Chapter 2 : Cloud Architecture, Services and Models

2.1 CLOUD ARCHITECTURE

Cloud computing is a virtual environment that delivers hosted services such as servers, databases, networking, analytics, and intelligence over the internet, ensuring innovation, flexibility, and cost-effectiveness. Cloud computing has transformed how people use to save documents and data previously.

You no longer need to save your data on a floppy disc, CD, or USB flash drive; cloud computing allows you to access them from any terminal at any time. But do you understand how it all works? To comprehend this, you must first understand the cloud computing architecture.

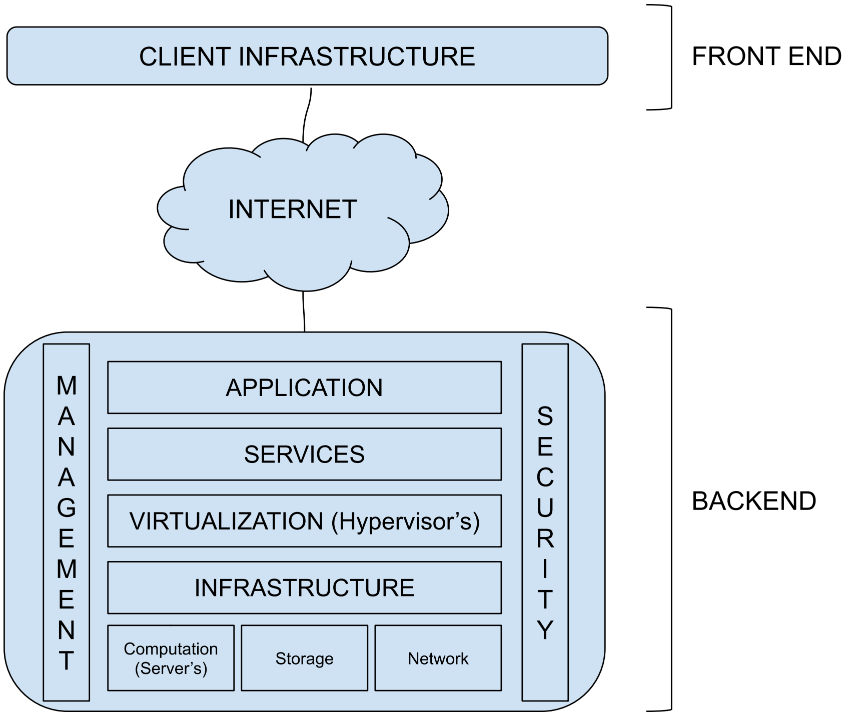
What is cloud computing architecture?

In layman’s terms, the architecture of cloud computing refers to how various technological components work together to create a cloud, in which resources are pooled and shared across a network using advanced technology, such as virtualization. Virtualization is the segmentation of one physical server into multiple logical servers. In a nutshell, “cloud computing architecture is a hybrid of (SOA) service-oriented architecture and (EDA) event-driven architecture.”

In other words, Cloud Computing Architecture refers to the components and subcomponents required for cloud computing. These components typically consist of a front-end platform (client-side interfaces), a back-end platform (servers, storage), and a network that connects these components. Together, they enable the scalable, flexible, and on-demand services that define cloud computing.

Cloud architecture consists of two major parts:

- Front End
- Back End



What is the Front End of cloud architecture?

Everything with which the end user interacts is part of the front-end infrastructure. The user interface is the result of integrating various sub-components, such as browsers, tablets, mobile devices, etc. With the help of the front end, the end user can connect to the cloud computing infrastructure. In short, "the front end is the end that the client interacts with."

What is the Back End of cloud architecture?

The back end is everything the user does not usually see and everything that processes the data. The service provider uses the back end to manage all the resources required to provide cloud computing services, such as data storage, security mechanisms, virtual machines, deploying models, servers, traffic control mechanisms, and so on. In short, "the back end is the end that service provider interacts with."

Components of cloud computing architecture

There are various components of cloud architecture. Some of those components are:

1. **Front End:**

   This is the part that interacts with the user (client), generally representing the user-facing side of cloud applications.

   - **Client Infrastructure**:

     The devices and software used by end-users to interact with cloud services. This could be a laptop, smartphone, or even a web browser. The client infrastructure is responsible for sending requests over the internet to access resources or services hosted on the cloud's back-end.

     Example: A user using a web browser to access Gmail or a mobile app for cloud storage like Google Drive.

2. **Internet**:

   This is the communication medium through which data is transmitted between the front-end (client infrastructure) and the back-end (cloud service). The internet connects the user’s device to the cloud infrastructure, enabling access to resources, applications, and services.

   Example: When you access a cloud service like Dropbox, your request to upload or download files is routed over the internet.

3. **Back End:**

   The back-end is the part of cloud computing that consists of infrastructure, services, and applications that operate behind the scenes.

- **Application**:

  These are the software programs or applications that run on the cloud and are accessed by users through the front-end. Applications are hosted on servers in the cloud and are usually provided as a service to the client (SaaS).

  Example: Applications like Google Docs, Microsoft Office 365, or Salesforce run in the back-end cloud infrastructure and are accessible to users over the internet.

- **Services**:

  Services refer to different cloud-based functions or tasks provided by the cloud system. A cloud service manages the type of service a client uses based on his needs. There are three types of services:

  - SaaS (software as a service),
  - PaaS (platform as a service),
  - IaaS (infrastructure as a service).

  Example: Cloud services like Amazon S3 (storage), Google Cloud Functions (serverless computing), and AWS Lambda.

- **Virtualization (Hypervisor's)**:

  Virtualization is the technology that allows for the creation of virtual machines (VMs), which run on top of physical servers. Hypervisors are software layers that allow multiple virtual machines to run on a single physical server, efficiently utilizing resources.

  Example: Using VMware or Hyper-V to create virtual environments where multiple operating systems can run on a single server.

- **Infrastructure**:

  The physical hardware (servers, storage, networking equipment) and resources that form the core of cloud computing. This includes computational servers, storage systems, and the network that connects everything together.

  - **Computation (Servers)**: Computation refers to the processing power provided by servers in a cloud infrastructure. These servers perform the necessary computing tasks, running applications, processing data, and handling user requests.
  - **Storage**: In cloud computing, storage refers to systems designed to store digital data securely and efficiently. It includes different types of storage solutions such as databases, file storage systems, and block storage. These systems are designed to hold large volumes of data for applications, backups, and user data.
  - **Network**: In cloud environments, the network refers to the infrastructure that interconnects the various components of a system, enabling communication between servers, storage, applications, and end-users. This includes physical networking hardware (switches, routers) as well as virtual networks created in the cloud.

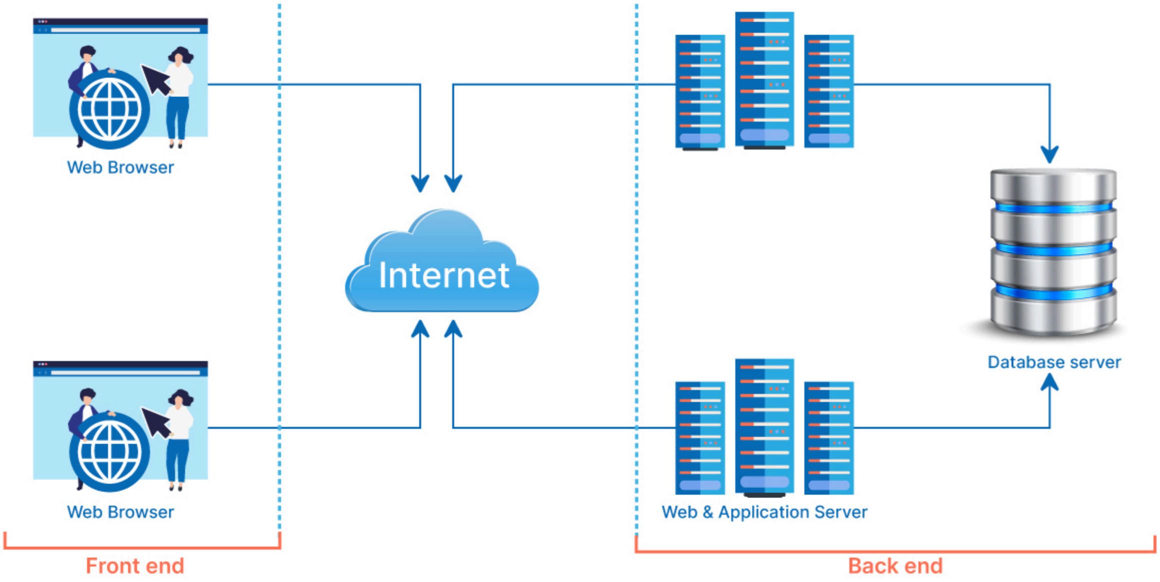
- **Management:**

  The management component is in charge of managing backend components such as storage services, applications, runtime cloud infrastructure, and security issues, as well as establishing coordination.

- **Security:**

  Security is a critical component of cloud computing, ensuring that all resources, data, and applications are protected from unauthorized access or cyber threats. This includes encryption, firewalls, identity access management, and more.

Example: Cloud providers offer services like AWS Identity and Access Management (IAM) or Google Cloud Security Command Center to manage user permissions and ensure data security.



Benefits of Cloud Computing Architecture:

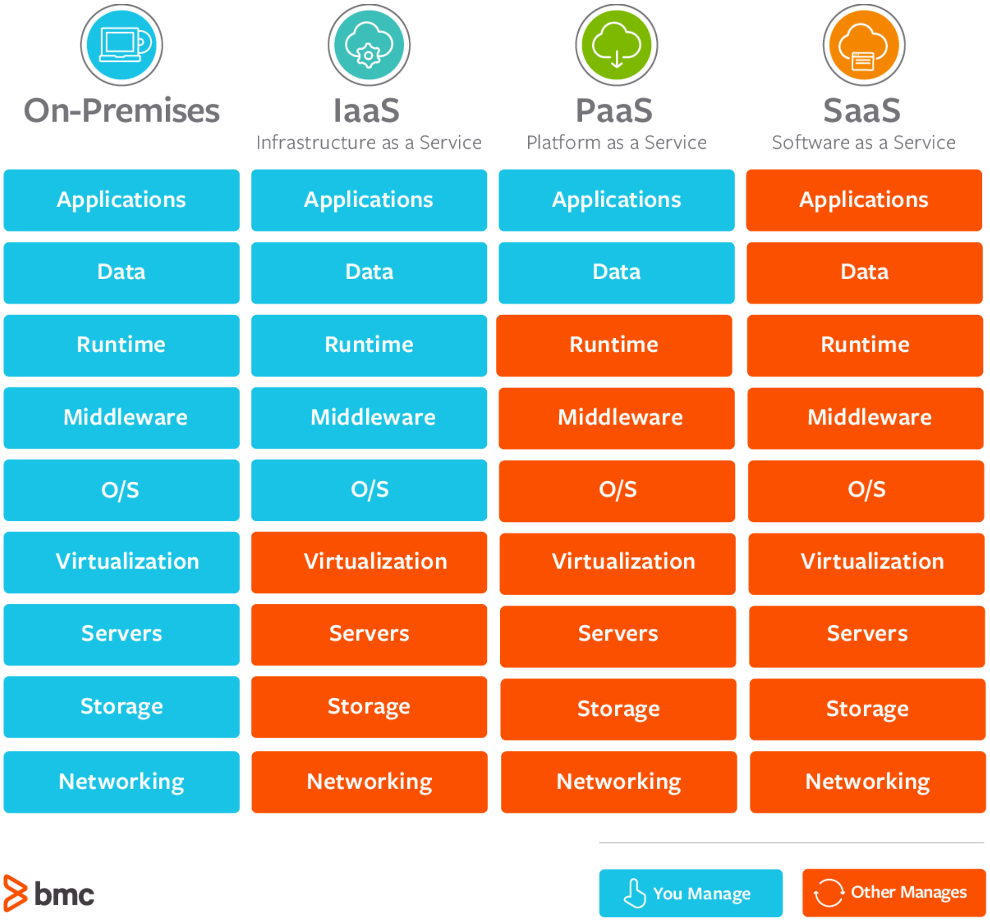
The cloud computing architecture is designed in such a way that:

- It solves latency issues and improves data processing requirements.
- It reduces IT operating costs and gives good accessibility to access data and digital tools.
- It helps businesses to easily scale up and scale down their cloud resources.
- It has a flexibility feature which gives businesses a competitive advantage.
- It results in better disaster recovery and provides high security.
- It automatically updates its services.
- It encourages remote working and promotes team collaboration.

2.2 CLOUD SERVICE MODELS (Types of Services)

A cloud service model refers to a framework that defines how cloud computing resources (such as storage, servers, and applications) are delivered to users. It describes the different levels of service that cloud providers offer, including Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS), each offering varying degrees of control and management responsibility for the user.

- ➔ IaaS, or infrastructure as a service, is on-demand access to cloud-hosted physical and virtual servers, storage and networking—the backend IT infrastructure for running applications and workloads in the cloud.
- ➔ PaaS, or platform as a service, is on-demand access to a complete, ready-to-use, cloud-hosted platform for developing, running, maintaining and managing applications.
- ➔ SaaS, or software as a service, is on-demand access to ready-to-use, cloud-hosted application software.



On-Premises	IaaS Infrastructure as a Service	PaaS Platform as a Service	SaaS Software as a Service
🟦 Applications	🟦 Applications	🟦 Applications	🟥 Applications
🟦 Data	🟦 Data	🟦 Data	🟥 Data
🟦 Runtime	🟦 Runtime	🟥 Runtime	🟥 Runtime
🟦 Middleware	🟦 Middleware	🟥 Middleware	🟥 Middleware
🟦 O/S	🟦 O/S	🟥 O/S	🟥 O/S
🟦 Virtualization	🟥 Virtualization	🟥 Virtualization	🟥 Virtualization
🟦 Servers	🟥 Servers	🟥 Servers	🟥 Servers
🟦 Storage	🟥 Storage	🟥 Storage	🟥 Storage
🟦 Networking	🟥 Networking	🟥 Networking	🟥 Networking

🟦 You Manage
🟥 Other Manages

Terms used in Diagram :-

1. **Applications**
   Applications are software programs designed to help users perform specific tasks such as document editing, email management, data analysis, or online collaboration.
2. **Data**
   Data is any information that is collected, processed, and stored by applications, ranging from simple text documents to complex databases containing financial records or customer information.
3. **Runtime**
   The runtime environment is the software layer that supports the execution of an application, providing the necessary libraries, services, and tools needed to run a program.
4. **Middleware**
   Middleware is software that acts as a bridge between applications and the lower-level layers of a system, such as the operating system or database, to enable communication and data management.
5. **Operating System (O/S)**
   An operating system is system software that manages computer hardware and provides common services for applications, such as resource management, file handling, and task scheduling.
6. **Virtualization**
   Virtualization is the process of creating virtual instances of physical resources such as servers, storage devices, and network resources, enabling multiple operating systems and applications to run on a single physical machine.
7. **Servers**
   Servers are powerful computers or virtual machines that provide services, resources, or data to other devices, known as clients, over a network.
8. **Storage**
   Storage refers to any computing hardware or service used to store digital data, encompassing technologies like hard drives, solid-state drives (SSD), and cloud storage services.
9. **Networking**
   Networking refers to the interconnected system of hardware and protocols that enable data transmission and communication between devices, applications, or servers across local or wide-area networks, including the internet.

2.2.1 Infrastructure as a Service (IaaS)

Definition : Infrastructure as a service (IaaS) is the on-demand availability of highly scalable computing resources as services over the internet. It eliminates the need for enterprises to procure, configure, or manage infrastructure themselves, and they only pay for what they use.

Explanation : IaaS, or Infrastructure as a Service, is a cloud computing model that provides on-demand access to computing resources such as servers, storage, networking, and virtualization.

IaaS is attractive because acquiring computing resources to run applications or store data the traditional way requires time and capital. Organizations must purchase equipment through procurement processes that can take months. They must invest in physical spaces, typically specialized rooms with power and cooling. And after deploying the systems, they need IT professionals to manage and maintain them.

All this is challenging to scale when demand spikes or business grows. You run the risk of running out of capacity or overbuilding and paying for infrastructure that you never use.

How does it work?

IaaS in cloud computing is when you rent access to cloud infrastructure resources as individual services from a cloud service provider (CSP), including servers, virtual machines, networking resources, and storage. IaaS helps eliminate much of the complexity and costs associated with building and maintaining physical infrastructure in an on-premises data center.

The Cloud Service Provider (CSP) is responsible for managing and maintaining the infrastructure, so you can concentrate on installing, configuring, and managing software and keeping your data secure. IaaS providers also offer additional services, such as detailed billing management, logging, monitoring, storage resiliency, and security.

You can access IaaS resources using a pay-as-you-go basis, allowing you to only pay to consume the resources that you need. In other words, you can easily increase or decrease resources, allowing you to pay less when needed or instantly provision and scale out resources to meet new demand.

Examples :

a) AWS:
   - ➔ Amazon EC2 (Elastic Compute Cloud): Virtual servers in the cloud with customizable compute power.
   - ➔ Amazon S3 (Simple Storage Service): Object storage service for storing and retrieving any amount of data.

b) Google Cloud (GCP):
   - ➔ Google Compute Engine: Virtual machines running in Google's data centers.

c) Microsoft Azure:
   - ➔ Azure Virtual Machines: On-demand scalable computing resources.

2.2.2 Platform as a Service (PaaS)

Definition : Platform as a Service (PaaS) is a complete cloud environment that includes everything developers need to build, run, and manage applications—from servers and operating systems to all the networking, storage, middleware, tools, and more.

Explanation : Platform as a Service, also known as PaaS, is a type of cloud computing service model that offers a flexible, scalable cloud platform to develop, deploy, run, and manage apps. PaaS provides everything developers need for application development without the headaches of updating the operating system and development tools or maintaining hardware. Instead, the entire PaaS environment—or platform—is delivered by a third-party service provider via the cloud.

PaaS helps businesses avoid the hassle and cost of installing hardware or software to develop or host new custom applications. Development teams simply purchase pay-as-you-go access to everything they need to build custom apps, including infrastructure, development tools, operating systems, and more.

The result is simpler, faster, and secure app development that gives developers the freedom to focus on their application code.

How does PaaS works?

Unlike IaaS or SaaS service models, PaaS solutions are specific to application and software development and typically include:

- ➔ Cloud infrastructure: Data centers, storage, network equipment, and servers
- ➔ Middleware software: Operating systems, frameworks, development kits (SDK), libraries, and more
- ➔ User interface: A graphical user interface (GUI), a command line interface (CLI), an API interface, and in some cases, all three

Platform as a Service is typically delivered as a secure online platform that developers can access over the internet, allowing them to work on projects from anywhere and collaborate freely with other members of their team. Applications are built directly on the PaaS system and can be immediately deployed once they are completed.

Examples :

a) AWS:
   - ➔ AWS Elastic Beanstalk: A service for deploying and scaling web applications and services with infrastructure management handled by AWS.
   - ➔ AWS Lambda: A serverless compute service that lets you run code without provisioning servers.

b) Google Cloud (GCP):
   - ➔ Google App Engine: A fully managed platform for building and deploying applications.
   - ➔ Google Cloud Functions: A serverless environment to build and connect cloud services.

c) Microsoft Azure:
   - ➔ Azure App Service: A platform for building, hosting, and scaling web apps and APIs.
   - ➔ Azure Functions: A serverless compute service that allows you to run small pieces of code in response to events.

2.2.3 Software as a Service (PaaS)

Definition:

Software as a Service (SaaS) is a cloud-based service where instead of installing and maintaining software, users access applications over the internet, eliminating the need for complex software and hardware management.

Explanation:

Software as a Service, or SaaS, is a cloud computing service model that allows users to access software applications hosted by a service provider over the internet. With SaaS, users don't need to worry about installing, managing, or upgrading software on their own devices. Instead, the software provider hosts the application on their own infrastructure, and users typically access it via a web browser.

SaaS solutions are subscription-based, meaning users pay on a monthly or yearly basis. The applications are centrally hosted and updated by the provider, ensuring that all users have access to the latest version of the software without needing to handle any updates or maintenance themselves. Common examples of SaaS applications include customer relationship management (CRM), email, office productivity software, and collaboration tools.

SaaS is highly advantageous for businesses because it removes the need to invest in expensive infrastructure and software licensing. Instead, users can access powerful software tools on a flexible pay-as-you-go basis, which lowers upfront costs and reduces IT workload. This model is scalable, allowing businesses to add or reduce users as needed, and offers easy accessibility from any device with an internet connection. The result is more efficient operations, increased collaboration, and the ability for users to focus on using the software rather than managing it.

How does SaaS work?

Unlike IaaS or PaaS, SaaS provides fully functional software applications that are managed and maintained by the service provider. The key components include:

- ➔ Cloud-hosted applications: Software that is stored and maintained on the service provider's cloud infrastructure.
- ➔ User Interface (UI): Typically accessed via a web browser, allowing users to interact with the software seamlessly from any location.
- ➔ Automatic Updates: The service provider manages updates and patches, ensuring users always have access to the latest features and security improvements.
- ➔ Subscription Model: Users pay a subscription fee based on usage, often per user or per organization.

SaaS is generally delivered through a web-based interface, enabling users to access applications from any device with an internet connection. This accessibility supports remote work and collaboration across teams, making SaaS an attractive option for businesses of all sizes.

Applications hosted on SaaS platforms can include anything from office suites, CRM systems, project management tools, to financial software and email services. Once the service is subscribed to, users can immediately start using the application without needing to install it on their local device.

Examples :

(a) AWS:

- ➔ Amazon Chime: A communication service for online meetings, video conferencing, and chats.
- ➔ Amazon WorkMail: A secure, managed business email and calendar service.

(b) Google Cloud (GCP):

- ➔ Google Workspace (formerly G Suite): Includes Gmail, Google Docs, Google Drive, and Google Calendar for collaboration and productivity.
- ➔ Google Maps API: Location-based services accessible over the web.

(c) Microsoft Azure:

- ➔ Microsoft 365: Includes Office apps like Word, Excel, and PowerPoint accessible via the cloud.
- ➔ Dynamics 365: A cloud-based business applications platform for managing customer relationships, operations, and financials.

2.2.4 Differences between IaaS, PaaS and SaaS

Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as Service (SaaS) are the three main categories of cloud computing service models. Each type of cloud computing provides organizations and individuals with fully managed resources over the public internet—from storage and virtualization to hardware and software to applications. The difference between them is which resources you manage and which are managed for you.

“As a Service” generally refers to a cloud computing service that is fully managed by a third-party cloud service provider. Understanding what you want to manage (and what you don’t) is one of the most important steps on your journey to the cloud.

Based on the service type you choose, the service provider is responsible for managing different elements in your computing stack:

- ➔ IaaS: The service provider gives you on-demand access to infrastructure services, including compute, storage, networking, and virtualization. You manage everything else—the virtual machines, operating systems, middleware, apps, and your data—but there is no need to maintain or update your own data center infrastructure.
- ➔ PaaS: The service provider delivers and manages all the hardware and software resources needed for application development. You write the code and manage all the apps and data, but you do not have to manage or maintain the software development platform. PaaS manages more resources higher up the "stack" to further reduce the operational burden on developers and IT operations teams.
- ➔ SaaS: The service provider delivers and manages the entire application stack—from the hardware infrastructure all the way to the application itself—through the internet. All updates, bug fixes, and other general maintenance to all components are handled by the provider. All you have to do is connect to the app.

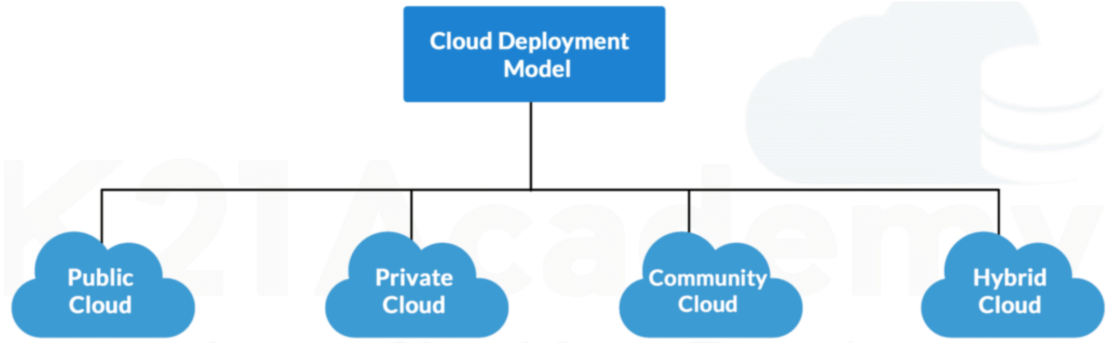
2.3 CLOUD DEPLOYMENT MODELS (Types of Clouds)

A cloud deployment model essentially defines where the infrastructure for your deployment resides and determines who has ownership and control over that infrastructure. It also determines the cloud's nature and purpose.

The first port of call for any organization looking to adopt cloud services is to understand the available deployment models. Once these are understood, a better decision can be made about which routes the business should pursue. Each model will offer advantages and disadvantages in areas such as governance, scalability, security, flexibility, cost, and management.

Types of Cloud Deployment Models

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.



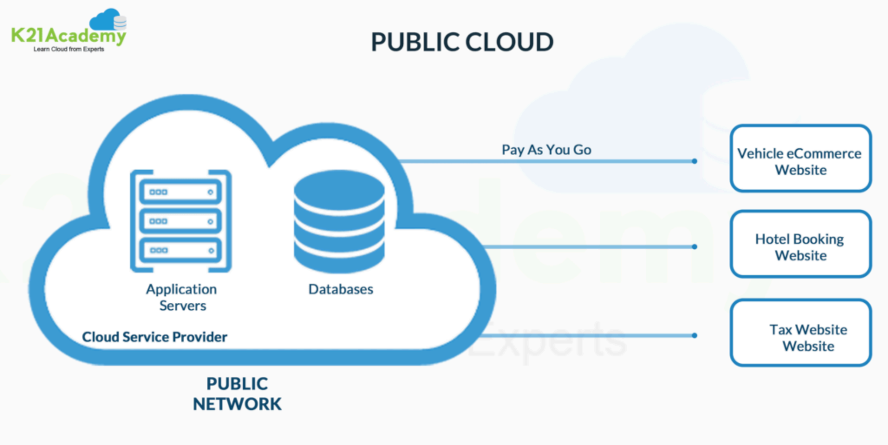
2.3.1 Public Cloud

Public cloud is a commonly adopted cloud model, where the cloud services provider owns the infrastructure and openly provides access to it for the public to consume.

As the name indicates, the public cloud is available for the general public who want to use computing resources such as software and hardware over the internet. It is a good choice for companies and organizations with low-security concerns. There is no need to manage these resources as cloud computing providers configure and manage these services.

As the service provider owns the hardware and supporting networking infrastructure, it is under the service provider's full control. The service provider is responsible for the physical security, maintenance, and management of the data center where the infrastructure resides. The underlying infrastructure is, therefore, outside of the customer's control and also away from the customer's physical location.

The cloud service provider will share infrastructure between multiple customers whilst keeping data separate and isolated, offering many layers of security controls where this is a concern. Some services can be hosted on dedicated or isolated hardware if required, usually at an additional cost. Cloud providers go to huge lengths to ensure physical data centers are extremely secure and are highly regulated environments, almost always exceeding the standards a customer could achieve themselves.



Characteristics:

- Cloud services provided by a third-party provider over the internet.
- Multiple tenants (organizations or users) share the same infrastructure.
- Resources are scalable and available on-demand.

Advantages:

- Cost-effective: Pay-as-you-go pricing with no capital expenditure.
- Scalable: Easily increase or decrease resources based on demand.
- Maintenance-free: No need to manage or maintain hardware or software.
- Accessibility: Accessible from anywhere with an internet connection.

Disadvantages:

- Security concerns: Data is stored on shared infrastructure, leading to potential security and privacy risks.
- Less control: Limited control over infrastructure and customization.
- Performance issues: Performance may degrade if the provider is serving many customers at once.

Technical Example: AWS, Google Cloud, Microsoft Azure.

Non-Technical Analogy: Using public transportation (bus or train). It's cheap and widely available, but you share it with other people, and you don't control its route or schedule.

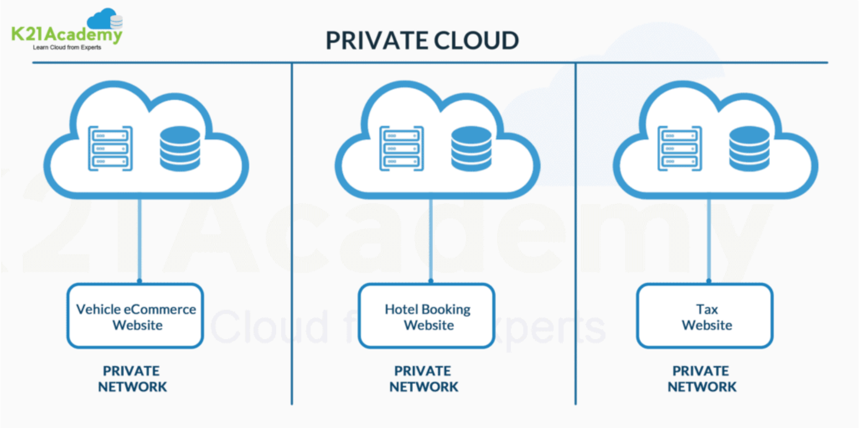
2.3.2 Private Cloud

As the name suggests, Private Cloud lets you use the infrastructure and resources for a single organization. Users and organizations do not share resources with other users. That is why it is also called as Internal or corporate model. Private clouds are more costly than public clouds due to their costly maintenance.

A private cloud can be thought of as an environment that is fully owned and managed by a single tenant. This option is usually chosen to alleviate any data security concerns that might exist with the public cloud offering. Any strict cloud governance requirements can also be more easily adhered to, and the private cloud can be more easily customized.

Full control of the hardware can lead to higher performance. A customer will typically run a private cloud within their own building (on-premises) or purchase rackspace in a data center in which to host their infrastructure.

However, the responsibility to manage the infrastructure also falls to the customer, creating a need for more staff with wider skills and increasing costs. A large initial investment may also be required to purchase the required hardware.



Characteristics:

- ➔ Dedicated cloud infrastructure used exclusively by one organization.
- ➔ Can be hosted on-premises or by a third-party provider.
- ➔ Offers a high level of security and customization.

Advantages:

- ➔ High security: Since resources are not shared, there’s more control over data privacy and security.
- ➔ Customization: Full control over the infrastructure, allowing organizations to tailor it to their specific needs.
- ➔ Better performance: Since it's dedicated to one organization, performance issues caused by other users are eliminated.

Disadvantages:

- ➔ High cost: Expensive to set up and maintain compared to public cloud due to hardware and operational expenses.
- ➔ Limited scalability: More difficult to scale up compared to public cloud unless extra resources are available.
- ➔ Maintenance responsibility: The organization is responsible for managing the infrastructure.

Technical Example: VMware, OpenStack, IBM Private Cloud.

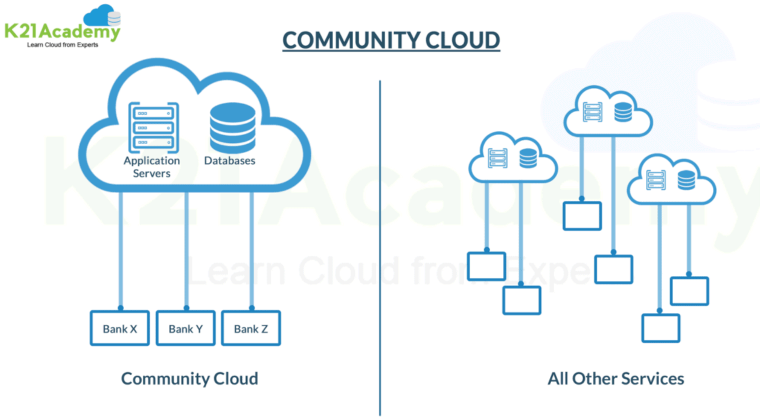
Non-Technical Analogy: Owning your personal gym at home. You have full control and privacy, but it's expensive to buy and maintain the equipment, and space is limited.

2.3.3 Community Cloud

The community Deployment Model is somewhat similar to the Private cloud. In the private cloud, only one user or organization owns the cloud server. In Community Cloud, several companies with the same backgrounds share the cloud server. If all organizations or companies have the same set of security protocols and performance requirements, and goals, this multi-tenant architecture can help them save cost and boost efficiency. This model can be used in the case of project development, implementation, and maintenance.

It is lesser-known and less-adopted deployment model, a Community cloud brings together infrastructure that is shared and jointly accessed by several organizations from a specific group that shares specific computing needs.

For example, the education sector could utilize a community cloud to enable a group of scholars and students to share academic content, making joint research easier.



Characteristics:

- Cloud infrastructure shared by multiple organizations with similar needs or interests (e.g., compliance, security).
- May be managed by one or more organizations or a third-party provider.

Advantages:

- Shared resources: Costs and responsibilities are shared among the organizations in the community.
- Security and compliance: Provides better security than public clouds because it's designed to meet the community's specific compliance and regulatory needs.
- Collaborative: Encourages collaboration between organizations that share infrastructure.

Disadvantages:

- ➔ Cost-sharing: Can still be expensive since it's a dedicated infrastructure shared by fewer organizations compared to public cloud.
- ➔ Less control: Each organization may have to compromise on certain customization or operational aspects to meet the community’s shared needs.
- ➔ Limited scalability: Less flexible than public cloud options when it comes to rapidly increasing capacity.

Technical Example: A group of hospitals sharing a cloud infrastructure to store patient records.

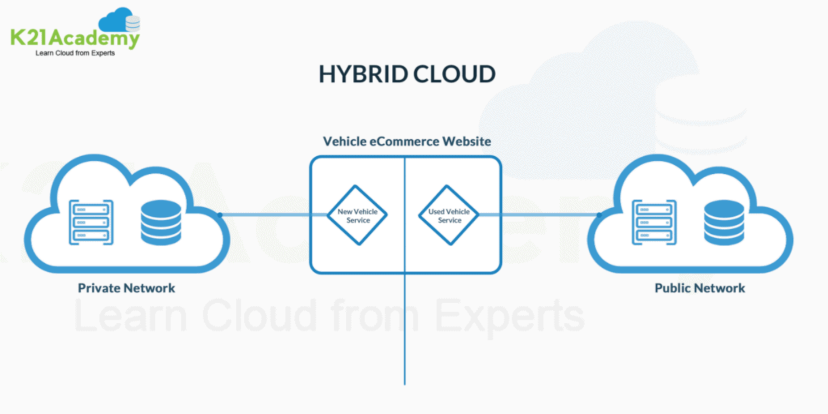
Non-Technical Analogy: Think of a gated community sharing a communal park and gym. The costs are shared, and it’s accessible only to community members, but each member must follow community rules, and personalization is limited.

2.3.4 Hybrid Cloud

The Hybrid Cloud is a combination of both public and private clouds. Very few companies and organizations can migrate their tech stack to cloud computing rapidly in one go. Hence, Cloud vendors came up with a hybrid cloud that offers a smooth transition with public and private cloud facilities. They keep the sensitive data in the private cloud and non-sensitive data in the public cloud.

The benefits of both the public and private cloud can be realized, as well as some of the disadvantages, such as increased management overhead and the initial challenge of setting up a hybrid infrastructure. Once realized, applications can be moved between infrastructure hosted in the public and private clouds, increasing flexibility and fault tolerance.

Typically businesses may have some presence on-premise, and utilizing this hardware until it has reached end-of-life in the private cloud will likely be an attractive option if the business already owns the hardware. In the hybrid model, this can be used to form part of the private cloud. Most businesses strive to alleviate the burden on the existing infrastructure, migrating to the public cloud where possible, and effectively utilizing the hybrid deployment model during the migration period.



Characteristics:

- ➔ A combination of public and private clouds, allowing data and applications to be shared between them.
- ➔ Provides flexibility for businesses to use public clouds for non-sensitive tasks while keeping sensitive data on private clouds.

Advantages:

- ➔ Flexibility: Organizations can choose the best cloud type for each task (e.g., public cloud for testing, private cloud for sensitive data).
- ➔ Cost-efficient: Balances the cost benefits of public cloud and the control of private cloud.
- ➔ Scalable: Public cloud resources can be used when there’s a spike in demand, avoiding the need for a full private infrastructure.

Disadvantages:

- ➔ Complex management: Managing a hybrid cloud environment can be complex due to the need to synchronize both public and private cloud environments.
- ➔ Security challenges: Ensuring security across both public and private clouds can be challenging.
- ➔ Higher costs: May involve higher costs than using a pure public cloud due to private infrastructure maintenance.

Technical Example: Using AWS for non-sensitive workloads and a private on-premises cloud for sensitive applications.

Non-Technical Analogy: Having both a private home gym and a membership to a public gym. You use the public gym for specialized equipment but rely on your private gym for daily use.

2.3.5 Comparison between Public, Private, Community & Hybrid Cloud

Important Factors to Consider	Public	Private	Community	Hybrid
Setup and ease of use	Easy	Requires professional IT Team	Requires professional IT Team	Requires professional IT Team
Data Security and Privacy	Low	High	Very High	High
Scalability and flexibility	High	High	Fixed requirements	High
Cost-Effectiveness	Most affordable	Most expensive	Cost is distributed among members	Cheaper than private but more expensive than public
Reliability	Low	High	Higher	High