

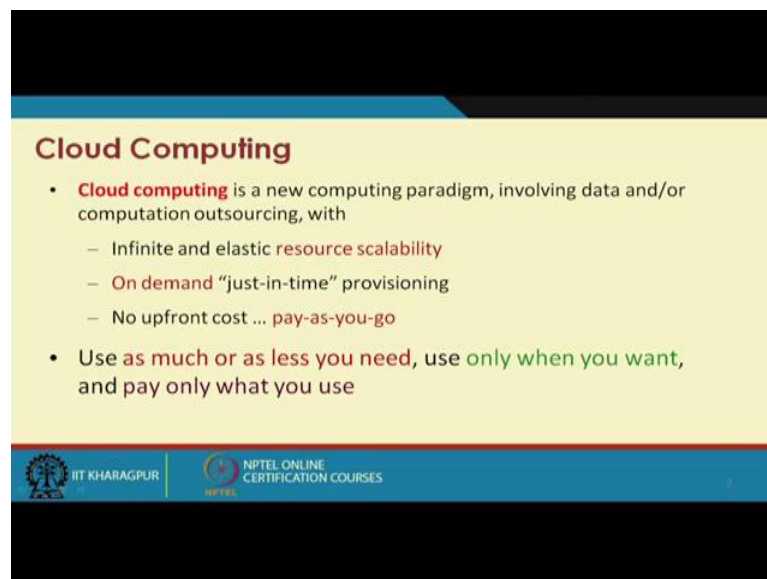
**Cloud Computing**  
**Prof. Soumya Kanti Ghosh**  
**Department of Computer Science and Engineering**  
**Indian Institute of Technology, Kharagpur**

**Lecture - 27**  
**Cloud Security – II**

Hi. Welcome to this Cloud Computing lecture series. Today, we will be discussing we will be continuing our discussion on Cloud Security. So, we will more now try to look at thus security with respect to more with respect to cloud perspective. So, as we have seen in our last lecture that the security has different aspects, right, like one is that security concepts or security components other part is the threats, there are issues of policies mechanisms there are issues of trust assumptions and those or risk.

So, all those things are need to be looked into when we are review on to implement the things. So, as it is; as we have to; as we have seen or discussed that these are manifested in any type of information system in including cloud, but cloud has different other some few more characteristics, right. So, we will try to see that what are the different characteristics and why this security becomes the important component; when we talk about cloud computing.

(Refer Slide Time: 01:38)



**Cloud Computing**

- **Cloud computing** is a new computing paradigm, involving data and/or computation outsourcing, with
  - Infinite and elastic **resource scalability**
  - **On demand** “just-in-time” provisioning
  - No upfront cost ... **pay-as-you-go**
- Use **as much or as less you need**, use **only when you want**, and pay only what you use

IIT KHARAGPUR | NPTEL ONLINE CERTIFICATION COURSES

So, as If we try to boil down cloud to a very simplistic are what we do one part is it is a resource elastic resource scalability, right, you can go up and go down in your resources

and resources can be anything right it is studying from computing power to memory to any type of a network resources bandwidth and so on. So, it is infinite and elastic resource scalability theoretically another thing is on demand just in time provisioning if I require, it should be on demand just in time provisioning should be there; there is another important aspect, thirdly it should be no its should be in a model what we say pay a metered service, right, pay as you go model, right as you use or as you go model, right.

So, when a what I pay for the things; that means, the resources are being acquired released escalated skill down as path the ways of the things this whole paradigm of security need to be over around these type of these policies, right; so that becomes a serious challenge and for that that number of organisation are not are little reluctant in going to the fully cloud even that is economically at times beneficial, right.


So, use as much as you use as much or as less as you need use only when want and pay only what you use this is the whole philosophy of going towards that.

(Refer Slide Time: 03:21)

**Economic Advantages of Cloud Computing**

- For consumers:
  - No upfront commitment in buying/leasing hardware
  - Can scale usage according to demand
  - Minimizing start-up costs
    - Small scale companies and startups can reduce CAPEX (Capital Expenditure)
- For providers:
  - Increased utilization of datacenter resources

IIT KHARAGPUR | NPTEL ONLINE CERTIFICATION COURSES



So, if we already you have seen, but just to have a quick look economic advantage of cloud computing for the consumer no upfront cost can scale uses as and when required minimize that of course, for provider increased utilization of the data centre resources. So, provider has a huge volume of resources and that has a increase utilization of the resources is the one of the major aspects.

(Refer Slide Time: 03:46)

**Why aren't Everyone using Cloud?**

Clouds are **still** subject to traditional data confidentiality, integrity, availability, and privacy issues, plus some additional attacks

IIT KHARAGPUR | NPTEL ONLINE CERTIFICATION COURSES

So, if it is win-win situation; why not everybody is using cloud, right.

So, one of the major thing is that cloud are still subject to traditional data confidentiality, integrity, availability, privacy issues plus some additional attacks, right. So, this is a serious concern that any state. So, if it is if the provider is happy if the consumer is happy why not the things everything a going to cloud immediately because of this type of scenario because of SaaS scenario of that there are issues of data confidentiality integrity availability privacy, etcetera plus some additional cloud related things.

(Refer Slide Time: 04:28)

**Concern...**

Q: Rate the **challenges/issues** ascribed to the 'cloud'/on-demand model  
(1=not significant, 5=very significant)

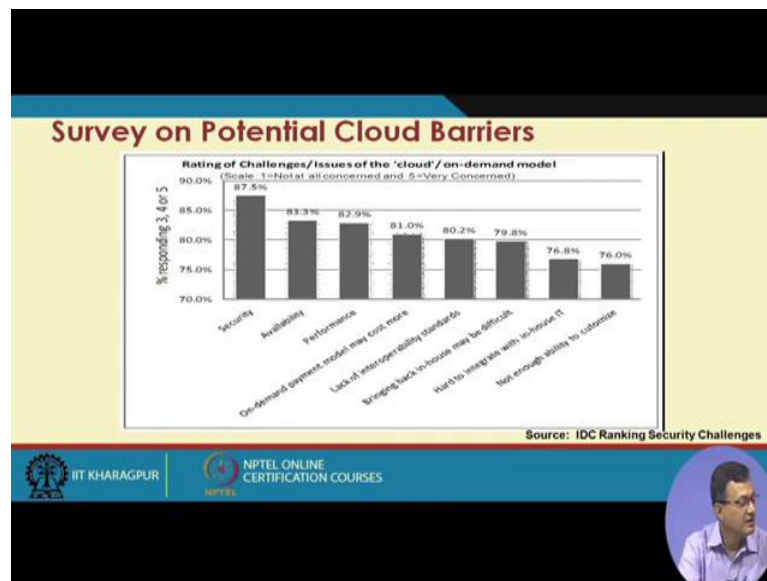
Challenge/Issue	% responding 4 or 5
Security	74.6%
Performance	63.1%
Availability	63.1%
Hard to integrate with in-house IT	61.1%
Not enough ability to customize	55.8%
Worried on-demand will cost more	50.4%
Bringing back in-house may be difficult	50.0%
Regulatory requirements prohibit cloud	49.2%
Not enough major suppliers yet	44.3%

Source: IDC Enterprise Panel, August 2008 n=244

IIT KHARAGPUR | NPTEL ONLINE CERTIFICATION COURSES

If we look some references that IDC inter price panel in 2008, they say that the major challenges or issue is the security right then the performance then availability and so and so forth, right. So, this is a from their survey it has been seen that the security still at the top level when you look at the challenges and issues in the things, it is not like that is insecure it is like at I am not able to define it is not only insecurity that thing, but also I failed to defined the things which we are define in more precisely there or I am not having that much trust or confidence on systems or the providers.

(Refer Slide Time: 05:09)



So, similarly survey on potential cloud barriers that also say that what we is blocking that going to the things is also that you look at it is a security plays a major role here.

(Refer Slide Time: 05:24)



**Why Cloud Computing brings New Threats?**

- Traditional system security mostly means keeping attackers out
- The attacker needs to either compromise the authentication/access control system, or impersonate existing users
- But cloud allows **co-tenancy**: Multiple independent users share the same physical infrastructure
  - An attacker can legitimately be in the same physical machine as the target
- Customer's **lack of control** over his own data and application.
- **Reputation fate-sharing**

IIT KHARAGPUR | NPTEL ONLINE CERTIFICATION COURSES

So, what this may new threats come into play here one is the traditional systems security mostly keeps means keeping attackers out right. So, if I say that IIT Kharagpur need to be secured as a enterprise with this network and I have a very very very strong. So, that the attackers are out I have different mechanism to keep my internal attackers also out right maybe. But my concern is that how to keep these attackers out is the thing the attacker needs to either compromise the authentication or access control system or impersonate existing user in order to do that whereas, in case of cloud I voluntarily they provide consumer or the user voluntarily gives keep their data services etcetera at the providers place; that means, it is by nature it is co-tenancy is there.

So, it is cotenant. So, multiple impendent users share the same physical infrastructure. So, I know that the infrastructure I am sharing my some attacker or some other parties also sharing the infrastructure. So, attacker can legitimately use the same physical machine as the target it is not like that digit into or for into the things it can legitimately use customer's lack of control over his own data and application right it is on the premises of the service provider.

So, it is less control or lack of control over the services applications and there can be reputation fate sharing right it is a; what we say that I; if as I go together as we go together. So, I share the fate of each other, right. So, that is also there is also a challenge. So, these are the things if you see co tenancy lack of control reputation fate sharing these

are the things which are not there in that a big way in case of a traditional things traditional security measures. And this becomes a new way of looking at the security in some cases.

(Refer Slide Time: 07:33)

**Security Stack**

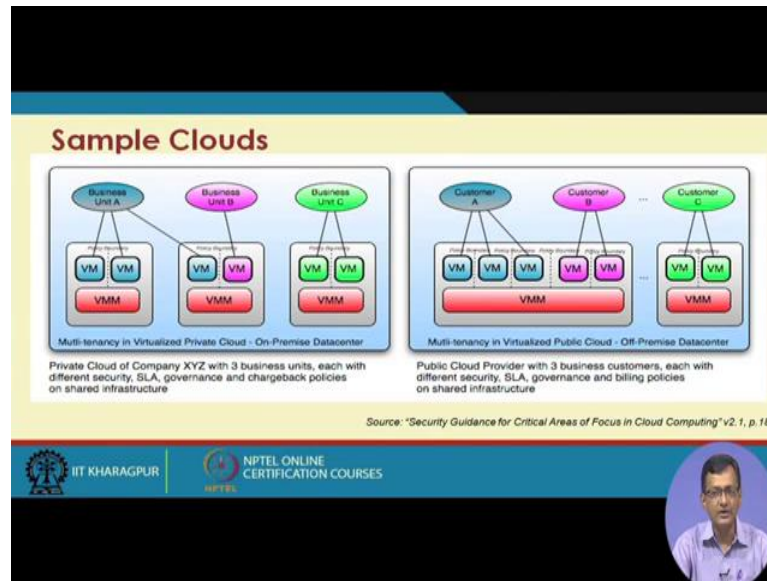
- **IaaS:** entire infrastructure from facilities to hardware
- **PaaS:** application, middleware, database, messaging supported by IaaS
  - Customer-side system administrator manages the same with provider handling platform, infrastructure security
- **SaaS:** self contained operating environment: content, presentation, apps, management
  - Service levels, security, governance, compliance, liability, expectations of the customer & provider are contractually defined

↑ Increase in Provider's Security Responsibility  
↓ Increase in Customer's Security Responsibility

IIT KHARAGPUR | NPTEL ONLINE CERTIFICATION COURSES

Now, if we look at the different 3 prominent service model IaaS, PaaS and SaaS. So, in case of the IaaS, the infrastructure why is the provider is there rest of the thing is the responsibility of the consumer so; that means, the increase providers responsibility is whenever I go to IaaS, PaaS to SaaS, right, the provider has more responsibility or in other sense if I have the increase consumer responsibility. So, the when it goes the IaaS, it is the maximum, right. So, whenever somebody is taking IaaS, PaaS, etcetera, this one is definitely need the organizational of the individual need along with that need to look at that the type of security aspects now we need to need to deploy on my system.

(Refer Slide Time: 08:28)



Now, to typical scenario whatever we are discussing is one is that in case of private cloud say organisational cloud say IIT Kharagpur cloud. So, it has 3 business; you need business A, business B and business C and there is a chance that I the business A is sharing one of the VMs of the; in the data centre or the infrastructure where the business B is there where the C is isolated.

So, this type of scenarios are there so; that means, the services or data are residing on one physical or one or in the physical systems, right whereas, in case of a public; similarly for a public cloud I can have different customer who are sharing the same infrastructure and there is a possibility of a channel of communication between the things, it can be thing the VMM if might having compromised or there are some attack on though those things which are there. So, these are the there can be different type of things which is beyond a control of the consumer do not have or the cloud service consumer or the users do not have any control over this or not much control over this other than basically relying on the SLAs and the how the reporting of the providers are there.

(Refer Slide Time: 10:00)

**Gartner's Seven Cloud Computing Security Risks**

- Gartner:
  - <http://www.gartner.com/technology/about.jsp>
  - Cloud computing has “unique attributes that require risk assessment in areas such as data integrity, recovery and privacy, and an evaluation of legal issues in areas such as e-discovery, regulatory compliance and auditing,” Gartner says
- Security Risks
  - Privileged User Access
  - Regulatory Compliance & Audit
  - Data Location
  - Data Segregation
  - Recovery
  - Investigative Support
  - Long-term Viability

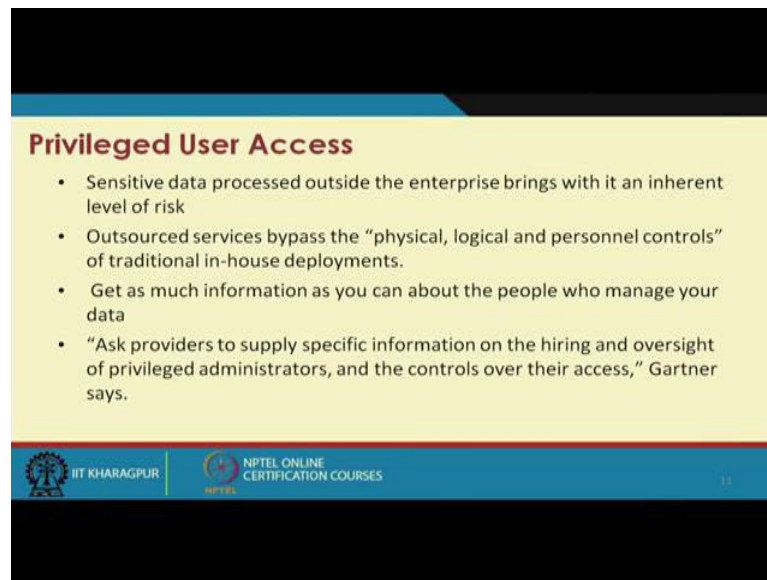
IIT KHARAGPUR | NPTEL ONLINE CERTIFICATION COURSES

So, Gartner's have seven cloud computing security risk parameters, right. So, there is a Gartner's seven point things. So, rather Gartner's cloud computing according Gartner's has a unique attributes that require risk assessment in areas such as data integrity recovery and privacy and evaluation of legal issues in the areas the of e-discovery regulatory compliance and type of things, right.

So, these are five securities which Gartner point out in a report that is the one is privileged user access that is one securities regularity compliance and audit is another thing data location where the data is located with why whether; I how much control; I am having data segregation is another problem recovery mechanisms investigative support like if I want to do some post mortem type of things then how much investigated support what I am having and long term viability, right. So, there is a there is a chance of vender locking then that will see that how that long and viability will be there.



(Refer Slide Time: 11:04)



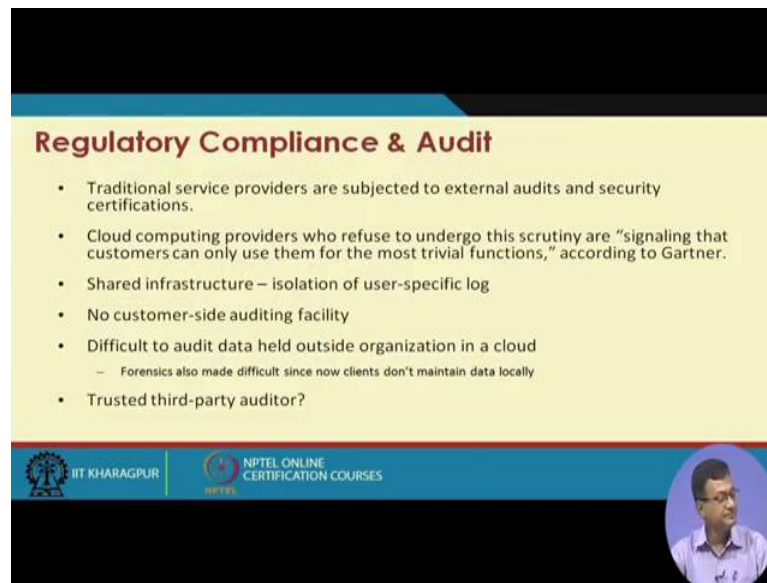
**Privileged User Access**

- Sensitive data processed outside the enterprise brings with it an inherent level of risk
- Outsourced services bypass the “physical, logical and personnel controls” of traditional in-house deployments.
- Get as much information as you can about the people who manage your data
- “Ask providers to supply specific information on the hiring and oversight of privileged administrators, and the controls over their access,” Gartner says.

IIT KHARAGPUR | NPTEL ONLINE CERTIFICATION COURSES

So, if we look at user privileged access sensitive data process outside enterprise brings with it an inherent level risk; right, any sensitive data which is beyond going beyond your premise as a risk into the things outsourced services bypass the physical logical and personnel controls, right which is there if you are doing those of traditionally in house deployment. So, all these traditional in house deployments we have we bypass this. So, like a Gartner says that ask providers to supplies specific information on hiring and oversight of privileged administrator and controls over their access. So, that is there, but as such I a organization may feel insecure that while will it loses its number of controls to the provider.

(Refer Slide Time: 11:54)



**Regulatory Compliance & Audit**

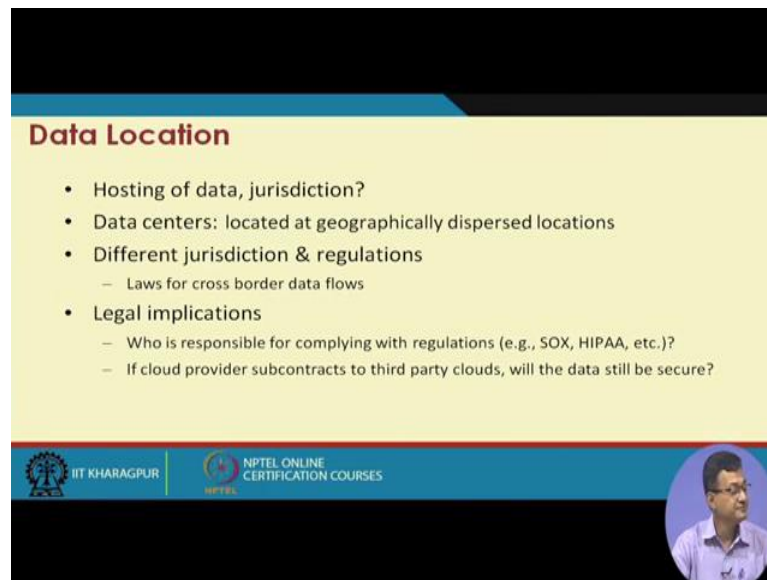
- Traditional service providers are subjected to external audits and security certifications.
- Cloud computing providers who refuse to undergo this scrutiny are “signaling that customers can only use them for the most trivial functions,” according to Gartner.
- Shared infrastructure – isolation of user-specific log
- No customer-side auditing facility
- Difficult to audit data held outside organization in a cloud
  - Forensics also made difficult since now clients don't maintain data locally
- Trusted third-party auditor?

IIT KHARAGPUR | NPTEL ONLINE CERTIFICATION COURSES

Next is the regulatory compliance and audit like traditional services are subject to external audits and security certification, right. So, so our traditionally in house services are there computing cloud computing provider who refuse to undergo a scrutiny signalling that the customer can only use them for the most trivial functions etcetera. So, in case of a cloud computing providers this type of things making audit etcetera become a tricky things right. So, because your data is there, but you do not have the control over the infrastructure. So, making the audit successful or compliance successful whether it will be compliance of that what the provider sends or what the provider supposed to do it or your compliance and things are like that. So, though the SLA tries to address this is but still there is a there are risk or what we say security loopholes there.

So, there are usually no customer side audit facilities difficult to audit data held outside organisation in a cloud trusted third party auditor maybe a thing then again how this auditor will be there and said that there is another question.


(Refer Slide Time: 13:09)



**Data Location**

- Hosting of data, jurisdiction?
- Data centers: located at geographically dispersed locations
- Different jurisdiction & regulations
  - Laws for cross border data flows
- Legal implications
  - Who is responsible for complying with regulations (e.g., SOX, HIPAA, etc.)?
  - If cloud provider subcontracts to third party clouds, will the data still be secure?

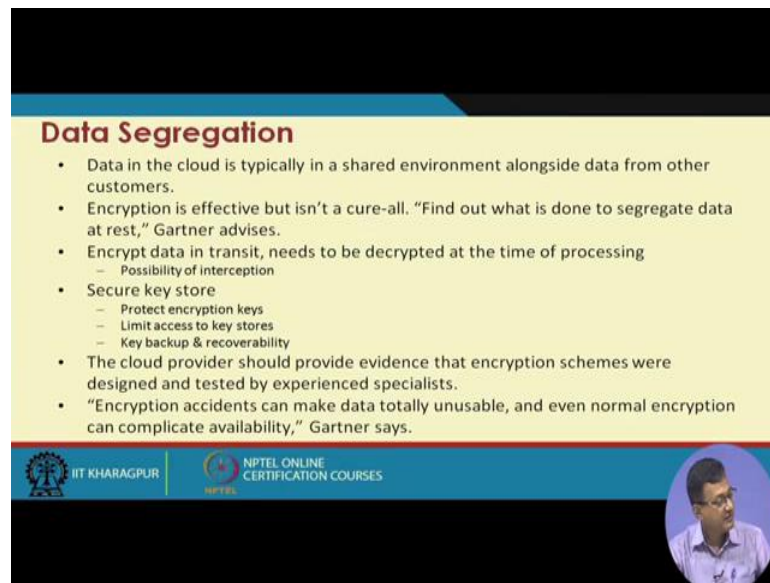
IIT KHARAGPUR | NPTEL ONLINE CERTIFICATION COURSES



Data location is a major issue, right where I share the data in the things where my data are hosted I do not have any clue whether in this country or outside country whether these jurisdiction of our own country or not or etcetera we do not want state it and either types of things up we do not have think.

So, that becomes a major issue data centres located at geographically dispersed location different jurisdictions and regulations and legal implications these has different legal implications like say held data they keep of protected in U.S. or other some other countries, but we do not have; we have a different type of things here and that it creates a problem that if are the data is store there that whose law will prevail on the thing.


(Refer Slide Time: 13:58)



**Data Segregation**

- Data in the cloud is typically in a shared environment alongside data from other customers.
- Encryption is effective but isn't a cure-all. "Find out what is done to segregate data at rest," Gartner advises.
- Encrypt data in transit, needs to be decrypted at the time of processing
  - Possibility of interception
- Secure key store
  - Protect encryption keys
  - Limit access to key stores
  - Key backup & recoverability
- The cloud provider should provide evidence that encryption schemes were designed and tested by experienced specialists.
- "Encryption accidents can make data totally unusable, and even normal encryption can complicate availability," Gartner says.

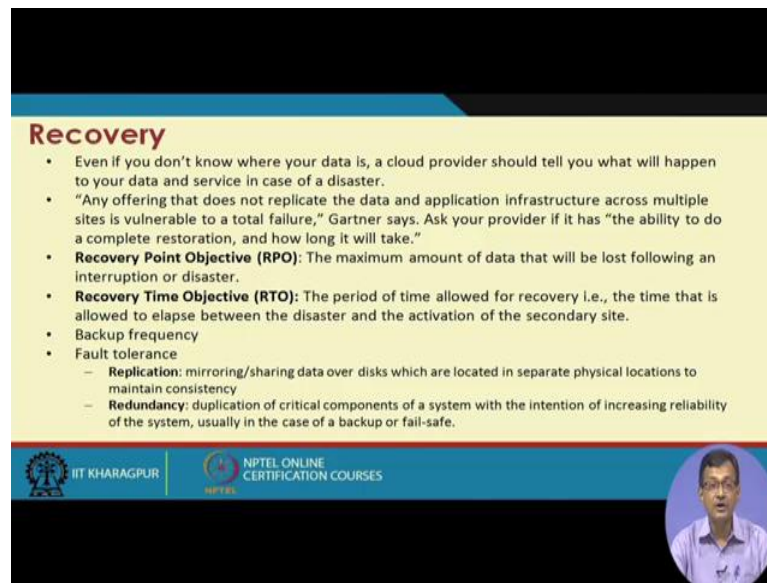
IIT KHARAGPUR | NPTEL ONLINE CERTIFICATION COURSES



Data segregation is another issue another which a pointed out by Gartner the data in the cloud is typically in a shared environment alongside data from other end customers, right encryption effective, but is in that cure all type of solution, right find out what is done to segregate data at rest.

So, encryption data encrypt data in transit needs to be decrypted at the time of processing another major issue, right. So, where the key will lie at types of things. So, there should be a secure key store resource the cloud provider should provide evidence that the encryption schemes were designed and tested by experienced specialist or what is the test mechanisms and what should the encryption scheme and type of things. So, these are several challenges which are data segregation related things which are not there in a big way when we have used additional systems.


(Refer Slide Time: 14:58)



**Recovery**

- Even if you don't know where your data is, a cloud provider should tell you what will happen to your data and service in case of a disaster.
- "Any offering that does not replicate the data and application infrastructure across multiple sites is vulnerable to a total failure," Gartner says. Ask your provider if it has "the ability to do a complete restoration, and how long it will take."
- **Recovery Point Objective (RPO):** The maximum amount of data that will be lost following an interruption or disaster.
- **Recovery Time Objective (RTO):** The period of time allowed for recovery i.e., the time that is allowed to elapse between the disaster and the activation of the secondary site.
- Backup frequency
- Fault tolerance
  - **Replication:** mirroring/sharing data over disks which are located in separate physical locations to maintain consistency
  - **Redundancy:** duplication of critical components of a system with the intention of increasing reliability of the system, usually in the case of a backup or fail-safe.

IIT KHARAGPUR | NPTEL ONLINE CERTIFICATION COURSES



Another point and what we are we are extremely concerned is the recovery right if something goes wrong what sees the recovery mechanism even if you do not know where the data your data is data providers is to tell you what happens to your data and services in case of a disaster if there is a disaster then or outrage; then what happened to my data, right a store I in a say share data storage I store my data and if goes for some problem, then what happened whether how much time it will take recovery at all whole recovery is possible or not these are the things which will be questioned, right.

So, there are there are 2 concepts if you will try to use one is the recovery point objective the maximum amount of data that will be law has to following a interruption or disaster. So, that is the RPO; recovery point objective; there is RTO; there is a period time period allowed for recovery that the time that is allow to elapse between the disaster and activation of the secondary side, right. So, that that they how much time, even it is recovered how long it will take. So, that my business process not does not get much affected. So, fault tolerance 2 type of things, it is followed one is that replication that of the same thing or redundancy or duplication of critical components of the systems and type of things.

(Refer Slide Time: 16:25)



**Investigative Support**

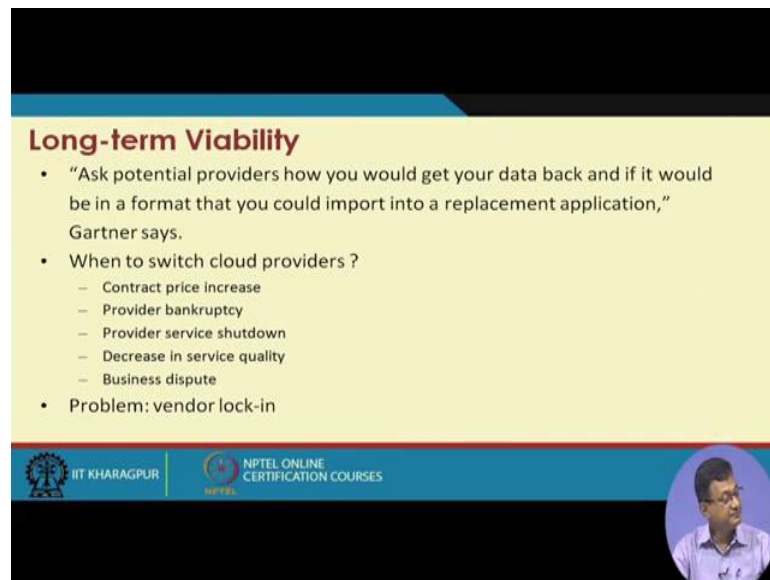
- Investigating inappropriate or illegal activity may be impossible in cloud computing
- Monitoring
  - To eliminate the conflict of interest between the provider and the consumer, a neutral third-party organization is the best solution to monitor performance.
- Gartner warns. "Cloud services are especially difficult to investigate, because logging and data for multiple customers may be co-located and may also be spread across an ever-changing set of hosts and data centers."

IIT KHARAGPUR | NPTEL ONLINE CERTIFICATION COURSES



Then investigative support another risk component as mentioned by things like investigation investigating inappropriate or illegal activity may be impossible in cloud computing like how to investigate on the things especially there is not much control on the customer side. So, neither there is much control on monitoring the things.


(Refer Slide Time: 16:51)



**Long-term Viability**

- "Ask potential providers how you would get your data back and if it would be in a format that you could import into a replacement application," Gartner says.
- When to switch cloud providers ?
  - Contract price increase
  - Provider bankruptcy
  - Provider service shutdown
  - Decrease in service quality
  - Business dispute
- Problem: vendor lock-in

IIT KHARAGPUR | NPTEL ONLINE CERTIFICATION COURSES



Long term viability; so, I leverage the things my work processes work flows or my deferent organisational processes into the cloud and I end up in a long term viability things or long term arrangement with the things, right.

Ask potential provider; how would you get your data back if it would be in a format that would import from a replacement application etcetera. So, if there is a; from one provider to another provider then how the data will be there and how data can I can recover my data if there is the if there is a problem with the provider. So, when to switch cloud provider contract price increase provider bankruptcy provider service shutdown decrease in service quality business dispute and all those things mainly to for thus consumer to switch cloud providers the major is vender logging vender lock in. So, that with the particular provider the consumer gets locked in and it is very difficult to recover from that lock in phase.

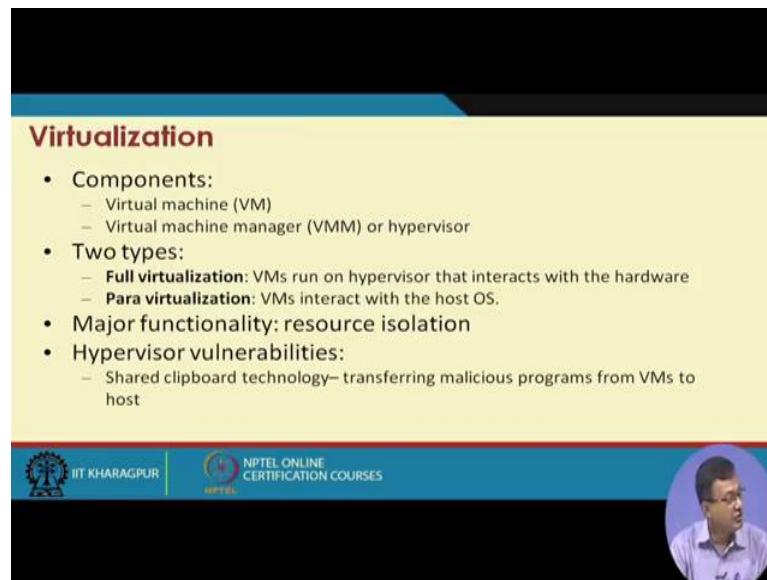
(Refer Slide Time: 18:01)



So, these are the major Gartner issues. So, there are few more issues which are which are critical which are critical. So, there is one is virtualization, access control and identity management, application security, data life data lifecycle management, right. So, one is the issue of the virtualization what you have seen the virtualization is primarily done by that VMM or the hypervisor, right.

So, the virtualization becomes the key of this cloud computing. So, if I have a VM so; that means, it is evolved from the basically handled by the VMM. Now if the VMM is compromised or then my I am in trouble even though even that different processes of the VM, etcetera to some level compromise then the whole system is in trouble.


(Refer Slide Time: 18:59)



**Virtualization**

- Components:
  - Virtual machine (VM)
  - Virtual machine manager (VMM) or hypervisor
- Two types:
  - **Full virtualization:** VMs run on hypervisor that interacts with the hardware
  - **Para virtualization:** VMs interact with the host OS.
- Major functionality: resource isolation
- Hypervisor vulnerabilities:
  - Shared clipboard technology– transferring malicious programs from VMs to host

IIT KHARAGPUR | NPTEL ONLINE CERTIFICATION COURSES



So, if you look at the virtualization there are 2 component one is virtual machine one at VMM or the hypervisor or virtual machine monitor as we have seen. So, 2 type of primarily 2 type of virtualization one is full virtualization VMs run on the hypervisor that interacts with the hardware.

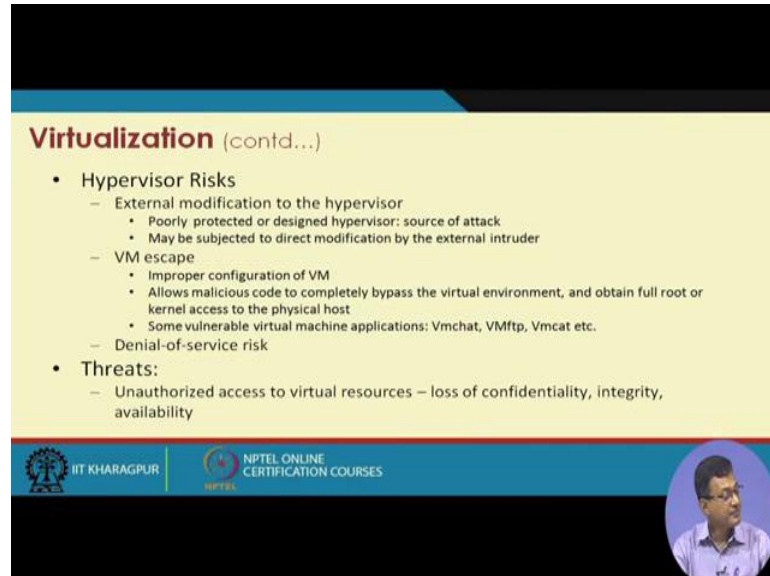
So, that the VM is there in between hypervisor and the rest of the hardware it interacts another is a para virtualization when a VM interacts with the host OS directly; that means, it penetrates to a level higher; so that 2 type of things major functionality resource isolation, right. So, what it tries to do it tries to isolate this consumer or the user with the rest of the infrastructure at the back bone and so that it basically tries to provide difference scalable services over the things, right. So, hypervisor vulnerabilities; now if there is a hypervisor vulnerability that will cropping and basically put the whole system in trouble; so, shared clipboard technology transferred malicious programs from VMs from VMs to the host and type of things. So, hypervisor vulnerability key stroke logging; so, 1 bun one such things that some VM technologies enable logging of key stores and the screen updates to be passed across virtual terminals in the single virtual machine.

So, these are some of the properties of the things and that becomes a threat right there are hypervisor risk like there can be a rogue hypervisor root kits initiate a rogue hypervisor and it its creates a havoc into the system hide itself from the normal malware detection



system create a covert channel to dump unauthorised codes right it can create even create a covert channel to dump with the unauthorised codes.


(Refer Slide Time: 20:59)



**Virtualization (contd...)**

- **Hypervisor Risks**
  - External modification to the hypervisor
    - Poorly protected or designed hypervisor: source of attack
    - May be subjected to direct modification by the external intruder
  - VM escape
    - Improper configuration of VM
    - Allows malicious code to completely bypass the virtual environment, and obtain full root or kernel access to the physical host
    - Some vulnerable virtual machine applications: Vmchat, VMftp, Vmcat etc.
  - Denial-of-service risk
- **Threats:**
  - Unauthorized access to virtual resources – loss of confidentiality, integrity, availability

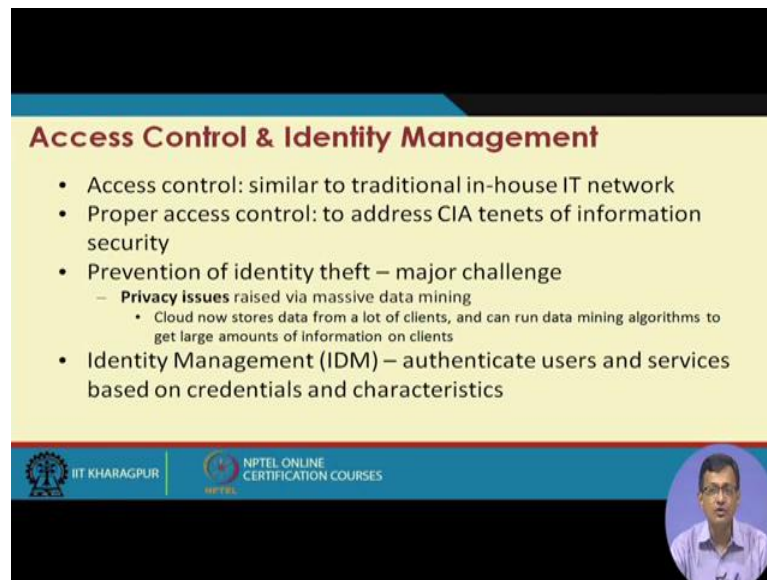
IIT KHARAGPUR | NPTEL ONLINE CERTIFICATION COURSES



There are other hypervisor risks like that external modifications of the hypervisor or VM escape in proper configuration of the VM. So, there can be other issues there are denial of services attacks.

So, there are issues of threats unauthorized access to virtual resources loss of confidentiality integrity availability and these are these are the different issues of these are the different threats which are there is a high loss of confidentiality integrity availability. That means, what we refer to these types of CIA related issues will come in to play.


(Refer Slide Time: 21:42)



**Access Control & Identity Management**

- Access control: similar to traditional in-house IT network
- Proper access control: to address CIA tenets of information security
- Prevention of identity theft – major challenge
  - **Privacy issues** raised via massive data mining
    - Cloud now stores data from a lot of clients, and can run data mining algorithms to get large amounts of information on clients
- Identity Management (IDM) – authenticate users and services based on credentials and characteristics

IIT KHARAGPUR | NPTEL ONLINE CERTIFICATION COURSES



Access control is a big gain as those who have gone through access control things like one is that troll base access control and different type of MAC; DAC type of things. So, those issues are there. So, access control similar to traditional in house it network in here also proper access control to address CIA tenets of information security, right. So, prevention of identity theft major challenge primarily privacy issues via massive data mining.

So, that I whether I can have some learning techniques and data mining techniques to find out the identity of the user or the cloud service consumer identity management is another challenge it is a challenge not only here it is a challenge across if any distributed or in type of system. So, identity management authenticate users and services based on credential and characteristics right. So, it based on different features said it tries to look at that um that I have to authenticate the users and services.

(Refer Slide Time: 22:56)

**Application Security**

- Cloud applications – Web service based
- Similar attacks:
  - **Injection attacks:** introduce malicious code to change the course of execution
  - **XML Signature Element Wrapping:** By this attack, the original body of an XML message is moved to a newly inserted wrapping element inside the SOAP header, and a new body is created.
  - **Cross-Site Scripting (XSS):** XSS enables attackers to inject client-side script into Web pages viewed by other users to bypass access controls.
  - **Flooding:** Attacker sending huge amount of request to a certain service and causing denial of service.
  - **DNS poisoning and phishing:** browser-based security issues
  - **Metadata (WSDL) spoofing attacks:** Such attack involves malicious reengineering of Web Services' metadata description
- Insecure communication channel

IIT KHARAGPUR | NPTEL ONLINE CERTIFICATION COURSES

So, at the application level it is mostly there is cloud applications are web based; right.


Most of the applications are web based. So, similar type of attacks like injection attacks x xml signature element wrapping attack cross site scripting attack flooding DNAs poisoning and phishing metadata like WSDLs spoofing attacks; so, these are the different attacks which are still prevailed in case of a in case of application level cloud security, right. So, there can be insecure communication channel because at the application level your data is data is more vulnerable right. And that insecure communication channel can lead to interrupts and of the services eavesdropping and so and so forth.

(Refer Slide Time: 23:56)

**Data Life Cycle Management**

- Data security
  - Confidentiality:
    - Will the sensitive data stored on a cloud remain confidential?
    - Will cloud compromise leak confidential client data (i.e., fear of loss of control over data)
    - Will the cloud provider itself be honest and won't peek into the data?
  - Integrity:
    - How do I know that the cloud provider is doing the computations correctly?
    - How do I ensure that the cloud provider really stored my data without tampering with it?

IIT KHARAGPUR | NPTEL ONLINE CERTIFICATION COURSES



Data lifecycle management; so, need to look at that over all data lifecycle; so, one is that your confidentiality right will the sensitive data stored on cloud remains confidential that is one major question or major challenge we will cloud compromise leak confidential client data right fear of loss of control over the data. So, that is another problem will the cloud provider itself be honest and wont peek into the data that is a how much trust into the things. So, a trusting a provider is a is another challenge that is for of in our day to day life also if we need to trust or we need to build trust on deferent service provider.

So, there are lot of work going on; we will try to if time permits, we will try to see some of the aspects of this; how this task risk competence were together and we have a mechanism of a more security or how can I select a more trusted provider for a particular work; if there are more than one provider for that. So, that is one the confidentiality another aspect is the integrity; how do I know that the cloud provider is doing computations correctly right. So, I do some processing then how do I know that it is things because I push my data and process and I expect is result out of it.

How do I ensure that a cloud provider really stored my data without tempering it? So, how do I ensure that right availability?

(Refer Slide Time: 25:48)

**Data Life Cycle Management (contd.)**

- Availability
  - Will critical systems go down at the client, if the provider is attacked in a Denial of Service attack?
  - What happens if cloud provider goes out of business?
- Data Location
  - All copies, backups stored only at location allowed by contract, SLA and/or regulation
- Archive
  - Access latency

IIT KHARAGPUR | NPTEL ONLINE CERTIFICATION COURSES

With critical system go down at the client if the provider is attacked in a denial of service attack, right; so, this is another availability with the critical system go down at the client if the provider is at attacked in a denial if there is a dos type of a attack on the provider end; what will happen to my things right if that a even if the cloud provider goes out of business what will happen to my data and processes. So, these are very tricky issues and extremely difficult to address this type of challenges data locations as we have seen; if we look at the data lifecycle data location all copies beck up stored only at location allowed by the contract SLA or regulation, etcetera, right.

So, where the data are located which extension etcetera we do not have much control over the things then archive access latency these are the different other issues which are which are there in this type of scenarios. So, if we if we look at holistically that the overall cloud aspects. So, one major problem is co-tenancy; that means, you are your data processes are residing on the same system.

Another issue what we have seen that which is which is making it different from the traditional thing another issue is your data is located in somewhere where I do not have any control over the things data even my application function processes are located in the premises where I do not have much control other than looking at the SLAs and type of things. So, this is another major challenge of handling those type of a scenarios there are the other tricky issues which come up because if there are inter cloud communication,

then the issues are become more tricky, like a process at cloud 1 communicating to the cloud 2 communicating to the cloud 3 and so forth in doing. So, whether it is able to again that it is coming back to the originating cloud in doing. So, is it possible that I can there is a possibility or there is a chance that I violate the basic principle of access control like I am I am able to access a data which are otherwise I am not able to access it, right.

So, this is major challenge when there is a inter cloud communication things right. So, there is way that can be very much true because you are you have different provider consumers and a provider can be consumer for some other services and so on and so forth. So, that is another issues and there are other underlining threats like what will happen if the VM VMM is compromised if the hypervisor is compromised, then likely that all the VMs can be compromised, right or all the VMs are in a spin like which VM is up or down etcetera whether it is functioning properly or not we do not have any control.

So, there are underlining challenges at the IaaS level itself. So, these are the which need to be; access and finally, when selecting cloud providers or things; how can I trust each other, right how whether the SLA in the things or if I have more than one providers for a things whether there is a possibility or whether there is a mechanism that I can know that this is these are the different trust, etcetera.

So, the trust competence risk also plays a serious role into the things in looking at all these aspects we see that the cloud is this cloud security or the security issues in cloud plays a extremely vital role in making this cloud computing popular other than coming this coming that resource availability and other type of cross benefits of traditional versus cloud etcetera. This security issues become a major bottleneck going from say traditional to the cloud computing things.

So, with this we will wrap up our today's lecture and in the subsequent lecture we will see that other aspects of cloud.

Thank you.