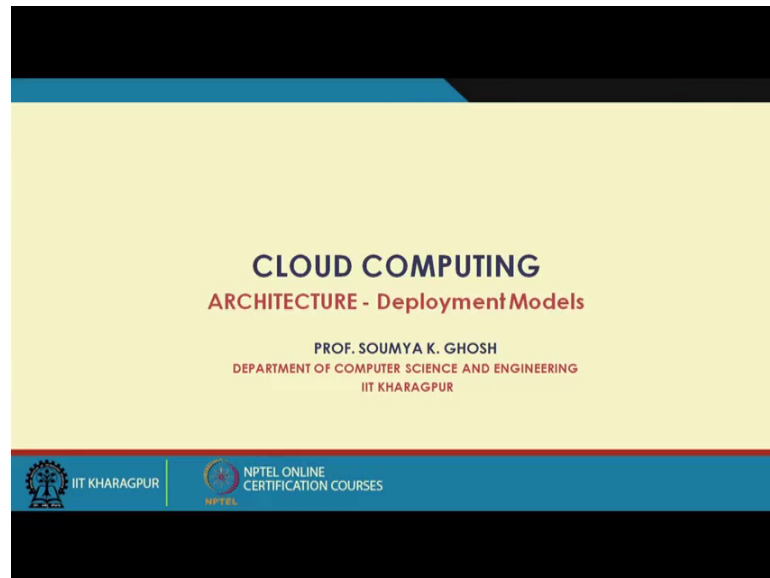


Cloud Computing
Prof. Soumya Kanti Ghosh
Department of Computer Science and Engineering
Indian Institute of Technology, Kharagpur

Lecture – 06
Architecture - Deployment Models

(Refer Slide Time: 00:41)



Hello, so welcome to our next lecture on cloud computing. Today, we will continue some of our discussion on cloud architecture and specially see some aspects of a cloud taken is cloud like one of the aspects is virtualization.

(Refer Slide Time: 00:48)

Deployment Models

- Public Cloud
- Private Cloud
- Hybrid Cloud
- Community Cloud

IIT KHARAGPUR | NPTEL ONLINE CERTIFICATION COURSES

So, as if we look at remember that earlier lectures we are discussing on different type of a service models, and also we have different type of deployment models in cloud namely public, private, hybrid and community cloud. Different aspects and all sort of services can be hosted in different type of deployment models, right.

(Refer Slide Time: 01:05)

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.
- Examples of Public Cloud:
 - Google App Engine
 - Microsoft Windows Azure
 - IBM Smart Cloud
 - Amazon EC2

Source: Marcus Hogue, Chris Jacobson, "Security of Cloud Computing"

IIT KHARAGPUR | NPTEL ONLINE CERTIFICATION COURSES

So, in case of a public cloud the as the name suggests it is available for public at large. So, it is you anyone can purchase that and it is somewhat omnipresent across the internet. Some of the very popular examples are Google app engine, Microsoft Azure, IBM cloud,

Amazon EC 2 and many others right many, many others clouds are there. So, what happened that we have this public cloud and enterprise or individual can subscribe this public cloud, subscribe this public cloud over the internet and can have that its services over this. So, the cloud infrastructure is provisioned for open use by general public, organization, enterprises and anyone who can pay and use the things, there are definitely some legal policies we need to be conformed too.

So, it may be owned managed and operated by a business, academics, government organization or some combination of them, right, it exists in the premise of the cloud provider. So, typically the physically the public cloud is at the CSPS premise or premises, so that means whatever the computing infrastructure storage infrastructure and other type of things are there those are residing in the CSPS of the cloud providers premises not at the private or not at the users premises, so that is one aspects of the thing.

(Refer Slide Time: 02:42)

Public Cloud

- 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).

The diagram illustrates a public cloud architecture. At the center is a cloud labeled 'A Cloud Provider'. To the left, various client types are shown: 'Clients utilizing services' (represented by small orange icons), 'Computers in a network providing services' (represented by server icons), 'Public clients accessing the cloud over a fire wall' (represented by a firewall icon), 'New hardware' (represented by server rack icons), and 'Cloud or dedicated hardware' (represented by server rack icons). To the right, 'Optional subscription-controlled security gateway' is shown, leading to 'Clients accessing the public cloud from within the security perimeter' (represented by orange icons). Below this, 'Subscribed to facility' is shown, leading to 'Clients terminating services' (represented by orange icons). The source is cited as 'Source: LeeBadger, and Tim Grance "NIST DRAFT Cloud Computing Synopsits and Recommendations"'.

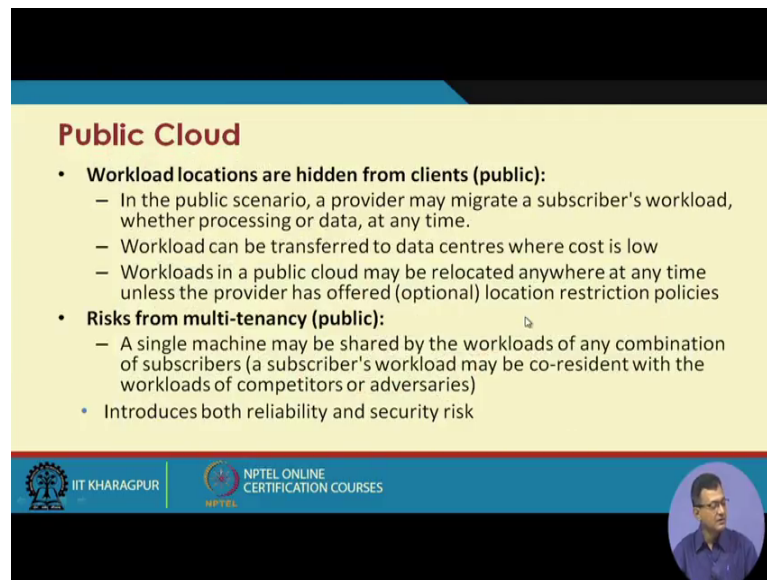
Source: LeeBadger, and Tim Grance "NIST DRAFT Cloud Computing Synopsits and Recommendations"

IIT KHARAGPUR | NPTEL ONLINE CERTIFICATION COURSES

49

And in public setting, provider's computing and storage resources are potentially large, right, so it is serving to all. Communication links can be assumed to be implemented over public internet, services; and the cloud service serves a diverse pool of client and may be out of them do not all faithful clients there can be some attackers, hackers etcetera, etcetera. So, it is open to anybody who can subscribe a typically it can have a service provider and you can there can be different type of users at the things.


(Refer Slide Time: 03:19)



Public Cloud

- **Workload locations are hidden from clients (public):**
 - In the public scenario, a provider may migrate a subscriber's workload, whether processing or data, at any time.
 - Workload can be transferred to data centres where cost is low
 - Workloads in a public cloud may be relocated anywhere at any time unless the provider has offered (optional) location restriction policies
- **Risks from multi-tenancy (public):**
 - A single machine may be shared by the workloads of any combination of subscribers (a subscriber's workload may be co-resident with the workloads of competitors or adversaries)
 - Introduces both reliability and security risk

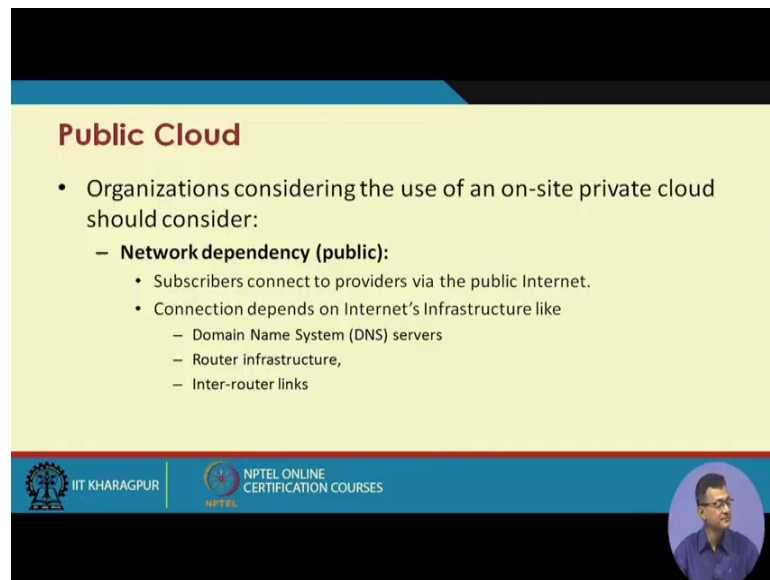
IIT KHARAGPUR | NPTEL ONLINE CERTIFICATION COURSES



So, what are the typical features workload locations are hidden from the cloud, one of the clients that is one of the major thing. Like you do not know where your virtual machine is you do not know where your actually the data is residing, which server which location and with whom it is residing, so it is all are hidden. So, as for as if you are not very stringent on the legal and policy matter about the security and other aspects though it is fine that you do not care, so long your services are. There are risk from multi-tenancy; that means, your logically or it may be theoretically always possible that your computing your storage where it is residing somebody else's things are there. Now, if it is somebody with some organization or some person who is not very faithful, or we are not very comfortable, so that 2 things twosome 2 different user can reside can work on the same things.

So, in other sense there is a risk there is this; what we say multi-tenancy and there are risks of multi-tenancy because I do not know that where things are there, where there though whether there is a underlining channel to access my data services and other type of things. So, there is a risk of multi-tenancy. So, single machine can be shared by workloads by any combination of subscriber, subscriber workload maybe co-resident with the workload of the competitor or adversaries, so it introduce both reliability and security risk.


(Refer Slide Time: 04:55)



Public Cloud

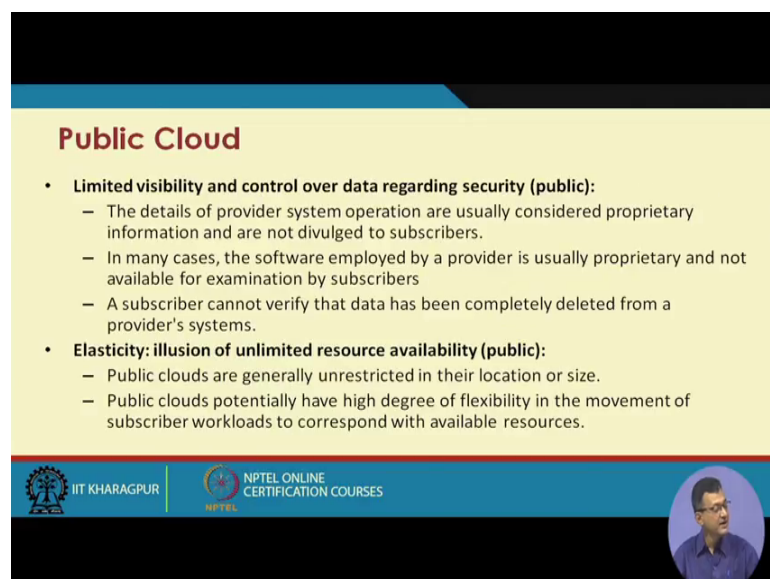
- Organizations considering the use of an on-site private cloud should consider:
 - **Network dependency (public):**
 - Subscribers connect to providers via the public Internet.
 - Connection depends on Internet's Infrastructure like
 - Domain Name System (DNS) servers
 - Router infrastructure,
 - Inter-router links

IIT KHARAGPUR | NPTEL ONLINE CERTIFICATION COURSES



So, organization considering use of onsite public cloud should consider network dependency. So, whenever suppose IIT, Kharagpur things that all is or some of its labs will be running on public cloud, so that our overall maintaining and etcetera reduces cost of maintenance or overall load on maintenance etcetera reduces. Now, there first dependency is the network. So, it will be always available the network connectivity should be always available up to a mark. So, there is one dependency.


(Refer Slide Time: 05:31)



Public Cloud

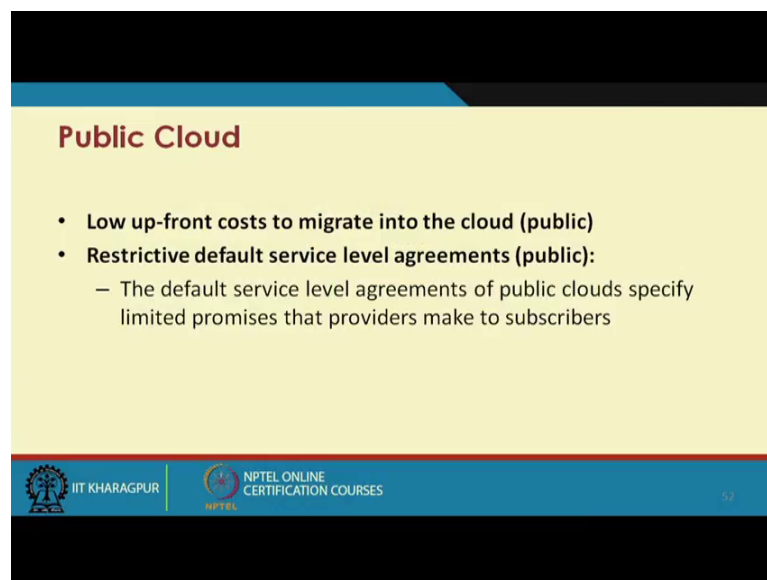
- **Limited visibility and control over data regarding security (public):**
 - The details of provider system operation are usually considered proprietary information and are not divulged to subscribers.
 - In many cases, the software employed by a provider is usually proprietary and not available for examination by subscribers
 - A subscriber cannot verify that data has been completely deleted from a provider's systems.
- **Elasticity: illusion of unlimited resource availability (public):**
 - Public clouds are generally unrestricted in their location or size.
 - Public clouds potentially have high degree of flexibility in the movement of subscriber workloads to correspond with available resources.

IIT KHARAGPUR | NPTEL ONLINE CERTIFICATION COURSES



There are limited visibility and control over the data regarding the security. So, I have we are mentioning that I have limited visibility of the data. I do not where the data is and how it is secured only thing what I have is some sort of a SLA or some sort of a MOU between provider and me that this data is secured and so and so forth. So, there is a issue of elasticity or illusion of unlimited resource availability. So, this is when you use public cloud, this is pretty fine because theoretically I have infinite amount of elasticity like if I need more computing power it will be provision if I one more other storage things it will be provisions when I do not require I releases it, or de provision it. So, those things are feasible. So, theoretically infinite scaling up, scaling down is possible.

(Refer Slide Time: 06:31)



Public Cloud

- **Low up-front costs to migrate into the cloud (public)**
- **Restrictive default service level agreements (public):**
 - The default service level agreements of public clouds specify limited promises that providers make to subscribers

IIT KHARAGPUR | NPTEL ONLINE CERTIFICATION COURSES

Another important thing is the low up-front cost to migrate into the cloud. So, if you want to make a private cloud of your own then you have to purchase the thing make provision where it will be housed, install software and etcetera; run it test it there are issues of maintenance so and so. Here the up-front, there is no there is very low up-front cost, you pay and use it. Restrictive default service level agreements, so there is a now whenever we purchase something there is a somewhere other we need to confirm to the that standard or what we say quote, unquote restrictive service level agreements between the provider and the consumer. So, most of the cases we need to follow the terms and condition provide like whatever is given by the provider unless you do for a large-scale deployment where you negotiate at special rate with special SLA and type of things. But

normally for a small institution and public at large we need to confirm to the; whatever is being provided.

(Refer Slide Time: 07:38)

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.

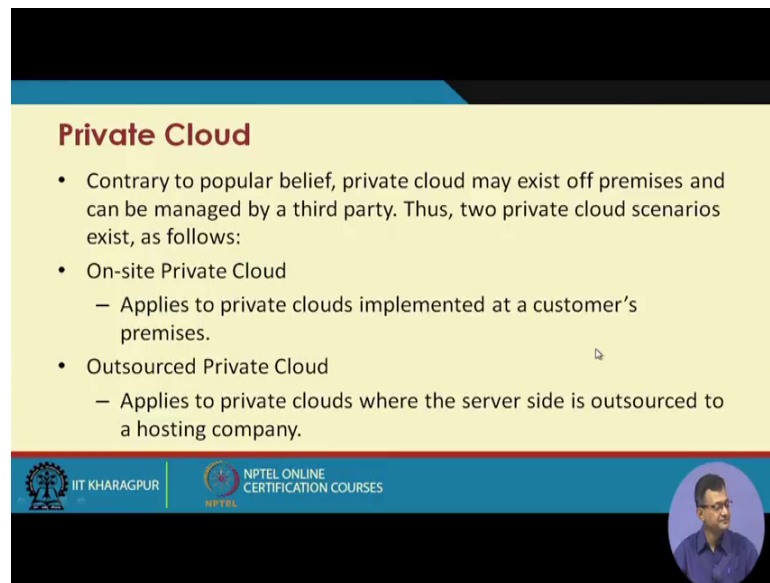
The diagram illustrates the relationship between a Public Cloud and a Private Cloud. The Public Cloud (top) provides Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). The Private Cloud (bottom) provides Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). An Enterprise (bottom) is shown interacting with both the Public and Private Clouds. The Private Cloud is also shown interacting with the Enterprise's internal infrastructure.

IIT KHARAGPUR | NPTEL ONLINE CERTIFICATION COURSES

So, totally other means the other aspects from the public is the private. So, you have your own cloud and you have all your resources which can be working on it right. So, the cloud infrastructure is provision for exclusive use of a single organization comprising a multiple consumers or business units like a same organization say IIT KGP private cloud my catering all the things which in the IIT departments, etcetera. May be owned managed and operated by the organization or it can be outsourced by a third party managing resources out here, but it is in your premises under your jurisdiction under your network control and type of things. And it may exist on or off premises also.

So, that there are usually on premises or I can say I have a private things or what we say outsource private cloud, where I can at the off premises, but nevertheless it is jurisdiction or my policy stipulated rules or the organization rules which driven. So, there are some of the open source and other public cloud one is that Eucalyptus pretty popular, there are open stack, Ubuntu Enterprise Cloud, Amazon VPC - virtual private cloud, VMware Cloud Infrastructures Suite, Microsoft ECI data centers and so on and so forth. So, there are several things which gives private cloud into the thing.


(Refer Slide Time: 09:04)



Private Cloud

- 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.

IIT KHARAGPUR | NPTEL ONLINE CERTIFICATION COURSES



So, contrary to popular belief, private cloud may exist off premises and can be managed by third party. So, not only means take the responsibility or I basically I want to maintain the control over the whole thing, but I basically may off premise or I installed out with the help of a third party to a separate thing also. There is 2 private cloud scenarios one is on-site private cloud which is the de facto or which is immediately come to which comes to our mind when we are talking about anything which is private, applies to private clouds implemented as the customer's premises. Another is the outsource private cloud like I have a private chunk of the things which is outside outsource out of my premises, but never the less it is private to me, right. So, applies to private cloud where the server side is outsourced to the hosting company wherever it is there.

(Refer Slide Time: 10:02)

On-site Private Cloud

- The security perimeter extends around both the subscriber's on-site resources and the private cloud's resources.
- Security perimeter does not guarantee control over the private cloud's resources but subscriber can exercise control over the resources.

Source: Leebadger, and Tim Grance "NIST DRAFT Cloud Computing Synopsis and Recommendations"

IIT KHARAGPUR | NPTEL ONLINE CERTIFICATION COURSES

So, in case of on-site private cloud the security perimeter extends around both the subscriber's on-site resources and private cloud's resources. So, your security perimeter or your legal control is basically have to encompass the private cloud right. Security perimeter does not guarantee control over private cloud resources, but the subscriber can exercise control over the other resources over the resources like. So, that it is in case of on-site like whatever the private cloud it is there, I can have an overall control over the whole resources of the private cloud.

(Refer Slide Time: 10:39)

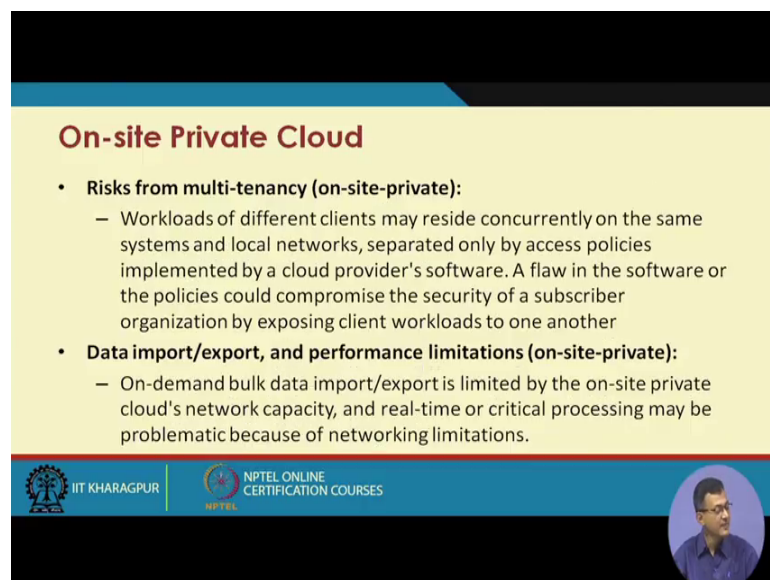
On-site Private Cloud

- Organizations considering the use of an on-site private cloud should consider:
 - **Network dependency (on-site-private):**
 - **Subscribers still need IT skills (on-site-private):**
 - Subscriber organizations will need the traditional IT skills required to manage user devices that access the private cloud, and will require cloud IT skills as well.
 - **Workload locations are hidden from clients (on-site-private):**
 - To manage a cloud's hardware resources, a private cloud must be able to migrate workloads between machines without inconveniencing clients. With an on-site private cloud, however, a subscriber organization chooses the physical infrastructure, but individual clients still may not know where their workloads physically exist within the subscriber organization's infrastructure

IIT KHARAGPUR | NPTEL ONLINE CERTIFICATION COURSES

So, there are some issues characteristics pros and cons of the maintaining on site private cloud one is the network dependency on-site private right. Subscriber, so it is dependency on the on your internet network should be here. Subscriber still needs IT skill my organization is meeting my own cloud or the organization meeting own cloud. So, there should be some sort of a skill to maintain that. Workload location are hidden from the client even, if my clients are different differ in my subunits that also this is hidden from the client. Like even if it is within the premises or on-site private cloud that actually infrastructure is hidden from the cloud, where client is my own organization things or my own clients are on the other side.


(Refer Slide Time: 11:24)



On-site Private Cloud

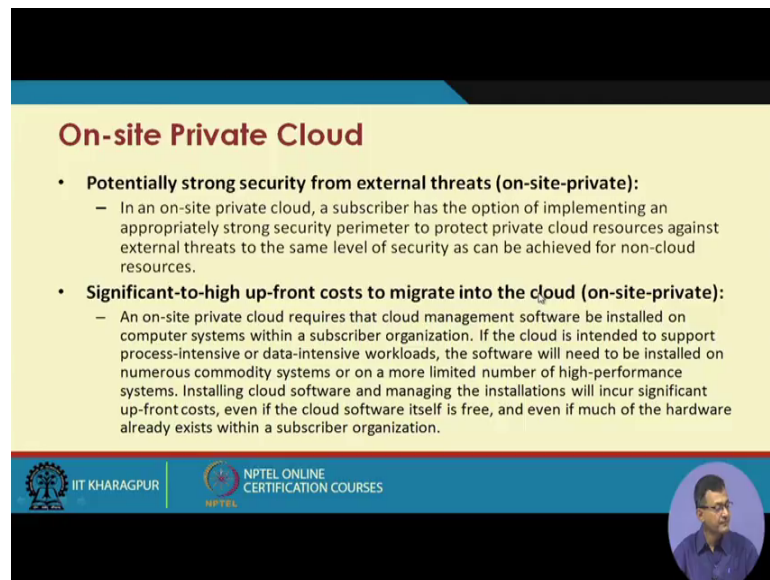
- **Risks from multi-tenancy (on-site-private):**
 - Workloads of different clients may reside concurrently on the same systems and local networks, separated only by access policies implemented by a cloud provider's software. A flaw in the software or the policies could compromise the security of a subscriber organization by exposing client workloads to one another
- **Data import/export, and performance limitations (on-site-private):**
 - On-demand bulk data import/export is limited by the on-site private cloud's network capacity, and real-time or critical processing may be problematic because of networking limitations.

IIT KHARAGPUR | NPTEL ONLINE CERTIFICATION COURSES



Risk from multi-tenancy again the same issues of within things also come into play. Data import export and performance limitation there can be issues of data import export because there are lot of data, which will be going out and going down. So, that on demand bulk data import export is limited on on-site private clouds network capacity or real time critical processing maybe problematic because of network limitation.

(Refer Slide Time: 11:55)



On-site Private Cloud

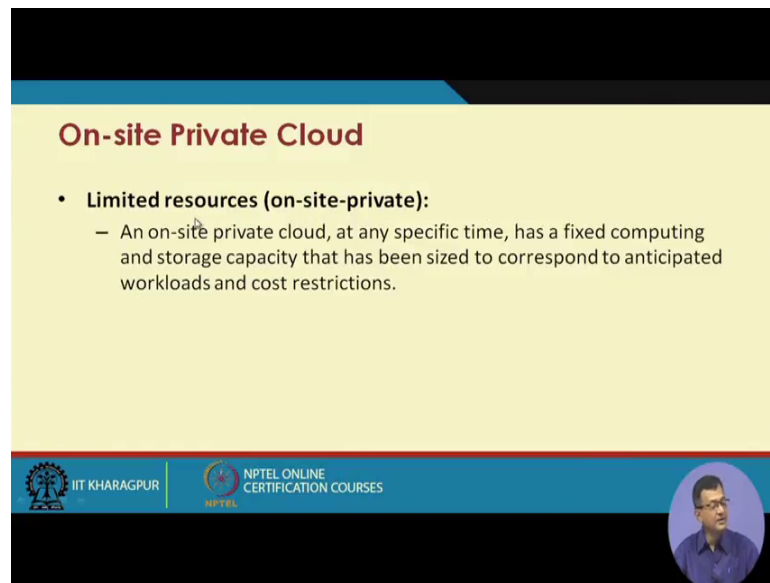
- **Potentially strong security from external threats (on-site-private):**
 - In an on-site private cloud, a subscriber has the option of implementing an appropriately strong security perimeter to protect private cloud resources against external threats to the same level of security as can be achieved for non-cloud resources.
- **Significant-to-high up-front costs to migrate into the cloud (on-site-private):**
 - An on-site private cloud requires that cloud management software be installed on computer systems within a subscriber organization. If the cloud is intended to support process-intensive or data-intensive workloads, the software will need to be installed on numerous commodity systems or on a more limited number of high-performance systems. Installing cloud software and managing the installations will incur significant up-front costs, even if the cloud software itself is free, and even if much of the hardware already exists within a subscriber organization.

IIT KHARAGPUR | NPTEL ONLINE CERTIFICATION COURSES



Potentially strong security from external threats usually if it is a private within your network boundary all your network other features come into play. Like as I was mentioning in some of my in one of my earlier lecture that IIT, Kharagpur has installed or has developed a private cloud for its research purpose what is Meghamala, but it is within my network premise. So, what whatever the network security parameters or features are there for IIT, Kharagpur is also applied for this infrastructure. So, what happens that it has a potentially strong security features. Significant to high upfront cost to migrate into the cloud, so that is another issue, right. Whenever you have a private cloud. So, there is a significant cost in installing maintaining and there is may be a significant cost in migrating the whole thing into the private cloud, our own say.


(Refer Slide Time: 12:50)



On-site Private Cloud

- **Limited resources (on-site-private):**
 - An on-site private cloud, at any specific time, has a fixed computing and storage capacity that has been sized to correspond to anticipated workloads and cost restrictions.

IIT KHARAGPUR | NPTEL ONLINE CERTIFICATION COURSES



There is a limited resources all if you have your thing that anything, you want to augment you need to purchase install not only that even to need to properly interoperate with the existing things. So, in doing so, you have a times, you have a limited resources like suddenly I can go up or down on the resources. So, as on-site private cloud any specific time has a fixed computing and storage capacity that can be sized to corresponding, correspond to the anticipated workloads and cost. So, what we do whenever I install a private cloud, so I have a estimate of the things like storage, computing, etcetera and then keeps some provision like of it is a buying that the staff at x amount or I install 1.5 amount. But that is the thing that I am limited to that x 1.5 x amount of the thing.

(Refer Slide Time: 13:47)

Outsourced Private Cloud

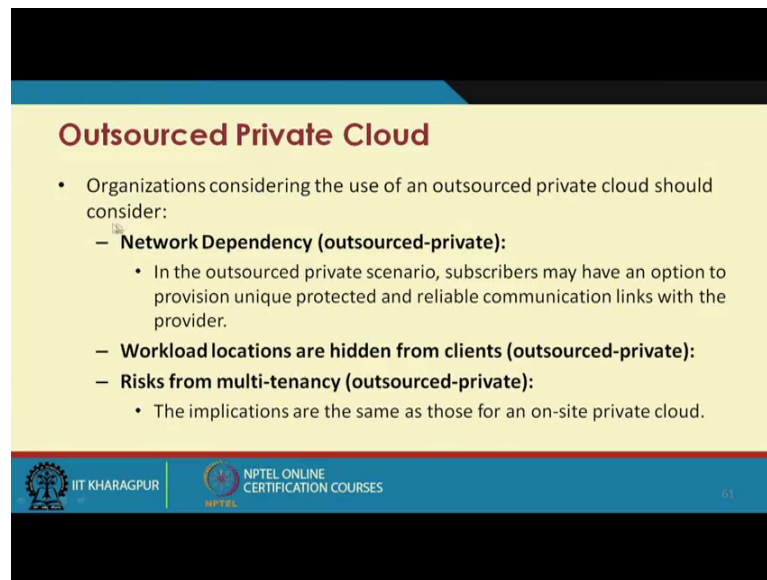
- Outsourced private cloud has two security perimeters, one implemented by a cloud subscriber (on the right) and one implemented by a provider.
- Two security perimeters are joined by a protected communications link.
- The security of data and processing conducted in the outsourced private cloud depends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

IIT KHARAGPUR | NPTEL ONLINE CERTIFICATION COURSES

So, there is another variant of the things I keep this as private, but I outsource it, so that maintaining installing etcetera I do not means organization do not take care, but it is outsource it, so outsource without source. Outsource private cloud has 2 security perimeters one implemented by the cloud subscriber, whoever is there on the right and the implemented by the provider. So, one this is a perimeter. So, what is happening it has a some sort of a channel which connects this to this private cloud which is outsource in some other premises right or maybe a subset of a cloud service provider.

So, I have a channel which hooks into the things, but the whole stuff at that end is a private to me. So, the security of data and processing conducted on the outsourced private cloud depends on the strength and availability of both security perimeters and of the protected communication. So, what we require that my infrastructure to be secured at the external things, another the channel where by the network channel or the network communication link which I talk over which I communicate or over which my organization communicate with the cloud should be secured in up to a particular level or expected level.

(Refer Slide Time: 15:13)



Outsourced Private Cloud

- Organizations considering the use of an outsourced private cloud should consider:
 - **Network Dependency (outsourced-private):**
 - In the outsourced private scenario, subscribers may have an option to provision unique protected and reliable communication links with the provider.
 - **Workload locations are hidden from clients (outsourced-private):**
 - **Risks from multi-tenancy (outsourced-private):**
 - The implications are the same as those for an on-site private cloud.

IIT KHARAGPUR | NPTEL ONLINE CERTIFICATION COURSES

61

So, there are again some consideration pros and cons of using outsource private cloud. One is network dependency that again I am dependent on how things will be connected. Workload location are hidden from the client again those type of issues, it is from multi tenancy, where I am hosting my private cloud other people may be hosting also the private cloud. So, data import, export and performance limitation same thing exist. Potentially strong security from external threat because of you have still have a private things, it is not fully public and not all people are jumping on your cloud, but nevertheless you are maybe sharing some infrastructure may be more thereat at the much more lower level at the highest level and so on. But at the higher level you are not allowing anybody to enter into the things.

(Refer Slide Time: 16:01)

Outsourced Private Cloud

- **Modest-to-significant up-front costs to migrate into the cloud (outsourced-private):**
 - In the outsourced private cloud scenario, the resources are provisioned by the provider
 - Main start-up costs for the subscriber relate to:
 - Negotiating the terms of the service level agreement (SLA)
 - Possibly upgrading the subscriber's network to connect to the outsourced private cloud
 - Switching from traditional applications to cloud-hosted applications,
 - Porting existing non-cloud operations to the cloud
 - Training

IIT KHARAGPUR | NPTEL ONLINE CERTIFICATION COURSES

Modest to significant up-front costs to migrate clouds, so those are same as whatever we are having at the things. And most of the cases you need to negotiate in terms SLA with the provider who is providing your or the third party who is provide you this cloud.

(Refer Slide Time: 16:16)

Outsourced Private Cloud

- **Extensive resources available (outsourced-private):**
 - In the case of the outsourced private cloud, a subscriber can rent resources in any quantity offered by the provider. Provisioning and operating computing equipment at scale is a core competency of providers.

IIT KHARAGPUR | NPTEL ONLINE CERTIFICATION COURSES

Extensive resource availability is maybe an advantage, because this is not limited. I am taking a chance, so I request for increase it may it is very much possible to increase at the other end, the provider is not out of resources usually they have lot of resource at their backbone.

(Refer Slide Time: 16:38)

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 of Community Cloud:
 - Google Apps for Government
 - Microsoft Government Community Cloud



The diagram illustrates the Community Cloud model. It shows a central cloud infrastructure labeled 'Community Cloud' which is connected to a 'Community' of organizations. The community is represented by a group of icons (people and buildings) and is linked to the cloud via a 'Network'. The cloud infrastructure is shown as a stack of layers: 'Cloud (Public or Private)', 'Network', and 'Infrastructure'. The cloud infrastructure is also connected to a 'Data Center' and a 'Storage' component. The diagram is titled 'Community Cloud' and includes a small logo for 'NPTEL'.

IIT KHARAGPUR | NPTEL ONLINE CERTIFICATION COURSES

So, one side is private one side is public another typical type of cloud is community cloud right. So, it basically tries to as we have discussed it basically tries to serve a particular community per say, it is usually can operate in a public or private both, and it basically cater to a particular community which has a somewhat same domain of operation or same focus of interoperating. So, cloud infrastructure is provision for a exclusive use of a specific community of consumer from organization that are shared concerned that means, they have a light minded concern that is there can be same missions, security requirement, policy compliance consideration, etcetera, it may be owned managed operated by one or more organization in the community.

So, a third party or some combination of that it may exist on or off premises. So, it can be a on premises off premises, there are several community cloud and which are being provided by different service provider.

(Refer Slide Time: 17:47)

On-site Community Cloud

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

The diagram illustrates an on-site community cloud architecture. It shows several organizations, each with its own security perimeter. These organizations are connected to a central cloud resource pool. The diagram labels various components: 'Organizational security perimeter', 'Community resource security perimeter', 'Cloud resources that community cloud uses with their security perimeter', 'Community organizations providing and consuming cloud resources', and 'Community organizations (only) consuming cloud resources'. The source is cited as: Source: LeeBadger, and Tim Grance "NIST DRAFT Cloud Computing Synopsis and Recommendations".

IIT KHARAGPUR | NPTEL ONLINE CERTIFICATION COURSES

So, there are there can be one thing that like there are several A, B, C organization there x, y, z organization and there can they can form different set of combinations like ABC, xyz can be one community; A with x, y can be another community and so and so forth. So, there is possibility of bringing things together there is also possibility that I a community can be existing as some point of time; at the some other point of time it may not existing, I may be a organization can be more than one community of the things like our day-to-day life. I may be a part of my office group; also I am part of my say residential community.

So, there can be different policies and etcetera things are there and, but it is the primary objective is that there are like or same type of concerned or same type of workflow it may so happened that this community making them in a single community will help in productivity.

(Refer Slide Time: 18:58)



On-site Community Cloud

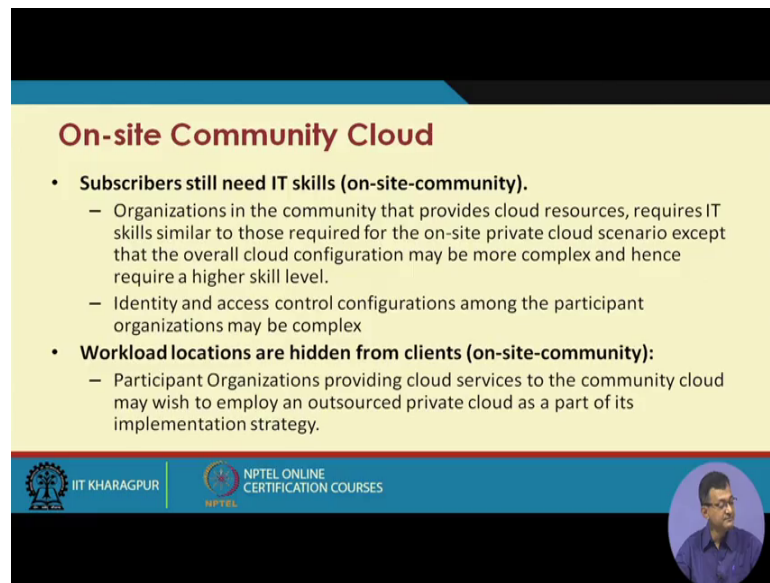
- The participant organizations are connected via links between the boundary controllers that allow access through their security perimeters
- Access policy of a community cloud may be complex
 - Ex. :if there are N community members, a decision must be made, either implicitly or explicitly, on how to share a member's local cloud resources with each of the other members
 - Policy specification techniques like role-based access control (RBAC), attribute-based access control can be used to express sharing policies.

IIT KHARAGPUR | NPTEL ONLINE CERTIFICATION COURSES



There are again lots of characteristics pros and cons, etcetera. The participant organization are connected by a links between the boundary controllers, and allow access through their security parameters like whatever the firewall policies or that type of boundary policies are there. Access policy of a community cloud may be a pretty complex, because you can have number of community. So, at what way access which you do not access whether there is a leakage of information, I get some information someone community pass it to the other community, so these need to be properly restricted. So, policy specification techniques like role based access control, attribute based access control are there; like based on my role I access some data, right. And like other form of deployment models, here also we have network dependency.


(Refer Slide Time: 19:48)



On-site Community Cloud

- **Subscribers still need IT skills (on-site-community).**
 - Organizations in the community that provides cloud resources, requires IT skills similar to those required for the on-site private cloud scenario except that the overall cloud configuration may be more complex and hence require a higher skill level.
 - Identity and access control configurations among the participant organizations may be complex
- **Workload locations are hidden from clients (on-site-community):**
 - Participant Organizations providing cloud services to the community cloud may wish to employ an outsourced private cloud as a part of its implementation strategy.

IIT KHARAGPUR | NPTEL ONLINE CERTIFICATION COURSES



Subscriber still need some IT skills because, it need to maintain with different community things. Workload locations are hidden from the client again.

(Refer Slide Time: 20:00)



On-site Community Cloud

- **Data import/export, and performance limitations (on-site-community):**
 - The communication links between the various participant organizations in a community cloud can be provisioned to various levels of performance, security and reliability, based on the needs of the participant organizations. The network-based limitations are thus similar to those of the outsourced-private cloud scenario.
- **Potentially strong security from external threats (on-site-community):**
 - The security of a community cloud from external threats depends on the security of all the security perimeters of the participant organizations and the strength of the communications links. These dependencies are essentially similar to those of the outsourced private cloud scenario, but with possibly more links and security perimeters.

IIT KHARAGPUR | NPTEL ONLINE CERTIFICATION COURSES



Data import export performance limitations there are issues on that like how between the community things etcetera whether the data or within the community, when multiple subscriber come in to play that how things will be there, and number of cases this communities can be loosely couples, so that things becomes more critical to manage potentially strong security from the external thing because still you are in the one

community, so that you have a better resistance to the external threats based on your community policies along with your own policy.

(Refer Slide Time: 20:34)

On-site Community Cloud

- **Highly variable up-front costs to migrate into the cloud (on-site-community):**
 - The up-front costs of an on-site community cloud for a participant organization depend greatly on whether the organization plans to consume cloud services only or also to provide cloud services. For a participant organization that intends to provide cloud services within the community cloud, the costs appear to be similar to those for the on-site private cloud scenario (i.e., significant-to-high).

IIT KHARAGPUR | NPTEL ONLINE CERTIFICATION COURSES

High variable up-front costs to migrate to the cloud, so there is as we have seen in case of a truly private cloud there is a high variable upfront cost to the migrate of the migration to the cloud because it is not publicly available. So, you need to create the things.

(Refer Slide Time: 20:52)

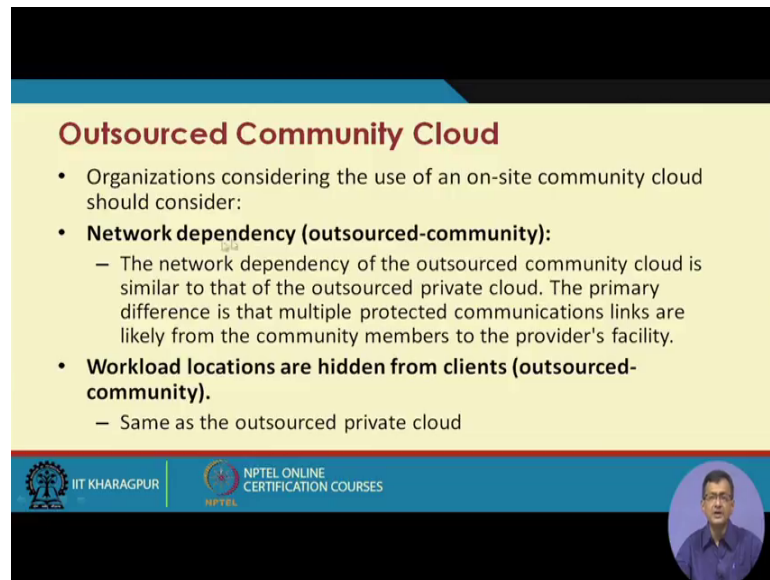
Outsourced Community Cloud

Source: Leebadger, and Tim Grance "NIST DRAFT Cloud Computing Synopsis and Recommendations"

IIT KHARAGPUR | NPTEL ONLINE CERTIFICATION COURSES

And there can be different sort of things like there are three organizations forming a community with some boundary controller, where with a private subscriber and those issues come into play.

(Refer Slide Time: 21:04)



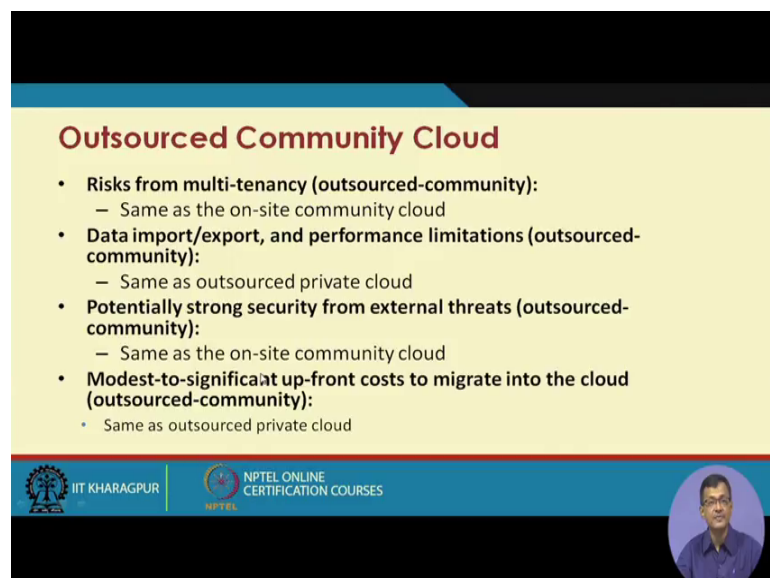
Outsourced Community Cloud

- Organizations considering the use of an on-site community cloud should consider:
- **Network dependency (outsourced-community):**
 - The network dependency of the outsourced community cloud is similar to that of the outsourced private cloud. The primary difference is that multiple protected communications links are likely from the community members to the provider's facility.
- **Workload locations are hidden from clients (outsourced-community).**
 - Same as the outsourced private cloud

IIT KHARAGPUR | NPTEL ONLINE CERTIFICATION COURSES

Community cloud can be on the premises or the community cloud can be out of means premises that means, the community cloud can be outsource as we have seen that in case of a private cloud. So, once we outsource the network dependency, workload location are not known or hidden from the clients.

(Refer Slide Time: 21:25)



Outsourced Community Cloud

- **Risks from multi-tenancy (outsourced-community):**
 - Same as the on-site community cloud
- **Data import/export, and performance limitations (outsourced-community):**
 - Same as outsourced private cloud
- **Potentially strong security from external threats (outsourced-community):**
 - Same as the on-site community cloud
- **Modest-to-significant up-front costs to migrate into the cloud (outsourced-community):**
 - Same as outsourced private cloud

IIT KHARAGPUR | NPTEL ONLINE CERTIFICATION COURSES

Risk from multi-tenancy, data import export and performance limitation issues, this will come into play potentially strong security from external threats as we have mentioned that is still you are on the community. Modest-to-significant up-front cost, if it is outsource there are lot of loads are taken up by the outsource this is in organization. So, there is a chance that the overall loading maybe overall up-front cost will be much less than if you are maintaining in premises. And theoretically if you are outsourcing extensive resource availability are possible.

(Refer Slide Time: 22:07)

Hybrid Cloud

- The cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability
- Examples of Hybrid Cloud:
 - Windows Azure (capable of Hybrid Cloud)
 - VMware vCloud (Hybrid Cloud Services)

The diagram illustrates a Hybrid Cloud architecture. It shows an 'Enterprise' (green oval) connected via 'Intranet' to a 'Private Cloud' (blue oval). The Private Cloud is further connected via 'Internet' to a 'Public Cloud' (blue oval). The Public Cloud is also connected via 'Internet' to another 'Public Cloud' (blue oval). The diagram also shows 'Data Center' and 'Cloud Services' components within each cloud environment.

IIT KHARAGPUR | NPTEL ONLINE CERTIFICATION COURSES

So, part from this as we can theoretically see or practically see that I can have a cloud which is combination of all those things. So, I can have private, public, community things. Specially with the public private cloud I can have a cloud which is combination of such more than one type of deployment models. The cloud infrastructure is a composition of 2 more distinct cloud infrastructure private, community or public. So, I have three type of things, and then I want to realize a cloud which has a combination of a these three things.

Why, this is important, first of all it is all depends that what sort of user's pattern, I am having. Like some of the user's pattern what I am having is more critical or more vulnerable to security threats that I want to keep as a more private. I do not want to I have a appropriate network boundary or network perimeter security to be implemented on the things. There are some of the resources which may not be I may not want those to

be so much secure or I do not care about all those security of the all those things and that can be made some of the things public. Like if I say if there are practice sessions for say computing labs for students, so the level of security is much less than when I am keeping say student records or students examination things etcetera, right.

So, though same type of operations may be there, but one I could have gone away with and an outsource this and gone to the public cloud to do it all right. And whereas the other one even it is economical, I want to keep those as my private things. Now, I can have a private combinations, right. As number of cases what sometimes it happens that you do something with the private, and you require some resources to be provisioned due to sudden increase of the things. Then suddenly in a private cloud increasing the resource provisioning or purchasing etcetera is a long process. So, you purchase the thing on a public cloud from a for a short period of time, so long your process is in place and this goes to the things.

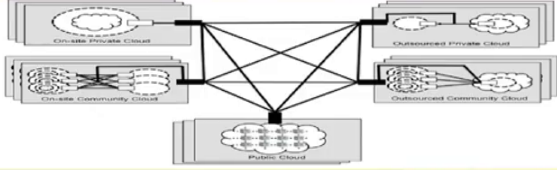
So, the infrastructure community that remains unique entities, but are bounded together in standardize or proprietary technology enables data and application to be portable this is important. So, portability not only with respect to data, whenever I have this private, public, community all together or a combination of 2 or more together, then there are the issue of intra operative come into play like the data which is working fine here when I take some application from the other whether we still workout the things.

So, the both data and at times the applications suppose your application was running on a private cloud with some resources, now you provision a VM which basically goes to the public domain. Now, the types of applications whether the application wants need to be resized or there are portability issues of the applications need to be looked into. So, there are examples of hybrid cloud some of the popular Windows Azure capable of hybrid cloud VMware V cloud; there are capability of hybrid cloud and as I have mentioning that there are several other providers which provide this type of things.

(Refer Slide Time: 25:45)

Hybrid Cloud

- A hybrid cloud is composed of two or more private, community, or public clouds.
- They have significant variations in performance, reliability, and security properties depending upon the type of cloud chosen to build hybrid cloud.



Source: LeeBadger, and Tim Grance "NIST DRAFT Cloud Computing Synopsis and Recommendations"

IIT KHARAGPUR | NPTEL ONLINE CERTIFICATION COURSES

So, the hybrid cloud is composed of 2 or more private public etcetera, they have a significant variation in performance, reliability, security property depending upon the type of cloud chosen to build a hybrid, right. If it is a community cloud or public and etcetera it will there will be difference in the performance different in the security features, etcetera.

(Refer Slide Time: 26:02)

Hybrid Cloud

- A hybrid cloud can be extremely complex
- A hybrid cloud may change over time with constituent clouds joining and leaving.

IIT KHARAGPUR | NPTEL ONLINE CERTIFICATION COURSES

So, a hybrid cloud can be extremely complex that is one of the major things. Like suppose your particular application is going on and need to run over a combination of

public and private cloud then the overall underlining architecture maybe very complex, so that your application runs seamlessly over the things. So, at times these private clouds can be extremely complex. A hybrid cloud may change over time with constituent clouds joining or leaving there is another big factor. So, what we are trying that it may so happened that you build a hybrid cloud with your own private cloud and 2 other public clouds.

So, now it may so change that some of the public cloud may go may wants to disconnect based on your terms and conditions and subscription ends, they do not want to again re subscribe and they have a different pricing model, even some of the thing may go red right there the organization the cloud may not be there. So, in that case, you need to there can be joining, leaving, and joining of new things or sometimes you may require more resources. So, you add some more public or community cloud into the things. All these becomes extremely complex phenomena to handle, right, so that means, over time the constituent clouds may leave or joined and making the whole process pretty complex.

So, now what should I choose, right; what should be my deployment model is another big question right. It totally depends on your requirement. Like if I have a small organization or individuals my public cloud may be a good solution. So, long my business is not going up-front on the something which compiles me to go to a own private cloud. There are other constant like I do business for somebody else, right I have some other subscriber base or client base, now this client may be interned looking for a things like suppose I have a storage provider, data storage provider. Now, I may either I have all this storages on my premises or I outsource this resources or provision this resources from other public clouds.

Now, it may be so happened that the my clients which may be something miss and critical clients like may be a financial sector or defense sector they want that no, no, no, it cannot happen, you need to have your own thing. So, it all depends that how what should be my way of looking at it right. I can have a combination as we have talking about hybrid I can have a combination of private public and so forth based on my requirement. Or whether I can classify my application into different things, my data, my applications into different categories, and then I say that this bunch can go to the private, this bunch can go to the public this can go to the community and type of things.

So, managing all those things is a another big challenge or for the organization or institution to handle that. So, with this, we will we close this lecture; and we will continue our lecture on other aspects of cloud computing in the subsequent talks.

Thank you.