which you should receive an email from oraclecloudadmin_ww@oracle.com titled Action Required : Your new Oracle Enterprise Performance Management instance in Cloud Account xxxx is ready.
- The EPM application tile is now added to the My Services (OCI). Click the name of the tile to view instance and environments details.

*Lab Manual Ends*

□□□