Work Integrated Learning Programmes

M.Tech Software Engineering

Cloud Computing - Assignment 1

Submitted By

Pavithra.S

2022MT93172

TABLE OF CONTENTS

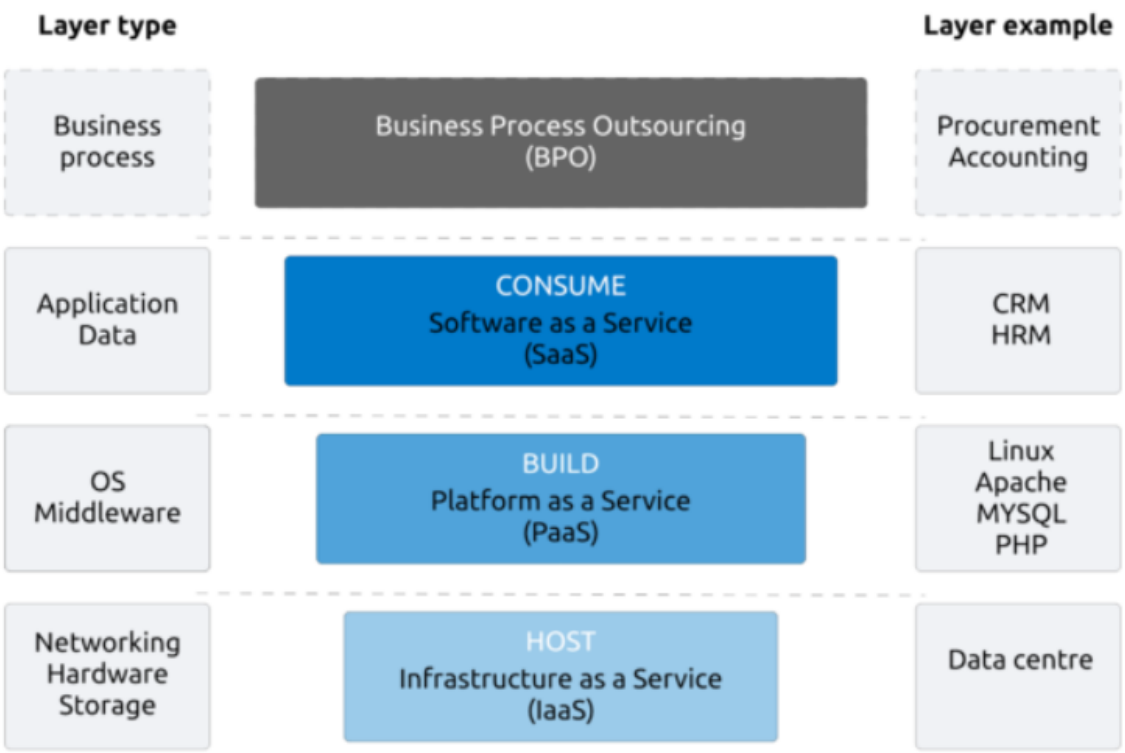
Question 1: Which are the different layers that define cloud architecture?

Answer:

Cloud architecture is the way technology components combine to build a cloud, in which resources are pooled through virtualization technology and shared across a network.

The different layers that define a cloud architecture are,

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



Business Process Outsourcing (BPO) refers to the process in which a company outsources standard business functions to a third-party provider. This is often done to save time and money on removing that in-house administrative task. Since BPO is not a technology like the other cloud layers, there is an ongoing debate whether BPO should be regarded as a cloud layer at all. We believe that it should since it deals with vendor services, just like the other layers do.

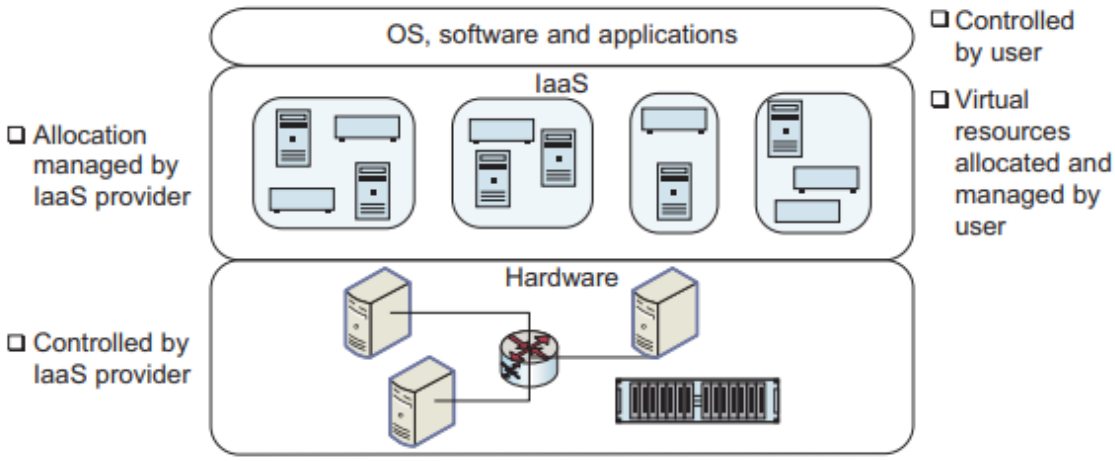
Infrastructure as a Service (Iaas)

The basic layer of cloud is the infrastructure –IaaS (Infrastructure as a service). This layer is basically hardware and network. The IaaS model is about providing compute and storage resources as a service. What distinguishes this from a regular server or hosting company are mainly two things:

- Scalability
- Virtualization

According to NIST, IaaS is defined as follows:

> The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, deployed applications, and possibly limited control of select networking components (e.g., host firewalls).



The user of IaaS has single ownership of the hardware infrastructure allotted to him (may be a virtual machine) and can use it as if it is his own machine on a remote network and he has control over the operating system and software on it.

The IaaS provider has control over the actual hardware and the cloud user can request allocation of virtual resources, which are then allocated by the IaaS provider on the hardware (generally without any manual intervention).

Therefore, IaaS is well suited for users who want complete control over the software stack that they run. For example, the user may be using heterogeneous software platforms from different vendors, and they may not like to switch to a PaaS platform where only selected middleware is available.

Well-known IaaS platforms includes,

- Amazon EC2
- Rackspace
- Rightscale.

Additionally, traditional vendors such as HP, IBM and Microsoft offer solutions that can be used to build private IaaS.

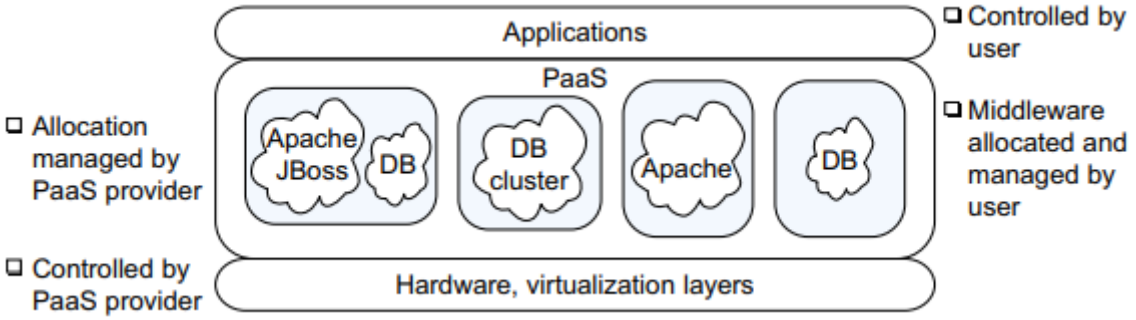
Platform as a Service (PaaS)

The second layer of the cloud is the platform – the PaaS (Platform as a service). The platform layer provides resources to actually build applications. In combination with IaaS, PaaS provides the ability to develop, test, run, and host applications.

The platform layer opens up for third parties to add their software (or integrations) to a cloud service. An example of a well-known PaaS is Microsoft Azure. This platform provides developers with swift access to a full development and deployment environment and even let you host the application you are building.

NIST defines PaaS as follows:

> The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages and tools supported by the provider. 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 application hosting environment configurations.



The hardware, as well as any mapping of hardware to virtual resources, such as virtual servers, is controlled by the PaaS provider. Additionally, the PaaS provider supports selected middleware, such as a database, web application server, etc. The cloud user can configure and build on top of this middleware, such as define a new database table in a database.

PaaS platforms are well suited to those cloud users who find that the middleware they are using matches the middleware provided by one of the PaaS vendors. This enables them to focus on the application.

Some well-known PaaS platforms are,

- Windows Azure
- Google App Engine
- Hadoop

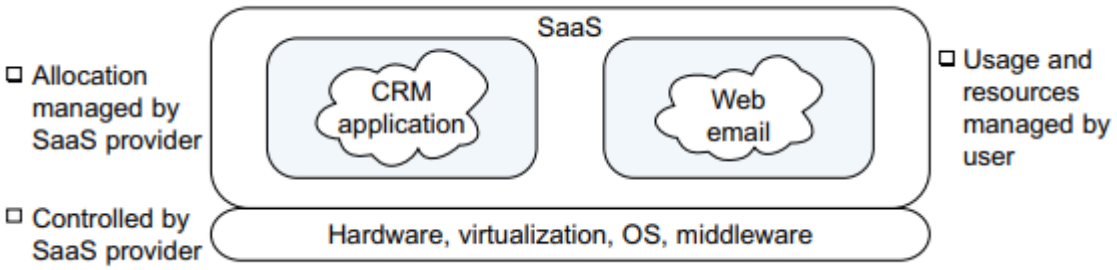
As in the case of IaaS, traditional vendors such as HP, IBM and Microsoft offer solutions that can be used to build private PaaS.

Software as a Service (SaaS)

The third cloud layer is the actual Software – the SaaS (Software as a service). Software as a Service SaaS is about providing the complete application as a service. The SaaS layer must be web-based and hence accessible from everywhere and preferably on any device.

SaaS has been defined by NIST as follows:

> The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through a thin client interface such as a web browser (e.g., web-based email). The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.



The SaaS provider controls all the layers apart from the application. Users who log in to the SaaS service can both use the application as well as configure the application for their use.

For example, users can use Salesforce.com to store their customer data. They can also configure the application, for example, requesting additional space for storage or adding additional fields to the customer data that is already being used. When configuration settings are changed, the SaaS infrastructure performs any management tasks needed (such as allocation of additional storage) to support the changed configuration.

Prominent SaaS applications include Salesforce.com for CRM, Google Docs for document sharing, and web email systems like Gmail, Hotmail, and Yahoo! Mail. IT vendors such as HP and IBM also sell systems that can be configured to set up SaaS in a private cloud.

Question 2: What are the security aspects provided with the cloud?

Answer:

Security is one of the major aspects which come with any application and service used by the user. Companies or organizations remain much more concerned with the security provided with the cloud.

Cloud infrastructure in itself is a secured infrastructure, because of the network being connected with several servers, providing back up to each other. However, there are certain areas of concern for the Cloud users. Some of the data of the users are stored in the environment of the Cloud vendor. This data may not comply with the security norms and with the policies, pertaining to security. This makes this data vulnerable to various lapses or to unwarranted attacks.

There is always the risk of having a virus in the environment of the Cloud vendor. This makes all users exposed to the attacks, made by hackers. The other risk factors include issues such as leakage of data or loss of data. This is very damaging to the reputation of the business organization clients. It may also put the business organization to huge financial loss.

Cloud is adopting certain security measures to counteract these threats to the security of client's data.

These security measures are:

-- Every user must be completely isolated from each other. This is possible through use of technology of virtualization with use of firewalls. The methods to detect intrusions and methods for prevention also help in this.

-- The process of data communication between the provider of Cloud service and the user must be kept absolutely secured. This is done through use of Virtual Private Network or VPN.

-- The users of Cloud computing have to use a process of authentication to authenticate their identities. This process of authentication of the user's identity only will allow to get an access to the data of the organization, that is stored on the Cloud. This authentication of identity service is a federated service. This service provides integration of identity management of a business organization and the provider of the Cloud service.

-- The security policies of the Cloud service provide is a very important subject. It is always best for the user to first go through the security policies of the Cloud service provider thoroughly.

-- Cloud computing provides features such as On Demand availability of computing resources. It also provides pooling of resources, fast elasticity and access to data through internet service. All these features are very important and beneficial for the business organization clients.

Security Requirements and Best Practices

The security requirements and best practices for cloud can be divided into the requirements for,

- Physical Security
- Virtual Security

Physical Security

Physical security implies that the data center the cloud is hosted in should be secure against physical threats. This includes not only attempts at penetration by intruders, but also protection against natural hazards and disasters such as floods, and human error such as switching off the air conditioning.

To ensure physical security, a multi-layered system is required.

This includes:

i. A central monitoring and control center with dedicated staff.
ii. Monitoring for each possible physical threat, such as intrusion, or natural hazards such as floods.
iii. Training of the staff in response to threat situations.
iv. Manual or automated back-up systems to help contain threats (e.g., pumps to help contain the damage from floods).
v. Secure access to the facility. This requires that the various threats to the data.
vi. center be identified, and appropriate procedures derived for handling these threats.

Virtual Security

The following best practices have been found to be very useful in ensuring cloud security.

1. Cloud Time Service

If all systems in the datacenter are synchronized to the same clock, this is helpful both to ensure correct operation of the systems, as well as to facilitate later analysis of system logs. It is particularly important in correlating events occurring across geographically distributed systems. A common way to do this is by use of the Network Time Protocol (NTP). NTP is a protocol that synchronizes the clock on a computer to a reference source on the Internet.

2. Identity Management

Identity management is a foundation for achieving confidentiality, integrity and availability.

Some of the requirements for identity management are that:

i. It should scale to the number of users typically found in a cloud system.

ii. Due to possible heterogeneity in cloud systems, a federated identity management system that allows establishing a single identity and single sign-on across multiple different types of systems may be needed.
iii. The identity management system should satisfy applicable legal and policy requirements (for example, allow deleting of users across the system within a specified time period).
iv. Maintain historical records for possible future investigation.

3. Access Management

The core function of access management is to allow accesses to cloud facilities only to authorized users.

Additional requirements are to:

i. Not allow unrestricted access to cloud management personnel.
ii. Allow implementation of multi-factor authentication (e.g., use of a password together with a digital key) for very sensitive operations.

It is also good practice to:

i. Disallow shared accounts, such as admin.
ii. Implement white-listing of IP addresses for remote administrative actions.

4. Break-Glass Procedures

It is desirable for the access management system to allow alarmed break-glass procedures, which bypass normal security controls in emergency situations. The analogy is with breaking the glass to set off a fire alarm. Clearly, it is important to ensure that the break-glass procedure can be executed only in emergencies under controlled situations, and that the procedure triggers an alarm.

5. Key Management

In a cloud, with shared storage, encryption is a key technology to ensure isolation of access. The cloud infrastructure needs to provide secure facilities for the generation, assignment, revocation, and archiving of keys. It is also necessary to generate procedures for recovering from compromised keys.

6. Auditing

Auditing is needed for all system and network components. The audit should capture all security-related events, together with data needed to analyze the event such as the time, system on which the event occurred, and user id that initiated the event. The audit log should be centrally maintained and secure. It should be possible to sanitize or produce a stripped-down version of the audit log for sharing with cloud customers, in case their assistance is needed to analyze the logs.

7. Security Monitoring

This includes an infrastructure to generate alerts when a critical security event has occurred, including a cloud-wide intrusion and anomaly detection system. The intrusion detection systems may be installed both on the network as well as the host nodes. It may also be necessary to allow cloud users to implement their own intrusion and anomaly detection systems.

8. Security Testing

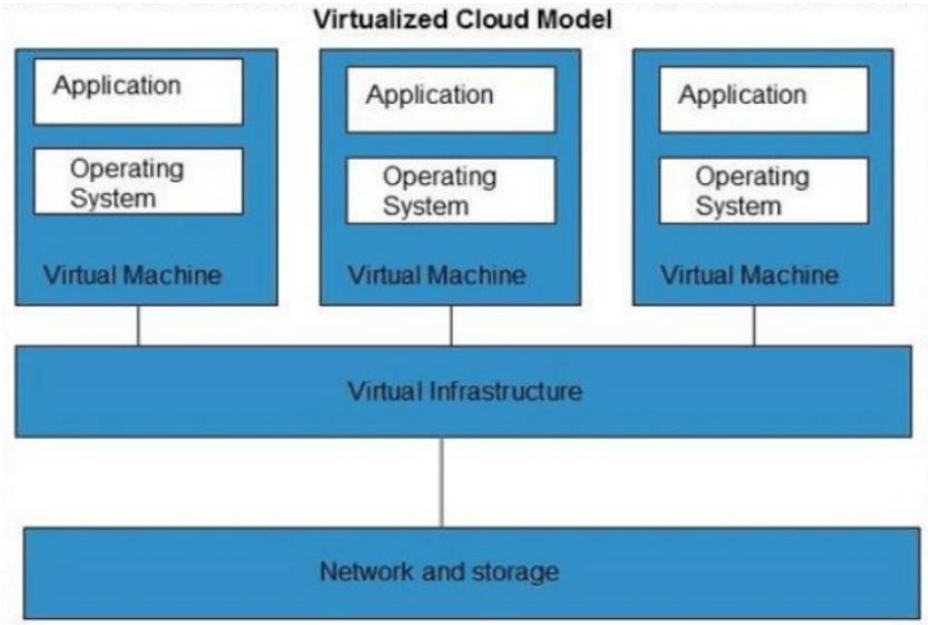
It is important to test all software for security before deployment in an isolated test bed. Patches to software should also be tested in this environment before being released into production. Additionally, security testing should be carried out on an ongoing basis to identify vulnerabilities in the cloud system. Depending upon the risk assessment, some of these tests may be carried out by third parties. There should also be a remediation process to fix identified vulnerabilities.

Question 3: What is the requirement of virtualization platform in implementing cloud?

Answer:

Virtualization is the simulation of the software and/or hardware upon which other software runs. This simulated environment is called virtual machine (VM). Each VM can run its own operating systems and applications as if it were in a physical machine.

The basic cloud infrastructure is empowered by virtualization.



Key aspects achieved through virtualization are as follows:

1. It enables the delivery of intricate cloud services that can be easily scaled in a cost-effective manner. The cloud computing users can run virtual machines without investing and maintain the hardware, bandwidth and other data center infrastructure.

2. Virtualization has enabled dealing with infrastructure that cannot be touched and is used to deploy the three major components of cloud computing that include,

- Infrastructure as a Service (IaaS)
- Platform as a Service (PaaS)
- Software as a Service (SaaS)

3. One fundamental attribute of virtualization is the concept of partitioning. This enables supporting of multiple operating systems under one single server. This ensures more segregation and seclusions to the machines from one another and effectively isolates them from an infected machine.

4. Virtualization has enabled the cloud to be sold as a commodity based on utility. Users can choose any platform without being locked in to any one vendor and they pay only for what they use.

5. Your server is not affected even if a neighbor machine is hacked or infected with a virus. Being in an individually enclosed environment assures of enhanced security without being intruded by the other machines being served in the environment.

6. Yet another feature of virtualization is its ability to share the hardware on the Linux and Windows operating systems. Instead of purchasing and maintaining an entire computer for one application, each application can be given its own operating system, and all those operating systems can reside on a single piece of hardware. It also enables shifting of operating systems over different hardware when multiple applications are running.

7. Virtualization allows an operator to control a guest operating system's use of CPU, memory, storage, and other resources, so each guest receives only the resources that it needs.

8. Certain features of a cloud are essential to enable services that truly represent the cloud computing model and satisfy expectations of consumers, and cloud offerings must be,

i. Self-service,
ii. Per-usage metered and billed,
iii. Elastic, and
iv. Customizable.

The feature "per-usage metered and billed" is practical only in presence of flexibility and efficiency in the back end. This efficiency is readily available in Virtualized and Machines.

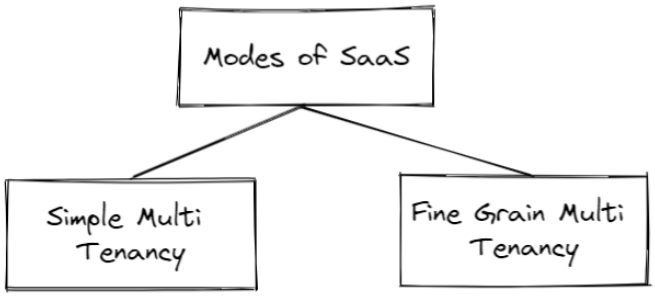
Question 4: Explain what are the different modes of software as a service (SaaS)?

Answer:

Software as a service (SaaS) is a cloud computing model where a third-party provider offers software applications to consumers over the internet. The services are scalable and can be modified by the users as they find necessary for their business. The SaaS applications can be accessed and used by multiple consumers simultaneously.

The users are reduced of the infrastructure costs and the expenses are shared among the multiple users. The main purpose is to share the data resources between multiple users while maintaining data isolation between the users.

The services are delivered in two modes

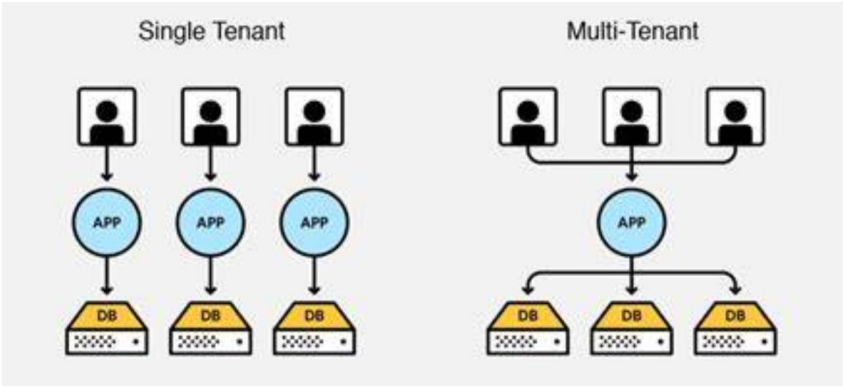


Simple Multi-Tenancy or Cross-Grain Multi-Tenancy

It is a hosted service model where the users have their own resources that are independent of other users. It is not instantly scalable and users have to be content with low margins due to high competition. The advantage is it is simple and does not require any code modifications.

Fine Grain Multi-Tenancy

This again involves sharing of the same database among multiple users. The data is kept separate although the computing resources are shared. It is easily scalable and offers efficiency in services.



Question 5: Before going for cloud computing platform what are the essential things to be taken in concern by users?

Answer:

Before moving to cloud computing platform, the following essential things should be taken into consideration.

1. Integrity of data

Data integrity in cloud storage is most critical concern of cloud clients. Assurance of data integrity means data remain as it is on server for long time. Client cannot physically access the data from the cloud server directly. Without client's knowledge, Cloud Service Provider (CSP) can alter or delete data which are either unused by client from a long a time or takes large memory space. Hence, there is need of reconciliation of data periodically, for its integrity.

2. Continuity of business

For continual business, you need to ensure that the provider's plans fit your requirements for availability and return to service - so look at the service level agreements. Also, Check the provider's indemnity and check support availability because some SaaS providers may only run support services during US working hours and you'll want a heavy UK focus.

3. Uptime

A growing challenge for applications is obtaining optimal availability at all times. Today, cloud-based infrastructures are often built with a large number of systems geared for elastic scalability while hardware costs should be kept to a minimum. These flexible scenarios mean that certain components are geared to fail. Availability in this context is how much time the service provider guarantees that your data and services are available. This is typically documented as a percent of time per year, e.g. 99.999% (or five nines) uptime means you will be unable to access resources for no more than about five minutes per year

4. Protection from loss of data:

Basic types of data loss include data destruction, data corruption and unauthorized data access. The reason for these types of loss a varied and include infrastructure malfunctions, software errors and security breaches. Due to the complexities around data center and cloud security, this article will deal destruction and corruption of data only.

5. Data storage

Cloud storage is a model of computer data storage in which the digital data is stored in logical pools. Data storage issues may lead to data breaches, data theft, and unavailability of cloud data. This thing demands an urgency to figure out our requirement. More people are sourcing there data storage to cloud providers because of the cost savings and ease of use, as well as

makes accounting, payroll and employee management simpler. There are three basic types of data storage. It can be:

- Private Cloud Storage
- Public Cloud Storage
- Hybrid Cloud Storage

So based on the level of security we want we can decide which storage type we can go for.

6. Compliance with the rules and regulations

Cloud compliance is an issue for anyone using cloud storage or backup services. The first thing that organizations need to do is to be fully aware of the type of cloud services that they use. Once they have done that, they can look at the data that they are going to move to the cloud. It's important to understand that for security and compliance reasons, organizations may decide that some highly confidential data will always remain on an internal network and will not move to the cloud. Or, if they move it to a cloud infrastructure it will be a private cloud that will be hosted on the premises. The second thing to look at once you know which data you are going to put on the cloud is to look at the contracts with your cloud provider. So, if it is an internal cloud, are you going to have internal SLAs and internal compliance checklists? If it's external, you have to clearly identify with the provider what type of data should reside on their cloud services, how they're going to protect it, how they're going to back it up and how you may reserve the right to audit the security and compliance framework that they build around your data. Also, check whether they have an incident response plan for alerting you if something goes wrong with your data on the cloud.

7. Ensuring Access

Because cloud applications are always connected, they can easily be targeted, which makes the timely identification and elimination of vulnerabilities critical. To keep ahead of threats, companies should deploy a vulnerability management process that identifies and triages vulnerabilities and can rapidly automate remediation with a web application firewall (WAF). A WAF is a critical web security control that can buy a company time by blocking an attack while the development team works to fix the code.

8. Security

Service providers promise that they can be more secure than physical data centers. Protection of expertise and assets is a key requirement. Cloud applications need to protect data being transferred over the net. This includes not only encryption of transmission data, but also encryption of stored data. Certificates, such as SAS 70 or ISO 27001, can be good indicators for good security measures. Customers should be aware of the physical location of their data and the available security features. This awareness facilitates a holistic security view of your cloud service provider.

9. Adaptability

Heterogeneous usage contexts demand a certain amount of adaptability from a cloud solution. The way of accessing a solution, the platform that is used, and the way users are dealing with the system are diverse and are constantly changing. The latest trend in usage contexts is the transition to mobile computing. People become focused on mobile technologies and have adopted its concepts (for example. app stores, always-on, location-based services, and so on) in their private life. They have the same expectations for their business life. As an IT department, it becomes important to satisfy the demand for mobile technologies. The next generation of business leaders is used to accessing every service with their smartphone and is aware of the competitive advantages of mobile computing.

10. Integration

Typical applications rely on data from other applications. The worst case would be to have separate data pools with unsynchronized content, which can lead to redundancy and inconsistency across applications. Data from other applications can enrich cloud services and provide comprehensive insight. In general, most services offer web services interfaces. Some do also provide a REST interface. Complex interfaces require a tool to handle connectivity and transformation, and manage future challenges. The use of XML as a data format offers the best possibilities to make data handling comfortable.

11. Migration

The aspect of integration leads us to the next point: migration. What do you do, if your cloud provider goes out of business? Are you able to migrate your valuable business data to another platform or have you locked-in a particular vendor? These questions should be asked before the decision for a particular provider is made. The longer a cloud service is being used, the more important and valuable are the assets that have been developed. Common standards can help to make your resources reusable. A (potential) migration strategy sustains your possibilities to react on market changes and future innovations.

12. Scalability

It is not very common that providers offer information about the scalability of their solution. SaaS and PaaS offerings promise to scale automatically. IaaS offerings might provide additional tools to control scalability. In hybrid cloud environments, scalability becomes very important because the decision to provision new instances must be based on reliable data. Multi-tenancy is essential for most cloud applications to provide reasonable scalability.

Question 6: State the list of a need of virtualization platform in implementing cloud?

Virtualization software allows multiple operating systems and applications to run on the same server at the same time, and, as a result, lowers costs and increases efficiency of a company's existing hardware. It's a fundamental technology that powers cloud computing.

Virtualization is needed in the implementation of the cloud due to the following reasons:

- Cloud operating system.
- In order to manage the service policies.
- In order to keep the backend level and user level concepts different from each other.

Virtualization is used for deployment of models of cloud hosting services includes:

- Infrastructure as a Service (IaaS)
- Platform as a Service (PaaS)
- Software as a Service (SaaS)

The three Important Attributes of Virtualization that Signify its Role in Cloud Computing are:

- Partitioning can be used for supporting a multitude of operating systems and applications within a single physical system such as a web server.
- Isolation imparts protection to virtual machines from any events such as virus attacks or crashes in other machines. Additionally, encapsulation is also used for protection of every application to prevent it from interfering with other applications.
- Virtual machines can use encapsulation for being represented as well as stored as single files in order to facilitate their identification and presentation to other applications.

List of Virtualization in Cloud

Virtualization can be used for almost any component including applications, operating systems, hardware, networks, memory, and storage to name a few. Virtualization is important for cloud computing because of its ability of decoupling hardware from software.

1. Hardware/Server Virtualization

It helps in achieving maximum hardware utilization and application uptime. In this arrangement, many small physical servers are integrated into one large physical server to let the processor function effectively. The operating system that is running on a physical server gets converted into a well-defined OS that runs on the virtual machine. In this case, the virtualization manager controls the processor, memory, and other components by enabling different OS to run on the same machine.

This is further categorized in three types namely:

- Full virtualization
- Para Virtualization

- Partial Virtualization

The benefits of server virtualization are:

- 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.

2. Network Virtualization

Under this arrangement, management and monitoring of a computer network is established as a single managerial entity from a single software-based administrator's console. The arrangement helps to improve network optimization of data transfer rates, scalability, reliability, flexibility, and security. Using network virtualization, companies can easily automate network administrative tasks. If you run a network that is huge, rapid and consumes massive resource, you may go for network virtualization. The primary benefit of this arrangement is improved network productivity and efficiency.

3. Storage Virtualization

This is another important virtualization type in cloud computing. Here, multiple network storage resources are present as a single storage device for easier and more efficient management of these resources. The benefits of this type of virtualization includes improved storage management, better availability of resources, reduced downtime and better storage utilization.

4. Memory Virtualization

This is a way to dissociate memory from the server. The disintegration is done to provide a shared, distributed or networked function. It eventually accelerates performance by providing greater memory capacity without any addition to the main memory. This is why a portion of the disk drive serves as an extension of the main memory. The integration is categorized in two ways: application-level integration and operating system level integration.

5. Software Virtualization

It enables main computer to run and create one or more virtual environments. This type of virtualization primarily used to enable a complete computer running as a guest OS. For instance, letting Linux to run as a guest that is natively running a Microsoft Windows OS (or vice versa, running Windows as a guest on Linux). The virtualization is of different kind including operating system virtualization, application virtualization and service virtualization.

6. Desktop Virtualization

Desktop virtualization for cloud provides businesses the work convenience and security they need. As the arrangement allows access remotely, administrators can access resources and work from any location and on any PC. This virtualization offers complete flexibility for employees to work from home or on the go and protects confidential data from being lost or stolen.