Cloud Computing Assignment

Module -1 (Fundamentals)

1- What is cloud computing?

Cloud computing is the on-demand access of computing resources—physical servers or virtual servers, data storage, networking capabilities, application development tools, software, AI-powered analytic tools and more—over the internet with pay-per-use pricing.

The cloud computing model offers customers greater flexibility and scalability compared to traditional on-premises infrastructure.

Cloud computing plays a pivotal role in our everyday lives, whether accessing a cloud application like Google Gmail, streaming a movie on Netflix or playing a cloud-hosted video game.

Cloud computing has also become indispensable in business settings, from small startups to global enterprises. Its many business applications include enabling remote work by making data and applications accessible from anywhere, creating the framework for seamless omnichannel customer engagement and providing the vast computing power and other resources needed to take advantage of cutting-edge technologies like [generative AI](https://research.ibm.com/blog/what-is-generative-AI) and [quantum computing](https://www.ibm.com/topics/quantum-computing).

A cloud services provider (CSP) manages cloud-based technology services hosted at a remote [data center](https://www.ibm.com/topics/data-centers) and typically makes these resources available for a pay-as-you-go or monthly subscription fee.

2-Describe cloud computing deploy model

In cloud computing, we have access to a shared pool of computer resources (servers, storage, programs, and so on) in the cloud. You simply need to request additional resources when you require them. Getting resources up and running quickly is a breeze thanks to the clouds. It is possible to release resources that are no longer necessary. This method allows you to just pay for what you use. Your cloud provider is in charge of all upkeep.

Cloud Deployment Model functions as a virtual computing environment with a deployment architecture that varies depending on the amount of data you want to store and who has access to the infrastructure.

3-Describe different type of cloud service

The cloud deployment model identifies the specific type of cloud environment based on ownership, scale, and access, as well as the cloud’s nature and purpose. The location of the servers you’re utilizing and who controls them are defined by a cloud deployment model. It specifies how your cloud infrastructure will look, what you can change, and whether you will be given services or will have to create everything yourself. Relationships between the infrastructure and your users are also defined by cloud deployment types. [Different types of cloud](https://www.geeksforgeeks.org/types-of-cloud/) computing deployment models are described below.

* [Public Cloud](https://www.geeksforgeeks.org/difference-between-public-cloud-and-private-cloud/)
* Private Cloud
* [Hybrid Cloud](https://www.geeksforgeeks.org/public-cloud-vs-private-cloud-vs-hybrid-cloud/)
* Community Cloud
* [Multi-Cloud](https://www.geeksforgeeks.org/overview-of-multi-cloud/)

**1 - Public Cloud**

The public cloud makes it possible for anybody to access systems and services. The public cloud may be less secure as it is open to everyone. The public cloud is one in which cloud infrastructure services are provided over the internet to the general people or major industry groups. The infrastructure in this cloud model is owned by the entity that delivers the cloud services, not by the consumer. It is a type of cloud hosting that allows customers and users to easily access systems and services. This form of cloud computing is an excellent example of cloud hosting, in which service providers supply services to a variety of customers. In this arrangement, storage backup and retrieval services are given for free, as a subscription, or on a per-user basis. For example, Google App Engine etc.

**2 - Private Cloud**

The private cloud deployment model is the exact opposite of the public cloud deployment model. It’s a one-on-one environment for a single user (customer). There is no need to share your hardware with anyone else. The distinction between [private and public clouds](https://www.geeksforgeeks.org/difference-between-public-cloud-and-private-cloud/) is in how you handle all of the hardware. It is also called the “internal cloud” & it refers to the ability to access systems and services within a given border or organization. The cloud platform is implemented in a cloud-based secure environment that is protected by powerful firewalls and under the supervision of an organization’s IT department. The private cloud gives greater flexibility of control over cloud resources.

**3 - Hybrid Cloud**

By bridging the public and private worlds with a layer of proprietary software, hybrid cloud computing gives the best of both worlds. With a hybrid solution, you may host the app in a safe environment while taking advantage of the public cloud’s cost savings. Organizations can move data and applications between different clouds using a combination of two or more cloud deployment methods, depending on their needs.

**4 - Community Cloud**

It allows systems and services to be accessible by a group of organizations. It is a distributed system that is created by integrating the services of different clouds to address the specific needs of a community, industry, or business. The infrastructure of the community could be shared between the organization which has shared concerns or tasks. It is generally managed by a third party or by the combination of one or more organizations in the community.

**5 - Multi-Cloud**

We’re talking about employing [multiple cloud providers](https://www.geeksforgeeks.org/overview-of-multi-cloud/) at the same time under this paradigm, as the name implies. It’s similar to the hybrid cloud deployment approach, which combines public and private cloud resources. Instead of merging private and public clouds, multi-cloud uses many public clouds. Although public cloud providers provide numerous tools to improve the reliability of their services, mishaps still occur. It’s quite rare that two distinct clouds would have an incident at the same moment. As a result, multi-cloud deployment improves the high availability of your services even more.

4 -Describe cloud computing Architect

[Cloud Computing](https://www.geeksforgeeks.org/cloud-computing/) , which is one of the demanding technology of the current time and which is giving a new shape to every organization by providing on demand virtualized services/resources. Starting from small to medium and medium to large, every organization use cloud computing services for storing information and accessing it from anywhere and any time only with the help of internet. In this article, we will know more about the internal architecture of cloud computing.

Transparency, scalability, security and intelligent monitoring are some of the most important constraints which every cloud infrastructure should experience. Current research on other important constraints is helping cloud computing system to come up with new features and strategies with a great capability of providing more advanced cloud solutions.

**Cloud Computing Architecture :**  
The cloud architecture is divided into 2 parts i.e.

* Frontend
* Backend

Architecture of cloud computing is the combination of both [SOA (Service Oriented Architecture)](https://www.geeksforgeeks.org/service-oriented-architecture/) and EDA (Event Driven Architecture). Client infrastructure, application, service, runtime cloud, storage, infrastructure, management and security all these are the components of cloud computing architecture.

**{ 1 } Frontend :**

Frontend of the cloud architecture refers to the client side of cloud computing system. Means it contains all the user interfaces and applications which are used by the client to access the cloud computing services/resources. For example, use of a web browser to access the cloud platform.

* **Client Infrastructure –** Client Infrastructure is a part of the frontend component. It contains the applications and user interfaces which are required to access the cloud platform.
* In other words, it provides a GUI( Graphical User Interface ) to interact with the cloud.

**{ 2 }Backend :**

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

* **Application –**  
  Application in backend refers to a software or platform to which client accesses. Means it provides the service in backend as per the client requirement.
* **Service –**  
  Service in backend refers to the major three types of cloud based services like [SaaS, HYPERLINK "https://www.geeksforgeeks.org/cloud-based-services/"PaaS HYPERLINK "https://www.geeksforgeeks.org/cloud-based-services/" and HYPERLINK "https://www.geeksforgeeks.org/cloud-based-services/"IaaS](https://www.geeksforgeeks.org/cloud-based-services/). Also manages which type of service the user accesses.
* **Runtime Cloud-**  
  Runtime cloud in backend provides the execution and Runtime platform/environment to the Virtual machine.
* **Storage –**  
  Storage in backend provides flexible and scalable storage service and management of stored data.
* **Infrastructure –**  
  Cloud Infrastructure in backend refers to the hardware and software components of cloud like it includes servers, storage, network devices, virtualization software etc.
* **Management –**  
  Management in backend refers to management of backend components like application, service, runtime cloud, storage, infrastructure, and other security mechanisms etc.
* **Security –**  
  Security in backend refers to implementation of different security mechanisms in the backend for secure cloud resources, systems, files, and infrastructure to end-users.
* **Internet –**  
  Internet connection acts as the medium or a bridge between frontend and backend and establishes the interaction and communication between frontend and backend.
* **Database**– Database in backend refers to provide database for storing structured data, such as SQL and NOSQL databases. Example of Databases services include Amazon RDS, Microsoft Azure SQL database and Google CLoud SQL.
* **Networking**– Networking in backend services that provide networking infrastructure for application in the cloud, such as load balancing, DNS and virtual private networks.
* **Analytics**– Analytics in backend service that provides analytics capabillities for data in the cloud, such as warehousing, bussness intellegence and machine learning.

**Benefits of Cloud Computing Architecture :**

* Makes overall cloud computing system simpler.
* Improves data processing requirements.
* Helps in providing high security.
* Makes it more modularized.
* Results in better disaster recovery.
* Gives good user accessibility.
* Reduces IT operating costs.
* Provides high level reliability.
* Scalability.

Master Software Testing and Automation in an efficient and time-bound manner by mentors with real-time industry experience. Join our [Software Automation Course](https://www.geeksforgeeks.org/courses/complete-guide-to-software-testing-automation?utm_source=geeksforgeeks&utm_medium=article_bottom_text&utm_campaign=courses) and embark on an exciting journey, mastering the skill set with ease!

5 - What is components of cloud computing?

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

**A - Client Infrastructure**

Client infrastructure is a significant part of the frontend system that offers a graphical user interface (GUI) for seamless cloud communication.

**B - Application**

It can either be a piece of software or a platform. The application delivers the outcome to the user along with the resources in the back end, depending on the client’s needs.

**C - Service**

Based on the client’s needs, a cloud computing architecture service controls the type of service you can access. Cloud architecture computing provides three types of services, including: Understand the 3 major types of [cloud service models](https://herovired.com/learning-hub/blogs/service-models-of-cloud-computing/).

* **Software as a Service (SaaS):** SaaS is also called cloud application services. SaaS apps typically run immediately via the web browser, eliminating the need for download and installation. Cisco WebEx, Google Apps, HubSpot, and Salesforce are a few examples of SaaS.
* **Platform as a Service (PaaS):** It is also called Service for Cloud Platforms. It has much resemblance with SaaS. While PaaS offers a platform for seamless software development, SaaS allows you to access the software through the Internet without any hassle. OpenShift and Magento Commerce Cloud are two good examples.

. **Infrastructure as a Service (IaaS):** it is also referred to as cloud

infrastructure services. It is in charge of overseeing the runtime,

middleware, and data environments for applications. AWS EC2, Cisco

Metapod, and Google Compute Engine are a few examples of IaaS.

Want to learn more about cloud computing deployment? Check this

out: [Introduction to Cloud Deployment Models](https://herovired.com/learning-hub/blogs/cloud-deployment-model/).

**D - Runtime Cloud**

Virtual machines can access a runtime and execution environment via the runtime cloud.

**E - Storage**

Storage is yet another crucial element of cloud computing architecture. It offers a sizable quantity of cloud storage space for managing and storing data.

F - **Infrastructure**

Cloud architecture offers network-level, application-level, and host-level services. To support the concept of cloud computing architecture, cloud infrastructure comes with software and hardware elements, including storage, virtualization software network devices, and other storage resources.

**G - Management**

This component oversees the management of backend components such as storage infrastructure, runtime clouds, storage applications, and other security-related issues. Also, it promotes coordination among them.

**H - Security**

Security is a core component of a backend cloud architecture. It offers users secure access to cloud architecture, resources, information, and systems. Also, it leverages virtual firewalls to deploy security management services to the cloud server. This aids in data loss prevention.

I –Internet

A backend and frontend can interact and communicate with one another thanks to an internet connection, which serves as a mediator or bridge between them .

6 - cloud computing advantage and disadvantage

\* Below are the advantages of cloud storage:

**1. Cost Saving**

By using cloud storage, there is no need to buy as many hard drives, enclosures to house them in, RAID cards to enable data redundancy, electricity to power them, or hardware warranty services to safeguard them. However, it also cuts management expenses by decreasing the need for in-depth capacity planning, streamlining monitoring, and minimizing on-premise hardware and software management. Administrators can instead concentrate on other, more crucial activities.

**2. Data Redundancy and Replication**

The majority of cloud storage providers maintain numerous copies of data, even inside of a single “Data Center”, and they provide excellent object durability to lower the risk of data loss. Geographic replication options, however, can spread out several copies of data across areas if you’re searching for even greater security. Others provide replication services that swiftly transfer data between data centers, while some offer geo-replication as a storage class option. Your backups are adequately shielded.

**3. Data Tiering for Cost Savings**

Various storage classes and data tiers are offered by numerous cloud storage providers. Choose based on how regularly and rapidly one restores backups, as well as how long one wants to retain the backups. Consider using the vendor’s hot storage for backups that require quick and/or frequent restores because it offers the fastest and most economical retrieval. Consider shifting data to archive storage for long-term archiving, Although data retrieval may be more time-consuming and expensive, storage expenses are far lower, especially if one intends to preserve backups for many years. The ability to automatically shift data between tiers is a feature that some vendors offer. This minimizes administration and makes it easier to obtain cost savings.

**4. Regulatory Compliance**

For regulatory compliance, keeping backups in the same area as the data’s origin may be the best option. Worldwide alternatives for data centers are provided by many cloud suppliers. Look for a cloud storage provider that can accommodate if one needs to store EU client data in an EU data center. Moving data to cloud storage within the same region is also advantageous for performance. Even if you are not subject to regulation, the enhanced performance might be valuable to you.

**5. Ransomware/Malware Protection**

Ransomware is plain nasty. Unfortunately, it frequently makes the news. The malware will search the network for shares that contain files and documents to encrypt in addition to the locally infected computer, which is one of the more frightening characteristics of ransomware. You might be relieved to learn that your cloud storage can assist prevent ransomware by providing some backup security advantages because it’s more difficult to access without proper authentication if you’re hit by ransomware or another type of malware that is encrypting or destroying files.

\* Below are the disadvantages of cloud storage:

**1. Vulnerability**

The majority of PCs and servers that save data require an internet connection. Cloud solutions are internet-based by nature, which means that they are linked to other computers and servers. Thus, making them vulnerable to attacks by malicious users on the network.

**2. Internet Dependency**

The internet starts to be reliant on your storage. Due to the fact that the internet will govern our world in 2022, this disadvantage will diminish. One can always save files while offline and access them later. However, an internet connection will be required for the update and sync.

**3. Issues in Security and Privacy**

Uncertainties about privacy and security on the cloud are the next significant point to be made in relation to the drawbacks of cloud storage. Confidential data must be given over to a third-party organization in order to be stored in the cloud. One must therefore have complete faith in the cloud vendor.

**4. Limitations on Control**

After the user moves data to the cloud, the vendor is now in charge of it. This implies that users must rely on the vendors to maintain their services in a safe, stable, up-and-running, and fully functional manner. This limits the influence on data safety Nearly all reliability is left up to the storage vendor, along with accessibility.

**5. Cost**

Although cloud storage options are normally a cost-effective choice, they could not be available if utilized for short-term or very small-scale projects, depending on the cloud vendor. Users can be on the hook for 18 more months than needed, which is not financially feasible if the demand for data storage is for 6 months but the vendor’s minimum offer is 2 years.