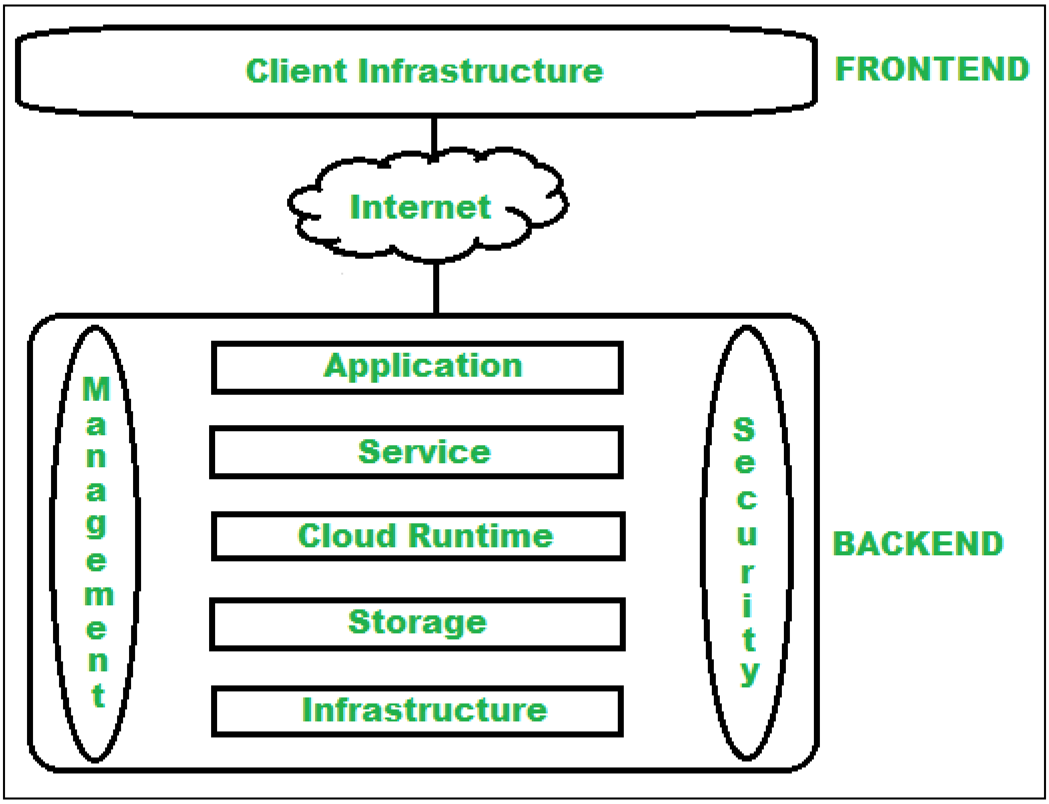
Cloud architecture

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.

Cloud computing architecture

The cloud architecture is divided into 2 parts i.e.

1. Frontend
2. Backend



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, PaaS and IaaS. Also manages which type of service the user accesses.
   - **Runtime cloud**:
     Runtime cloud in backend provides the execution and Runtime platform/environment to the Virtual machine.
   - **Storage**:
     Storage in backend provides flexible and scalable storage service and management of stored data.
   - **Infrastructure**:
     Cloud Infrastructure in backend refers to the hardware and software components of cloud like 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.

Actors in cloud computing

Cloud Service Providers: A group or object that delivers cloud services to cloud consumers or end-users. It offers various components of cloud computing. Cloud computing consumers purchase a growing variety of cloud services from cloud service providers. There are various categories of cloud-based services mentioned below:

1. **IaaS Providers:** In this model, the cloud service providers offer infrastructure components that would exist in an on-premises data center. These components consist of servers, networking, and storage as well as the virtualization layer.
2. **SaaS Providers:** In Software as a Service (SaaS), vendors provide a wide sequence of business technologies, such as Human resources management (HRM) software, customer relationship management (CRM) software, all of which the SaaS vendor hosts and provides services through the internet.
3. **PaaS Providers:** In Platform as a Service (PaaS), vendors offer cloud infrastructure and services that can access to perform many functions. In PaaS, services and products are mostly utilized in software development. PaaS providers offer more services than IaaS providers. PaaS providers provide operating system and middleware along with application stack, to the underlying infrastructure.

Cloud Carrier: The mediator who provides offers connectivity and transport of cloud services within cloud service providers and cloud consumers. It allows access to the services of the cloud through Internet networks, telecommunication, and other access devices. Network and telecom carriers or a transport agent can provide distribution. A consistent level of services is provided when cloud providers set up Service Level Agreements (SLA) with a cloud carrier. In general, Carrier may be required to offer dedicated and encrypted connections.

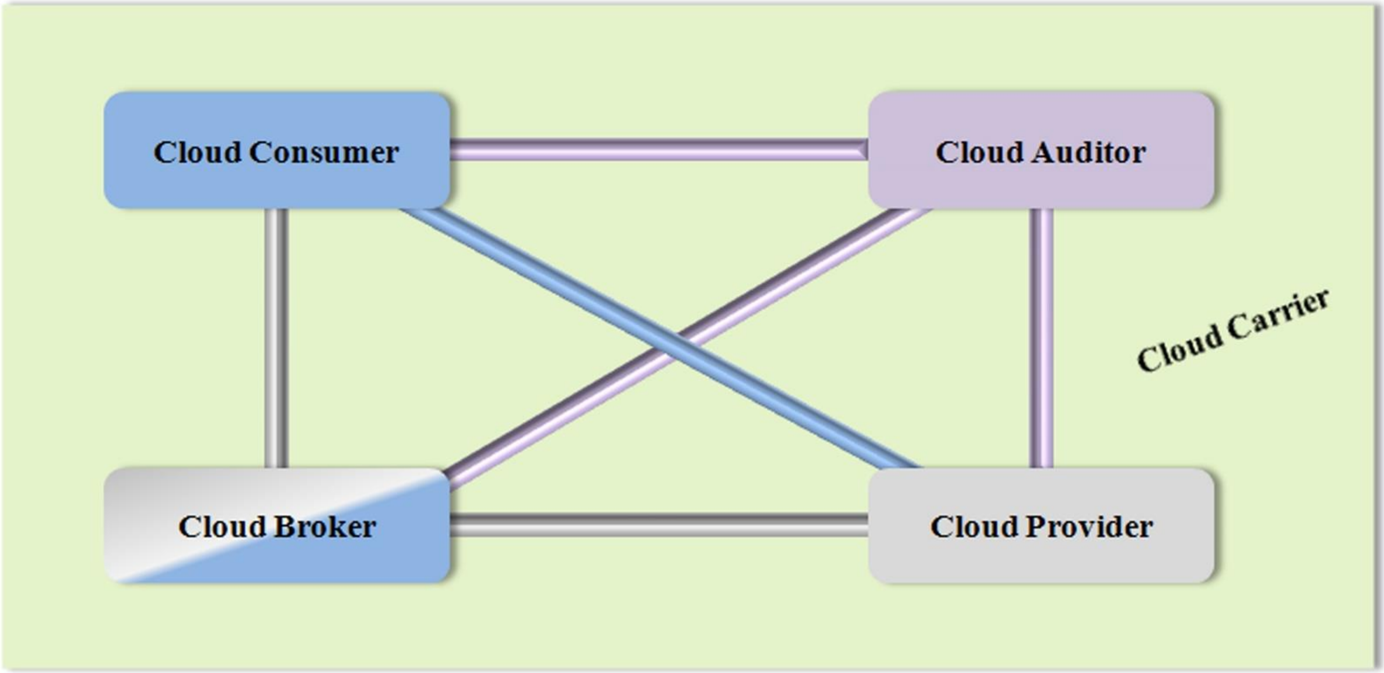
Cloud Broker: An organization or a unit that manages the performance, use, and delivery of cloud services by enhancing specific capability and offers value-added services to cloud consumers. It combines and integrates various services into one or more new services. They provide service arbitrage which allows flexibility and opportunistic choices. There are major three services offered by a cloud broker:

- Service Intermediation.
- Service Aggregation.
- Service Arbitrage.

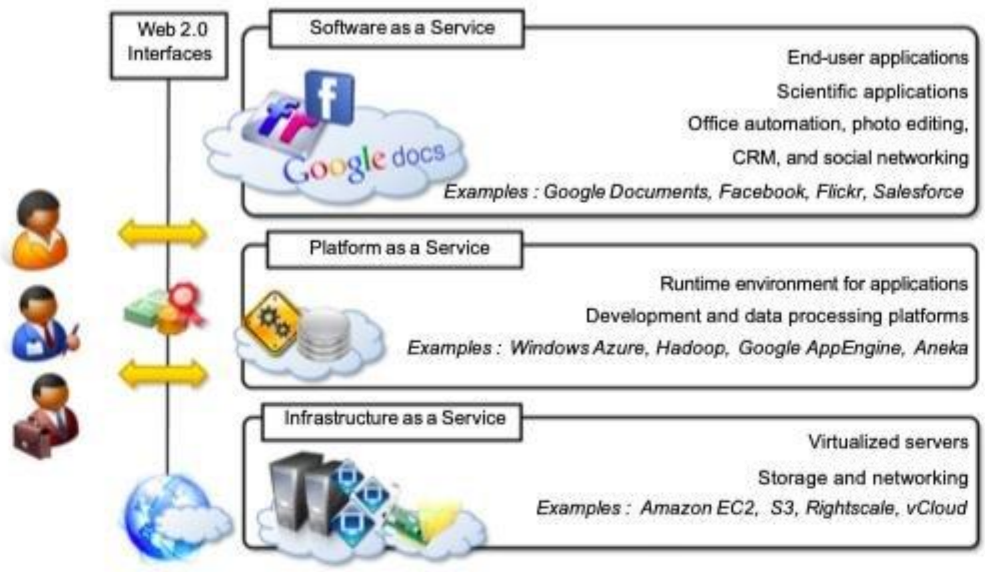
Cloud Auditor: An entity that can conduct independent assessment of cloud services, security, performance, and information system operations of the cloud implementations. The services that are provided by Cloud Service Providers (CSP) can be evaluated by service auditors in terms of privacy impact, security control, and performance, etc. Cloud Auditor can make an assessment of the security controls in the information system to determine the extent to which the controls are implemented correctly, operating as planned and constructing the desired outcome with respect to meeting the security necessities for the system. There are three major roles of Cloud Auditor which are mentioned below:

- Security Audit.
- Privacy Impact Audit.
- Performance Audit.

Cloud Consumer: A cloud consumer is the end-user who browses or utilizes the services provided by Cloud Service Providers (CSP), sets up service contracts with the cloud provider. The cloud consumer pays peruse of the service provisioned. Measured services utilized by the consumer. In this, a set of organizations having mutual regulatory constraints performs a security and risk assessment for each use case of Cloud migrations and deployments.



Cloud reference model


Web 2.0 Interfaces
Software as a Service
End-user applications
Scientific applications
Office automation, photo editing,
CRM, and social networking
Examples : Google Documents, Facebook, Flickr, Salesforce
Platform as a Service
Runtime environment for applications
Development and data processing platforms
Examples : Windows Azure, Hadoop, Google AppEngine, Aneka
Infrastructure as a Service
Virtualized servers
Storage and networking
Examples : Amazon EC2, S3, Rightscale, vCloud

IaaS:

Infrastructure as a Service (IaaS) offers storage and computer resources that developers and IT organizations use to deliver custom/business solutions. IaaS delivers computer hardware (servers, networking technology, storage, and data center space) as a service. It may also include the delivery of OS and virtualization technology to manage the resources. Here, the more important point is that IaaS customers rent computing resources instead of buying and installing them in their data centers. The service is typically paid for on a usage basis. The service may include dynamic scaling so that if the customers need more resources than expected, they can get them immediately.

PaaS:

Platform as a Service is a strategy that offers a high level of abstraction to make a cloud readily programmable in addition to infrastructure-oriented clouds that offer basic compute and storage capabilities (PaaS). Developers can construct and deploy apps on a cloud platform without necessarily needing to know how many processors or how much memory their applications would use. A PaaS offering that provides a scalable environment for creating and hosting web applications is Google App Engine, for instance.

SaaS:

Software as a Service (SaaS) is a form of application delivery that relieves users of the burden of software maintenance while making development and testing easier for service providers. The cloud delivery model's top layer is where applications are located. End customers get access to the services this tier offers via web portals. Because online software services provide the same functionality as locally installed computer programs, consumers (users) are rapidly switching from them. Today, ILMS and other application software can be accessed via the web as a service. In terms of data access, collaboration, editing, storage, and document sharing, SaaS is unquestionably a crucial service. Email service in a web browser is the most well-known and widely used example of SaaS, but SaaS applications are becoming more cooperative and advanced.

Types of Cloud

Public cloud:

Public clouds are managed by third parties which provide cloud services over the internet to the public, these services are available as pay-as-you-go billing models. They offer solutions for minimizing IT infrastructure costs and become a good option for handling peak loads on the local infrastructure. Public clouds are the go-to option for small enterprises, which can start their businesses without large upfront investments by completely relying on public infrastructure for their IT needs. The fundamental characteristics of public clouds are multitenancy. A public cloud is meant to serve multiple users, not a single customer. A user requires a virtual computing environment that is separated, and most likely isolated, from other users.

Private cloud:

Private clouds are distributed systems that work on private infrastructure and provide the users with dynamic provisioning of computing resources. Instead of a pay-as-you-go model in private clouds, there could be other schemes that manage the usage of the cloud and proportionally billing of the different departments or sections of an enterprise. Private cloud providers are HP Data Centers, Ubuntu, Elastic-Private cloud, Microsoft, etc.

Hybrid cloud:

A hybrid cloud is an IT environment comprising several environments that appear to be connected by LANs, WANs, VPNs, or APIs to form a single, unified environment. You should be able to link many machines and combine IT assets using hybrid clouds. Finance, healthcare, and higher education are three industries that mostly use hybrid clouds. However, when apps may move in and out of many distinct yet connected environments, every IT system turns into a hybrid cloud. These environments must be derived from centralized IT resources that can scale as needed, at the very least. And a platform for integrated management and orchestration must be used to manage each of those environments as a single environment.

Open challenges

1. **Data security and privacy:**
   Data security is a major concern when switching to cloud computing. User or organizational data stored in the cloud is critical and private. Even if the cloud service provider assures data integrity, it is your responsibility to carry out user authentication and authorization, identity management, data encryption, and access control. Security issues on the cloud include identity theft, data breaches, malware infections, and a lot more which eventually decrease the trust amongst the users of your applications.
2. **Cost management:**
   Even as almost all cloud service providers have a "Pay As You Go" model, which reduces the overall cost of the resources being used, there are times when there are huge costs incurred to the enterprise using cloud computing. When there is under optimization of the resources, let's say that the servers are not being used to their full potential, add up to the hidden costs. If there is a degraded application performance or sudden spikes or overages in the usage, it adds up to the overall cost. Unused resources are one of the other main reasons why the costs go up.
3. **Multi cloud environment:**
   Due to an increase in the options available to the companies, enterprises not only use a single cloud but depend on multiple cloud service providers. Most of these companies use hybrid cloud tactics and close to 84% are dependent on multiple clouds. This often ends up being hindered and difficult to manage for the infrastructure team. The process most of the time ends up being highly complex for the IT team due to the differences between multiple cloud providers.
4. **Performance challenges:**
   Performance is an important factor while considering cloud-based solutions. If the performance of the cloud is not satisfactory, it can drive away users and decrease profits. Even a little latency while loading an app or a web page can result in a huge drop in the percentage of users. This latency can be a product of inefficient load balancing, which means that the server cannot efficiently split the incoming traffic so as to provide the best user experience.
5. **Interoperability and flexibility:**
   When an organization uses a specific cloud service provider and wants to switch to another cloud-based solution, it often turns up to be a tedious procedure since applications written for one cloud with the application stack are required to be re-written for the other cloud. There is a lack of flexibility from switching from one cloud to another due to the complexities involved. Handling data movement, setting up the security from scratch and network also add up to the issues

encountered when changing cloud solutions, thereby reducing flexibility.

6. **High dependence on network:**
   Since cloud computing deals with provisioning resources in real-time, it deals with enormous amounts of data transfer to and from the servers. This is only made possible due to the availability of the high-speed network. Although these data and resources are exchanged over the network, this can prove to be highly vulnerable in case of limited bandwidth or cases when there is a sudden outage. Even when the enterprises can cut their hardware costs, they need to ensure that the internet bandwidth is high as well there are zero network outages, or else it can result in a potential business loss.
7. **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.