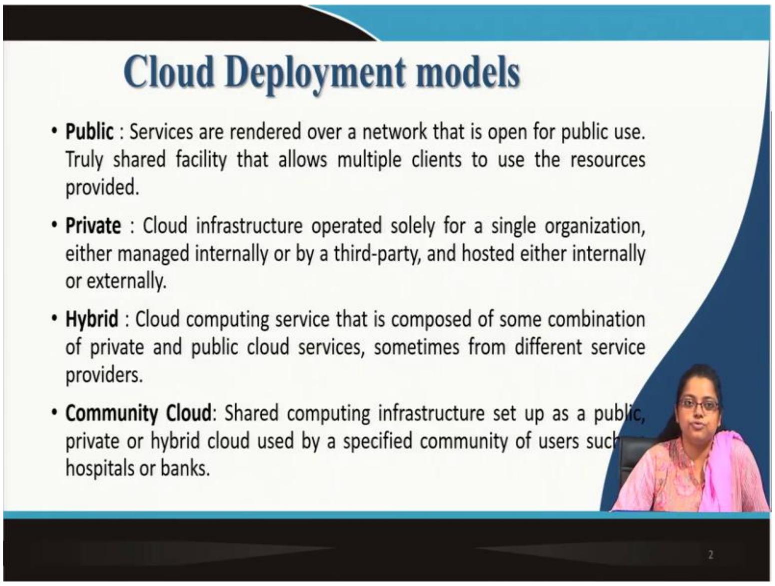
Management Information System
Prof. Saini Das
Vinod Gupta School of Management
Indian Institute of Technology, Kharagpur

Module – 09
Emerging Technologies Cloud Computing Part - II
Lecture – 41
Cloud Computing Part - II

Hello, so we are in module-9! And in the previous lecture, we had discussed about Cloud Computing. So, we in this particular module, in fact, we are going to discuss 'Emerging Technologies' as I had already mentioned. So, we had begun with 'cloud computing' and in the previous session, we had discussed about the differences between cloud computing architecture and traditional computing architecture.

And we had also spoken about the advantages of cloud computing over traditional computing. We had also discussed about the various cloud service models. So, today we will be dedicating this entire session to cloud deployment models.

(Refer Slide Time: 01:07)



Cloud Deployment models

- **Public** : Services are rendered over a network that is open for public use. Truly shared facility that allows multiple clients to use the resources provided.
- **Private** : Cloud infrastructure operated solely for a single organization, either managed internally or by a third-party, and hosted either internally or externally.
- **Hybrid** : Cloud computing service that is composed of some combination of private and public cloud services, sometimes from different service providers.
- **Community Cloud**: Shared computing infrastructure set up as a public, private or hybrid cloud used by a specified community of users such hospitals or banks.

So, what are the different cloud deployment models? The first one is public cloud. In essence, public cloud is what you know whenever the word cloud computing is mentioned, public cloud is essentially a true representation of what cloud computing is.

So, public in public cloud services are rendered over a network that, is open for public use. It is truly shared facility that allows multiple clients to use the resources provided.

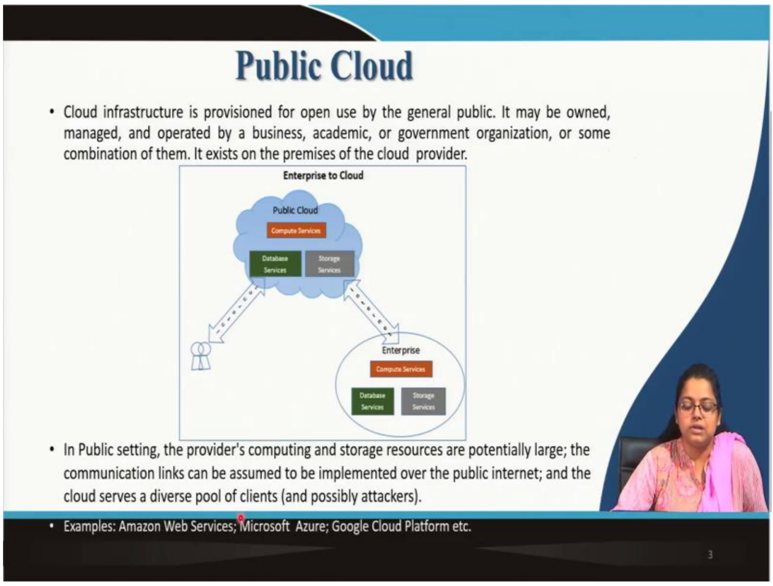
We will be discussing about further details about each of these deployment models in the subsequent slides. To move ahead with the different cloud deployment models, the next model is related to private cloud. So, a private cloud is very different from what a public cloud is, because it is solely operated for a single organization. It could be managed internally or by a third party and hosted either internally or externally.

But, the major difference between a private cloud and a public cloud is that public cloud is shared the services are shared between multiple clients, whereas in private cloud the cloud infrastructure is available only for a single organization or a single client. So, moving ahead there is the third category of cloud deployment model which pertains to hybrid cloud which is could be a combination some sort of a combination of private and public clouds, sometimes from different service providers also.

So, the public cloud could be provided by a particular service provider, whereas the private cloud could be provided by a totally different service provider that is also a very very feasible scenario. Moving ahead the fourth category is community cloud which is a shared computing infrastructure setup as either a public, private or hybrid cloud used by a specified community of users, this is very important.

The term community cloud itself suggests that this particular cloud is available for use by but you know a community of users with certain specified specific interests in mind, such as hospitals, banks, research communities. So, they could have their own community clouds for a specific purpose. So, these are the four different cloud deployment models which we will study in detail in the subsequent sessions, side, slides.

(Refer Slide Time: 03:57)



Public Cloud

- Cloud infrastructure 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.

- In Public setting, the provider's computing and storage resources are potentially large; the communication links can be assumed to be implemented over the public internet; and the cloud serves a diverse pool of clients (and possibly attackers).
- Examples: Amazon Web Services; Microsoft Azure; Google Cloud Platform etc.

3

So, to begin with public cloud. This is a cloud; this cloud infrastructure 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. So, a public cloud exists on the premises of the service provider as you can see in this particular diagram here.

So, this suggests that here we have the public cloud infrastructure and it can it is shared. So, it is available to multiple individuals. Here we see multiple individuals. Here we see an enterprise there could be multiple enterprises which are availing the services of this particular public cloud.

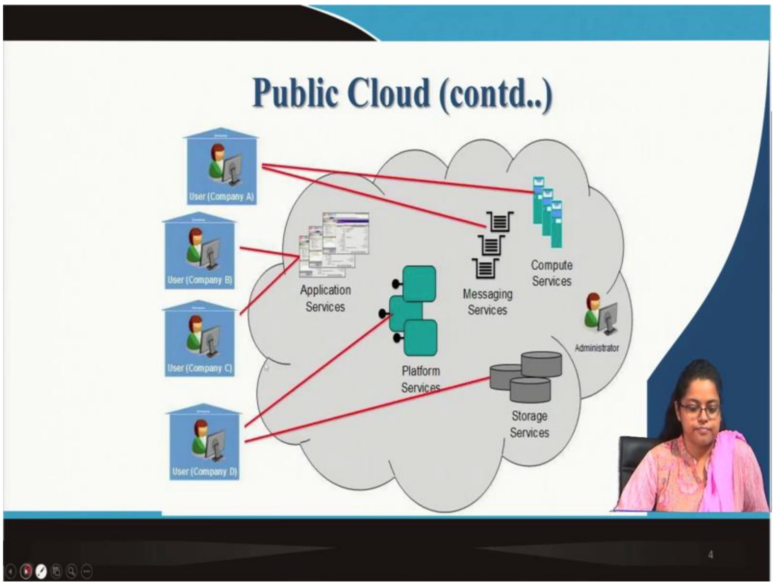
In public setting, the providers computing and storage resources are potentially large, of course, it has to be because it has to be shared between multiple-multiple clients. The communication links can be assumed to be implemented over the public internet, and the cloud serves a diverse pool of clients and possibly attackers.

Why this is mentioned is? It is quite possible that among the diverse pool of clients who are availing the services of a public cloud, there could be two competitors, or there could be you know some attackers or hackers who are there with the malicious intent.

They are availing the services of the public cloud in order to, you know, sneak into particular organizations' data and processing and in order to steal or hack there, you know, network or their infrastructure.

So, that is possible with the public cloud if appropriate precautionary measures are not taken by the service provider. So, we will talk about this in detail in the subsequent slides.

(Refer Slide Time: 06:09)

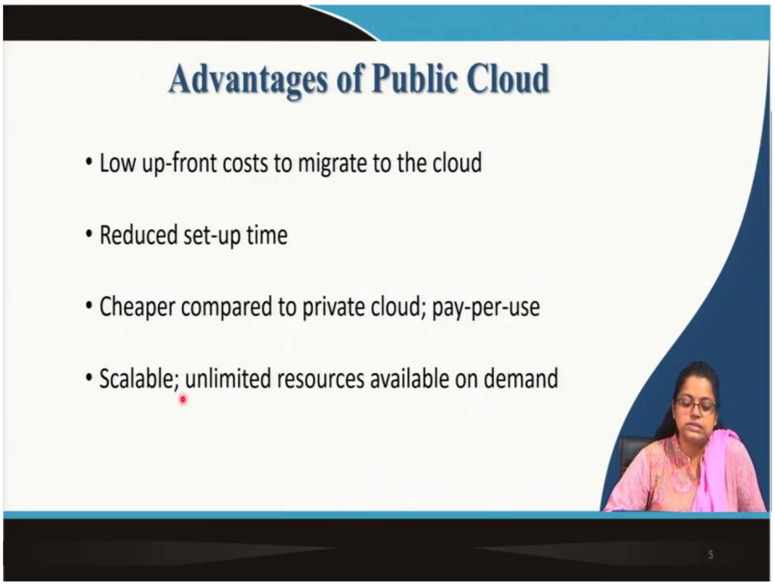


Public Cloud (contd..)

Now, examples of public cloud are Amazon Web Services, Microsoft Azure, Google Cloud Platform. So, all of them have their own public cloud services. Now, this again is a representation of the public cloud that we have just spoken of.

So, there are multiple users who could be individuals or multiple companies. And, they are all availing services of one particular public cloud provided by a particular service provider. So, different types of services could be availed by different entities here.

(Refer Slide Time: 06:34)



Advantages of Public Cloud

- Low up-front costs to migrate to the cloud
- Reduced set-up time
- Cheaper compared to private cloud; pay-per-use
- Scalable; unlimited resources available on demand

Moving on advantages of public cloud. So, most of the since I mentioned in the beginning of the session that a public cloud is a typical representation of you know of cloud computing, what cloud compute computing stands for. Therefore, most of the advantages have already been discussed when I was talking about the advantages of cloud computing per se overall.

So, some of them again to reiterate low up-front cost to migrate to the cloud, of course, because the client does not need to have any infrastructure on his or her premises. The infrastructure entirely lies with the public cloud which is already there, and now it has to be designated to the client alone.

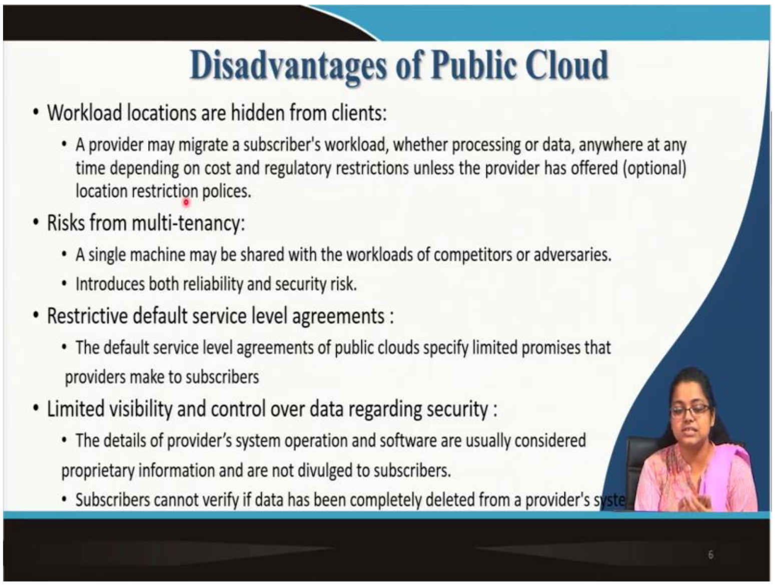
So, designation take certain amount of time other than that no time required to set up the entire infrastructure. So, the up-front you know the setup time as well as the cost both are minimal.

So, we are covering here the first two points. The time required and the costs are absolutely minimal because we have discussed that you know public cloud does not require any infrastructure. So, it is treated more of an opex rather than a capex. So, both cost as well as time required to set up the infrastructure is minimal.

Again cheaper than private cloud; we have already mentioned this. So, because we go on a pay per use or a pay as you go basis. So, the amount that you consume, you pay only for that and not the rest compared to a private cloud. The scenario pertaining to private cloud we will discuss in a later slide.

And finally, scalable, so because you are simply availing the services of a service provider it is scalable and unlimited resources are available on demand. So, as your demand increases or decreases, you know you can procure resources as per your requirement of the cloud. Therefore, it is scalable. So, these are the advantages of public cloud.

(Refer Slide Time: 08:36)



Disadvantages of Public Cloud

- Workload locations are hidden from clients:
  - A provider may migrate a subscriber's workload, whether processing or data, anywhere at any time depending on cost and regulatory restrictions unless the provider has offered (optional) location restriction polices.
- Risks from multi-tenancy:
  - A single machine may be shared with the workloads of competitors or adversaries.
  - Introduces both reliability and security risk.
- Restrictive default service level agreements :
  - The default service level agreements of public clouds specify limited promises that providers make to subscribers
- Limited visibility and control over data regarding security :
  - The details of provider's system operation and software are usually considered proprietary information and are not divulged to subscribers.
  - Subscribers cannot verify if data has been completely deleted from a provider's syste

6

Now, coming to the disadvantages. Let us spend some time on them. Workload locations are hidden from the client. What this means is a provider may migrate to a subscribers migrate a subscribers workload could be processing could be data, anywhere at any time. So, it means that you know at any point in time or the data of a particular client can be migrated to any location depending on cost, depending on that particular geographies regulatory restrictions and several other factors.

So, this is a disadvantage because as a client you may not be aware of where your organizations workloads are stored on the cloud. So, that is that might be a disadvantage unless the provider has offered some location restriction policies which are rare.

The second disadvantage arises from multi tenancy, because a single machine is shared with the workloads of competitors or adversaries there could be the risk a lot of risk related to reliability and security. So, as we had mentioned it is quite possible that your workloads are shared with your adversaries who may have a malicious intent in mind.

So, they may you know in turn you know take avail the services of a hacker, and they could try to hack into your organization’s data or organization’s infrastructure in order to commit some malicious activities therein. At the same time if there could be a reliability risk also. So, because of multi tenancy there could be certain problems, as there are multiple clients you know the services may also be unreliable at times.

The third point here, third disadvantage is related to restrictive default service level agreements. What this means is you know the default service level agreements of public cloud specify limited promises that providers make to subscribers. So, providers make only limited promises to subscribers, and subscribers have to abide by that. They cannot demand more services because public service cloud service providers generally have some a set of you know service level agreements which are standardized.

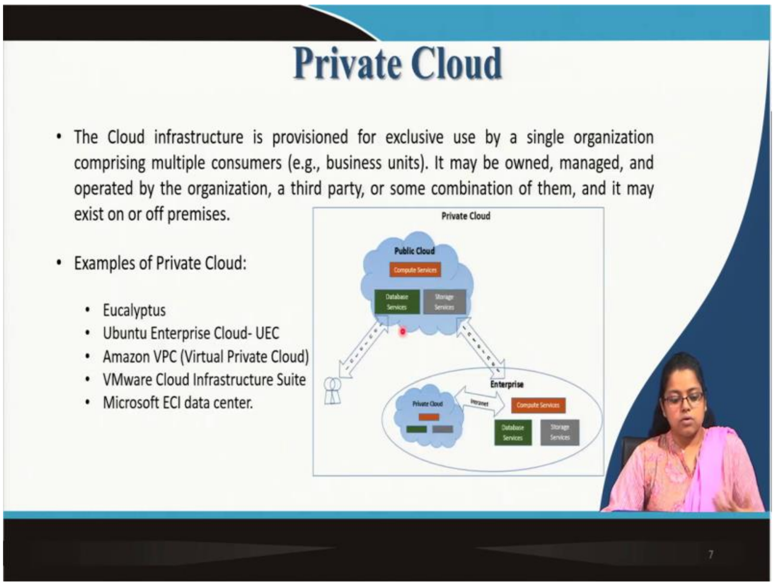
So, standardized level of set of service level agreements available to all subscribers. Generally, customized SLAs are difficult to obtain. So, of course, they the clients have to do with some default service level agreements that could be a problem if they want specialized service level agreements from a provider.

Finally, limited visibility and control over data secure data regarding security, of course, we had discussed this earlier also. But, the problem becomes even more intense because the details of the provider system operation and software are usually considered proprietary information and are not divulged to subscribers. So, subscribers do not have much information about their data or the software that the provider is using or the system operations of the provider.

So, more or less the subscribers are left in the dark. So, there, there is limited control and also limited visibility. Moreover, if you know as a subscriber you want to stop availing the services of a provider and you would want to maybe have your own on premise applications or you would want to switch to a another provider, you it is very difficult for you to verify that your data that resided with the particular service provider has been completely deleted.

So that can create a problem because your data may remain in the provider systems, and you may not even be aware of it that may give rise to a lot of issues because that can lead to a data theft, data misuse, data mishandling, and your data can go into the hands of unauthorized entities. So, that is something that has to be taken care of.

(Refer Slide Time: 13:04)



Private Cloud

- The Cloud infrastructure 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.
- Examples of Private Cloud:
    - Eucalyptus
    - Ubuntu Enterprise Cloud- UEC
    - Amazon VPC (Virtual Private Cloud)
    - VMware Cloud Infrastructure Suite
    - Microsoft ECI data center.

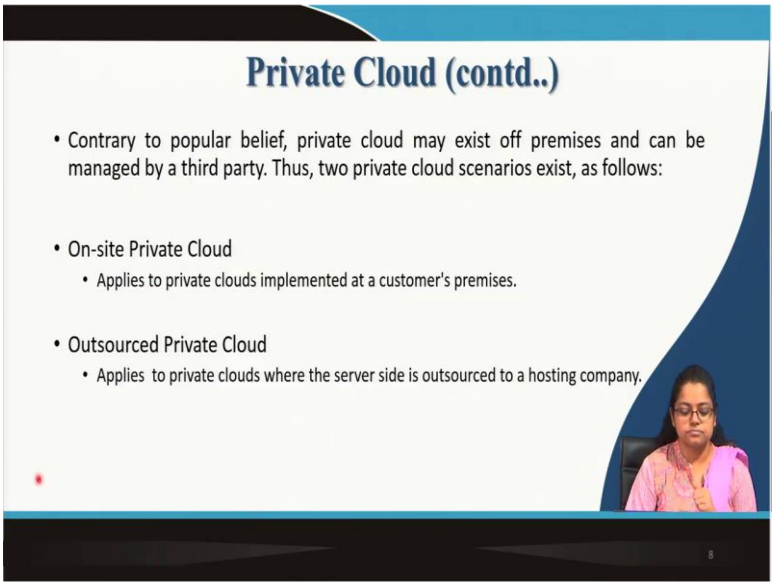
Now, we have spoken detail about the advantages and disadvantages of private cloud public cloud. So, moving on to private cloud, the cloud infrastructure is provisioned for exclusive use by a single organization; contrary to that in case of a public cloud provider, where the cloud infrastructure could be shared by multiple parties or multiple clients. Here it is provision for exclusive use by a single organization comprising multiple consumers.

So, there could be multiple business units within one particular organization, and all of them could be availing the services of a particular private cloud. But the private cloud service is available to an only a single organization. It may be owned managed and operated by the organization, a third party or a combination of them. And, it may exist on or off premises. It could also exist off premises.

This is exactly what is represented in this particular diagram here. So, please have a look at this. Now, this particular private cloud cannot be accessed by any other person other than only this enterprise. So, or so any business unit residing within the enterprise can avail the services of the private cloud, but nobody from outside can.

So, some popular examples of private cloud are Eucalyptus very popular one, Amazon Virtual Private Cloud, VMware Cloud infrastructure Suite, Microsoft data center ECI data center. So, all of them have their own dedicated private cloud services.

(Refer Slide Time: 14:51)



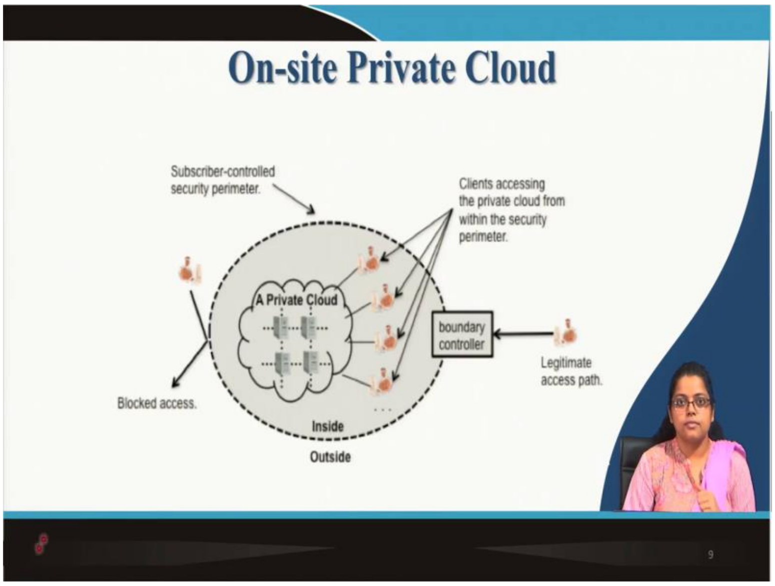
Private Cloud (contd..)

- Contrary to popular belief, private cloud may exist off premises and can be managed by a third party. Thus, two private cloud scenarios exist, as follows:
- On-site Private Cloud
  - Applies to private clouds implemented at a customer's premises.
- Outsourced Private Cloud
  - Applies to private clouds where the server side is outsourced to a hosting company.

Moving on so this is a very interesting thing that I want to discuss here, interesting point, contrary to popular belief, private cloud may exist off premises and can be managed by a third party. We generally have the perception that private clouds reside within an organization organizations premises, but a private cloud could also be could also exist off premises, and could be managed by a third party.

Therefore, two distinct private cloud scenarios exist as follows. On-site private cloud which applies to private clouds implemented at customer’s premises, of course, on-site so within the customer’s premises. And outsourced-private cloud which applies to private clouds where the service side is outsourced to a hosting company. So, here this is outsourced, but nonetheless it is a private cloud because it is available for use only by a single organization.

(Refer Slide Time: 16:01)

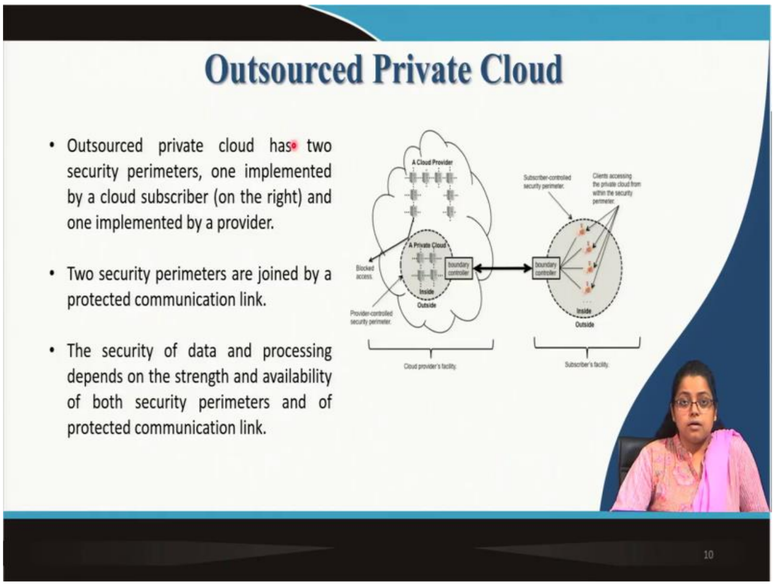


On-site Private Cloud

Subscriber-controlled security perimeter.
Clients accessing the private cloud from within the security perimeter.
A Private Cloud
boundary controller
Legitimate access path.
Blocked access.
Inside
Outside
9

So, this is a diagrammatic representation of what we have discussed regarding an on-site private cloud. Here we see the private cloud resides within the premises of the organization. And this is the security perimeter of the organization, and see subscriber control security perimeter which is controlled by the subscriber. And we see that any third party from outside is unable to access the private cloud.

(Refer Slide Time: 16:32)



Outsourced Private Cloud

- Outsourced private cloud has two security perimeters, one implemented by a cloud subscriber (on the right) and one implemented by a provider.
- Two security perimeters are joined by a protected communication link.
- The security of data and processing depends on the strength and availability of both security perimeters and of protected communication link.

A Cloud Provider
Subscriber-controlled security perimeter.
Clients accessing the private cloud from within the security perimeter.
A Private Cloud
boundary controller
Blocked access.
boundary controller
Inside
Outside
Provider-controlled security perimeter.
Inside
Outside
Cloud provider's facility.
Subscriber's facility.
10

Now, coming to outsourced-private cloud that we have just discussed. Outsourced-private cloud has two they have has two security perimeters. One implemented by the cloud subscriber as we see here; one is implemented by the cloud subscriber and is available within the, you know, the premises just outside the organizations' premises, and the other because this is outsourced, it is available within the cloud providers' facility. So, this is a security parameter.

And the two security parameters, one that is within the subscribers' facility and the other that is within the cloud providers' facility, both of them are joined by a protected communication link that we see here. This is the protected communication link. The security of data and processing depends on the strength and availability of both security perimeters, and of course, of the protected communication link.

So, security of data relies on both. The security of the perimeter within the cloud provide us facility and the perimeter within the subscribers' facility as well as the security of the communication link. Now, this is very important because if there is a problem here then there would be a it could be compromised very easily.

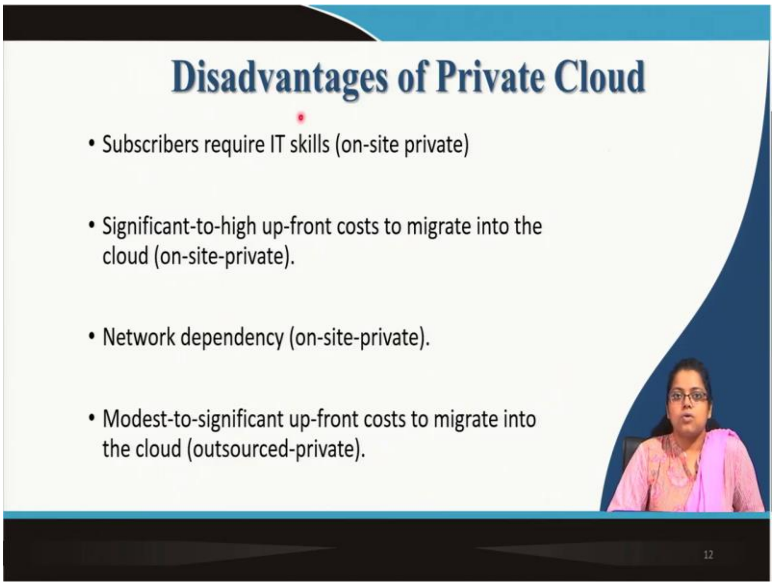
(Refer Slide Time: 18:00)

Advantages of Private Cloud

- Potentially strong security from external threats (both on-site and outsourced private)

Now, moving on advantages of private cloud of course as we have seen private cloud is available to only one service to only one client. So, it is it has potentially strong security from external threats. It, cannot be compromised by others who are also availing the same services. So, it has much more security both on-site and outsourced-private cloud, of course, on-site private cloud has much more security compared to outsourced-private cloud as we have seen before.

(Refer Slide Time: 18:34)



Disadvantages of Private Cloud

- Subscribers require IT skills (on-site private)
- Significant-to-high up-front costs to migrate into the cloud (on-site-private).
- Network dependency (on-site-private).
- Modest-to-significant up-front costs to migrate into the cloud (outsourced-private).

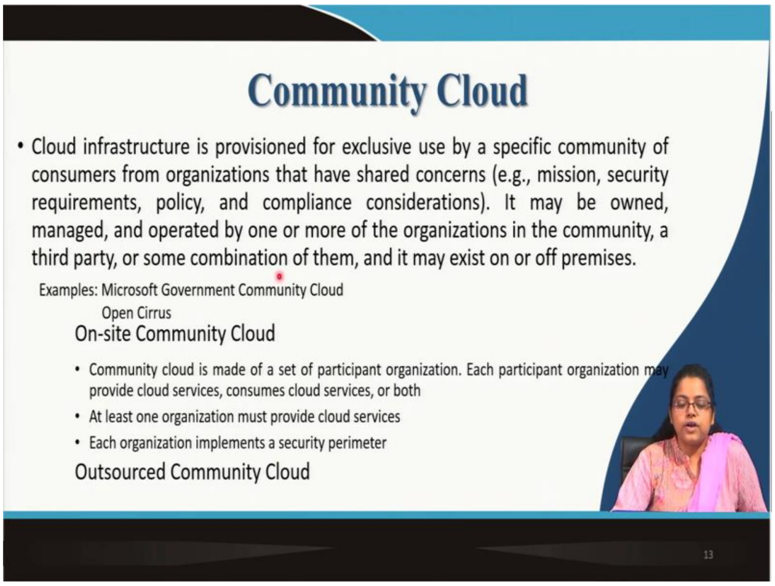
Now coming to disadvantages of private cloud, subscribers require IT skills especially in case of on-site private cloud because within the premises the organization has to maintain its own setup of private cloud and has to maintain the security perimeter also. Therefore, subscribers require in house IT skills.

Now, significant to high up-front cost to migrate to the cloud again in case of on-site private cloud because you have to again set up the infrastructure within your premises network dependency again in case of onsite private cloud it is highly dependent on the network availability within your premises, but all of these are not relevant for outsourced-private clouds.

But the major problem with respect to outsourced-private cloud is as we have mentioned in the previous slide, there are security risks which are subsequently significantly higher compared to that in case of a on-site private cloud. And also there are modest to significant up-front cost to migrate into the cloud.

So, because though it is completely outsourced, there will be you have to maintain the communication link between your organization and the provider cloud provider, you also have to maintain some amount of security in your premises. So, as a result these are all the disadvantages of private cloud. Some of them pertain entirely to on-site private cloud, and the rest are relevant for outsourced-private cloud.

(Refer Slide Time: 20:14)



Community Cloud

- Cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be owned, managed, and operated by one or more of the organizations in the community, a third party, or some combination of them, and it may exist on or off premises.

Examples: Microsoft Government Community Cloud
Open Cirrus

On-site Community Cloud

- Community cloud is made of a set of participant organization. Each participant organization may provide cloud services, consumes cloud services, or both
- At least one organization must provide cloud services
- Each organization implements a security perimeter

Outsourced Community Cloud

13

Moving on coming to the third category of cloud, the deployment model community cloud. So, this is a cloud infrastructure which is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns.

So, the shared concerns could be a particular mission that you are pursuing, it could be a security requirements, it could be due to certain policy requirements or maybe compliance conditions that you want to be a part of a certain community and avail the services of that community cloud.

It can also pertain to people with special interest, for example, a healthcare organizations together could have you know certain hospitals together could have one community cloud where they could interchange or exchange information, group of banks or financial institutions could have a community cloud.

So, we have already discussed this before. So, community clouds may be owned managed and operated by one or more of the organizations in the community or a third party, and a third party altogether, or maybe some combination of them.

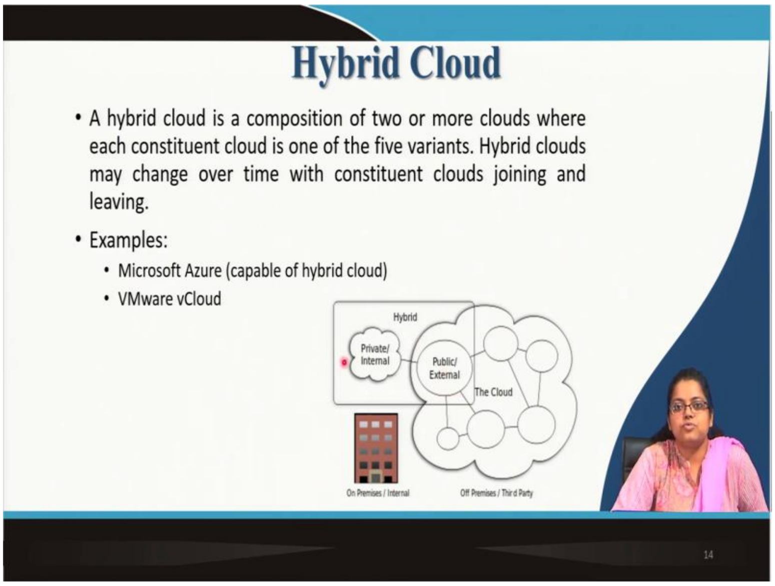
And it may exist on or off premises. Now, some popular examples are Microsoft Government Community Cloud which is used by governments to share you know some of their best practices. Open Cirrus, Open Cirrus is a community cloud which pertains to the research community.

So, it has a lot of subscribers such as you know who pursue some joint research endeavours such as there are some very large IT players who are members of this; Intel is there; HP is a part of this; then there are universities who are a part of Open Cirrus, Carnegie Mellon University for example is one which is a part of Open Cirrus though it is maintained by them also. So, this community cloud is used for mission so mission critical research projects.

Now, coming to on-site community cloud, this community cloud is made of a set of participant organization. Each participant organization may provide cloud services consumer cloud services or both. At least one organization must provide the cloud services, and each organization implements a security perimeter.

So, as we have mentioned earlier that you know if there is a loophole in any of the organizations which are implementing the cloud that entire cloud can be breached by a malicious entity. Therefore, each organization has to be very careful when the organization decides to implement a security perimeter. And then outsourced community cloud is again entirely outsourced to a third party.

(Refer Slide Time: 23:15)



Hybrid Cloud

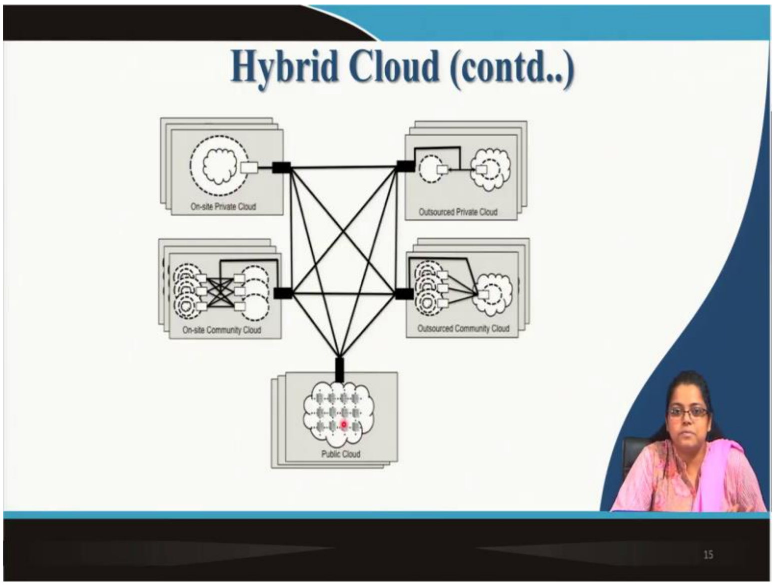
- A hybrid cloud is a composition of two or more clouds where each constituent cloud is one of the five variants. Hybrid clouds may change over time with constituent clouds joining and leaving.
- Examples:
  - Microsoft Azure (capable of hybrid cloud)
  - VMware vCloud

The last category of cloud deployment model that we will discuss today is related to the hybrid cloud. A hybrid cloud is a combination of two or more clouds, where each constituent cloud is one of the five variants. Why five variants? We will talk about it in the next slide.

Hybrid clouds may change over time with constituent clouds joining or leaving, so this could be a major problem with hybrid clouds, because if today there the hybrid cloud is made up of a private cloud and a public cloud. If the organization decides that you know the organization requires a lot more security they can entirely move to up to the private cloud and so the hybrid cloud now becomes a private cloud or it could be vice versa.

So, hybrid clouds are generally volatile and they change over time, which creates some issues related to management of hybrid clouds. Some popular examples of hybrid clouds are Microsoft Azure is capable of hybrid cloud, VMware vCloud is a hybrid cloud. So, this is the diagrammatic representation of a hybrid cloud where this hybrid cloud is made up of a combination of a public and a private cloud.

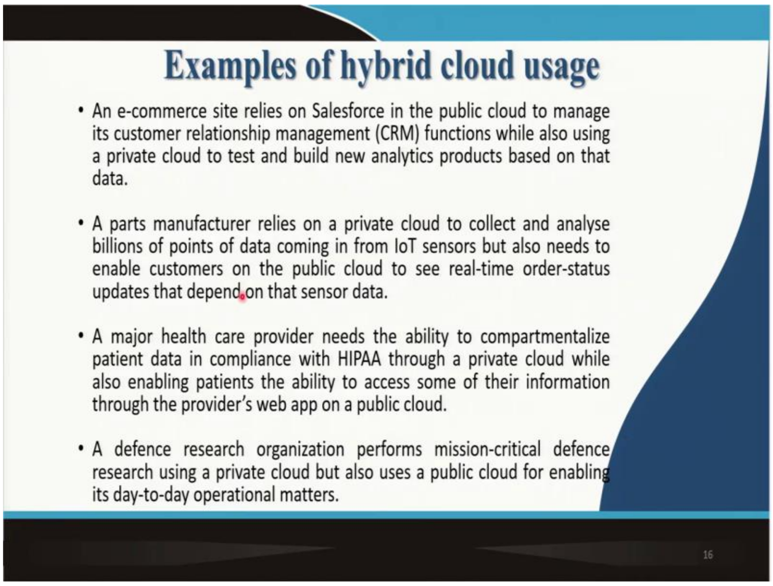
(Refer Slide Time: 24:41)



Hybrid Cloud (contd..)

So, in the previous slide, we have mentioned that a hybrid cloud could be a combination of any of these five categories of clouds. So, you know it could be a combination of one or more of these five categories of clouds that we have discussed in the previous slide. So, it could either be a public cloud, an on-site private cloud, outsourced-private cloud, on-site community cloud, or outsourced community cloud. So, any possible combination out of these five could be a hybrid cloud.

(Refer Slide Time: 25:18)



Examples of hybrid cloud usage

- An e-commerce site relies on Salesforce in the public cloud to manage its customer relationship management (CRM) functions while also using a private cloud to test and build new analytics products based on that data.
- A parts manufacturer relies on a private cloud to collect and analyse billions of points of data coming in from IoT sensors but also needs to enable customers on the public cloud to see real-time order-status updates that depend on that sensor data.
- A major health care provider needs the ability to compartmentalize patient data in compliance with HIPAA through a private cloud while also enabling patients the ability to access some of their information through the provider's web app on a public cloud.
- A defence research organization performs mission-critical defence research using a private cloud but also uses a public cloud for enabling its day-to-day operational matters.

16

Now, let us talk about some examples of hybrid clouds. So, some scenarios or you know examples where hybrid cloud becomes very useful. The first one an e-commerce site relies on sales force in the public cloud to manage its customer relationship management functions while also using a private cloud to test and build new analytics products based on the data.

So, you observe that you know the e-commerce site relies on so you know when it is using for you know a cloud to build some new analytics products which it does not wanted to reveal to its competitors or share with others it is very maybe it could be a source of competitive advantage for the organization; so that in that scenario it uses a public cloud. For but for generic day to day operations to manage its CRM functions it uses a public cloud.

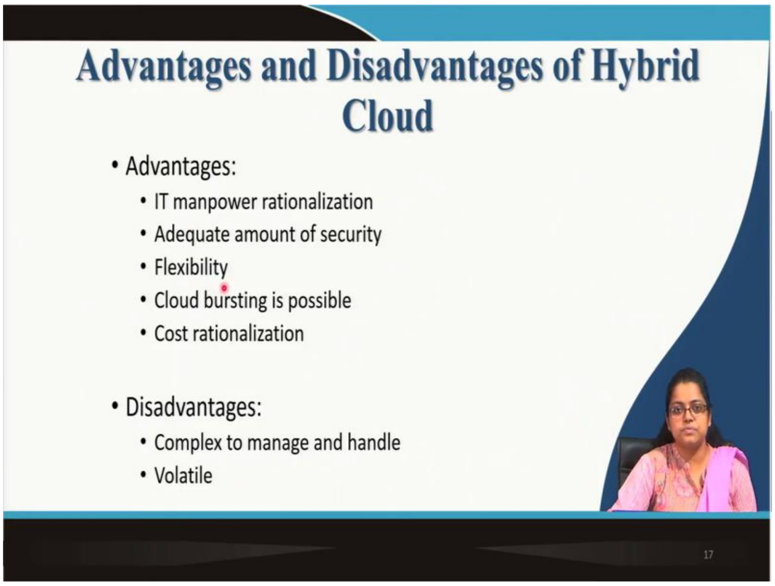
Similarly, if we so all of these examples talk about you know similar scenarios. So, here a parts manufacturer relies on a private cloud to collect and analyse billions of points of data coming in from IoT sensors, but also needs to enable customers on the public cloud to see real time order status updates that depend on that sensor data.

So, day-to-day data you know real time data which is constantly coming constantly flowing through the system can be managed through a public cloud. But if you need to collect and analyse some data coming from sensors IoT sensors it is the organization relies on a private cloud for that.

Similarly, the other two the last the second last one talks about a health care provider which again needs a combination of private and public cloud in a particular scenario. And the fourth one a defence research organization performs mission critical defence research using a private cloud, but also uses a public cloud for enabling its day-to-day operational matters.

So, in general you know when organizations use a combination of public and private cloud, the public cloud is generally used for day-to-day operational data or operational purposes, whereas the private cloud is used for some mission critical you know data analysis research or very confidential patient data, customer data and so on which should not be compromised at any cost.

(Refer Slide Time: 28:03)



Advantages and Disadvantages of Hybrid Cloud

- Advantages:
  - IT manpower rationalization
  - Adequate amount of security
  - Flexibility
  - Cloud bursting is possible
  - Cost rationalization
- Disadvantages:
  - Complex to manage and handle
  - Volatile

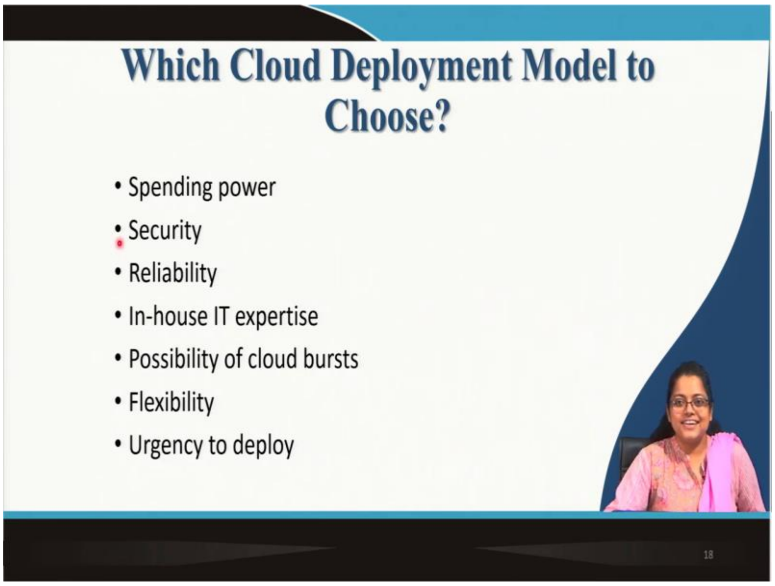
17

So, advantages and disadvantages of hybrid cloud. Advantages are IT manpower rationalization, because since there is a private and a public cloud a lot of manpower is not required to maintain the private cloud alone. There is adequate amount of security because there is a lot of you know the most critical data resides within the private cloud. Flexibility, yes, because you can move some data or some processes to the public cloud, and the rest can be on the private cloud, so there is flexibility.

Cloud bursting is possible because you know if you want scalability at a certain point in time, say there is a lot of processing or a lot of data handling that has to be happened at a particular point in time, so cloud bursting is possible because there is the private public cloud, and you can automatically avail the services of the service provider additional services of the service provider at extra cost.

And cost rationalization, again because it is a combination of public and private cloud. Private clouds in general are costlier, but since there is a combination of public and private cloud there is cost rationalization. Disadvantage coming to disadvantages we have discussed them earlier also. Hybrid cloud could be very volatile, therefore, it is in general complex to manage and handle.

(Refer Slide Time: 29:29)



Which Cloud Deployment Model to Choose?

- Spending power
- Security
- Reliability
- In-house IT expertise
- Possibility of cloud bursts
- Flexibility
- Urgency to deploy

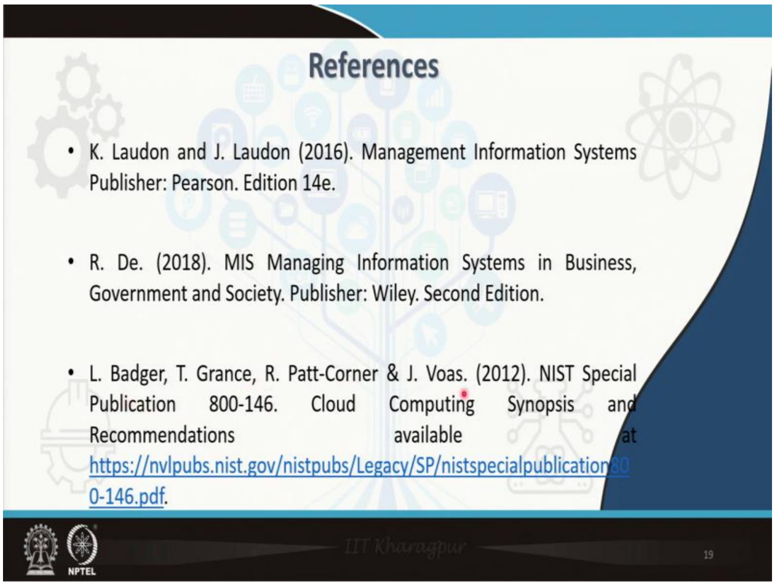
Finally, after having spoken about the four cloud deployment models, which cloud deployment model would you choose for your organization? That depends on certain organizational parameters or organization dependent variables such as your spending power.

So, if you think that you know you do not have too much of spending power you are a very new a start up you would want to avail the services of the cloud, it is always better to go ahead with the public cloud if you do not have very critical data, customer data or any other data.

Then, but if you require a lot of security, it is always advisable to go ahead with the private cloud. Other parameters that determine the choice of a cloud deployment models model are reliability, in-house IT expertise. So, if you have in-house IT expertise and you want security and reliability, you may prefer to go for a private cloud over a public cloud. Possibility of cloud bursts; you would always prefer a public cloud. Flexibility, again you would want to go and maybe wanted to go in for a hybrid cloud an urgency to deploy.

So, if you have urgency to deploy, it is always suggested that you go ahead with the public cloud because private cloud deployments in general could take a very much longer period of time compared to that of a public cloud deployment. So, these are some of the very essential parameters context specific or organization specific parameters that would determine your choice of a cloud deployment model.

(Refer Slide Time: 31:08)



References

- K. Laudon and J. Laudon (2016). Management Information Systems Publisher: Pearson. Edition 14e.
- R. De. (2018). MIS Managing Information Systems in Business, Government and Society. Publisher: Wiley. Second Edition.
- L. Badger, T. Grance, R. Patt-Corner & J. Voas. (2012). NIST Special Publication 800-146. Cloud Computing Synopsis and Recommendations available at https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-146.pdf.

IIT Kharagpur

19

So, these are some of the references that I have used in this particular slide. The session, the last one is a very insightful reference. If possible, please go through it because this provides a lot of insights related to the different cloud deployment models. So, in this, I think we are done with this particular session on cloud computing.

We have discussed, in cloud computing, we have discussed the various in the previous session and this session together, we have spoken about cloud, the various advantages and disadvantages of cloud computing over traditional computing. We have also spoken about the various cloud service models, the cloud service providers, cloud deployment models.

And in this session, we entirely spoke about deployment models, and the choice of the reasons why an organization would go for any one or a combination of these deployment models. So, with that, we will we come to the end of this session. And in the next session, we will focus on another very important emerging technology that is ‘internet of things’.

Thank you!