Cloud Computing

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

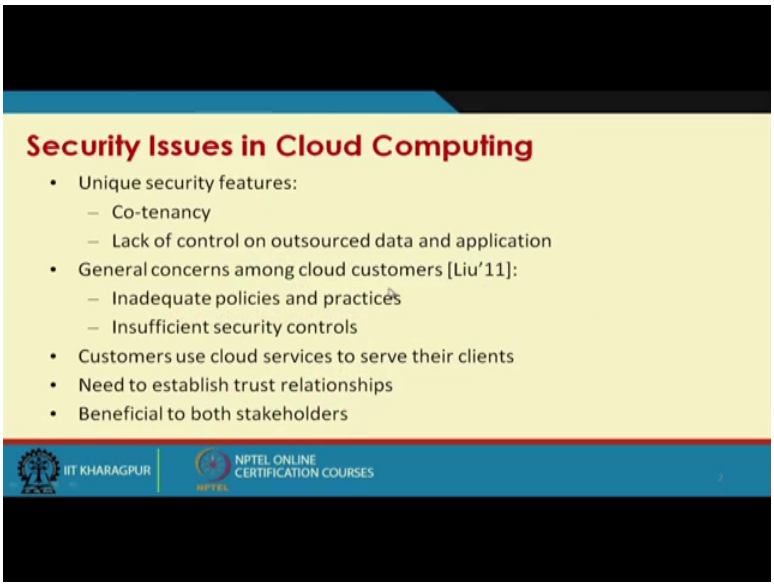
Lecture – 28
Cloud Security – IV

Hello. We will be continuing our discussion on Cloud Computing. Today we will talk about some aspects of a cloud security rather we will look at a sort of a scenario where how this security plays a role and what are the different aspects. This is primarily with the SaaS a type of cloud more of collaborating SaaS clouds. So, this what we are looking that you had presently or in near future that lot this sort of clouds will be communicating between each other; that means, in other sense this a this consumer or different stakeholders having their application in the in the cloud will be communicating with other applications in other cloud.

So, in other sense it is a collaborative SaaS cloud or collaborative collaboration at the application level of the cloud. So, today's discussion will be looking at one of this what are different security aspects when we collaborate between each other we will see that there are very tricky issues of each comes into play. So, this one of this approach this is work of one of my PhD scholar (Refer Time: 01:44) a goes he his work will be describing, but we will be looking at more broader aspects that how things should be there.

So, this will be good to for many of you who are looking at some sort of a research or some sort of a more studying into these aspects of the things.

(Refer Slide Time: 02:11)



So, it is security issues in collaborative SaaS cloud. So, as a just to recap if you look the look at the security issues in cloud computing. So, which are typically or unique to this cloud is one is co tenancy right. Numbers of applications are residing or different user are residing in the same physical infrastructure. So, co tenancy is a major issue. And lack of control on outsource data and applicants that is another typically or uniqueness of this type of cloud platform right.

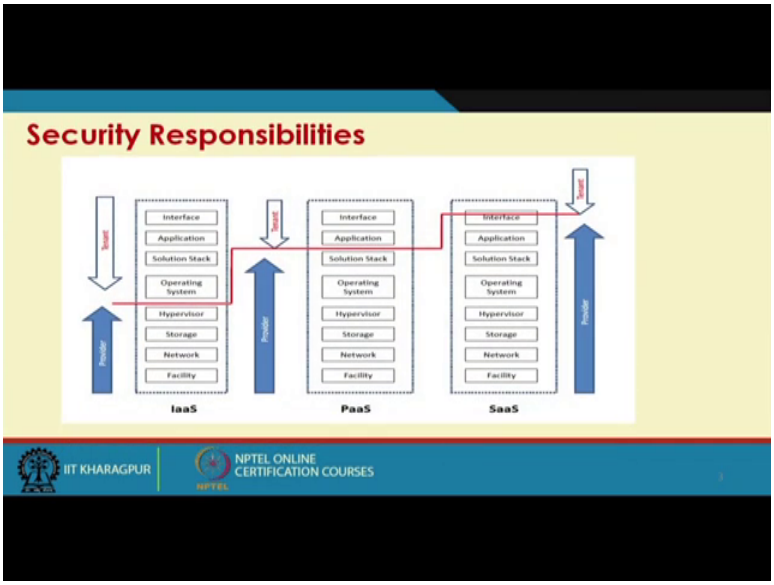
So, we have once I off load my data and application on or outsourced in a cloud, then we do not have much control over that things. Or our control is decided by the provider right. The whatever we I can control or whatever the handlers I am having for the control is primarily decided the by the service provider. So, these are this in other sense if we look at the security point of view this, this is a constraint of how my data and you need to be secured, what is the what is the how much it is exposed to the external other applications and other type of users and all those things.

There are other general concern like inadequate policies and practices, that is another concerned and insufficient security control as we are looking talking about. So, customers use cloud services to serve their clients. So, customers and can use a cloud services to serve their clients. So, running the applications on those cloud services needs to establish trust relationships right. So, it is there is requirement that how much I trust this service provider. So, there is a major requirement for that and there are this can be

beneficial for both the stakeholders the customer and provider. So, it is not only the provider how the customer trust the provider there is a question of how much whom I am if I am a service cloud service provider if the customers for me or the consumer of the service services, should be also trust out this.

So, there should not be malicious customer who will create a problem out of the things it is not always that it is not that thing because the cloud service provider their business is selling the services. So, they may not be malicious or they may not have any malicious instead any malicious intent. However, you can in the process you can have some malicious customers which are usually the scenario, who can use the services use the platform to attack or peep into others data and type of things.

(Refer Slide Time: 05:10)



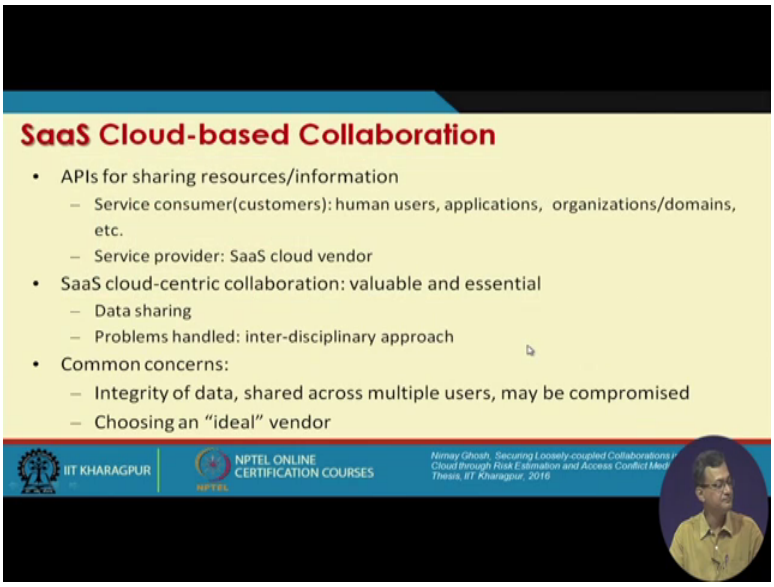
So, if I this is a thing which is available in it is a various literature we have also seen. That if you look at the security responsibilities in case of IaaS the responsibility up to the hypervisor end after that it is having the operating system or the guest operating system so and so forth, it goes to the tenant right. So, the providers responsibility up to hypervisor in case of PaaS cloud provider responsibility is up to that platform or that were are the solutions stack is there.

In case of a SaaS it is responsibility goes up to the interface application interface right. So, it is the things like if I am using a say a API for what processing. So, it is up to that level the responsibility of providers coming to play, for the for the consumer it is it is it is

up to that up to that application level the services are there this security are handled by the provider.

So, we can see that at various type of clouds we have different type of level of security. So, in case of a SaaS there is lot of things which depend on the on the providers send. Like I am if I am using a say what processing service or any type of text (Refer Time: 06:33) service. So, as I am using that API somebody else also maybe using that API.

(Refer Slide Time: 06:46)

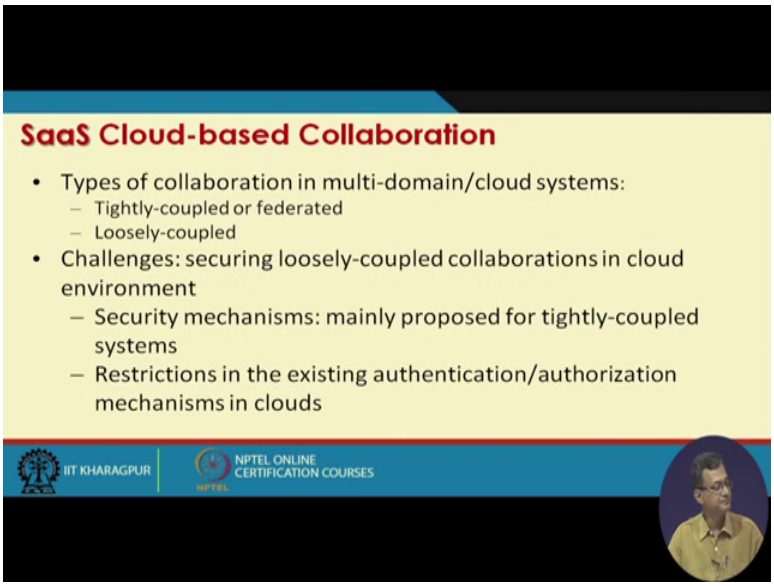


So, it is the same application level I can have different instances which are working for different type of things. So, SaaS cloud base collaboration. So, what broadly we try to mean that API for sharing resources, and information service consumer or customers human users applications organization domains. And anybody service provider are the cloud vendor SaaS cloud, SaaS clouds centric collaboration. So, they are there are some of the essential things like data sharing issues problems handled like interdisciplinary approaches human to be taken to handle different type of issues.

So, common concerned is integrity of the data shared across multiple user may be compromised things right. A as there is a the data is being shared across or the basic platform is share across multiple users. So, there may be a compromises and there may be a chance of being compromised. And how do I choose a ideal vendor or a service provider is one of the major challenge if there a number of provider then how do I choose the provider.

So, as am I send this is work of my one of my PhD student is doctor nirnay ghosh who worked on this area. And we will be taking some part of his work to describe and the more we will be taking the challenges we taken up in this particular problem. So, it will be good to look at those a type of things.

(Refer Slide Time: 08:18)



So, type of collaboration in multi domain or cloud systems is tightly coupled or federated can be one way of looking at it. Where I have strong connectivity between this type of federating clouds or they are loosely coupled systems. So, that they there are federally cloud, but they are loosely coupled system. So, I have instances in different cloud may be in the same cloud, but they are loosely coupled. So, they are not very strongly coupled.

So, there are various changes securing loosely coupled collaboration in cloud environment is a major problem, and security mechanisms mainly proposed for tightly coupled systems. So, what loosely coupled there are not much security mechanism. So, whenever you look for the security mechanism as we discuss earlier, it send to in phenomena. So, there is the requirement is goes hand in hand. So, in turn it comes to be more tightly coupled thing restriction in the existing authentication authorization mechanisms in cloud there is another problem that the type of each mechanisms you are having at in the present day cloud may be a restrictive to having those secretive phenomena in place.

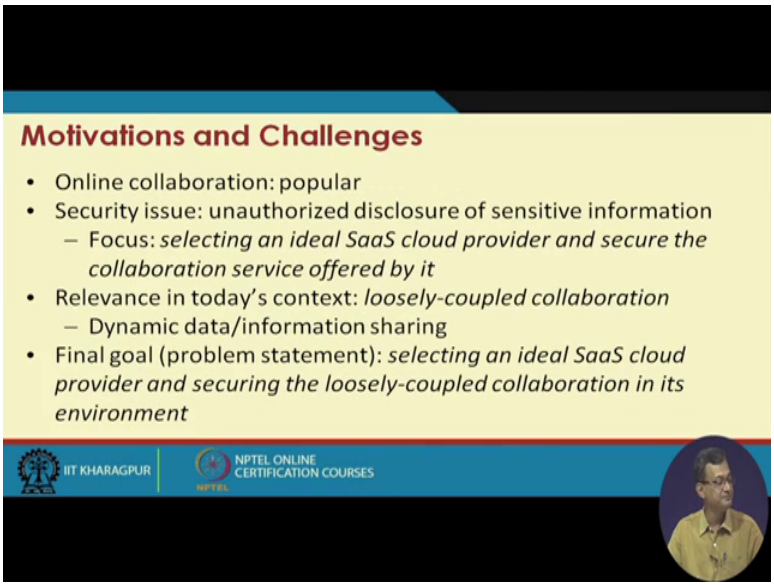
(Refer Slide Time: 09:30)

So, there are a lot of challenges and which motivates or I if you look at in the other way these are the motivation for having research or study in this area, like SaaS cloud delivery model, So maximum lack of control right. So, whole control on the service provider end; so these has the minimal that the control on the consumer end. No active data stream audit trails outage reports are directly available to the things, whatever is provided by the consumer need to be looked into.

So, major concern in uses of the cloud services; so broad scope address security issues in the cloud we need to address. So, there is a concept of cloud marketplace coming up like that rapidly growing due to recent advancements. So, we have a typically a cloud market place where numbers of providers number of consumers there is a economic model is goes on I am not talking about a cloud economics talking about that where you go for better services not only pricing quality of services better a sale is better security and things are there.

So, availability of multiple service provider is a major challenge of choosing that which service provider we need to look at like. So, there is inconsistent in service and a guarantees no standard clauses. So, there is a selecting an ideal SaaS cloud provider and is a issue, and how to if I after selection what are the different other security challenges can come up.

(Refer Slide Time: 11:10)

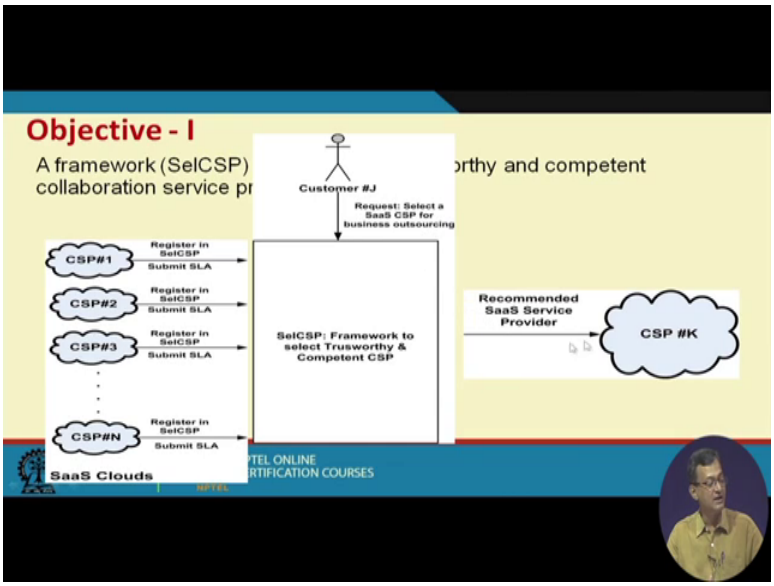


So, there are other things like online collaborations are becoming pretty popular right. There are several security issues I finding a ideal provider. Relevance of today's context there is a loosely coupled collaboration dynamic data information sharing like if you look at any e marketplace or look at any type of service provider like what we see that any type of things where you purchase and over online purchase selection etcetera, even your travel booking centers.

So, there are different parties which are being connected and mostly they are loosely coupled there are parties who are provider of the products, there are parties who are provider of the financials area like credit card debit card to other types of services, there are parties who are courier services and type of things then they are being connected over in a loosely couple doing.

So, our goal is to select an ideal SaaS cloud provider and securing loosely coupled collaboration in it is environments. So, what are the different aspects. So, what are what they looking for a typical approach for that it is not like that that there are there are cannot be other approaches, but what way we can go into this particular problem.

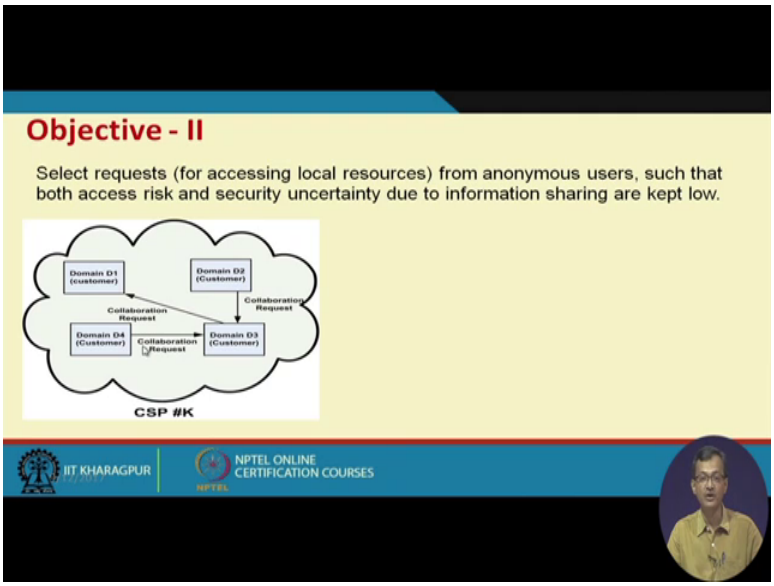
(Refer Slide Time: 12:34)



So, if you look at our one of the objective is to whether we can developed a framework like as I mentioned that in this particular work we developed a framework or sel a SelCSP selecting a trustworthy and competent collaboration service provider right.

So, there can be different CSP's in set of CSP's and registered in that particular some sort of a central authority. And the customer requesting to select a SaaS provider for business outsourcing, and it recommends that CSP particular k, or CSPi is the base suited for it is requirement looking primarily at the security aspects right. So, that is the goal of the thing.

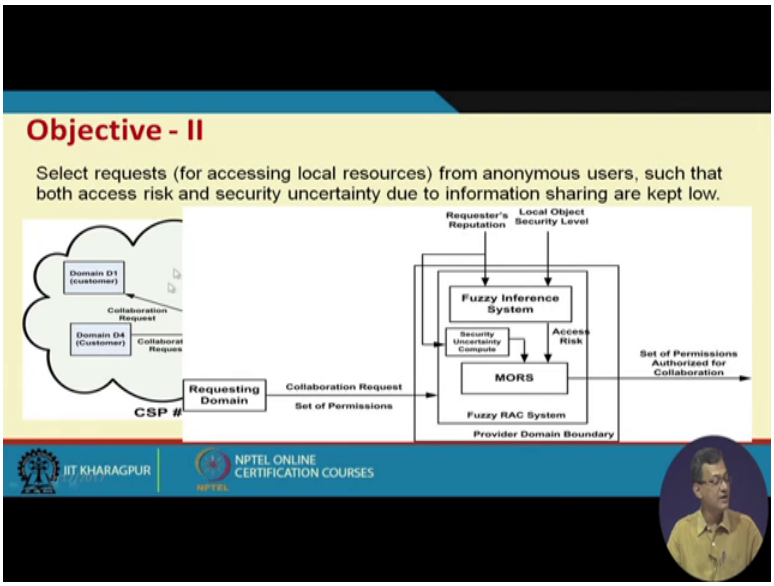
(Refer Slide Time: 13:23)



There can be there after the selection there can be select the request for accessing the local resource. So, once I once I select the particular CSPs, then we want to look at the select request for accessing local resources within the cloud, for anonymous user because we do not know who are the users, such that both access risk and the security uncertainty due to the information sharing are kept low.

So, our objective is to that access risk and security uncertain c for information sharing should be kept low or minimum. So, if I have that different customer in different domain, like a domain one domain 2 domain 3.

(Refer Slide Time: 14:18)



And they are collaborating in some somewhere other, say we need to have some sort of a mechanisms here we worked on a fuzzy inference system, which keeps a that. So, requesting domain collaborate request and set up permissions right. And say request reputation request are reputation local object security level like, and set up permission authorized for the collaboration. So, it is it is may So happen that I request for set of operations, and then I based on the basic policy engine and based on requester any reputation and local objects security level, I grant a set up permission authorized for the collaboration right.

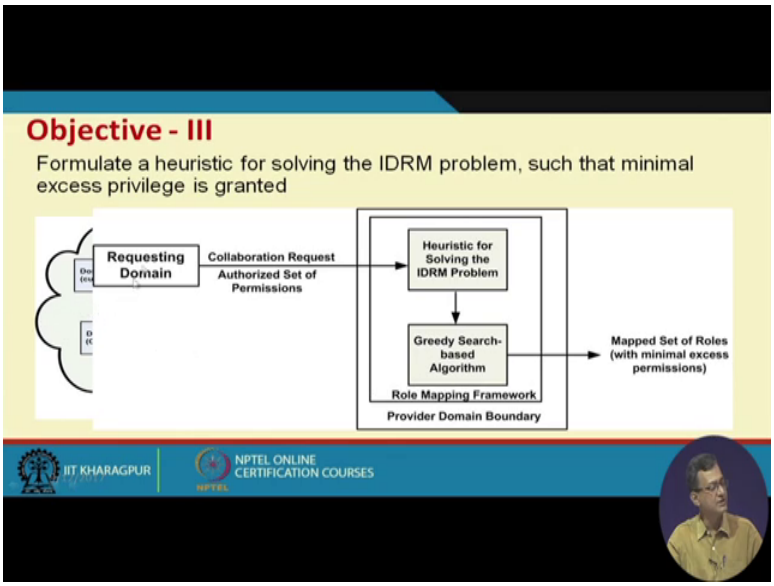
So, it is if some sort of a analogy we try to do, like I want to access some a particular office or type of things. And then based on the based on my reputation or credential I maybe given access to different type of things like I can be said that you can enter the campus you can enter the (Refer Time: 15:32) launch, but you cannot enter the actual office with based on my reputation another type of credential I may be allowed to inter the actual office, but; however, I cannot enter the say computing system lab or the where actual labs are there.

So, it based on your level of authority and your requirement and requesting domain you go on things like I go to a bank. And if I am just going to deposits some check or some documents then I go somewhere, if I want to look at meet the manager I go to some other level of accessibility and type of things and it depends that my requirement type of

things. Or in other sense if this miss access one misses or access role are decided by the by the my requesting role, and what is the permissible things for different type of objects like if my accessing a particular section of the thing is a if they if will take a object then based on needs access policy I be I need to be filter.

So, in case of a collaborative cloud, then when the customer comes with a type of request based on it is reputation another type of access policies on the objects. It has been granted a set of things, it not likely that whatever the particular customer has requested everything has been permitted, but a subset of that as can be permitted based on it is reputation.

(Refer Slide Time: 16:51)



So, other objective can be formulate a heuristic to look at that IDRM problem inter domain role mapping problem, such that minimal access privilege is granted.

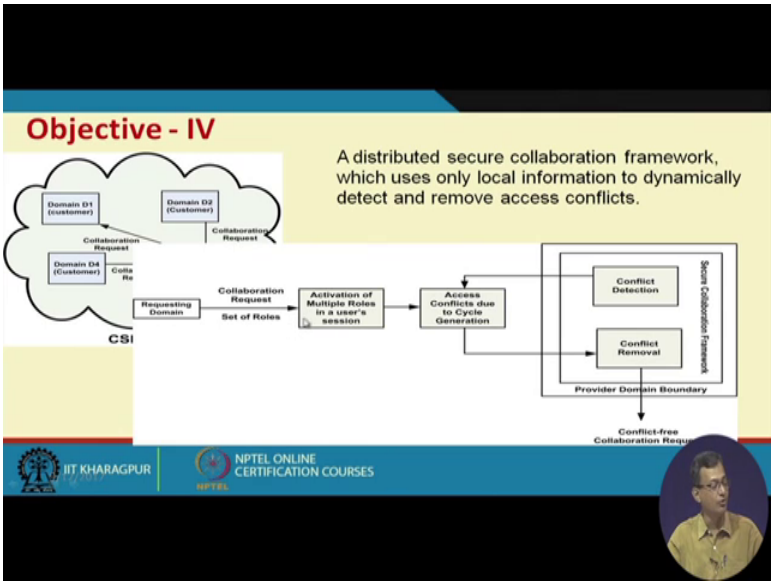
So, that is that is that is a problem for different type of things like, if I say from organizing a I want to access something at organization b, then the role of organization the role I am having in organization a need to be map to a equivalent role in the other organizations right. Like I am accessing as a financial organization from organization say 1, 2 another some as some data in the organization 2, and here I am accessing as a say a manager of level 1. And that data in order to which is equivalent to manager of level 2 they are. So, then my role need to be map to that particular level otherwise I cannot

access the thing. So, this is a this is a roll mapping problem is a is a problem which is there already and when need to look at it is there in this type of collaborating cloud also.

So, here also we try to say that requesting domain collaborating request authorized a set of permissions, and based on some heuristic for solving the IDRM problem we will see that this is a hard problem. And so, we need to have a some greedy research based algorithm and try to have a mapped a set up roles with a minimal excess permissions. So, minimal excess permission which it tries to say that I need to given that level of permission, which that minimal set of permission which I need to which is the which is required to execute the things.

Suppose I want to read a document. So, I can be given only read permission I can be given read and right permission. So, the minimal said maybe the reading the thing right. So, so that it is no x excess permission are no excess permissions are given to the thing. And another objective may be a distributed secure collaborative framework which uses only local information to dynamically detect and remove excess conflicts there is another major challenge in any type of loosely coupled these systems.

(Refer Slide Time: 18:52)



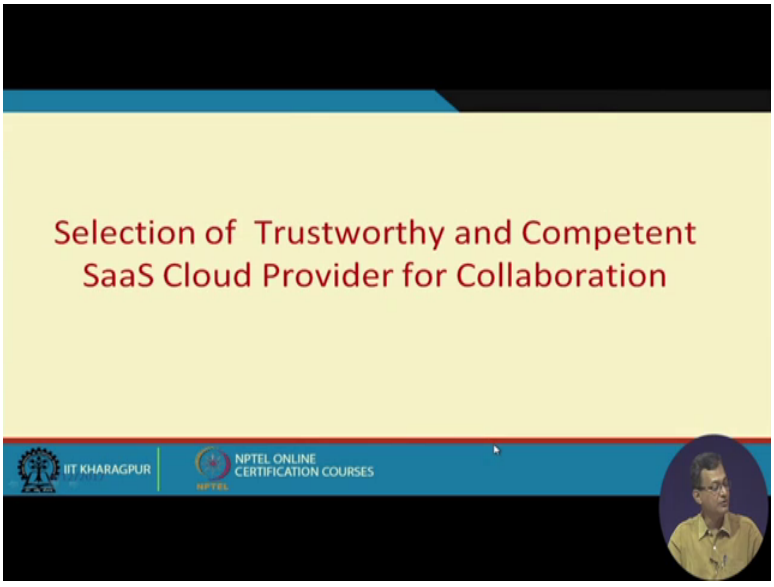
So, how I can have a dynamic framework with a only local informations? Now I want to excess organization one from or a organization one running into cloud instance in a cloud say in cloud providers cs CSP 1, want to access another data in CSP 2 of another

organization, then I may not have all the information of this either the CSP or the excess write of the things.

So, I need to I need to look at my local resources or local information and try to have the maximum security. In other sense when you have a loosely coupled things you may not carry all the credentials whatever it is having into collaborative. So, you should be there should be a mechanisms or there should be a way or there should be an approached that how I map it into the into my way of looking at it.

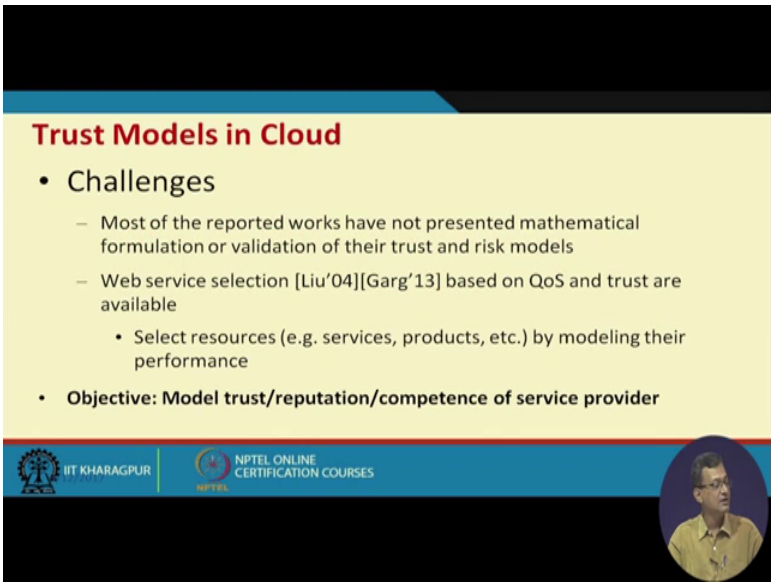
So, here also we tried a requesting domain collaborating request with a set of roles, activation of multiple roles in the users sessions right. And access conflicts due to the cyclic cycle generation there can if there is a cycle generation there can be a access conflict; that means, some document one way I am not able to access due to my particular role in a particular organization, but if it is goes to a cycle like an reach to this type of things.

(Refer Slide Time: 20:39)



So, there can be access conflicts. So, I need to have a conflict detection and conflict remover and then I should have a conflict free collaboration request right. So, this sort of mechanisms we need to look into.

(Refer Slide Time: 20:46)



So, one is the selection of trustworthy and competent SaaS cloud provider for collaboration. So, there are challenges of most of the reported works have not presented. So, there are several challenges objective is the model trust model trust reputation competence of the service provider. So, there are we are looking at 3 component, trust, reputation, competence. So, they are very much interlinked, but again there are they have some distinct property.

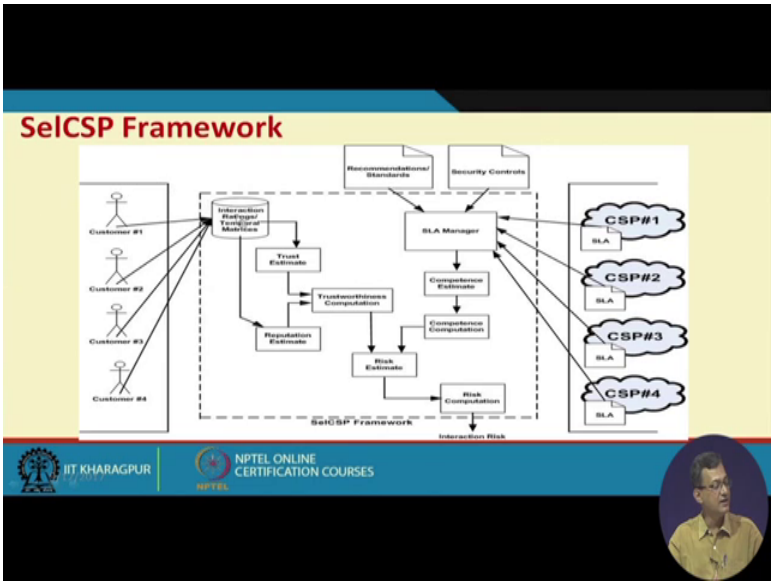
(Refer Slide Time: 21:19)

So, how much it is trusted? Whether it is competent to do that? And how what is it reputation right of doing a particular things or security type of things?

So, there are again challenges if you look at the SLA's because someone may argue that the SLA's tries to cover this, like majority of the cloud providers guaranteed availability of services right. Consumer not only demand availability of guarantee, but also other performance related assurance which are equally business critical. So, I am not only looking at the availability as a consumer, but also that assurances that this will be done this type of in timeframe or in a up to the compensation.

Present day clouds SLA's contain nonstandard clauses regarding assurance and compensation following a violation. So, there are compensation of the penalty scheme they follow some nonstandard present, nonstandard in the since there is no standardize mechanism across the cloud thing. So, one again a establish a standard set of parameters for cloud SLA's since it reduces the perception risk of the outsourced services. So, there should be way to reduce the perception resource.

(Refer Slide Time: 22:21)

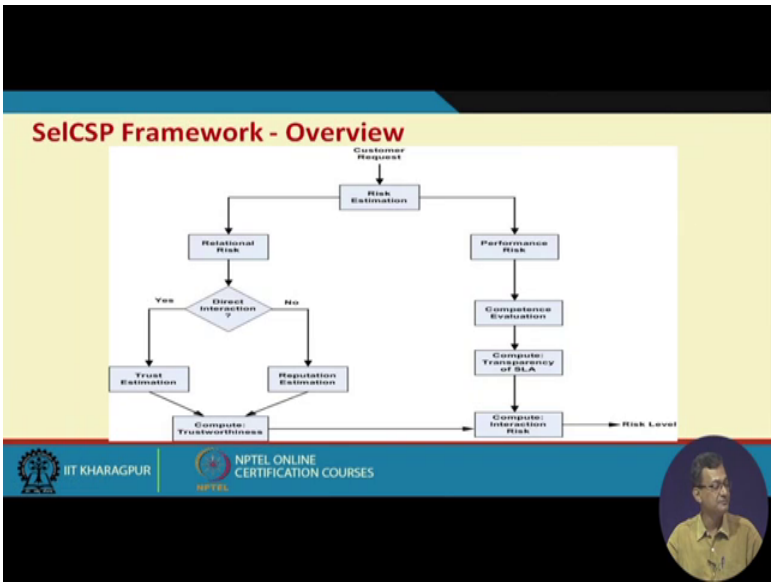


So, this is again a we try to look at a framework whether there are different customer. So, interaction rating and temporal matrices are complete computed. So, trust estimation reputation estimation trust worthy the compu worthiness of the computation then risk estimation and risk computation. On the other hand what we have recommendation and

standard security controls which drives the SLA's managers and this all this with the service provider there are a SLA's, right.

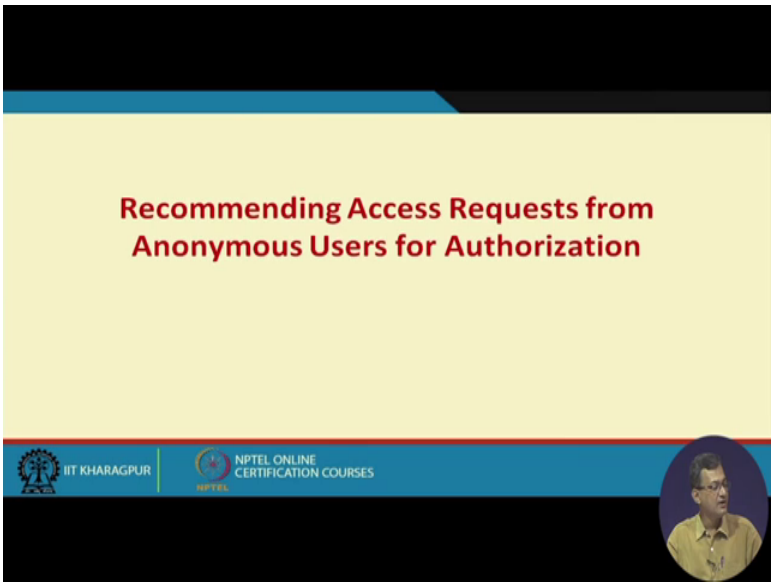
They provides some level of SLA's then competence estimation competence computation one side that we calculate trust worthiness another side competence, risk estimation, risk computation of the particular things and interests in risk. Out of that we try to find out interaction these between for different service provider.

(Refer Slide Time: 23:10)



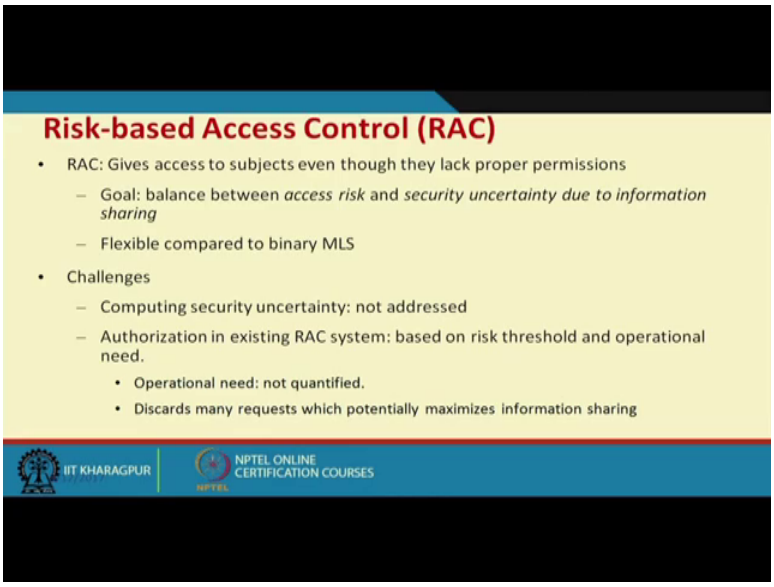
So, there are different flow of these is SelCSP framework, that is a one is risk estimation and can be relational risk direct interaction trust estimation same thing We want to put in it in the flow chat.

(Refer Slide Time: 23:30)



The second is recommending access request from anonymous users for authorization.

(Refer Slide Time: 23:36)



So, one is that risk based access control right. So, though we have heard about other type of access control, I role based access control this we term as a risk base access control.

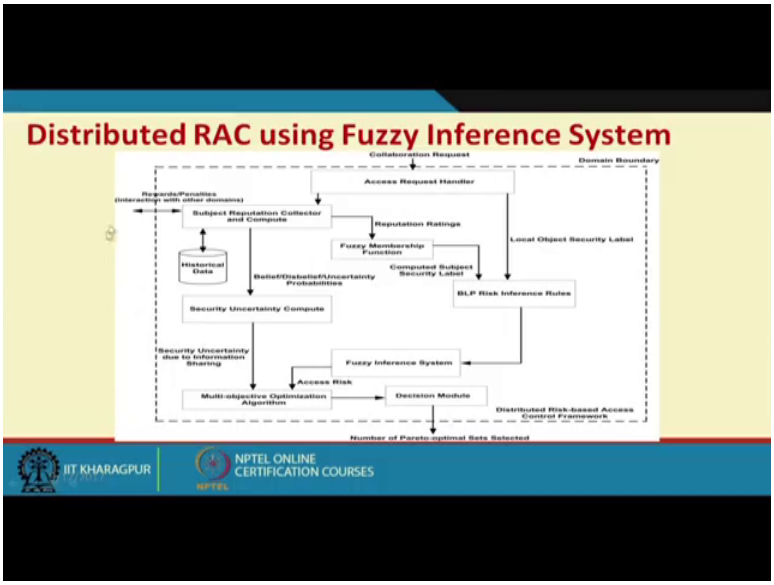
So, gives access to a subjects, even though they lack proper permissions right. So, I have I do not have to have the whole set of permissions which are fully coupled. So, can whether I can give the access with some amount of risk involving it right. It is not that is

binary stop on or off, but those sort of things. Goal balance between the accesses risk an security uncertainty due to information sharing right.

Flexible compared to the binary MLS. So, that is little bit of as we are talking about that instead of binary I take care of little bit of risk right. So, challenges computing security uncertainty is not a fully addressed stuff right. So, how to I look at computing security uncertainty right? Authorization in existing risk base access control system based on risk threshold sold and operational needs, right. Operational need not is quantified. It is difficult to quantified, operational risk did discards many request which potentially maximize information sharing right.

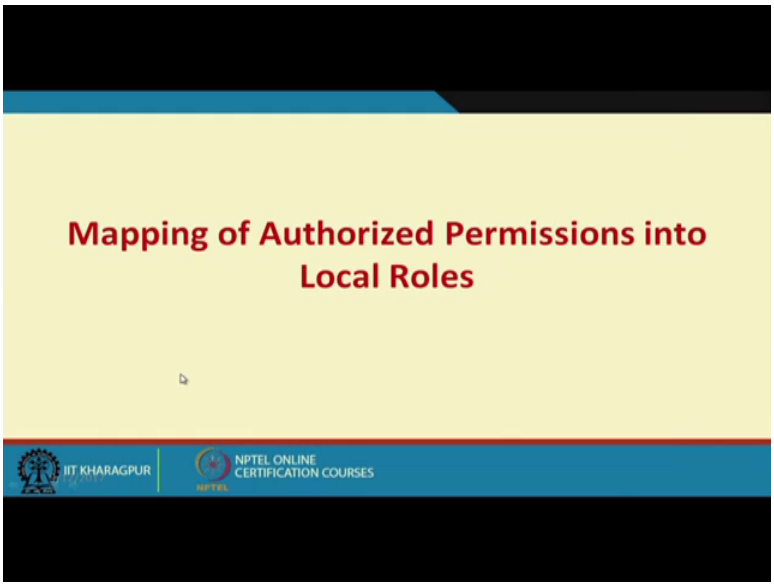
So, in order to reduce it we discards many request which prove purse potentially maximize the information sharing so that my overall risk come down. So, in other sense in order to reduce the risk we try to reduce the collaboration itself right.

(Refer Slide Time: 25:29)



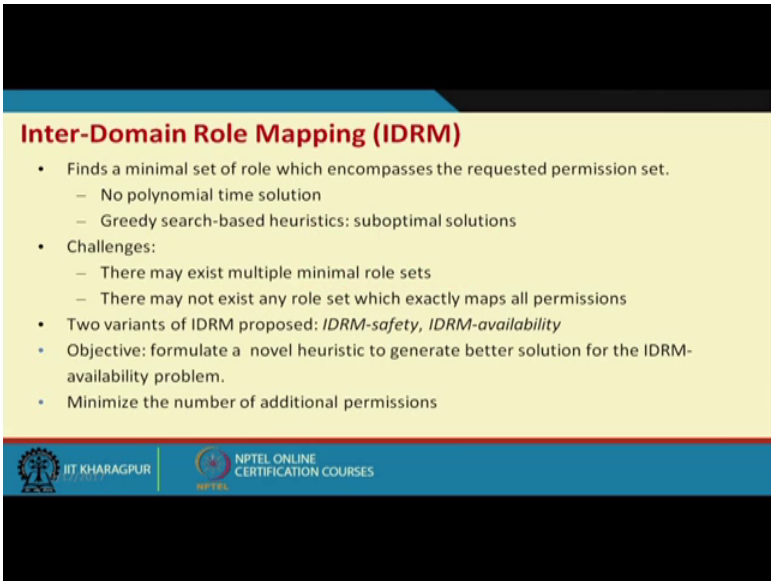
So, that it is one of the looking at it. So, there is a distributed frame work as we used a file fuzzy inference system to look at it. And it tries to find out a distributed racking to the thing.

(Refer Slide Time: 25:40)



The next one is mapping authorize permission into local roles right. So, inter domain roll mapping thing IDRM.

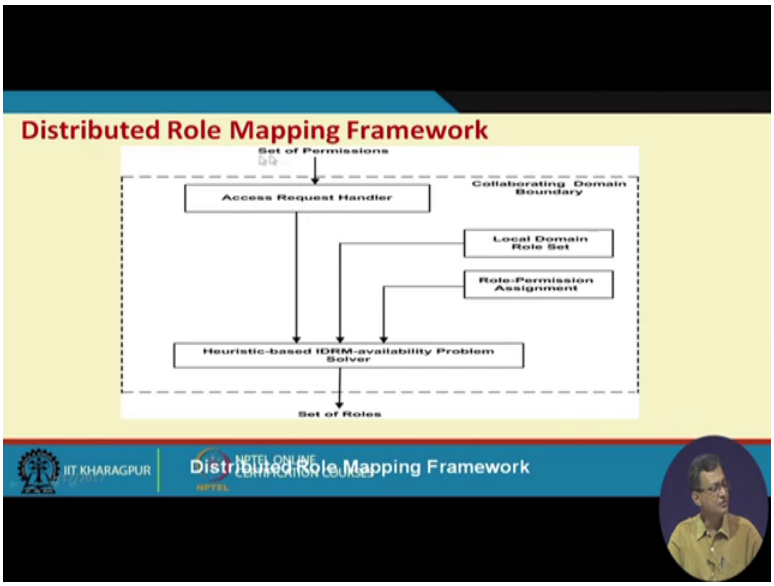
(Refer Slide Time: 25:45)



So, we what you have the finds a minimal set of roles which in compasses the requested permission set. No polynomial time solutions are available greedy search based heuristics sub optimal solutions. Challenges they are may exist multiple minimal role set right. So, that there can be existing minimum multiple minimal role set they are may not exist here any roles set which exactly map to the all permissions.

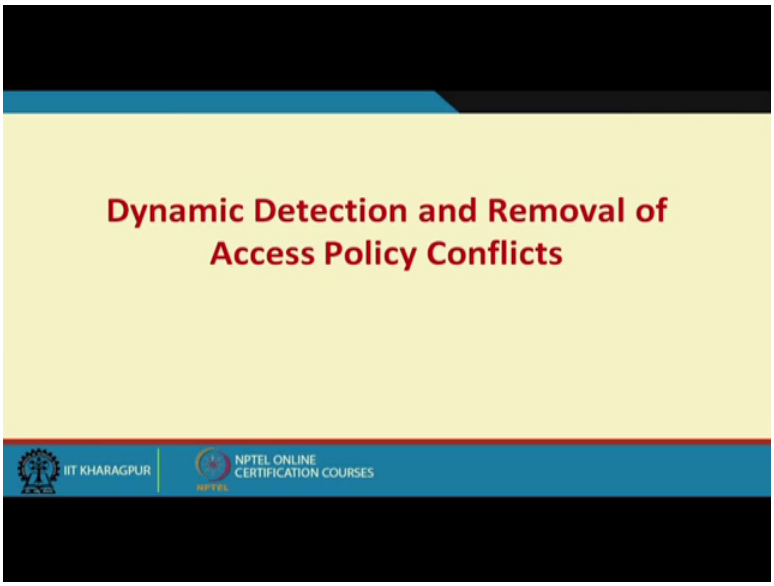
So, there are different types of problems or challenges. So, 2 variant of a IDRMs are there one is IDRM safety and IDRM availability; so IDRM availability and safety. Objective to formulate a novel heuristic generate better solution to IDRM availability is problem minimize the number of ability permission.

(Refer Slide Time: 26:37)



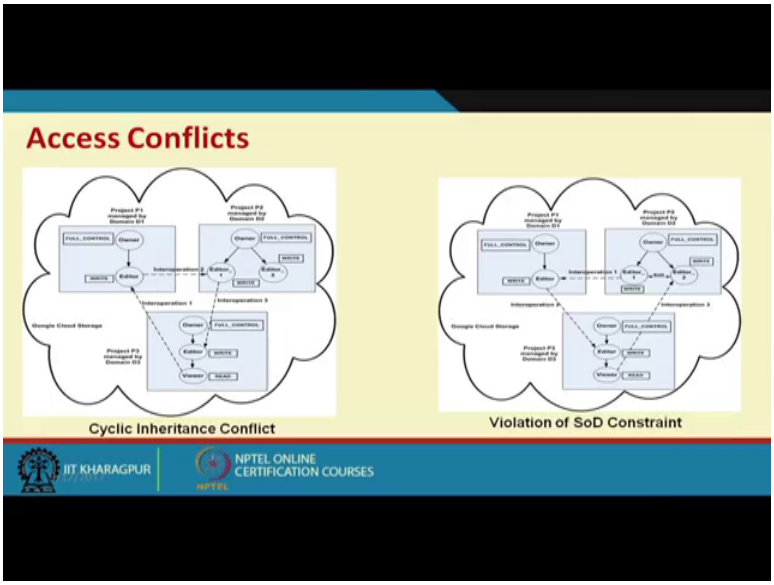
So, here also if you look at the distributed role mapping framework; so I have a set of permission access request handler. And we have local domains role set roll permission align assignment that role to permission set. So, which are set of permissions and heuristic, based idea availability problem solver what we try to formulate or propose and which keeps a set of role which is a minimal set up role.

(Refer Slide Time: 27:04)



And finally, there is the other aspect of dynamic detection and removal of access conflict. So, this is another major problem whenever we have multiple collaborations. So, there may be a chance that you may there may be a cyclic access cycle. And it may lead to accessing some objects which are other way a particular subject is not suppose to access right.

(Refer Slide Time: 27:36)



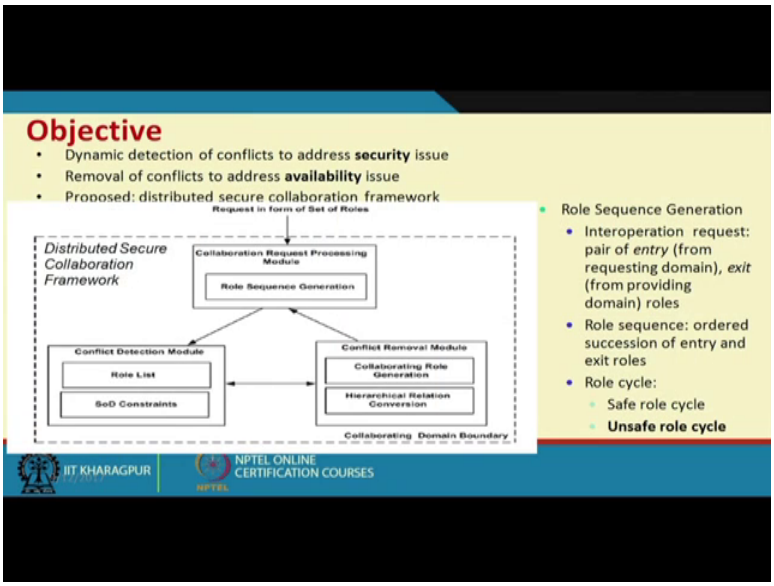
Like If you look at this cyclic inheritance conflict like this viewer this particular things is not allow to write or as editor permission, but I can have access to another domain which

has a right permission that is a allowed from they are to another editing which has a reading permission.

So, in other sense I cannot right. To this particular subject cannot write to this particular object, but I can have a cyclic way of this. So, inheritance cyclic way and write to this. So, in other sense I have done a conflicting situations which other way I am not supposed to do. There can be violation of sod constant. So, sod constant is the separation of duty really, like I can say a typical analogy like say in a bank the person who is issuing a demand draft cannot verify the demand draft like I am I am in the issue counter. So, if I am issuing the thing, issuing the draft then the verification I cannot do the same thing right. So, there should be has to be a separate things. So, it is a separation of duties has to be there sod what we to popularly known as a sod constant, which is they are in any security information security mechanisms.

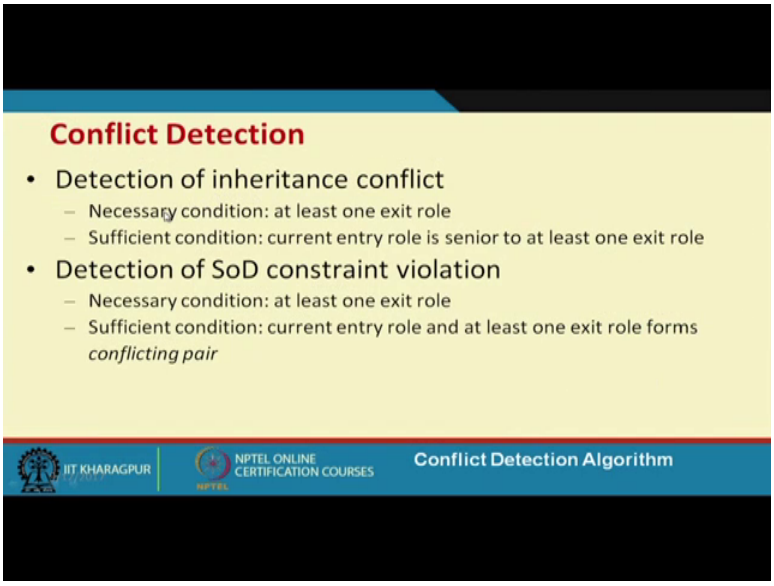
So, here also we can see there may be a conflict in the sod constant itself. Like here I can have a right. On the things and I can have another channel with having this editor writing on these editor there is a communication here. So, I can basically though there is a sod constant, I communicate between through a different channel right. So, there is there can be a violation of things, these things happens whenever there is a multiple communicating partner and specially when they are loosely coupled; that means, you do not know the whole security scenario of the other things or security settings of the other party.

(Refer Slide Time: 29:53)



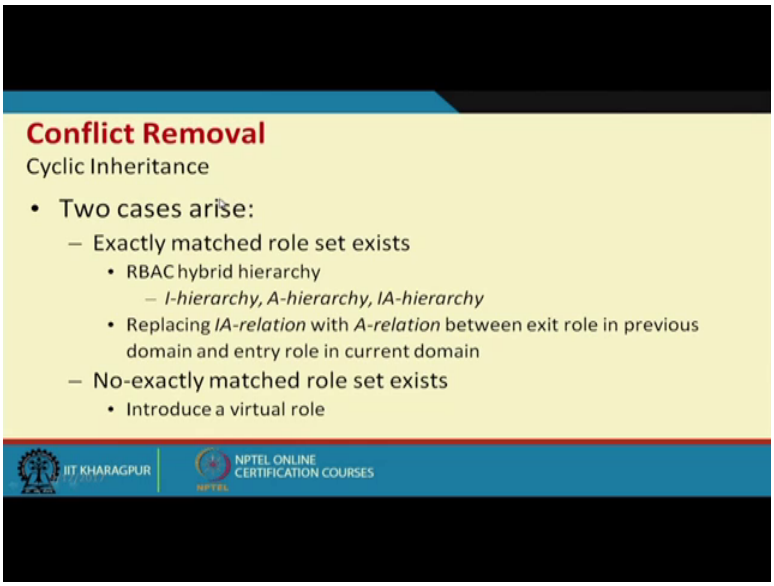
So, here also we try to for a particular distributed security collaborative frame work, which takes a set of roles and based on collaborating request processing modules, and conflict detection and conflict remover module come up with a set of a scenario which will be complete. So, role sequence interoperation request pair of a entry from the domain exist from a providing roles right role sequence order success of entry and exist role. So, I can have a safe role cycle unsafe role cycle.

(Refer Slide Time: 30:38)



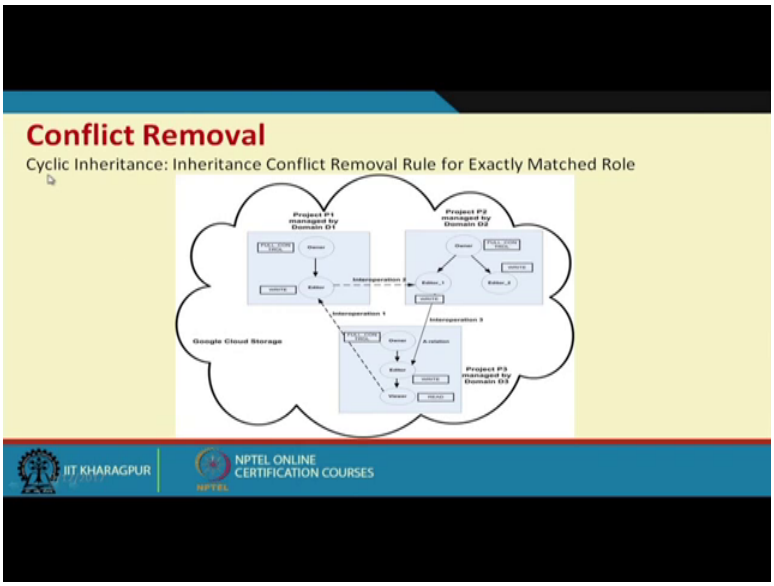
So, it as we understand it has too think one is that role a detection, that is there if there if there is a conflict they are need to detection it has to part detection of the inheritance conflict detection of the sod constant violation. So, this to need to be detected what and other is the now we need to remove the things.

(Refer Slide Time: 30:50)



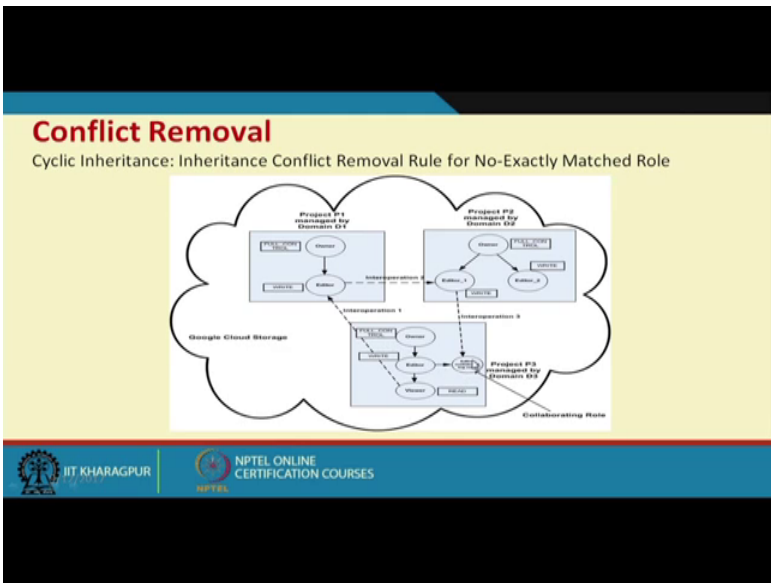
Then once detected that those conflicts need to be removed; so one is that 2 cases may arise exactly match role set exist. So, r back hybrid hierarchy or there can be no exactly role set exists right I can. So, I can have a virtual role into the things. So, I can create a dummy role and look at it.

(Refer Slide Time: 31:20)



Like if you look at cyclic redundancy inheritance the cyclic inheritance conflict removal role for exactly match roles what we do here.

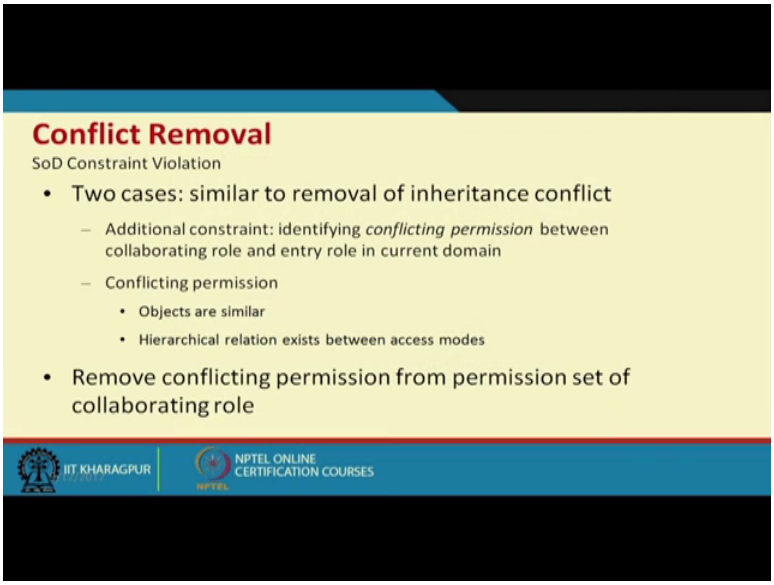
(Refer Slide Time: 31:40)



So, instead of this after the conflict removal we create a collaborating role. See here it was basically it was a cycle to end up in this editor whereas, here inheritance conflict removal for no exactly match role. So, as there is no exactly match role of looking at it. So, we create a another sub roll or a new roll which is fall back.

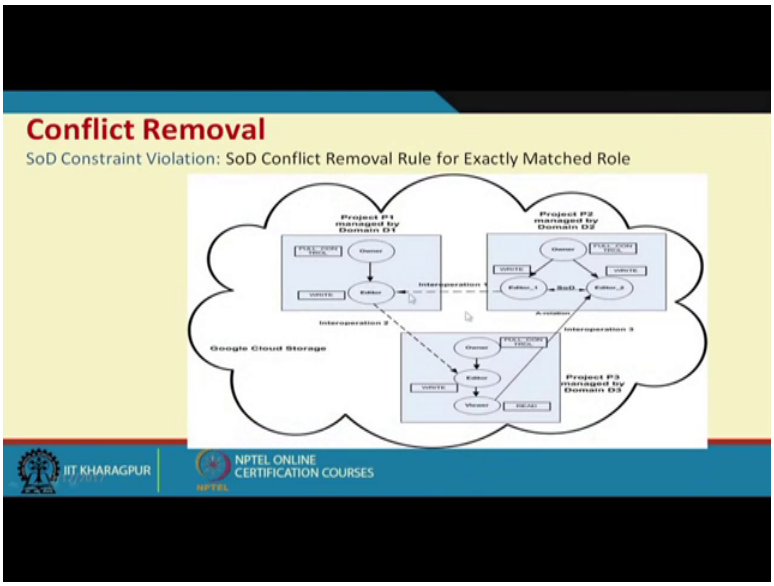
Now, this viewer there is no way of going to this particular editor. So, that I am not going a there is no conflict.

(Refer Slide Time: 32:12)



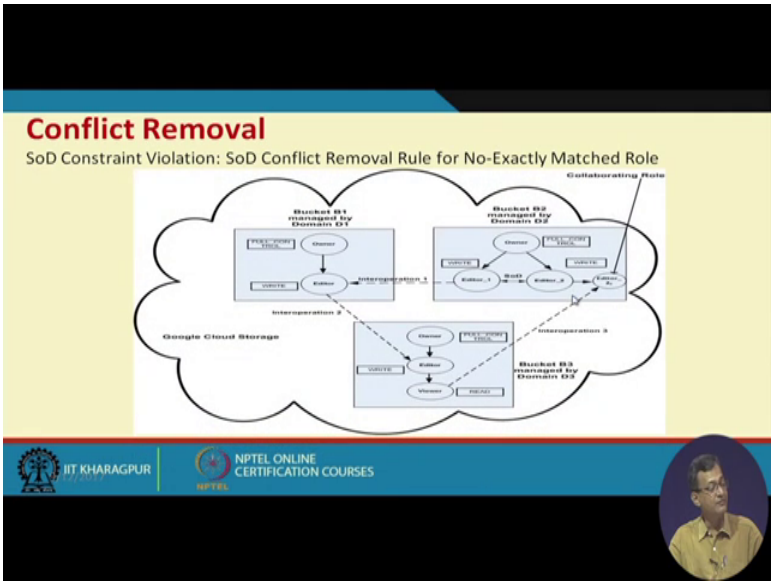
Similarly, for conflict removal also, we can have a to sod constraint removal thing here also we have. So, this was our earlier scenario where this editor rights here and this viewer this editor can right has access to these and to and finally, it goes to this editor one and took though there as sod. So, there is a chance of a cycle which violates this sod.

(Refer Slide Time: 32:21)



So, here also if there is no exact match we created a collaborating role right. So, it collaborating role of the editor 2.

(Refer Slide Time: 32:42)



So, editor 2 c and it is ends up there. So, there is no sod violence in between the editor one and editor 2, right. So that means what we are trying to look at that in doing so.

(Refer Slide Time: 33:02)

We may in the or may basically formulate a scenario where this where there is healthy collaborations between the things without security violences. So, this is a typical approach we try to show that how secure collaborated in the sass cloud can be possible,

and definitely this is a very brief overview, but that is good enough or it will help you those who are interested in this sort of research. See there is in need of infrastructure is minimal, but; however, you can basically work on a this sort of problem right.

So, one is that selection of the trustworthy and competent cloud provider and after the selection we have the recommending access request from the anonymous users for authorization. Then mapping of authorized permission to the local roles, and detect dynamic detection removal the access control conflicts. Like there can be cyclic inheritance problem conflict or sod type of conflict can be there which can be it. So, what we try today what we discussed today is that looking at one of the one of the very tricky issue of security where collaborating SaaS cloud in a in a loosely coupled way.

So, what are the major what are the typical security issues can come up, and how to approach those problem to address is there can be different other approaches. You can find in the literature and even you can think of other approaches, but this is a typical way of looking at it. And this is a problem which is very much part intent, and which has very much true for today’s cloud scenario collaborating cloud scenario.

Thank you.