# CE644 Cloud Computing and Applications

# Cloud Deployment Models: *private, public, community, and hybrid*

- The deployment models are the different ways in which the ***cloud computing environment can be set up***, that is, the several ways in which the ***cloud can be deployed***.
- The classification of the cloud is based on several parameters such as the **size of the cloud** (number of resources), **type of service provider, location, type of users, security**, and other issues. The **smallest in size** is the **private cloud.**

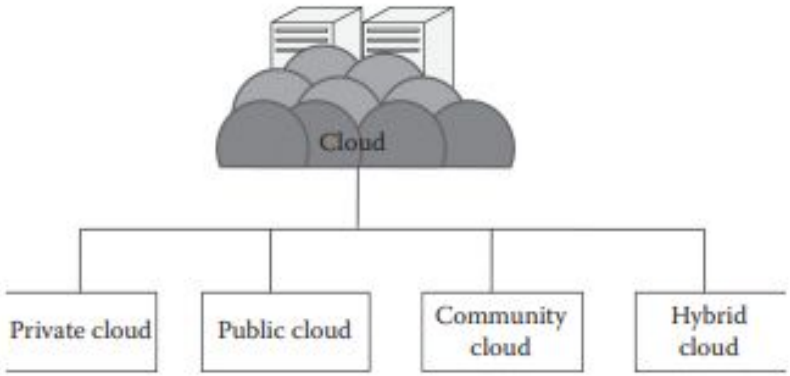


**FIGURE 4.1**
Cloud deployment models.

- *Private Cloud*: deployed by a **single organization for its personal use**. It is **not shared by other organizations**, and it is **not allowed for public use.**
- It is usually **on premise** but **can be outsourced** also.
- *Community Cloud:* which is an extension of the private cloud. Here, the **cloud is the same as the private cloud but is shared by several organizations**. The community cloud is established for a **common cause**.
- *Public Cloud:* This cloud allows **access from any place in the world and is open to the public**. This cloud is **biggest in size** among all other deployment models. The public cloud model is one of the **most popular** deployment models. The public cloud service provider **charges the users on an hourly basis** and serve the users according to the **service-level agreements (SLAs).**
- *Hybrid Cloud:* It consists of the **private and public clouds combined**. Several properties of the private cloud are used with the properties of the public cloud.

# Private Cloud

- Definition: According to National Institute of Standards and Technology (NIST), private cloud can be defined as the cloud infrastructure that is provisioned for **exclusive use by a single organization comprising multiple consumers** (e.g., business units). It may be **owned, managed, and operated by the organization, a third party, or some combination of them**, and it may exist **on or off premises**.
- The private cloud is **small in size** as compared to other cloud models.

Characteristics:

1. Secure: The private cloud is **secure**. This is because usually the private cloud is **deployed and managed by the organization itself**, and hence there is least chance of data being leaked out of the cloud. In the case of **outsourced cloud**, the **service provider may view the clou**d (though governed by SLAs), but there is no other risk from anybody else as all the users belong to the same organization.
2. Central control: The organization mostly has **full control** over the cloud as usually the private cloud is managed by the organization itself. Thus, when managed by the organization itself, there is no need for the organization to rely on anybody.
3. Weak SLAs: Formal SLAs **may or may not exist** in a private cloud. But if they exist they are **weak** as it is between the **organization and the users of the same organization**.

Suitability (most suitable conditions and environment where this cloud model can be used):

- The organizations or enterprises that require a **separate cloud for their personal or official use**.
- The organizations or enterprises that have a **sufficient amount of funds** as **managing and maintaining a cloud** is a costly affair.
- The organizations or enterprises that consider **data security** to be important.
- The organizations that want **autonomy and complete control over the cloud**.
- The organizations that have a ***less number of users***.
- The organizations that have **prebuilt infrastructure** for deploying the cloud and are ready for **timely maintenance** of the cloud for efficient functioning.
- *Special care needs to be taken and resources should be available for troubleshooting*.

The private cloud platform is *not suitable* for the following:

- The organizations that have ***high user base***
- The organizations that have **financial constraints**
- The organizations that **do not have prebuilt infrastructure**
- The organizations that **do not have sufficient manpower to maintain and manage the cloud**.

According to NIST, the private cloud can be classified into several types based on their **location and management**:

- *On-premise private cloud:* Cloud is **deployed in organizational premises** and is **connected to the organizational network**.
- *Outsourced private cloud:* A **third party** manages the whole cloud.

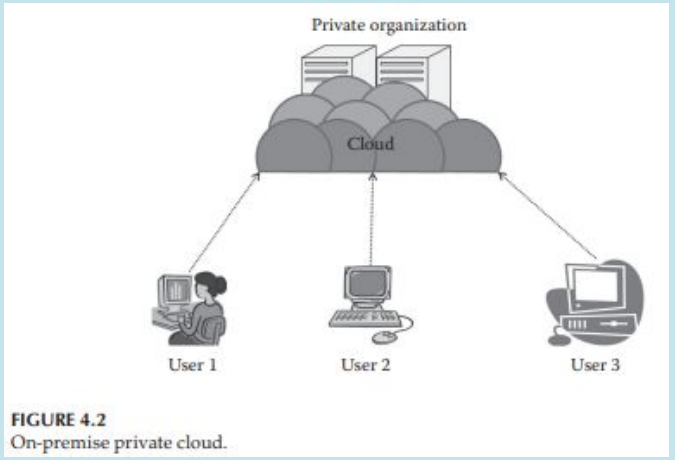

FIGURE 4.2
On-premise private cloud.

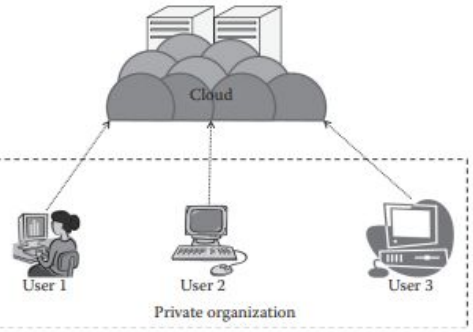

FIGURE 4.3
Outsourced private cloud.

# On-premise private cloud: Issues

- SLA: For any cloud to operate, there must be certain **agreements between the user and the service provider**.
- The **service provider** will **agree upon certain terms and conditions** regarding the service delivery.
- Here in the private cloud, the **SLAs** are defined between an **organization and its users**, that is, mostly employees. Usually, these users have broader access rights than the general public cloud users.
- Similarly in the service provider's side, the service providers are able to **efficiently provide the service because of the small user base and mostly efficient network.**
- Network: The cloud is **totally dependent on the network that is laid out**. The network usually consists of a **high bandwidth and has a low latency**.
- Performance: The performance of a cloud delivery model primarily depends on the **network and resources**. Since here the networks are managed **internally**, the performance can be controlled by the **network management team**, and mostly this would have good performance as the **number of resources is low**.

- Security and data privacy: Affect the private cloud the **least**.
- As the data of the users are solely **managed by the company** and most of the **data would be related to the organization or company**, here there is a lesser chance that the data will be leaked to people outside as there are no users outside the organization.
- Hence, comparatively, the private cloud is **more resistant to attacks** than any other cloud type purely because of the **type of users and local area network**. But, **security breaches** are possible if an internal user misuses the privileges.
- Location: In a private cloud, the **data are internal** and are usually **stored in the same geographical location** where the cloud users, that is, organization, are present (on-premise cloud).
- If a company has several physical locations, then the cloud is distributed over several places.
- In this case, there is a possibility that cloud resources have to be accessed using the Internet (by establishing a virtual private network [VPN] or without a VPN).

- Cloud management: Cloud management is a broad area where the **entire cloud-related tasks are managed** in order to provide **seamless services** to the customers.
- This involves several tasks such as **resource scheduling, resource provisioning, and resource management**.
- The **number of users, the network size, and the amount of resources** are some of the important parameters that affect the management of the cloud.
- Here, the network is small, and the numbers of users and the amount of resources are less.
- Multitenancy: The cloud basically has a **multitenant architecture**. As multitenant architecture supports **multiple tenants with the same physical or software resource**, there is a **chance of unwanted access of data**, and **it will have less effect** in the private cloud as all the **issues will be intra-organizational**.
- Maintenance: The cloud is maintained by the organization where the cloud is deployed.
- The number of resources is less in the private cloud, so **maintenance is comparatively easier**.

# Outsourced private cloud: Issues

- SLA: The SLA is between the **third party and the outsourcing organization**.
- The SLAs are usually followed strictly as it is a third-party organization.
- Network: The cloud is fully deployed at the third-party site.
- The **cloud's internal network is managed by a third party**, and the organizations connect to the third party by means of either a **dedicated connection or through the Internet**.
- The **internal network of the organization is managed by the organization**, and it does not come under the purview of the SLA.
- Security and privacy: Security and privacy **need to be considered** when the cloud is outsourced.
- Here, the **cloud is less secure** than the on-site private cloud. The **privacy and security of the data mainly depend on the hosting third party as they have the control of the cloud**.

- Laws and conflicts: If this cloud is **deployed outside the country,** then the **security laws** pertaining to that will apply upon the data and the data are still not fully safe.
- Usually, private clouds are not deployed outside, but if the off-site location is outside the country's boundary, then several problems may arise.
- Location: The private cloud is usually **located off site** here.
- When there is a change of location, the **data need to be transmitted through long distances**.
- In few cases, it might be out of the country, which will lead to **certain issues regarding the data and its transfer**.
- Performance: The performance of the cloud depends on the third party that is outsourcing the cloud.
- Maintenance: The cloud is **maintained by a third-party organization** where the cloud is deployed. As mentioned, the defective resources (drives and processors) are replaced with the good resources. *Here, again the process is less complex compared to the public cloud*. **The cost of maintenance is a big issue.** If an organization owns a cloud, then the cost related to the cloud needs to be borne by the organization and this is usually high.

- The minimum configuration varies for each type of platforms, but in general, a machine with an **8 GB RAM, 250 GB hard disk, and at least an i7 processor** will allow the user to install a private cloud in it.
- Further, this private (**Infrastructure-as-a-Service [IaaS])** cloud can be used to create a **virtual machine**, and then a user can test these virtual machines.

Advantages of **Private cloud**

-The cloud is **small in size and is easy to maintain**.

-It provides a **high level of security and privacy to the user**.

-It is **controlled by the organization**.

Disadvantages of **private cloud**

-For the private cloud, **budget is a constraint**.

-The private clouds have loose **SLAs**.

# Public Cloud

- Definition: According to **NIST**, the public cloud is the cloud infrastructure that is provisioned for **open use by the general public**. It may be **owned, managed, and operated by a business, academic, or government organization, or some combination of them**.

- It exists on the **premises of the cloud provider**.

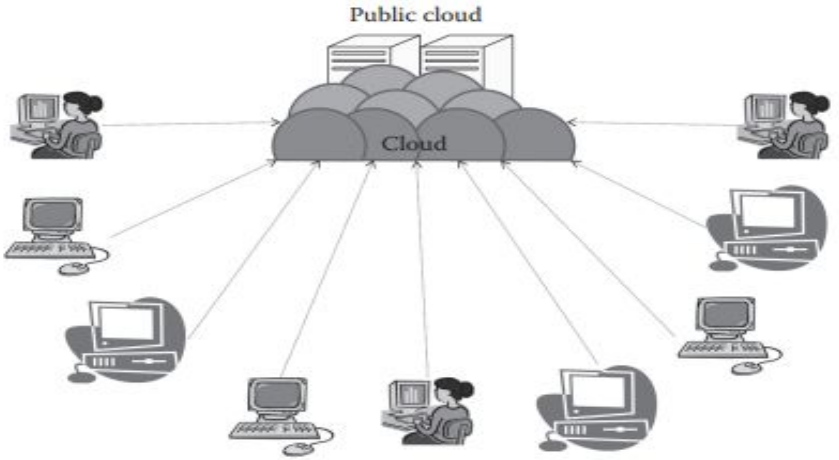


**FIGURE 4.4**
Public cloud.

Characteristics:

- Highly scalable: The public cloud is highly scalable. The resources in the public cloud are large in number and the service providers make sure that all the requests are granted. Hence, the public cloud is considered to be scalable.
- Affordable: The public cloud is offered to the public on a pay-as-you go basis; hence, the user has to pay only for what he or she is using (usually on a per-hour basis). And, this does not involve any cost related to the deployment.

- Less secure: The public cloud is less secure out of all the four deployment models. This is because the public cloud is offered by a third party and they have full control over the cloud. Though the SLAs ensure privacy, still there is a high risk of data being leaked.
- Highly available: The public cloud is highly available because anybody from any part of the world can access the public cloud with proper permission, and this is not possible in other models as geographical or other access restrictions might be there.
- Stringent SLAs: SLA is very stringent in the case of the public cloud. As the service provider's business reputation and customer strength are totally dependent on the cloud services, they follow the SLA strictly and violations are avoided. These SLAs are very competitive.

Suitability (most suitable conditions and environment where this cloud model can be used):

- The requirement for resources is large, that is, there is large user base.
- The requirement for resources is varying.
- There is no physical infrastructure available.
- An organization has financial constraints

The public cloud is not suitable, where the following applies:

- Security is very important.
- Organization expects autonomy.
- Third-party reliability is not preferred.

# Public cloud: Issues

- SLA: the number of users is more and so are the numbers of service agreements. The service provider is answerable to all the users. The users here are diverse. The SLA will cover all the users from all parts of the world. The service provider has to guarantee all the users a fair share without any priority. Having the same SLA for all users is what is usually expected, but it depends on the service provider to have the same SLA for all the users irrespective of the place they are.
- Network: Each and every user getting the services of the cloud gets it through the Internet. The services are accessed through the Internet by all the users, and hence, the service delivery wholly depends on the network. The service provider is responsible for providing proper service to the customer, and once the services are given from the service provider, it goes on in transit to the user. Network management is easier in this case.

- *Performance*: depends on the network and the resources. The service provider has to adequately manage the resources and the network. As the number of users increases, it is a challenging task for the service providers to give good performance.
- *Multitenancy*: The resources are shared, that is, multiple users share the resources, hence the term multitenant. Due to this property, there is a high risk of data being leaked or a possible unprivileged access.
- *Location*: The location of the public cloud is an issue. As the public cloud is fragmented and is located in different regions, the access to these clouds involves a lot of data transfers through the Internet. There are several issues related to the location.
- *Security and data privacy*: Security and data privacy are the biggest challenges in the public cloud. As data are stored in different places around the globe, data security is a very big issue. A user storing the data outside his or her country has a risk of the data being viewed by other people .
- *Laws and conflicts*: The data are stored in different places of the world in different countries. Hence, data centers are bound to laws of the country in which they are located. This creates many conflicts and problems for the service providers and the users.

- *Cloud management*: Here, the number of users is more, and so the management is difficult. The jobs here are time critical, and as the number of users increases, it becomes more difficult. Inefficient management of resources will lead to resource shortage, and user service might be affected. It has a direct impact on SLA and may cause SLA violation.

- *Maintenance*: Maintaining the whole cloud is another task. This involves continuous check of the resources, network, and other such parameters for long-lasting efficient delivery of the service. The resource provider has to continuously change the resource components from time to time. The task of maintenance is very crucial in the public cloud

## Advantages of **Public cloud**

- There is no need of establishing infrastructure for setting up a cloud.
- There is no need for maintaining the cloud.
- They are comparatively less costly than other cloud models.
- Strict SLAs are followed.
- There is no limit for the number of users.
- The public cloud is highly scalable.

## Disadvantages of **public cloud**

- Security is an issue.
- Privacy and organizational autonomy are not possible