Cloud Computing

Question Bank 1

1. Describe architecture and components of cloud computing

Ans

As we know, cloud computing technology is used by both small and large organizations to **store the information** in cloud and **access** it from anywhere at anytime using the internet connection.

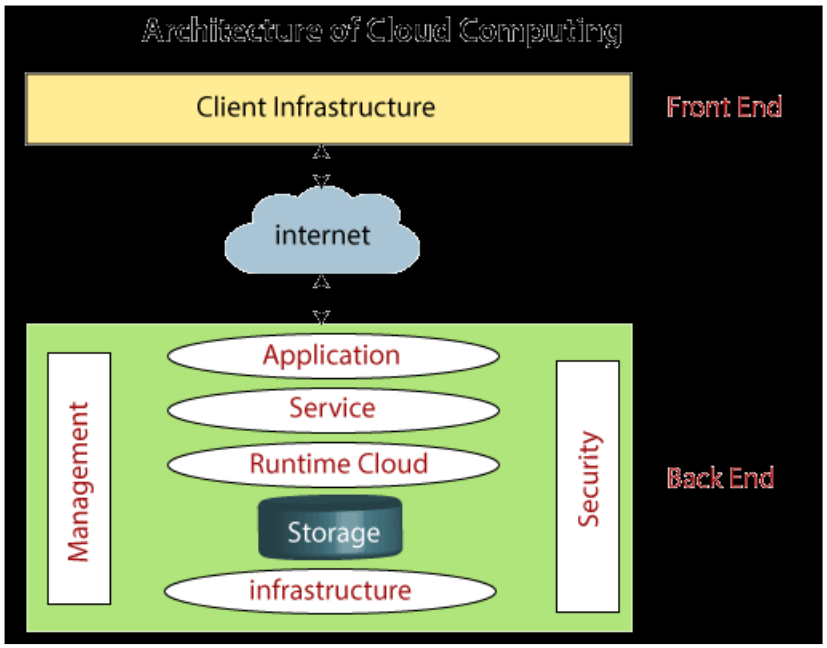
Cloud computing architecture is a combination of **service-oriented architecture** and **event-driven architecture**.

Cloud computing architecture is divided into the following two parts –

o Front End

o Back End

The below diagram shows the architecture of cloud computing –



Front End

The front end is used by the client. 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.

Back End

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

Components of Cloud Computing Architecture

There are the following components of cloud computing architecture -

1. Client Infrastructure

Client Infrastructure is a Front end component. It provides GUI (Graphical User Interface) to interact with the cloud.

2. Application

The application may be any software or platform that a client wants to access.

3. Service

A Cloud Services manages that which type of service you access according to the client's requirement.

Cloud computing offers the following three type of services:

i. Software as a Service (SaaS) – It is also known as **cloud application services**. Mostly, SaaS applications run directly through the web browser means we do not require to download and install these applications. Some important example of SaaS is given below –

Example: Google Apps, Salesforce Dropbox, Slack, Hubspot, Cisco WebEx.

ii. Platform as a Service (PaaS) – It is also known as **cloud platform services**. It is quite similar to SaaS, but the difference is that PaaS provides a platform for software creation, but using SaaS, we can access software over the internet without the need of any platform.

xample: Windows Azure, Force.com, Magento Commerce Cloud, OpenShift.

iii. Infrastructure as a Service (IaaS) – It is also known as **cloud infrastructure services**. It is responsible for managing applications data, middleware, and runtime environments.

Example: Amazon Web Services (AWS) EC2, Google Compute Engine (GCE), Cisco Metapod

4. Runtime Cloud

Runtime Cloud provides the **execution and runtime environment** to the virtual machines. **5. Storage**

Storage is one of the most important components of cloud computing. It provides a huge amount of storage capacity in the cloud to store and manage data.

6. Infrastructure

It provides services on the **host level**, **application level**, and **network level**. Cloud infrastructure includes hardware and software components such as servers, storage, network devices, virtualization software, and other storage resources that are needed to support the cloud computing model.

7. Management

Management is used to manage components such as application, service, runtime cloud, storage, infrastructure, and other security issues in the backend and establish coordination between them.

8. Security

13. State and Explain SOA in cloud computing.

Security is an in-built back end component of cloud computing. It implements a security mechanism in the back end.

9. Internet

The Internet is medium through which front end and back end can interact and communicate with each other.

2. Explain Cloud Computing Reference Model

Ans

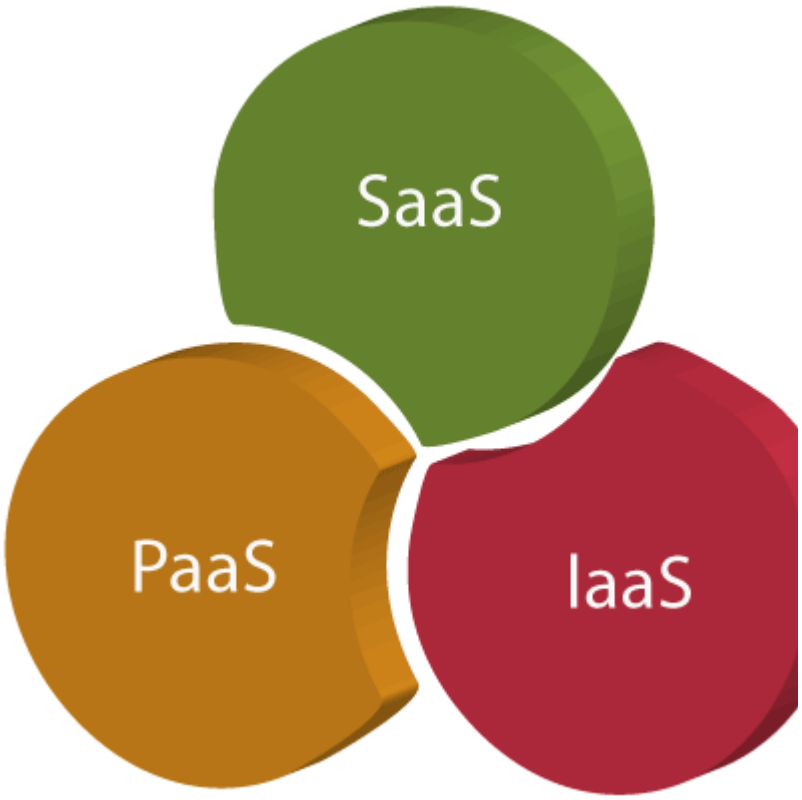
The Cloud Computing Reference Model is a conceptual framework that outlines the structure and key components of cloud computing systems. It helps to understand the roles, responsibilities, and relationships between different cloud service layers and delivery models. The model is typically divided into three main service layers and deployment models:

There are the following three types of cloud service models -

1. Infrastructure as a Service (IaaS)
2. Platform as a Service (PaaS)
3. Software as a Service (SaaS)

14. Describe SLA in cloud Computing.

.



Infrastructure as a Service (IaaS)

IaaS is also known as **Hardware as a Service (HaaS)**. It is a computing infrastructure managed over the internet. The main advantage of using IaaS is that it helps users to avoid the cost and complexity of purchasing and managing the physical servers.

Characteristics of IaaS

There are the following characteristics of IaaS -

- Resources are available as a service
- Services are highly scalable
- Dynamic and flexible
- GUI and API-based access
- Automated administrative tasks

Example: DigitalOcean, Linode, Amazon Web Services (AWS), Microsoft Azure, Google Compute Engine (GCE), Rackspace, and Cisco Metacloud.

Platform as a Service (PaaS)

PaaS cloud computing platform is created for the programmer to develop, test, run, and manage the applications.

Characteristics of PaaS

There are the following characteristics of PaaS -

- Accessible to various users via the same development application.
- Integrates with web services and databases.
- Builds on virtualization technology, so resources can easily be scaled up or down as per the organization's need.
- Support multiple languages and frameworks.
- Provides an ability to "**Auto-scale**".

Example: AWS Elastic Beanstalk, Windows Azure, Heroku, Force.com, Google App Engine, Apache Stratos, Magento Commerce Cloud, and OpenShift.

To know more about PaaS, click here.

Software as a Service (SaaS)

SaaS is also known as "**on-demand software**". It is a software in which the applications are hosted by a cloud service provider. Users can access these applications with the help of internet connection and web browser.

Characteristics of SaaS

There are the following characteristics of SaaS -

- Managed from a central location
- Hosted on a remote server
- Accessible over the internet
- Users are not responsible for hardware and software updates. Updates are applied automatically.

- The services are purchased on the pay-as-per-use basis

Example: BigCommerce, Google Apps, Salesforce, Dropbox, ZenDesk, Cisco WebEx, ZenDesk, Slack, and GoToMeeting.

3. **Explain web services in brief.**
   A Web Service **is can be defined by following ways:**

Ans

A Web Service can be defined in the following ways:

1. Interoperable Communication System: A web service is a standardized method that allows different applications, often on different platforms and written in different programming languages, to communicate with each other over the internet using open protocols like HTTP, XML, SOAP, and REST.**

2. Self-Contained, Modular Applications: Web services are self-contained software modules that can be described, published, discovered, and invoked over the network to provide specific functionalities, such as retrieving information, executing operations, or interacting with databases.**

3. **Platform-Independent Interface: Web services expose a platform-independent interface that enables applications to interact regardless of the underlying technology stack. For example, a Java application can communicate with a .NET application via web services.**

4. **Service-Oriented Architecture (SOA): Web services are integral components of SOA, where different services are made available to other systems on a network, enabling integration and interoperability.**

5. **Communication via Standard Protocols: Web services often rely on protocols like SOAP (Simple Object Access Protocol) for structured messaging or REST (Representational State Transfer) for lightweight web communication using HTTP.**

4. **Describe Properties and Characteristics of cloud computing.**

Ans

Characteristics of Cloud Computing The characteristics of cloud computing are given below:

1) Agility

The cloud **works in a distributed computing environment**. It shares resources among users and works very fast.

2) High availability and reliability

The availability of servers is high and more reliable because the **chances of infrastructure failure are minimum**.

3) High Scalability

Cloud offers **"on-demand" provisioning of resources on a large scale**, without having engineers for peak loads.

4) Multi-Sharing

With the help of cloud computing, **multiple users and applications can work more efficiently** with cost reductions by sharing common infrastructure.

5) Device and Location Independence Cloud computing enables the users to access systems using a web browser regardless of their location or what device they use e.g. PC, mobile phone, etc. **As infrastructure is off-site** (typically provided by a third-party) **and accessed via the Internet, users can connect from anywhere**.

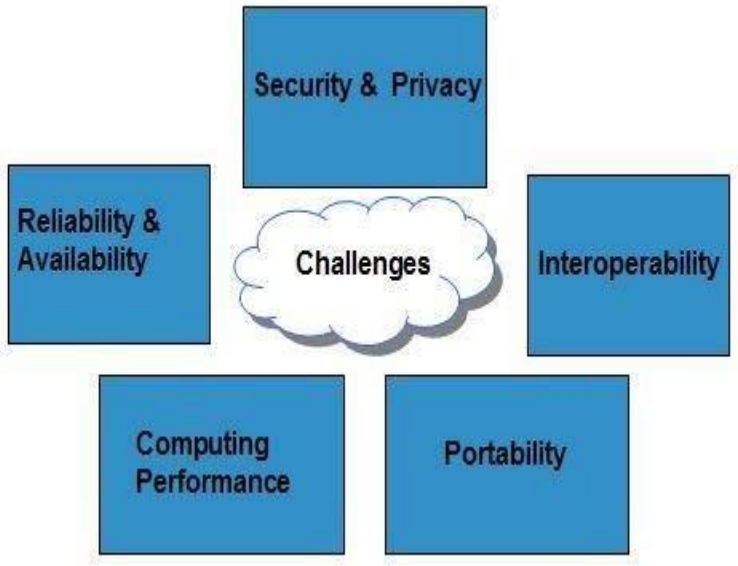
6) Maintenance Maintenance of cloud computing applications is easier, since they **do not need to be installed on each user's computer and can be accessed from different places**. So, it reduces the cost also.

7) Low Cost By using cloud computing, the cost will be reduced because to take the services of cloud computing, **IT company need not to set its own infrastructure** and pay-as-per usage of resources.

8) Services in the pay-per-use mode Application Programming Interfaces **(APIs) are provided to the users so that they can access services on the cloud** by using these APIs **and pay the charges as per the usage of services**.

5. **Explain challenges of Cloud computing.**

Ans



Security and Privacy

Security and Privacy of information is the biggest challenge to cloud computing. Security and privacy issues can be overcome by employing encryption, security hardware and security applications.

Portability

This is another challenge to cloud computing that applications should easily be migrated from one cloud provider to another. There must not be vendor lock-in. However, it is not yet made possible because each of the

cloud provider uses different standard languages for their platforms.

Interoperability

It means the application on one platform should be able to incorporate services from the other platforms. It is made possible via web services, but developing such web services is very complex.

Computing Performance

Data intensive applications on cloud requires high network bandwidth, which results in high cost. Low bandwidth does not meet the desired computing performance of cloud application.

Reliability and Availability

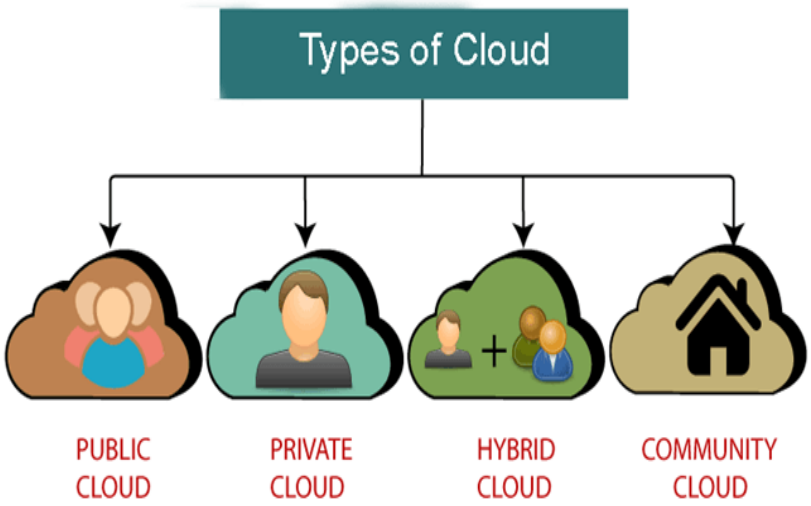
It is necessary for cloud systems to be reliable and robust because most of the businesses are now becoming dependent on services provided by third-party.

Lack of Knowledge and Expertise
Due to the complex nature and the high demand for research working with the cloud often ends up being a highly tedious task. It requires immense knowledge and wide expertise on the subject. Although there are a lot of professionals in the field they need to constantly update themselves. Cloud computing is a highly paid job due to the extensive gap between demand and supply. There are a lot of vacancies but very few talented cloud engineers, developers, and professionals. Therefore, there is a need for upskilling so these professionals can actively understand, manage and develop cloud-based applications with minimum issues and maximum reliability.

6. Describe types of cloud Computing.

Ans

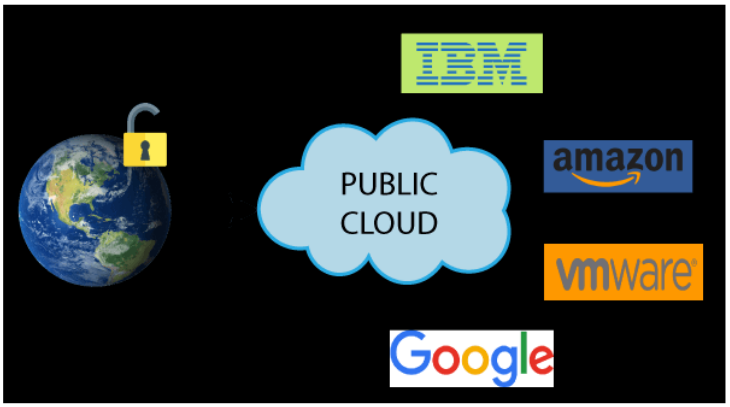
There are the following 4 types of cloud that you can deploy according to the organization's needs-



o Public Cloud
o Private Cloud
o Hybrid Cloud
o Community Cloud

Public Cloud

- Public cloud is **open to all** to store and access information via the Internet using the pay-per-usage method.
- In public cloud, computing resources are managed and operated by the Cloud Service Provider (CSP).
- **Example:** Amazon elastic compute cloud (EC2), IBM SmartCloud Enterprise, Microsoft, Google App Engine, Windows Azure Services Platform.



Advantages of Public Cloud

There are the following advantages of Public Cloud –

o Public cloud is owned at a lower cost than the private and hybrid cloud.

o Public cloud is maintained by the cloud service provider, so do not need to worry about the maintenance.
o Public cloud is easier to integrate. Hence it offers a better flexibility approach to consumers.
o Public cloud is location independent because its services are delivered through the internet.
o Public cloud is highly scalable as per the requirement of computing resources.
o It is accessible by the general public, so there is no limit to the number of users.

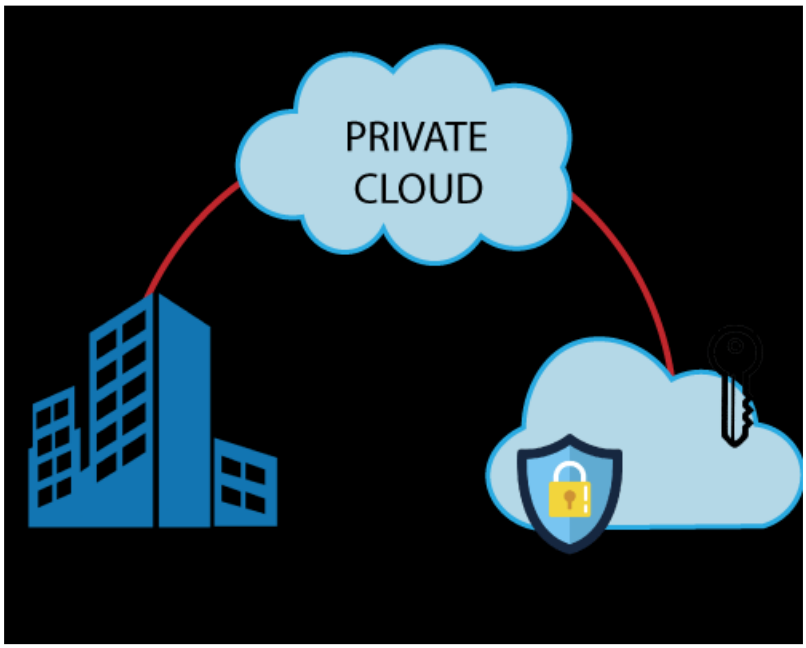
Disadvantages of Public Cloud

o Public Cloud is less secure because resources are shared publicly.
o Performance depends upon the high-speed internet network link to the cloud provider.
o The Client has no control of data.

Private Cloud

Private cloud is also known as an **internal cloud** or **corporate cloud**. It is used by organizations to build and manage their own data centers internally or by the third party. It can be deployed using Opensource tools such as Openstack and Eucalyptus.

Based on the location and management, National Institute of Standards and Technology (NIST) divide private cloud into the following two parts-o On-premise private cloud o Outsourced private clou



Advantages of Private Cloud

There are the following advantages of the Private Cloud –

o Private cloud provides a high level of security and privacy to the users.

o Private cloud offers better performance with improved speed and space capacity.

o It allows the IT team to quickly allocate and deliver on-demand IT resources.

o The organization has full control over the cloud because it is managed by the organization itself. So, there is no need for the organization to depends on anybody.

o It is suitable for organizations that require a separate cloud for their personal use and data security is the first priority

Disadvantages of Private Cloud

o Skilled people are required to manage and operate cloud services.

o Private cloud is accessible within the organization, so the area of operations is limited.

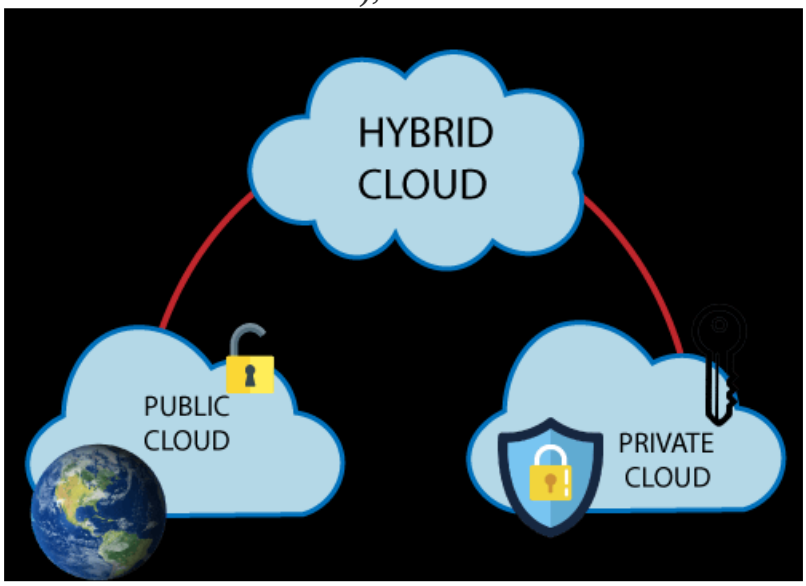
o Private cloud is not suitable for organizations that have a high user base, and organizations that do not have the prebuilt infrastructure, sufficient manpower to maintain and manage the cloud

Hybrid Cloud

Hybrid Cloud is a combination of the public cloud and the private cloud. we can say: ***Hybrid Cloud = Public Cloud + Private Cloud*** Hybrid cloud is partially secure because the services which are running on the

public cloud can be accessed by anyone, while the services which are running on a private cloud can be accessed only by the organization's users.

Example: Google Application Suite (Gmail, Google Apps, and Google Drive), Office 365 (MS Office on the Web and One Drive), Amazon Web Services.



Advantages of Hybrid Cloud

There are the following advantages of Hybrid Cloud –

o Hybrid cloud is suitable for organizations that require more security than the public cloud.

o Hybrid cloud helps you to deliver new products and services more quickly.

o Hybrid cloud provides an excellent way to reduce the risk.

o Hybrid cloud offers flexible resources because of the public cloud and secure resources because of the private cloud.

Disadvantages of Hybrid Cloud

o In Hybrid Cloud, security feature is not as good as the private cloud.

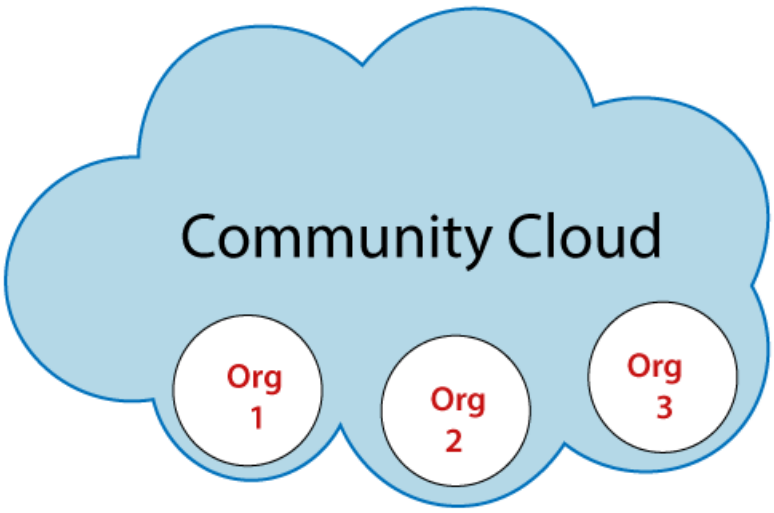
o Managing a hybrid cloud is complex because it is difficult to manage more than one type of deployment model.

o In the hybrid cloud, the reliability of the services depends on cloud service providers.

Community Cloud

Community cloud allows systems and services to be accessible by a group of several organizations to share the information between the organization and a specific community. It is owned, managed, and operated by one or more organizations in the community, a third party, or a combination of them.

Example: Health Care community cloud



Advantages of Community Cloud

There are the following advantages of Community Cloud –

o Community cloud is cost-effective because the whole cloud is being shared by several organizations or communities.

o Community cloud is suitable for organizations that want to have a collaborative cloud with more security features than the public cloud.

o It provides better security than the public cloud. o It provdes collaborative and distributive environment.

o Community cloud allows us to share cloud resources, infrastructure, and other capabilities among various organizations.

Disadvantages of Community Cloud o Community cloud is not a good choice for every organization. o Security features are not as good as the private cloud. o It is not suitable if there is no collaboration. o The fixed amount of data storage and bandwidth is shared among all community members.

7. **Explain Benefits of virtualization in cloud computing**.

ans

- The virtualization computing approach enables a single physical machine to act as multiple virtual computers.
- Software abstraction layers effectively segment one computer into several “virtual” machines.
- Developers can then run many independent operating systems on the same hardware.
- By egmenting a single physical machine into multiple virtual machines, you can make the most of available hardware, lower costs, and improve DevOps efficiency.

Virtualization offers substantial benefits for just about any business or development environment. It has become a core strategy for improving IT efficiency.

Let’s look at how virtualization can save money, streamline DevOps, and increase your service availability.

Reduced expenses

Computing power comes at a price. If the only way to get more resources is to purchase new hardware, that price becomes hefty. With virtualization tactics, you can take a hard look at your existing infrastructure and identify wasted or idle computing resources.

Too often, organizations deploy servers to run applications that consume only a fraction of their available resources. Such servers never make use of their full potential. To make matters worse, when their applications are not running, these servers sit entirely idle.

In a virtualized environment, you can assign each VM precisely the amount of computing power it

needs to do its job. The remaining resources are then available for other VMs and their applications.

Virtualization costs are almost always lower than the cost of purchasing and maintaining additional hardware.

Resiliency

A virtualized server environment is not bound to hardware like a traditional environment. **You can easily back up, copy, and clone VMs to different physical hardware.**

Waiting for new hardware to be ready for deployment can take days, weeks, or even months. Meanwhile, you can deploy a VM backup in a matter of minutes. When Murphy's Law finally catches up with you, you will be thankful you can rapidly deploy your VM on a different machine, in a different location, with minimal hassle.

High availability

Since you can clone a VM almost effortlessly, you can easily set up redundant virtualized environments with exceptionally high availability. By automatically monitoring VM status and rapidly switching to backup VMs in an outage, **virtualization provides an extremely reliable system with no single point of failure in hardware or software.**

These "failover" systems enable you to seamlessly continue operating your VM from its last working state. This maximizes service availability no matter what goes wrong.

You can remotely monitor, configure, and restart your entire virtual environment. This provides developers constant access, no matter how far they may be from the physical hardware, which helps further mitigate any potential downtime.

Increased efficiency

Virtual environments are much easier to maintain than physical environments. Rather than managing numerous

physical servers requiring individual attention, virtualization enables you to configure, monitor, and update all your VMs from a single machine. This saves time deploying updates, implementing security patches, and installing new software.

With less physical hardware to worry about, your IT department spends less time maintaining physical machines. Your developers enjoy the efficiency of rapidly spinning up a VM without having to worry about adding new hardware.

By nature, virtual environments are inherently scalable. You can easily deploy many instances of the same VM to help handle heavy load, offering efficient scalability that is always ready to support and sustain growth.

DevOps made easy

Virtualization is a developer's best friend. It effectively segments production and development environments without extra hardware.

It is simple to clone a VM to set up testing environments. You can test features and squash bugs without affecting your live product.

With traditional hardware-based environments, developers need to manage all the updates and maintenance for their development machines. Maintaining an accurate representation of live servers for testing is also an ongoing challenge.

VMs quickly solve all these issues. **Virtualization provides on-demand access to an infinite number of perfectly replicated virtual machines for developers to play with.**

Developers take advantage of virtualization to help them expedite updates, improve software security, and maintain an efficient pipeline between development, testing, and deployment.

Greener IT

In the long run, virtualization is an eco-friendly approach to IT. **Reducing hardware requirements also**

reduces power consumption, ultimately minimizing our carbon footprint.

This is good for both the environment and your bottom line. Power savings make it cheaper to maintain servers and data centers. You can then invest all that money in other ventures, like making your business even more environmentally friendly.

8. Explain Types of Virtualizations.

ANS

Virtualization is the "creation of a virtual (rather than actual) version of something, such as a server, a desktop, a storage device, an operating system or network resources".

In other words, Virtualization is a technique, which allows to share a single physical instance of a resource or an application among multiple customers and organizations. It does by assigning a logical name to a physical storage and providing a pointer to that physical resource when demanded.

Types of Virtualization:

1. Hardware Virtualization.
2. Operating system Virtualization.
3. Server Virtualization.
4. Storage Virtualization.

1) Hardware Virtualization:

When the virtual machine software or virtual machine manager *(VMM) is directly installed on the hardware system* is known as hardware virtualization.

The main job of hypervisor is to control and monitoring the processor, memory and other hardware resources.

After virtualization of hardware system we can install different operating system on it and run different applications on those OS.

Usage:

Hardware virtualization is mainly done for the server platforms, because controlling virtual machines is much easier than controlling a physical server.

2) Operating System Virtualization:

When the virtual machine software or virtual machine manager *(VMM) is installed on the Host operating system* instead of directly on the hardware system is known as operating system virtualization

Usage:

Operating System Virtualization is mainly used for testing the applications on different platforms of OS.

3) Server Virtualization:

When the virtual machine software or virtual machine manager *(VMM) is directly installed on the Server system* is known as server virtualization.

Usage:

Server virtualization is done because a single physical server can be divided into multiple servers on the demand basis and for balancing the load.

4) Storage Virtualization:

Storage virtualization is the *process of grouping the physical storage from multiple network storage devices so that it looks like a single storage device*.

Storage virtualization is also implemented by using software applications.

Usage:

Storage virtualization is mainly done for back-up and recovery purposes.

9. Explain Xen virtualization System.

ANS

- Xen is an open source hypervisor based on paravirtualization.

- It is the most popular application of paravirtualization.
- Xen has been extended to compatible with full virtualization using hardware-assisted virtualization.
- It enables high performance to execute guest operating system.
- This is probably done by removing the performance loss while executing the instructions requiring significant handling and by modifying portion of the guest operating system executed by Xen, with reference to the execution of such instructions. Hence this especially support x86, which is the most used architecture on commodity machines and servers.

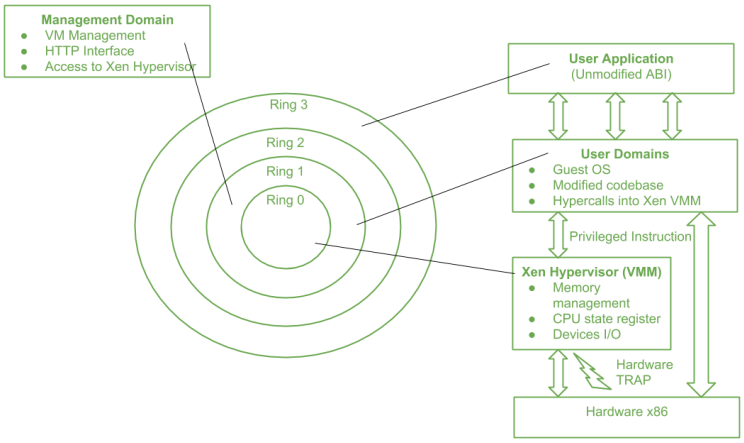


Figure -Xen Architecture and Guest OSnManagement

- Above figure describes the Xen Architecture and its mapping onto a classic x86 privilege model.
- A Xen based system is handled by Xen hypervisor, which is executed in the most privileged mode and maintains the access of guest operating system to the basic hardware.
- Guest operating system are run between domains, which represents virtual machine instances.
- In addition, particular control software, which has privileged access to the host and handles all other guest OS, runs in a special domain called Domain

0.

- This the only one loaded once the virtual machine manager has fully booted, and hosts an HTTP server that delivers requests for virtual machine creation, configuration, and termination. This component establishes the primary version of a shared virtual machine manager (VMM), which is a necessary part of Cloud computing system delivering Infrastructure-as-a-Service (IaaS) solution.

Various x86 implementation support four distinct security levels, termed as rings, i.e.,

Ring 0,

Ring 1,

Ring 2,

Ring 3

- Here, Ring 0 represents the level having most privilege and Ring 3 represents the level having least privilege.
- Almost all the frequently used Operating system, except for OS/2, uses only two levels i.e. Ring 0 for the Kernel code and Ring 3 for user application and non-privilege OS program.
- This provides a chance to the Xen to implement paravirtualization. This enables Xen to control unchanged the Application Binary Interface (ABI) thus allowing a simple shift to Xen-virtualized solutions, from an application perspective.
- Due to the structure of x86 instruction set, some instructions allow code execution in Ring 3 to switch to Ring 0 (Kernel mode).
- Such an operation is done at hardware level, and hence between a virtualized environment, it will lead to a TRAP or a silent fault, thus preventing the general operation of the guest OS as it is now running in Ring 1.
- This condition is basically occurred by a subset of system calls. To eliminate this situation, implementation in operating system requires a modification and all the sensitive system calls needs re-implementation with hypercalls.
- Here, hypercalls are the particular calls revealed by the virtual machine (VM) interface of Xen and by use of it, Xen hypervisor tends to catch the

execution of all the sensitive instructions, manage them, and return the control to the guest OS with the help of a supplied handler.

- Paravirtualization demands the OS codebase be changed, and hence all operating systems can not be referred to as guest OS in a Xen-based environment.
- This condition holds where hardware-assisted virtualization can not be free, which enables to run the hypervisor in Ring 1 and the guest OS in Ring 0.
- Hence, Xen shows some limitations in terms of legacy hardware and in terms of legacy OS.
- In fact, these are not possible to modify to be run in Ring 1 safely as their codebase is not reachable, and concurrently, the primary hardware hasn't any support to execute them in a more privileged mode than Ring 0.
- Open source OS like Linux can be simply modified as its code is openly available, and Xen delivers full support to virtualization, while components of Windows are basically not compatible with Xen, unless hardware-assisted virtualization is available.
- As new releases of OS are designed to be virtualized, the problem is getting resolved and new hardware supports x86 virtualization.

Pros:

a) Xen server is developed over open-source Xen hypervisor and it uses a combination of hardware-based virtualization and paravirtualization. This tightly coupled collaboration between the operating system and virtualized platform enables the system to develop lighter and flexible hypervisor that delivers their functionalities in an optimized manner.

b) Xen supports balancing of large workload efficiently that capture CPU, Memory, disk input-output and network input-output of data. It offers two modes to handle this workload: Performance enhancement, and For handling data density.

c) It also comes equipped with a special storage feature that we call Citrix storage link. Which allows a system administrator to uses the features of arrays from Giant companies- Hp, Netapp, Dell Equal logic etc.

d) It also supports multiple processor, Iive migration one machine to another, physical server to virtual machine or virtual server to virtual machine conversion

tools, centralized multiserver management, real time performance monitoring over window and linux.

Cons:

a) Xen is more reliable over linux rather than on window.

b) Xen relies on 3rd-party component to manage the resources like drivers, storage, backup, recovery & fault tolerance.

c) Xen deployment could be a burden some on your Linux kernel system as time passes.

d) Xen sometimes may cause increase in load on your resources by high input-output rate and and may cause starvation of other Vm's.

10. **Describe Type I & Type II hypervisor**.

ANS

- A hypervisor is a form of virtualization software used in Cloud hosting to divide and allocate the resources on various pieces of hardware.
- The program which provides partitioning, isolation, or abstraction is called a virtualization hypervisor.
- The hypervisor is a hardware virtualization technique that allows multiple guest operating systems (OS) to run on a single host system at the same time. A hypervisor is sometimes also called a virtual machine manager(VMM).

Types of 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.

- Such kinds of hypervisors are very efficient because they have direct access to the physical hardware resources(like Cpu, Memory, Network, and Physical storage).

- This causes the empowerment of the security because there is nothing any kind of the third party resource so that attacker couldn't compromise with anything.
- One problem with Type-1 hypervisors is that they usually need a dedicated separate machine to perform their operation and to instruct different VMs and control the host hardware resources.
- 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.
- An example of a Type 2 hypervisor includes VMware Player or Parallels Desktop. Hosted hypervisors are often found on endpoints like PCs.
- The type-2 hypervisor is very useful for engineers, and security analysts (for checking malware, or malicious source code and newly developed applications).

Pros & Cons of Type-2 Hypervisor:

Pros:

- Such kind of hypervisors allows quick and easy access to a guest Operating System alongside the host machine running.
- These hypervisors usually come with additional useful features for guest machines. Such tools enhance the coordination between the host machine and the guest machine.

Cons:

- Here there is no direct access to the physical hardware resources so the efficiency of these hypervisors lags in performance as compared to the type-1 hypervisors, and potential security risks are also there an attacker can compromise the security weakness if there is access to the host operating system so he can also access the guest operating system.

11. **Explain brownfield and green field deployment in cloud.**

Ans

In cloud computing, brownfield and **greenfield** deployments describe two different approaches to deploying applications or systems. Here's what each term means:

1. Greenfield Deployment

- Definition: A greenfield deployment refers to building a new system, application, or environment from scratch without any prior constraints or legacy systems.
- **Analogy**: The term "greenfield" originates from construction, where building on a fresh, undeveloped piece of land is like starting with a “green field.”
- **Characteristics**:
  - Freedom to design without legacy constraints.
  - Flexibility to use the latest technologies, architectures, and practices.
  - Easier to implement modern cloud-native strategies like microservices, containers, and serverless computing.
- **Example**: A startup creating a new e-commerce platform using the latest cloud-native technologies, without worrying about integrating or migrating older systems.

2. Brownfield Deployment

- **Definition**: A brownfield deployment involves updating or integrating with an existing system, infrastructure, or application. It deals with the challenges of working within the limitations of legacy systems.
- **Analogy**: The term “brownfield” comes from construction, where building or upgrading occurs on a site that has already been developed.
- **Characteristics**:
  - Involves working with legacy systems, which may require modernization or integration.
  - More complex due to existing dependencies, configurations, and technical debt.
  - Typically requires careful planning to avoid disruptions while integrating new solutions.
- **Example**: A company modernizing an old on-premises CRM system by migrating parts of it to the

cloud while keeping some components in their legacy environment.

Summary
- **Greenfield** = Starting fresh, building something entirely new without legacy constraints.
- **Brownfield** = Upgrading, integrating, or modernizing an existing system.

These concepts help in determining how to approach cloud deployments based on whether you're starting new or working with existing systems.

12. **Explain advantages of Server virtualization.**

- Improved server reliability and availability,
- Lower total operational cost.
- More efficient utilization of physical servers.
- More efficient utilization of power.
- Virtual machine creation: create virtual machine to customer's specifications for memory, CPU reservation, disk space and supported OS.

Server virtualization involves using software to divide a physical server into multiple virtual servers. Each virtual server can run independently with its own operating system and applications. Here are the key advantages of server virtualization:

1. **Efficient Resource Utilization**
- Virtualization allows you to maximize the use of your physical server's resources (CPU, memory, storage). Instead of one application or OS using only part of the resources, multiple virtual servers can share the same physical hardware, increasing efficiency.

2. **Cost Savings**
- By consolidating multiple virtual servers on a single physical server, you reduce the need for additional hardware. This leads to lower capital expenses (fewer servers to buy) and operational costs (less power, cooling, and maintenance).

3. **Easier Management and Flexibility**
- Virtual servers can be managed from a centralized interface, simplifying tasks like backups, updates, and monitoring. Additionally, deploying new virtual servers or scaling existing ones is faster and more flexible compared to provisioning new physical servers.

4. **Improved Disaster Recovery**
- Virtualization allows you to easily create snapshots and backups of entire virtual machines (VMs), which can be restored quickly in case of a failure. Replicating VMs to different physical locations for

disaster recovery is also straightforward.

5. **Better Testing and Development Environments**
- Virtualization provides isolated environments for testing and development without needing dedicated physical hardware. Developers can quickly create, modify, or delete virtual machines to simulate different scenarios, reducing risks to production environments.

6. **Scalability**
- Server virtualization enables easy scaling. As demand increases, new virtual machines can be deployed rapidly. If a particular VM requires more resources, adjustments can be made dynamically without physical hardware changes.

7. **Hardware Independence**
- Virtual machines are not tied to specific hardware. They can be moved between different physical servers or even different data centers with minimal downtime, providing more flexibility in managing workloads.

8. **Isolation and Security**
- Virtualization allows multiple operating systems to run on the same physical server without affecting each other. This isolation enhances security, as issues in one VM do not impact others.

9. **Legacy Application Support**
- Virtualization enables you to run older applications on modern hardware without the need for old, outdated physical servers. Legacy systems can be maintained while still benefiting from newer infrastructure.

Summary
Server virtualization provides a wide range of benefits, including cost efficiency, easier management, better resource utilization, scalability, and enhanced disaster recovery. These advantages make virtualization a key technology in modern IT infrastructure and cloud environments.

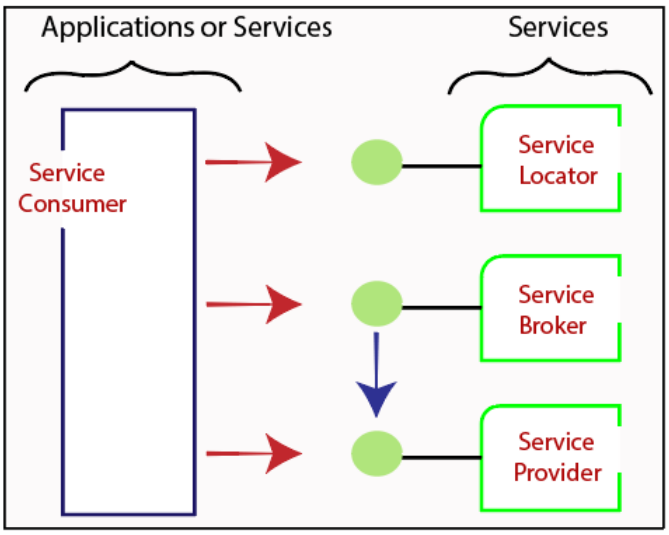
13. State and Explain SOA in cloud computing

ANS

- 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.

service-Oriented Terminologies

Let's see some important service-oriented terminologies:



- **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.

14 Describe SLA in cloud Computing

- A Service Level Agreement (SLA) is the bond for the performance of the negotiation between a cloud service provider and a client. Earlier, in cloud computing,
- all service level agreements were negotiated between a customer and a service consumer.
- With the introduction of large utilities such as cloud computing providers, most service level agreements are standardized until a customer becomes a large consumer of cloud services.
- Service level agreements are also defined at different levels, which are mentioned below:
- Customer-based SLA
- Service-based SLA
- Multilevel SLA

❖ Some service level agreements are enforceable as contracts, but most are agreements or contracts that are more in line with an operating level agreement (OLA) and may not be constrained by law.
❖ It's okay to have a lawyer review documents before making any major settlement with a cloud service provider.
❖ Service level agreements usually specify certain parameters, which are mentioned below:

- Availability of the Service (uptime)
- Latency or the response time
- Service components reliability
- Each party accountability
- Warranties

- If a cloud service provider fails to meet the specified targets of the minimum, the provider will have to pay a penalty to the cloud service consumer as per the agreement.
- So, service level agreements are like insurance policies in which the corporation has to pay as per the agreement if an accident occurs.

The importance of a cloud SLA

- Service-level agreements are fundamental as more organizations rely on external providers for critical systems, applications and data.
- Cloud SLAs ensure that cloud providers meet certain enterprise-level requirements and provide customers with a clearly defined set of deliverables.
- It also describes financial penalties, such as credit for service time, if the provider fails to meet guaranteed conditions.
- The role of a cloud SLA is essentially the same as that of any contract -- it's a blueprint that governs the relationship between a customer and a provider.
- These agreed terms form a reliable foundation upon which the Customer commits to use the cloud providers' services.
- They also reflect the provider's commitments to quality of service (QoS) and the underlying infrastructure.

15.Explain kernel based virtual machine with diagram.

- kernel-based Virtual Machine (KVM) is an open source virtualization technology built into Linux®. Specifically, KVM lets you turn Linux into a hypervisor that allows a host machine to run multiple, isolated

virtual environments called guests or virtual machines (VMs).

- Kernel-based Virtual Machine (KVM) is a software feature that you can install on physical Linux machines to create virtual machines.
- A virtual machine is a software application that acts as an independent computer within another physical computer.
- It shares resources like CPU cycles, network bandwidth, and memory with the physical machine. KVM is a Linux operating system component that provides native support for virtual machines on Linux. It has been available in Linux distributions since 2007.
- Kernel-based Virtual Machine (KVM) can turn any Linux machine into a bare-metal hypervisor.
- This allows developers to scale computing infrastructure for different operating systems without investing in new hardware.
- KVM frees server administrators from manually provisioning virtualization infrastructure and allows large numbers of virtual machines to be deployed easily in cloud environments.

How does KVM work?

- Kernel-based Virtual Machine (KVM) requires a Linux kernel installation on a computer powered by a CPU that supports virtualization extensions. Specifically, KVM supports all x86 CPUs, a family of computer chips capable of processing the Intel x86 instruction language.

Linux kernel

- Linux kernel is the core of the open-source operating system.

- A kernel is a low-level program that interacts with computer hardware. It also ensures that software applications running on the operating

system receive the required computing resources.

- Linux distributions, such as Red Hat Enterprise Linux, Fedora, and Ubuntu, pack the Linux kernel and additional programs into a user-friendly commercial operating system.

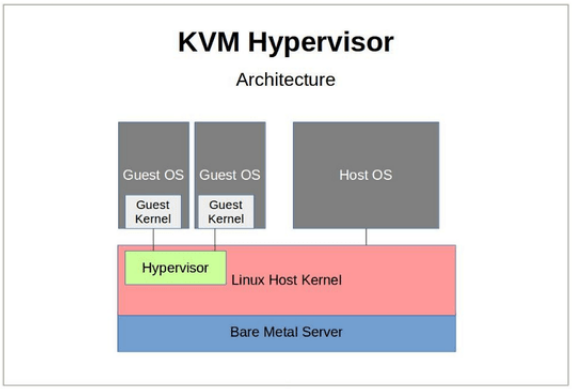
How to enable KVM

Once you have installed the Linux kernel, you need to install the following additional software components on the Linux machine:

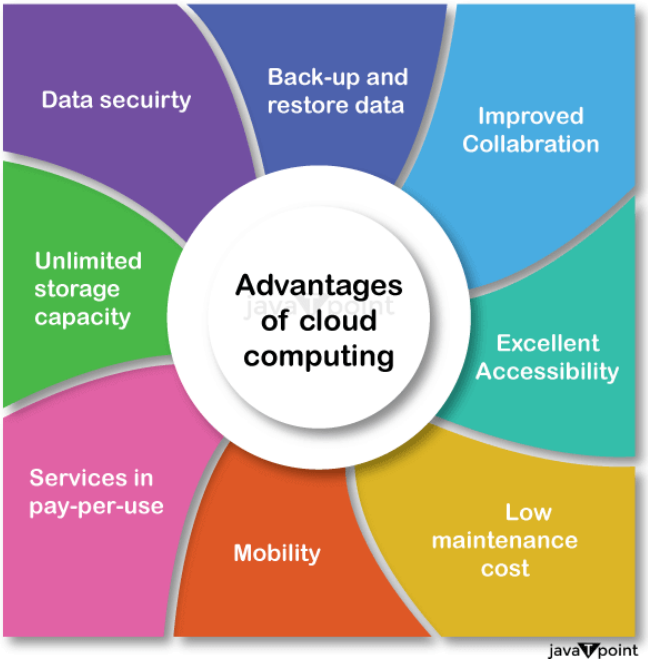
- A host kernel module
- A processor-specific module
- An emulator
- A range of other Linux packages for expanding KVM's capabilities and performance

Once loaded, the server administrator creates a virtual machine via the command line tool or graphical user interface.

KVM then launches the virtual machine as an individual Linux process. The hypervisor allocates every virtual machine with virtual memory, storage, network, CPU, and resources.



16 .Describe advantages and disadvantages of cloud computingng ?



Let's explore the advantages that cloud computing has to offer:

Data Backup and Restoration:

Cloud computing offers a quick and easy method for data backup and restoration. Businesses may simply access and restore their data in the event of any data loss or system failure by keeping it in the cloud.

Improved Collaboration:

Collaboration is improved because cloud technologies make it possible for teams to share information easily. Multiple users may work together on documents, projects, and data thanks to shared storage in the cloud, enhancing productivity and teamwork.

Excellent Accessibility:

Access to information stored in the cloud is made possible. Users can access their data from anywhere in the world with an internet connection, making remote work, flexibility, and effective operations possible.

Cost-effective Maintenance:

Organizations using cloud computing can save money on both hardware and software upkeep. Because cloud

service providers manage the maintenance and updates, businesses no longer need to make costly infrastructure investments or set aside resources for continuous maintenance.

Upkeep and Updates:

Cloud service providers take care of infrastructure upkeep, security patches, and updates, freeing organizations from having to handle these duties themselves.

This frees up IT teams' time and resources to work on higher-value projects like application development, data analysis, or strategic initiatives rather than wasting them on rote upkeep and updates.

Mobility:

Cloud computing makes it simple for mobile devices to access data. Utilizing smartphones and tablets, users can easily access and control their cloud-based applications and data, increasing their mobility and productivity.

Pay-per-use Model:

Cloud computing uses a pay-per-use business model that enables companies to only pay for the services they really utilize. This method is affordable, eliminates the need for up-front investments, and offers budget management flexibility for IT.

Scalable Storage Capacity:

Businesses can virtually store and manage a limitless amount of data in the cloud. The cloud offers a scalable and centralized storage option for all types of data, including documents, photos, audio, video, and other kinds of files.

nhanced Data Security:

Cloud computing places a high focus on data security. To guarantee that data is handled and stored safely, cloud service providers offer cutting-edge security features like encryption, access limits, and regular

security audits. Businesses can rest easy knowing that their important data is secure.

Disaster Recovery and Business Continuity:

Cloud computing provides reliable options for these two issues. Businesses can quickly bounce back from any unforeseen disasters or disruptions thanks to data redundancy, backup systems, and geographically dispersed data centers.

Agility and Innovation:

Businesses can continue to be innovative and nimble thanks to cloud computing. Organizations may quickly embrace new solutions, test out emerging trends, and promote corporate growth with access to a variety of cloud-based tools, services, and technology.

Green Computing:

By maximizing the use of computer resources, lowering energy use, and minimizing e-waste, cloud computing may support environmental sustainability.

By utilizing technologies like virtualization and load balancing to maximize the use of computer resources, cloud providers can operate large-scale data centers built for energy efficiency, resulting in lower energy usage and a smaller carbon footprint.

These benefits of cloud computing give companies the ability to use cutting-edge technology offered by cloud service providers while maximizing productivity, cost savings, scalability, and data security. They also enable them to concentrate on their core capabilities.

Disadvantages of Cloud Computing

When we talk about the "disadvantages of cloud computing," we're talking about any potential drawbacks or difficulties that businesses might have when utilizing cloud computing services. These drawbacks draw attention to some restrictions or risks related to cloud computing that businesses should take into account before making a choice.

Some of the Disadvantages of Cloud Computing are as follows:

- **Vendor Reliability and Downtime:**

Because of technological difficulties, maintenance needs, or even cyberattacks, cloud service providers can face outages or downtime. Users may not be able to access their data or applications during these times, which can interfere with business operations and productivity.

- **Internet Dependency:**

A dependable and fast internet connection is essential for cloud computing. Business operations may be delayed or interrupted if there are connectivity problems or interruptions in the internet service that affect access to cloud services and data.

- **Limited Control and Customization:**

Using standardized services and platforms offered by the cloud service provider is a common part of cloud computing. As a result, organizations may have less ability to customize and control their infrastructure, applications, and security measures. It may be difficult for some organizations to modify cloud services to precisely match their needs if they have special requirements or compliance requirements.

- **Data Security and Concerns about Privacy:**

Concerns about data security and privacy arise when sensitive data is stored on the cloud. Businesses must have faith in the cloud service provider's security procedures, data encryption, access controls, and regulatory compliance. Unauthorized access to data or data breaches can have serious repercussions, including financial loss, reputational harm, and legal obligations.

- **Hidden Costs and Pricing Models:**

Although pay-as-you-go models and lower upfront costs make cloud computing more affordable, businesses should be wary of hidden charges. Data transfer fees, additional storage costs, fees for specialized support or

technical assistance, and expenses related to regulatory compliance are a few examples.

- **Dependency on Service Provider:**

When an organization depends on a cloud service provider, it is dependent on that provider's dependability, financial security, and longevity. Users may have disruptions and difficulties switching to alternate options if the provider runs into financial difficulties, changes their pricing policy, or even closes down their services.

- **Data Location and Compliance:**

When data is stored in the cloud, it frequently sits in numerous data centers around the globe that may be governed by multiple legal systems and data protection laws. This may pose compliance issues, especially if some sectors of the economy or nations have stringent data sovereignty laws.

Organizations should carry out a comprehensive risk assessment, thoroughly examine the dependability and security procedures of possible cloud service providers, and build backup and disaster recovery strategies to counteract these drawbacks.

17.**Explain Cloud computing Services?**

- Cloud Computing can be defined as the practice of using a network of remote servers hosted on the Internet to store, manage, and process data, rather than a local server or a personal computer.
- Companies offering such kinds of cloud computing services are called *cloud providers* and typically charge for cloud computing services based on usage.
- Grids and clusters are the foundations for cloud computing.
- Types of Cloud Computing

Most cloud computing services fall into five broad categories:

- Software as a service (SaaS)

- Platform as a service (PaaS)
- Infrastructure as a service (IaaS)
- Anything/Everything as a service (XaaS)
- Function as a Service (FaaS)

- These are sometimes called the because they are built on top of one another
- . Knowing what they are and how they are different, makes it easier to accomplish your goals.
- These abstraction layers can also be viewed as a where services of a higher layer can be composed of services of the underlying layer i.e, SaaS can provide Infrastructure.

Software as a Service(SaaS)

Software-as-a-Service (SaaS)

- is a way of delivering services and applications over the Internet. Instead of installing and maintaining software, we simply access it via the Internet, freeing ourselves from the complex software and hardware management.
- It removes the need to install and run applications on our own computers or in the data centers eliminating the expenses of hardware as well as software maintenance.
- SaaS provides a complete software solution that you purchase on a basis from a cloud service provider. Most SaaS applications can be run directly from a web browser without any downloads or installations required. The SaaS applications are sometimes called Pay only for what you use.
- Users can run most SaaS apps directly from their web browser without needing to download and install any software. This reduces the time spent in installation and configuration and can reduce the issues that can get in the way of the software deployment.
- We can Access app data from anywhere.

Rather than purchasing new software, customers rely on a SaaS provider to automatically perform the updates.

- It allows the users to access the services and features on-demand.
- The various companies providing *Software as a service* are Cloud9 Analytics, Salesforce.com, Cloud Switch, Microsoft Office 365, Big Commerce, Eloqua, dropBox, and Cloud Tran.

- : SaaS solutions are typically not as customizable as on-premises software, meaning that users may have to work within the constraints of the SaaS provider's platform and may not be able to tailor the software to their specific needs
- : SaaS solutions are typically cloud-based, which means that they require a stable internet connection to function properly. This can be problematic for users in areas with poor connectivity or for those who need to access the software in offline environments.
- SaaS providers are responsible for maintaining the security of the data stored on their servers, but there is still a risk of data breaches or other security incidents.
- SaaS providers may have access to a user's data, which can be a concern for organizations that need to maintain strict control over their data for regulatory or other reasons.

Platform as a Service

- PaaS is a category of cloud computing that provides a platform and environment to allow developers to build applications and services over the internet.
- PaaS services are hosted in the cloud and accessed by users simply via their web browser.
- A PaaS provider hosts the hardware and software on its own infrastructure.
- As a result, PaaS frees users from having to install in-house hardware and software to develop or run a new application.
- Thus, the development and deployment of the application take place
- The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment.
- To make it simple, take the example of an annual day function, you will have two options either to create a venue or to rent a venue but the function is the same.

It provides much of the infrastructure and other IT services, which users can access anywhere via a web browser.

It charges for the services provided on a per-use basis thus eliminating the expenses one may

have for on-premises hardware and software.

It is designed to support the complete web application lifecycle: building, testing, deploying, managing, and updating.

It allows for higher-level programming with reduced complexity thus, the overall development of the application can be more effective.

The various companies providing *Platform as a service* are Amazon Web services Elastic Beanstalk, Salesforce, Windows Azure, Google App Engine, cloud Bees and IBM smart cloud.

PaaS providers typically manage the underlying infrastructure and take care of maintenance and updates, but this can also mean that users have less control over the environment and may not be able to make certain customizations.

: Users are dependent on the PaaS provider for the availability, scalability, and reliability of the platform, which can be a risk if the provider experiences outages or other issues.

PaaS solutions may not be able to accommodate certain types of workloads or applications, which can limit the value of the solution for certain organizations.

Infrastructure as a Service

Infrastructure as a service (IaaS) is a service model that delivers computer infrastructure on an outsourced basis to support various operations. Typically IaaS is a service where infrastructure is provided as outsourcing to enterprises such as networking equipment, devices, database, and web servers.

It is also known as

IaaS customers pay on a per-user basis, typically by the hour, week, or month. Some providers also charge customers based on the amount of virtual machine space they use.

It simply provides the underlying operating systems, security, networking, and servers for developing such applications, and services, and deploying development tools, databases, etc.

Eliminates capital expense and reduces ongoing cost and IaaS customers pay on a per-user basis, typically by the hour, week, or month.

Running websites using IaaS can be less expensive than traditional web hosting.

The IaaS Cloud Provider may provide better security than your existing software.

There is no need to manage the underlying data center or the introduction of new releases of the development or underlying software. This is all handled by the IaaS Cloud Provider.
The various companies providing *Infrastructure as a service* are Amazon web services, Bluestack, IBM, Openstack, Rackspace, and Vmware.

IaaS providers typically manage the underlying infrastructure and take care of maintenance and updates, but this can also mean that users have less control over the environment and may not be able to make certain customizations.

: Users are responsible for securing their own data and applications, which can be a significant undertaking.

Cloud computing may not be accessible in certain regions and countries due to legal policies.

Anything as a Service

It is also known as Everything as a Service. Most of the cloud service providers nowadays offer anything as a service that is a compilation of all of the above services including some additional services.

XaaS solutions can be easily scaled up or down to meet the changing needs of an organization.

XaaS solutions can be used to provide a wide range of services, such as storage, databases, networking, and software, which can be customized to meet the specific needs of an organization.

: XaaS solutions can be more cost-effective than traditional on-premises solutions, as organizations only pay for the services.

Users are dependent on the XaaS provider for the availability, scalability, and reliability of the service, which can be a risk if the provider experiences outages or other issues.

: XaaS solutions may not be able to accommodate certain types of workloads or applications, which can limit the value of the solution for certain organizations.

XaaS solutions may not be able to integrate with existing systems and data sources,

which can limit the value of the solution for certain organizations.

FaaS is a type of cloud computing service. It provides a platform for its users or customers to develop, compute, run and deploy the code or entire application as functions. It allows the user to entirely develop the code and update it at any time without worrying about the maintenance of the underlying infrastructure. The developed code can be executed with response to the specific event. It is also .
FaaS is an event-driven execution model. It is implemented in the serverless container. When the application is developed completely, the user will now trigger the event to execute the code. Now, the triggered event makes response and activates the servers to execute it. The servers are nothing but the Linux servers or any other servers which is managed by the vendor completely. Customer does not have clue about any servers which is why they do not need to maintain the server hence it is
Both PaaS and FaaS are providing the same functionality but there is still some differentiation in terms of Scalability and Cost.
FaaS, provides auto-scaling up and scaling down depending upon the demand. PaaS also provides scalability but here users have to configure the scaling parameter depending upon the demand.
In FaaS, users only have to pay for the number of execution time happened. In PaaS, users have to pay for the amount based on pay-as-you-go price regardless of how much or less they use.

Auto scaling is done by the provider depending upon the demand.
Pay only for the number of events executed.
FaaS allows the users to upload the entire application all at once. It allows you to write code for independent functions or similar to those functions.
Maintenance of code is enough and no need to worry about the servers.
Functions can be written in any programming language.
Less control over the system.
The various companies providing Function as a Service are Amazon Web Services – Firecracker, Google –

Kubernetes, Oracle – Fn, Apache OpenWhisk – IBM, OpenFaaS,

: Since FaaS functions are event-triggered, the first request to a new function may experience increased latency as the function container is created and initialized.

FaaS providers typically manage the underlying infrastructure and take care of maintenance and updates, but this can also mean that users have less control over the environment and may not be able to make certain customizations.

Users are responsible for securing their own data and applications, which can be a significant undertaking.

: FaaS functions may not be able to handle high traffic or large number of requests.

18. **Explain various challenges for virtualizations.**

ANS

Bad storage, server, and network configurations are just a few reasons why virtualization fails. These are technical in nature and are often easy to fix, but some organizations overlook the need to protect their entire virtualized environments, thinking that they're inherently more secure than traditional IT environments. Others use the same tools they use to protect their existing physical infrastructure. The bottom line is that a virtualized environment is more complex and requires a new management approach. These are the common problems talked about behind closed doors.

1. Resource distribution

The way virtualization partitions systems can result in varied ways — some might function really well, and others might not provide users access to enough resources to meet their needs. Resource distribution problems often occur in the shift to virtualization and can be fixed by working on capacity planning with your service provider.

2. VM Sprawl

VM sprawl, the unchecked growth of virtual machines in a virtual environment, as any virtualization admin knows, can cripple an otherwise healthy environment. It is problematic because its underlying cause often stays hidden until it manifests in resource shortages.

You should look at how virtual machines will be managed, who will be doing what, and what systems you're going to use. One of the optimal times to develop an overall management plan is when you're in a testing phase, before migration.

3. Backward compatibility

Using legacy systems can cause problems with newer virtualized software programs. Compatibility issues can be time-consuming and difficult to solve. A good provider may be able to suggest upgrades and workarounds to ensure that everything functions the way they should.

4. Performance monitoring
Virtualized systems don’t lend themselves to the same kind of performance monitoring as hardware like mainframes and hardware drives do. Try tools like VMmark to create benchmarks that measure performance on virtual networks and to monitor resource usage as well.

5. Backup
In a virtualized environment, there is no actual hard drive on which data and systems can be backed up. This means frequent software updates can make it difficult to access backup at times. Software programs like Windows Server Backup tools can make this process easier and allow backups to be stored in one place for easier tracking and access.

6. Security
Virtual systems could be vulnerable when users don’t keep them secure and apply best practices for passwords or downloads. Security then becomes a problem for virtualization, but the isolation of each VM by the system can mitigate security risks and prevent systems from getting breached or compromised.

Unlike some tech solutions, virtualization is not really a “set it and forget it” type of solution. You will need to manage it from the start if you want to be able to get the most out of your systems. This includes ensuring resources are being allocated properly, machines are created and shut down properly, apps and systems are updated, and more.

While virtualized solutions do require less management than their physical counterparts, they still require some management and you will need people to help you do that. One of the best solutions is to work with an IT partner like us who can help manage your systems and ensure that they are working efficiently.
In fact, we offer a wide variety of virtualization solutions. We can take on your virtualization initiatives so that you can focus on running your business. If you would like to learn more, contact us today to see how we can help.

19. **Describe virtualization security requirement.**

ANS

Virtualization introduces several security requirements to ensure that virtual environments remain secure. Here’s a summary of the key virtualization security requirements:

1. **Isolation Between Virtual Machines (VMs)**
- Each virtual machine should be isolated from others to prevent one VM from accessing or interfering with another. This is critical for multi-tenant environments, where different users or departments share the same physical infrastructure.

2. **Secure Hypervisor**
- The hypervisor (also known as the Virtual Machine Monitor or VMM) is the software layer that manages multiple VMs on a single physical server. Securing the hypervisor is crucial since a compromised hypervisor could lead to complete control over all hosted VMs.

3. **Access Control and Authentication**
- Implement strong access controls to restrict who can manage, create, and delete virtual machines. Use multi-factor authentication (MFA) and role-based access control (RBAC) to minimize unauthorized access to the virtualization infrastructure.

4. **Network Security**
- Virtualized environments require robust network security measures, such as firewalls, intrusion detection systems (IDS), and secure virtual networking. Ensure that each VM’s network traffic is monitored and protected, just like in a traditional physical network.

5. **Data Protection and Encryption**

- Protect data at rest and in transit within the virtual environment by implementing encryption. This includes securing virtual disk files, VM snapshots, and VM data transfers between hosts.

6. **Patch Management**
- Regularly update and patch hypervisors, virtual machine images, and virtualization management tools to address security vulnerabilities. Unpatched systems are a common entry point for attackers.

7. **Virtual Machine Lifecycle Management**
- Secure the entire lifecycle of a virtual machine, from creation to decommissioning. This includes securely wiping or destroying VM data when a VM is no longer needed to prevent data leakage.

8. **Monitoring and Logging**
- Implement continuous monitoring and logging of all activities within the virtual environment. This helps in detecting suspicious activities, tracking changes, and responding to incidents quickly.

9. **Backup and Disaster Recovery**
- Securely back up virtual machines and ensure that backups are encrypted and protected. In the event of a disaster, having a recovery plan in place for restoring virtual environments is crucial.

10. **Security for Management Interfaces**
- The interfaces used to manage virtualization infrastructure (like dashboards and APIs) should be secured using strong encryption (e.g., HTTPS) and restricted access. Exposing these interfaces to the internet without adequate security can lead to serious breaches.

11. **Segmentation and Zoning**
- Use network segmentation to separate VMs based on their function, sensitivity, or level of

trust. For example, separating production and test environments reduces the risk of unauthorized access or cross-contamination.

12. **Compliance and Regulatory Requirements**
- Ensure that the virtualization environment complies with industry-specific regulations like GDPR, HIPAA, or PCI-DSS. Virtual environments must meet the same security standards as traditional physical environments.

13. **Inter-VM Communication Security**
- Implement security controls to monitor and secure communication between VMs. This includes securing virtual network traffic, controlling VM-to-VM traffic, and ensuring no unauthorized access occurs between VMs.

14. **Incident Response and Forensics**
- Develop an incident response plan specifically for virtual environments. This should include procedures for investigating, containing, and recovering from security breaches in virtualized infrastructures.

15. **Resource Quotas and Limits**
- Control resource allocation to prevent resource exhaustion attacks. By setting quotas and limits for CPU, memory, and disk usage, you can avoid scenarios where one VM consumes excessive resources and affects others.

Summary
Virtualization security is about protecting the hypervisor, ensuring VM isolation, securing management interfaces, and addressing network and data protection. By implementing these security requirements, organizations can minimize risks and maintain a secure virtual environment.

20. **Differentiate VMware and Virtual Box hypervisor.**

ANS

Features	Virtualbox	VMware
Definition	VIt is a free and open-source hosted hypervisor that is designed and developed by Oracle Corporation.	It is an organization that offers different software and applications for virtualization.
Usage	VIt is mainly utilized for academic and private purposes.	It is mainly utilized for business and home purposes.
Interfaces	VIt offers a user-friendly interface.	It offers a complicated user interface.
Hypervisor	VIt is a Type 2 Hypervisor.	It is a Type 1 Hypervisor.
3D acceleration	VIt needs to be enabled manually.	It is enabled by default in Virtualbox.
Ease of Access	VIt doesn't allow ease of access.	It allows ease of access.
Disk formats	VIt allows support for VDI, VMDK, VHD, and HDD disk formats.	It allows support for VMDK disk format.
Shared Storage	VIt provides shared storage support with CIFS, NFS, and iSCSI.	It doesn't provide any shared storage support.

Virtual Machine Encryption	VVirtualbox provides it with an extension pack.	VMware provides limited Virtual Machine encryption.
Levels	VIt provides virtualization at both hardware and software levels.	It provides virtualization at the only hardware level.
Cost and Licenses	VIt is free under GNU General Public License.	VMware Workstation Player is free, whereas some other VMware products need a paid license.
Snapshots	VVirtualBox provides snapshots, which implies it can save and restore a virtual machine's state.	Snapshots are only available in premium virtualization products and not with VMware Workstation Player.
Video Memory	Video memory is limited to 128MB in Virtualbox.	Video memory is restricted to 2GB in VMware.