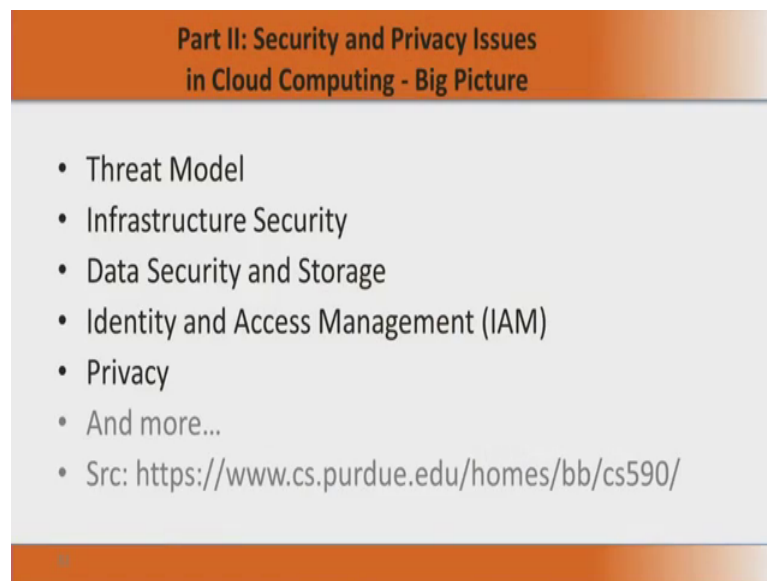


**Introduction to Information Security**  
**Prof. V. Kamakoti**  
**Department of Computer Science and Engineering**  
**Indian Institute of Technology, Madras**

**Lecture – 25**

So, in the previous session we discussed about what a cloud infrastructure is. And then we also saw many challenges in arriving at such a cloud infrastructure, but the thing that we concluded was one of the major challenge in a cloud infrastructure is security. And why security is a big issue, we saw many examples. We did see a taxonomy of fears what will the consumer fear about a cloud service. And we did come to a conclusion that it is going to be a very big challenge for a cloud infrastructure to provide necessary amount of security.

(Refer Slide Time: 01:01)



**Part II: Security and Privacy Issues  
in Cloud Computing - Big Picture**

- Threat Model
- Infrastructure Security
- Data Security and Storage
- Identity and Access Management (IAM)
- Privacy
- And more...
- Src: <https://www.cs.purdue.edu/homes/bb/cs590/>

Now, we will go a little more deep dive into this issue of security and privacy issues in cloud computing in this part. Many of the materials there are lot of materials in the link that is provided there the Purdue university link, which has which have ca course on cloud computing. And it has many a handouts, you are you can go and visit that and get many more details which would be related to these sessions.

Now, let us first look at the way we will you we look at security and privacy issue in cloud computing is to go and look at all these points. First we will understand what is reasonable threat model for the cloud infrastructure? then. So, what you mean by a threat model, the different ways and adversary can attack the system. Then we will look at what

is this what are the security challenges for the infrastructure, namely the servers networking components, the software, the platform, the operating system etcetera.

Then we will look at data. So, what are the different security issues involved in handling and storing data then access. So, how do we identify an user how do you verify is identity and perform the access management. What are the challenges? And then we will also look at privacy and some more issues as part of this set of sessions following now.

(Refer Slide Time: 02:55)



The slide has an orange header with the title 'Threat Model'. Below the header, on a light grey background, is a bulleted list. The first bullet point states that a threat model helps in analyzing a security problem, designing mitigation strategies, and evaluating solutions. The second bullet point is 'Steps:', followed by four sub-bullets: 'Identify attackers, assets, threats and other components', 'Rank the threats', 'Choose mitigation strategies', and 'Build solutions based on the strategies'. The slide has an orange footer.

## Threat Model

- A threat model helps in analyzing a security problem, design mitigation strategies, and evaluate solutions
- Steps:
  - Identify attackers, assets, threats and other components
  - Rank the threats
  - Choose mitigation strategies
  - Build solutions based on the strategies

Now, what is a threat model? A threat model is one which helps you analyze the security level in a system. Suppose I am saying that I am going to protect a system from attack. What are the types of attack need to be enumerated? So, the threat model attempts to enumerated different ways by which your system can be attacked. The threat model also paves way for you to come out with mitigation strategies. If I want to go and prevent an attack I first I should know what the attack is and then based on what that attack could be I could now give a mitigation strategy.


Once I propose a mitigation strategy we can go and find out how effective it would be in that context. So, a threat modeling is to enumerate the different types of threats to your system and then propose and based on that we go and propose certain mitigation strategies. And also evaluate how effective these mitigation strategies would be for those threats. So, that has as we as I just mentioned the steps as listed in the slides, you see that first we identify who can be the attackers what are the assets on which day will attack, what are the type of threats you can get, first we identify the assets and then what

are the type of attacks each attacker can do on those asset. And then we go and now ran the threats which is highly sensitive like stealing of password, maybe a very highly sensitive threat. Then we choose mitigation strategies in terms of this priority and then you build solutions based on this strategies. So, this is the very clear procedure for how to model threat and come out with solutions for the same.

In our context we will be looking at cloud and we will be looking at threat models for the cloud. Now, in the basic components of this threat model would be how do you model an attacker and how do you list his goals. And based on this what are all the possible vulnerabilities or threats your system will face. So, an attacker can be a person inside your system or it can be from outside the system.

Inside your system means who has close physical access to your systems or is part of your local area network. The insider is more dangerous than the outsider because the amount of protection your infrastructure has from an malicious user inside your system is much less than the amount of protection your infrastructure has from an external attacker. So, we need to choose from whom are we trying to who is this attacker is an insider or an outsider. And is he going to attack singly or it is going to be a collaborating is a collaborated type of attack or more than one malicious user is involved. It can be hybrid and outsider using an insider to attack the system. And what would be his motivation why should he attack the system and what is the, what are the capabilities of these attacker right. So, all these things put together will characterize an attacker. So, what is attacker modeling, you have to go and characterize him is he outside is he inside or is the attacker is a group. And they what is the motivation or they going to ah steal the confidentiality of your system or they going to corrupt your data and hence, spoil the integrity of your system or they going to deny service and make availability a issue. So, what sort of motivation they have and what are the capabilities. And what finally, would be the attackers goal is he going to look at confidentiality integrity right or availability.

(Refer Slide Time: 07:37)

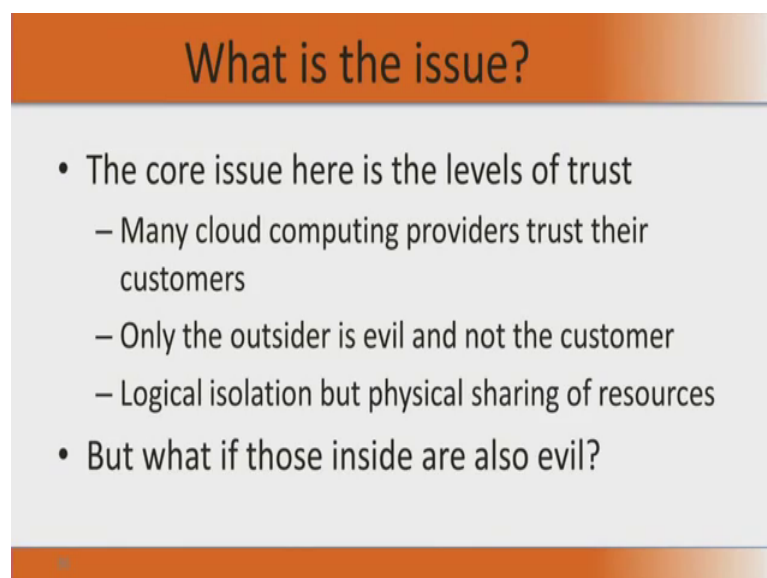


## Threat Model

- Basic components
  - Attacker modeling
    - Choose what attacker to consider
      - insider vs. outsider?
      - single vs. collaborator?
    - Attacker motivation and capabilities
  - Attacker goals
  - Vulnerabilities / threats

So, that would be a very very important point to be noted. And because of this goal and because of the attacker and his goal what are the possible vulnerabilities and threats your system will face. See all these things would essentially comprise that threat model. Now, the core issue in this whole stuff is the lack of trust. And the other thing is that the why there is going to be a lack of trust. And why there is going to be why there is going to be a problem because of this lack of trust we need to see that in a little more detail.

(Refer Slide Time: 08:10)



## What is the issue?

- The core issue here is the levels of trust
  - Many cloud computing providers trust their customers
  - Only the outsider is evil and not the customer
  - Logical isolation but physical sharing of resources
- But what if those inside are also evil?

First and foremost if I am a cloud service provider and you come to me for a service, for me consumer is god and so, I trust you. So, every cloud computing provider will trust their customers. So, the basic belief in a cloud service provider is that the his customers

are all very very good. They do not do any malice. They do not have any malice. If at all there is going to be an attack on my infrastructure it is going to be by an outsider who is not my customer.

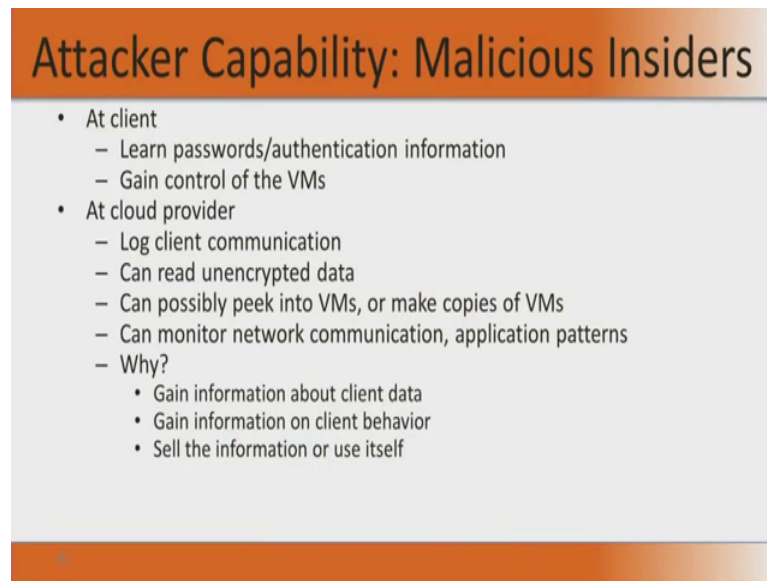
So, this is one basic feeling which many many physiological feeling and that actually puts lot more fear into each of the customers because again this trust is not transitive. So, I trust my customer the customer trust me as a cloud service provider. I also trust another customer. So, the customer trust me I trust another customer, but those two customers need not trust each other. So, but I as a cloud service provider believes that all the customers are good and I believe that anything evil could happen only from outside.

That is a major issue. And given that two customers need not trust themselves, though I trust both of them and both of them trust me as a cloud service provider. The issue of logical isolation, but physical sharing is going to be a of the cause of the major trust issue. There are two software one belonging to customer A another belonging to customer B, both handling sensitive data, but both are though running on isolated virtual machines they only logical isolation, but they can essentially run on the same server physically right.

So, two people who do not trust each other put their most sensitive software on the same physical server depending upon some software which assures them logical isolation. And that is the major issue here. So, the first thing that comes in mind is what if the other customer is evil, he is trying to steal my data and this a very very valid sort of fear. It is not some unfounded fear, it is a valid fear and. So, that forms a primary issue.

So, the multi tenant model, the absence of which makes cloud computing irrelevant is the first issue toward security. Now, when we look at attacker capabilities, if the person is an insider then he can learn passwords and authentication information from the client, he can also gain control over the virtual machines.

(Refer Slide Time: 11:45)



### Attacker Capability: Malicious Insiders

- At client
  - Learn passwords/authentication information
  - Gain control of the VMs
- At cloud provider
  - Log client communication
  - Can read unencrypted data
  - Can possibly peek into VMs, or make copies of VMs
  - Can monitor network communication, application patterns
  - Why?
    - Gain information about client data
    - Gain information on client behavior
    - Sell the information or use itself

So, if there is an if there is a malicious insider who is going to be a client he can basically because he is sharing physical resources with other clients, he can basically learn the passwords authentication information and kind control over the other VMs. When if he is a cloud provider himself. So, there is an employee of the cloud service provider who is malicious then he can log all the client communication and many times you store unencrypted data because this is your server right.

The cloud service provider says it is your server. So, he can read all your an unencrypted data he can possibly peek into all VMs and make copies of VMs. He can monitor all your network communication and application patterns and why does he do this because of this he can gain information about your data he can gain information on client behavior and he can sell this information or use it itself. So, all these things becomes, information sometimes become a very very important commercial entity. So, you can sell information even for some behavior analysis etcetera.

So, all these things could affect the business of the client from whom the data is stolen or these patterns or these type of analysis is done. So, if I have an insider who is malicious and the insider can be a customer or a client or he can be the employee of the data cloud service provider. Then these are all the things that he can do to basically create chaos in your organization. If the attacker is outside, is outside your is neither a client or a or the cloud service provider,(Refer Slide Time: 13:49)

## Attacker Capability: Outside attacker

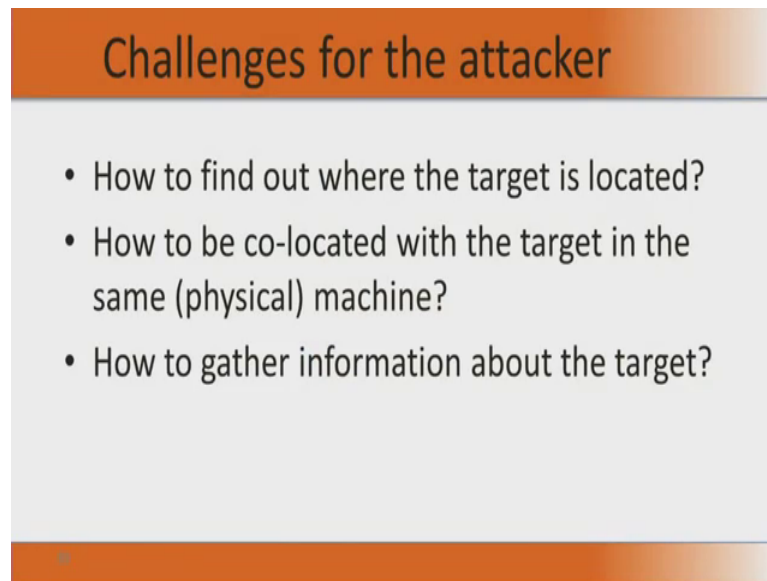
- What?
  - Listen to network traffic (passive)
  - Insert malicious traffic (active)
  - Probe cloud structure (active)
  - Launch DoS
- Goal?
  - Intrusion
  - Network analysis
  - Man in the middle
  - Cartography

then, he can do all that we have talked of in the earlier stuffs like he can listen to network traffic, passively he can insert malicious traffic. That means, he is an active attacker and he can also actually probe into a cloud structure. He can launch denial of service. All these things we can do and what will it achieve because of this, what is this goal he can intrude into your system, essentially making your integrity confidentiality and availability and issue.

He can do some network analysis, he can do all this man in the middle type of attacks trying to steal information while it is going from a client to the your cloud service provider. He can also do something called cartography. Cartography is the art of making maps now cloud cartography is actually a scheme of pin pointing the physical locations of web servers hosted on a third party cloud computing service.

So, what happens here? I can actually get the demo I can find out where the data is. I can find out within your server where your applications are running. If I can find out then I can do many more things especially in the multi tenant model that we discussed in the previous session, we can do many more things. We will give you some case study as this as we proceed.

(Refer Slide Time: 15:20)



## Challenges for the attacker

- How to find out where the target is located?
- How to be co-located with the target in the same (physical) machine?
- How to gather information about the target?

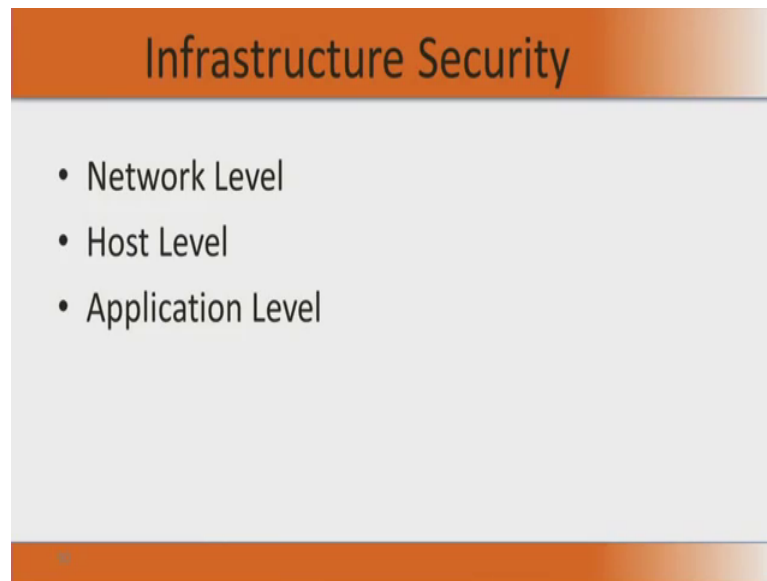
Now, somebody wants to attack the system. So, what are the challenges is going to face. First and foremost what is it train to attack, he will have some target in mind. So, let us take one cloud service provider he has some customer A who is running as a software B, software X. First and foremost he should locate find out where this software X of customer A is running. Then the next thing will try to do is you would like to co locate a malicious software along with this on the same server where this software X of customer A is running.

Then he will now try to gather information about that target. So, how to find out where the target is located. That is what we call as cartography right. Go up into the system and find out which server it is located and how to be co located with the target in the same physical machine. And then how to after co locating yourself how do you gather this information.

All these things are challenges for the attackers. So, when we go and comprehensively address these challenges by saying that we will put so, much production mechanism. So, let none of these challenges could be solved by the attacker, then the system can be for this particular threat model the system is safe. So, this is the approach of trying to come out with the threat modeling and the strategies for mitigating those threats.

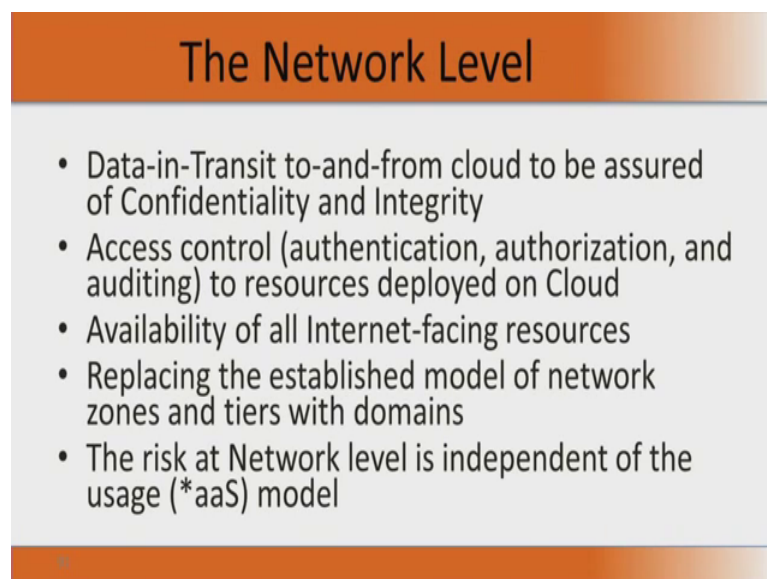


(Refer Slide Time: 17:02)



Now, what we will look at is; So, that threats that we have discuss so far essentially comes into securing our infrastructure. What we will like to secure? We would like to secure our network, we will try to provide security at the network level. We will try to somebody breaks through the network, we will now go and try to protect give security as the host level. If somebody break this host we will go and give security at the application level. So, we are looking at three tiers of security. So, that it we are very very sure that you have very very large extend nothing could be compromised easily.

(Refer Slide Time: 17:50)



Now, what do you mean by securing at the network level? The network level is that the client actually has a machine. Let us look at an off-site cloud service provide provision.

So, there is a cloud it is a public cloud and an organization is utilizing this cloud. So, when we have this type of off-site cloud installations, the data from the client will go through a public network, physical public network to the cloud. So, there will be a data in transit to and from the cloud to the particular client. And when the data is in motion we need to ensure confidentiality and integrity. The next important network level issue is access control. Somebody wants to access the cloud from outside then we need to have authentication mechanism strong authentication mechanism then authorization. Once you authenticate we authorized them to use certain resources and then both the authentication and authorization need to be audited.

This should be done for all the resources that are deployed on the code. So, the authentication, authorization and auditing of what the user is doing can be done at the network level because the user basically access the cloud through the network. So, all communication that happens from the keyboard of a client to server inside the cloud is going to go through this network. So, network becomes a very very important component for monitoring purposes.

The other important thing again when we look at security we set confidentiality, integrity and availability. All the internet facing resources in the organization should be available. The next thing is interesting that we have to move from the established model of network zones and tiers we have to move to domains. If you look at traditional data centers, data centers run for only one organization. Then it will be a tiered data center. Each tier there are three tiers in a data center if you can look at many many sites which describe the structure of a private data center. It is not shared across customers.

So, there will be something called a core there will be a something called a core layer or core tier and then there will be an aggregation tier and there will be an access tier. The access tier are the different servers they are access in the access tier there will be network switches and network appliances which would be connecting to it the different servers. All these connections are aggregated and then and the cores which and then they are fed into the cores layer, where the core in the core tier it is an interface to the external world.

So, the network appliances inside a data center can be divided into core aggregation and access tiers, but this is the traditional way and this is very much valid when we look at a single a data center serving a single customer. Now, when we look at data center serving multiple customers now this type of a tier alone will not worked. Especially from a

security angle. So, they go into setting up domains. So, setting up a domain shall deny access to outside traffic resulting in some additional security.

So, I could have different domains even within the data center and this can basically help a lot in achieving security. So, that is another very very important network level security feature. The risk at the network level again is independent of what type of service the client is asking from the data center. Already we saw some three models, the three service models software as a service, the platform as a service or infrastructure as a service irrespective of whether it is the S or the P or the I that is what we call star AAS.

The star can be anything the network security that we are trained to propose is independent of the way the client is actually using it. In the next session we will talk about host level security.