Network Security

Professor Gaurav S. Kasbekar

Department of Electrical Engineering

Indian Institute of Technology, Bombay

Week - 12

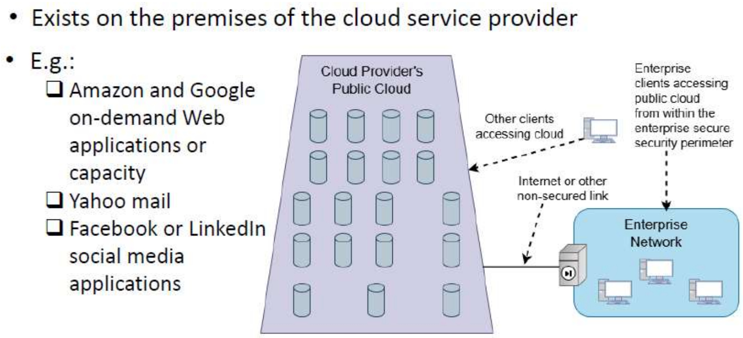
Lecture - 68

Cloud Security: Part 2

Hello, recall that in the previous lecture, we discussed the essential characteristics and service models of cloud computing. We will now continue our discussion on the basics of cloud computing in this lecture. We now discuss cloud deployment models. There are four cloud deployment models, which are shown here at the bottom of this figure. Public cloud, private cloud, hybrid cloud, and community cloud.

So, to summarize this, in a public cloud, the resources of the cloud can be accessed by any organization or any individual. In a private cloud, the resources are private to a single enterprise. This private cloud is either within the premises of the enterprise or it is in a private area of the cloud. Then, community cloud: a set of organizations can access the resources of the cloud. And a hybrid cloud is a composition of two or more of the previous three categories.

That is, public cloud, private cloud, and community cloud. Let's now discuss these four deployment models in detail. We start with the public cloud. The public cloud infrastructure is shown in this figure. This is the public cloud, and the resources of the public cloud can be accessed by individuals or users within an organization or enterprise.



- Exists on the premises of the cloud service provider
- E.g.:
  - ❑ Amazon and Google on-demand Web applications or capacity
  - ❑ Yahoo mail
  - ❑ Facebook or LinkedIn social media applications

Cloud Provider's Public Cloud
Other clients accessing cloud
Enterprise clients accessing public cloud from within the enterprise secure security perimeter
Internet or other non-secured link
Enterprise Network

So, this public cloud infrastructure is made available to the general public and/or to a large industry group. As shown here, some individuals can access the resources of the public cloud, and here one enterprise is shown, and the users within the enterprise access the resources of the public cloud. And this is the security perimeter of the enterprise network, and there is a link from the enterprise network to the public cloud, and over this link the users of the enterprise can access the resources of the public cloud. The public cloud infrastructure is owned by an organization which sells cloud services. There can be different ownership models for a public cloud.

It can be owned, managed, and operated by either a business, academic, or government organization or some combination of these. It exists on the premises of the cloud service provider. So, all these resources, for example, servers, processors, storage, and so on, they exist on the premises of the cloud service provider. So, these are the premises of the cloud service provider in this picture. Some examples of public cloud are as follows.

Amazon and Google on-demand web applications or capacity, Yahoo mail, Gmail, and so on, Rediff mail and so on. And Facebook or LinkedIn social media applications. These are all examples of public cloud. The advantages of public clouds are the following. Public clouds are inexpensive, and they can scale to meet needs.

So, that's why they are accessible to a large number of users because they are not costly. And they can also be easily scaled to meet needs. Since the resources of the public cloud provider are shared by a lot of users, if the provider finds out that there is often a shortage of resources, in that case it can add resources to the cloud. So, that way it can scale up the resources. But there are some downsides of public cloud.

One limitation is that public clouds do not provide service level agreements, or they provide lower service level agreements as compared to private or hybrid cloud offerings. And they also may not offer the guarantee against data loss or corruption of the kind that are provided by private or hybrid cloud offerings. So, these are some limitations of public cloud compared to private or hybrid clouds. Another limitation is that they do not necessarily provide for compliance with privacy laws, and privacy remains the responsibility of the subscriber or corporate end user. So, the data of all the users is present in a single area, and hence privacy can be breached.

So, from the point of view of privacy, public cloud is not as good as some of the other solutions, such as private cloud and hybrid cloud. So, we now discuss private cloud. It is implemented within the internal IT environment of the organization. So, by this we mean logically it is implemented within the internal IT environment, but physically it may be present in the premises of a cloud provider, or it may be within the enterprise security perimeter. So, the organization may choose to manage the cloud in-house, that is, within the campus of the enterprise which is using the private cloud, or the organization may contract the management function to a third party.

Cloud servers and storage devices may exist on-premise—that is, within the campus of the enterprise which is using the private cloud—or off-premise, typically within the premises of a cloud provider. Some examples of services delivered through private clouds are as follows. One is database on demand, then email on demand, and storage on demand. So, these are some examples of services that are delivered through private clouds. So, we mentioned that there are two typical private cloud configurations.

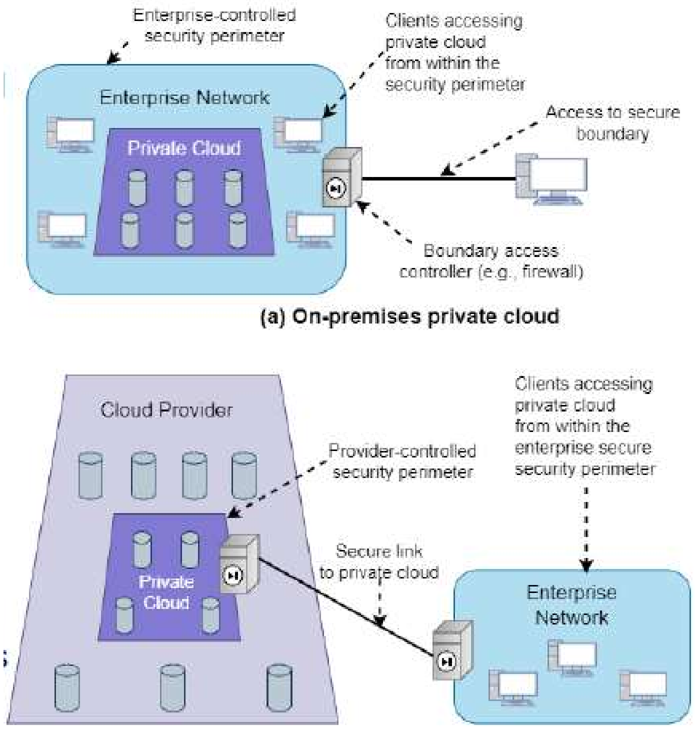
These are shown in this picture. The first one is an on-premise private cloud. This is the enterprise network and the private cloud, which includes all the servers, processors, and other cloud resources. This private cloud is present within the premises of the enterprise itself. So, users within the enterprise network's security perimeter, which is shown here, they can securely connect to the private cloud since it is within the security perimeter.

But often some users of the enterprise need to connect to the private cloud from outside the security perimeter. For example, they may be working from home, traveling, and so on. So, such a user is shown here. There is typically a secure link, for example, based on VPN, between the user who is outside the security perimeter and the private cloud, and they connect to the private cloud via this secure link, such as VPN. So, this is the first solution where the private cloud resources are present within the enterprise security perimeter.

This is the other possibility: outsourced private cloud, where this is the enterprise network and the security perimeter of the enterprise network is shown here. In this case, the private cloud is within the resources of a cloud provider. So, some part of the cloud provider's resources are used for providing this private cloud to the enterprise network. There is a secure link to the private cloud as shown here. So, this may be via VPN, for example.

And this is the provider-controlled security perimeter, which is shown here. And this is the private cloud. So, let's now discuss these two options in some more detail. In the case of on-premises private cloud, which is shown in the first picture here, it consists of an interconnected collection of servers and data storage devices, which host enterprise applications and data. So, these are located within the premises of the enterprise.

Local workstations have access to cloud resources from within the enterprise security parameters. Such local workstations are shown here. These are some examples of these local workstations. As we mentioned, there can also be remote users like this one. For example, they may be working from other branches of the same enterprise.


Enterprise-controlled security perimeter
Clients accessing private cloud from within the security perimeter
Enterprise Network
Private Cloud
Access to secure boundary
Boundary access controller (e.g., firewall)
Cloud Provider
Provider-controlled security perimeter
Clients accessing private cloud from within the enterprise secure security perimeter
Private Cloud
Secure link to private cloud
Enterprise Network

(a) On-premises private cloud

(b) Outsourced private cloud

For example, this private cloud may be in Mumbai, but there may be some users who are working in the Bangalore branch of the same corporation. They will connect securely via some solution like VPN to the private cloud resources. So, from satellite offices, users working from home, traveling, and so on, they have access through a secure link such as a VPN. That secure link is shown here. Then the other solution is shown in Figure (b), that is the outsourced private cloud.

Here, the cloud provider establishes and maintains the private cloud. So, the private cloud is shown here within the perimeter of the cloud provider's resources. It consists of dedicated infrastructure resources not shared with other cloud provider clients. So, that's a crucial aspect of a private cloud. These resources of the private cloud, they are not accessible to other users of the cloud provider.

Hence, that enhances the privacy of this solution as compared to a public cloud. And typically, there is a secure link between boundary controllers. For example, a dedicated lease line or VPN over the internet. So, these are the boundary controllers, and this is the secure link. It can either be a VPN link, or there can be a dedicated communications link that is leased out from some telecom provider.

So, this secure link provides communication between enterprise client systems and the private cloud. So, this is the enterprise network, and there is a secure link between the enterprise network and the private cloud. So, that was the second deployment model, that is private cloud. We now discuss the third deployment model, that is community cloud. So, it shares the characteristics of private and public clouds.

Like a private cloud, it has restricted access. But like a public cloud, the cloud resources are shared among a number of independent organizations. So, the word 'community' here refers to the fact that there is a community of independent organizations, all of whom can access the resources of the cloud. So, unlike a private cloud, it is not restricted to the users of a single enterprise, but the cloud resources are shared among a number of independent organizations. So, that's the word 'community'.

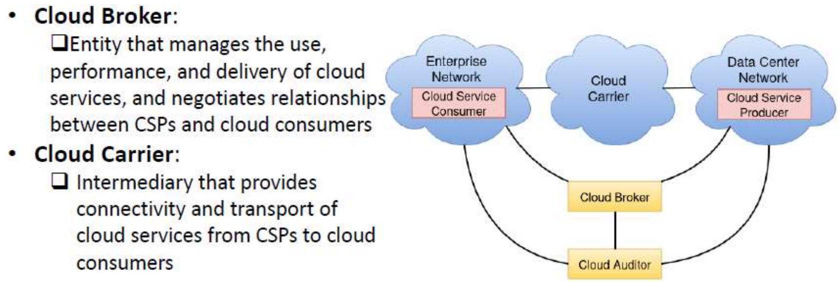
The organizations that share the community cloud have similar requirements and typically need to exchange data with each other. So, it's quite convenient; the fact that the resources of the cloud are at a single place and these resources can be accessed by any of the organizations in this community. So, they can easily exchange data with each other. An example is the healthcare industry, which uses the community cloud concept. So, for example, a lot of hospitals and other healthcare industry units, they may connect to the same community cloud and use its resources.

So, this is useful for sharing medical data among the different units that connect to the community cloud in the healthcare industry context. So, this was the third deployment model, that is, community cloud. We now discuss the fourth one, that is, hybrid cloud. It is a composition of two or more clouds: private, community, or public. So, what kind of composition is this?

So, these two or more clouds remain unique entities. But they are bound together by standardized or proprietary technology that enables data and application portability. For example, for load balancing between clouds. So, there are two or more clouds within this hybrid cloud, and there can be sharing between these different clouds. For example, for load balancing, data or processing may be moved from one of the clouds to the other cloud within the same composition of clouds, which constitutes the hybrid cloud.

Sensitive information can be placed in a private area of the cloud, and information which is not so sensitive can be placed in the public area of the cloud. So, this is our brief review of the hybrid cloud, which is the fourth kind of deployment model. So, that concludes our review of the different deployment models in cloud computing, namely public cloud, private cloud, community cloud, and hybrid cloud. We will now discuss the cloud computing reference architecture. So, in a typical scenario where cloud computing is used by some users, what are the different entities in the scenario?

So, there are five different entities which are shown in this figure. These are cloud service consumer, cloud service provider, cloud carrier, cloud broker, and cloud auditor. So, cloud service provider is the provider of the cloud resources. Cloud service consumers are the users or organizations which use the resources of the cloud. Then cloud carrier are the networking resources which transport the services of the cloud to the cloud service consumers.



- **Cloud Broker**:
  - ❑Entity that manages the use, performance, and delivery of cloud services, and negotiates relationships between CSPs and cloud consumers
- **Cloud Carrier**:
  - ❑ Intermediary that provides connectivity and transport of cloud services from CSPs to cloud consumers

Cloud brokers they add some value added services to the services of the cloud and they can also aggregate different clouds together and provide the resources of the aggregate to the cloud service consumers and cloud auditors are like other auditors; they examine the cloud service provider services and check them for security, privacy, performance, and other parameters. So, let’s discuss these five different parts of the cloud computing architecture in detail. So, these five are listed here. So, cloud service customer is a person or organization that maintains a business relationship with and uses the services from cloud providers that is shown here in this picture. Then cloud service provider is a person, organization, or entity responsible for making a cloud service available to interested parties.

So, that is shown over here. So, this can be of different types, which we studied earlier. Public cloud, private cloud, community cloud, or hybrid cloud. Then we have cloud auditor, which is shown over here. So, this is a party that can conduct independent assessment of cloud services, information system operations, performance, and security of cloud implementation.

So, in general, an auditor performs such an assessment of the party whom it is auditing. So, in the case, a cloud auditor performs assessment in terms of all these parameters, such as performance and security. Then we have cloud broker. It's an entity that manages the use, performance, and delivery of cloud services and negotiates relationships between CSPs and cloud consumers. It may add some evaluated services to the services of the cloud, and also it may aggregate different cloud services.

Then finally we have cloud carrier, which is shown over here. It's an intermediary that provides connectivity and transport of cloud services from the CSPs to the cloud consumers. A cloud carrier is typically some resources provided by the telecom operator. They provide a secure link, for example, between the cloud service provider and the cloud service consumer. So, this secure link with a certain amount of predetermined bandwidth.

So, that constitutes the cloud carrier. Now, out of these, let's study some of these in some more detail. So, we study these three, Cloud Carrier, Cloud Broker, and Cloud Auditor, in some more detail. Cloud Carrier is a networking facility. It consists of routers and communication links.

This networking facility provides connectivity and transport of cloud services between CSCs and CSPs. Typically, a CSP will set up service level agreements with a cloud carrier to provide services consistent with the level of SLAs offered to the CSCs. For example, the service level agreement may say that the cloud service provider has to provide a certain service within a certain delay guarantee. Then, clearly, the cloud carrier must transport the cloud services within that delay guarantee or within a delay that is more stringent than that guarantee. So, this is an example where these SLAs are consistent with the level of SLAs offered to the CACs by the cloud provider.

Then we discuss cloud broker in some more detail. A cloud broker is useful when cloud services are too complex for a cloud consumer to easily manage. The following are examples of areas of support that can be offered by cloud brokers. One is service intermediation. Here, the broker provides some value-added services such as identity management, performance reporting, and enhanced security.

There are the raw services provided by the cloud service provider, but the cloud broker provides some additional add-ons or evaluated services to the raw services. These include identity management, that is, managing the identities of different users and organizations using the cloud services, and performance reporting and announce security. These are enhanced services provided by the cloud broker. Another area of support that may be offered by cloud broker is this service aggregation, where the broker combines multiple cloud services to meet consumer needs not addressed by a single cloud service provider or to optimize performance or minimize cost. The cloud broker may be connected to multiple cloud service providers, and it may aggregate their services.

Hence, the users have access to a wider set of available resources. They don't have access to a single cloud's resources but to the resources of multiple clouds, so they can get better service. So, the performance is optimized, and the cost may be minimized. Then, finally, we have Cloud Auditor. It can evaluate the services provided by the cloud service provider in terms of various parameters, such as security controls, privacy impact, performance, and so on.

The auditor is an independent entity that can assure that the CSP conforms to a set of standards. So, there are some standardization organizations which specify some standards that cloud service providers must satisfy. So, the auditors are independent entities that can ensure the CSP conforms to the set of specified standards. So, this concludes our discussion of the cloud computing reference architecture. So, in summary, we discussed the different cloud deployment models, including public cloud, private cloud, hybrid cloud, and community cloud.

And we discussed the cloud computing reference architecture and the different actors within the reference architecture. This concludes our review of the basics of cloud computing. In the next lecture, we'll discuss cloud computing security. Thank you.