

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

Lecture - 28

Now, we will see what happens when there is a privacy breach. First and foremost these are all the questions. Now, I am customer of a cloud service provider. How will I know that a breach has occurred? If a breach has occurred in other words how do ensure that the cloud service provider whenever there is a breach will inform is that the breach has indeed occurred.

Now, who is to be responsible for managing the breach notification process. And the cost associated with the process. So, when actually when one of the most important thing that happens when contracts are signed, from a security point of view in these contracts, the things that could be there is mainly for privacy breaches. And when we are looking at privacy breaches all these points need to come. How can we identify that a breach has a happened and when an identification like that happens who should inform when should they inform how quickly they should inform.

Then how to what would be the next strategy to be followed immediately to manage that the breach the losses that are caused by the breach. Now, all these things should be part of the contract. Now, the next question is you strain an SLA and how do you go and enforce this contract and how do you go and determine whose fault is it at any point of time. So, these are all something that are very important, especially from a data privacy point of view when there is a breach in that privacy.

Note that this type of privacy breach will have cascading effect. A cascading effect in the sense that one privacy breach can leave to another privacy breach. And because of one privacy breach that second privacy breach need not be on the same customer in a cloud type of infrastructure right. So, by finally, what would happen is that there is a the credibility or there can be an organization which has signed a contract with a cloud service provider. Now, let us say that the cloud service provider it is his responsibility to see that there is no privacy breach, but when there is a privacy breach, the organization can certainly transfer all the liability because of the privacy breach, but they cannot transfer the accountability.

Still they are accountable to the customer. So, there is a bank there is a cloud service provider and the bank has an agreement with the cloud service provider, which basically says that if there is a privacy breach your responsible for all these things. Then there is a customer to this bank whose data this bank goes and saves on the cloud there is a privacy breach. Yes, liability because of that will be taken by the cloud service provider, but still the customer will not go and ask cloud service provider. He will make bank accountable for that. So, that is very very important and that is why all of us should be very keen on this protecting the privacy.

Both the customer to a cloud a service provider and the cloud service provider both should in the interest of both, should have this privacy policy very strong. So, this is the very nice case study.

(Refer Slide Time: 04:10)

Who is responsible for protecting privacy?

- Data breach
- **Who investigates this crime?**
 - Is it the Cloud Provider, even though Company X may fear that the provider will try to absolve itself from responsibility?
 - Is it Company X and, if so, does it have the right to use other data on the servers, including logs that may show access to the data of Companies Y and Z?
- Many new risks and challenges
 - The overall complexity of privacy protection in the cloud represents a big challenge.

data life

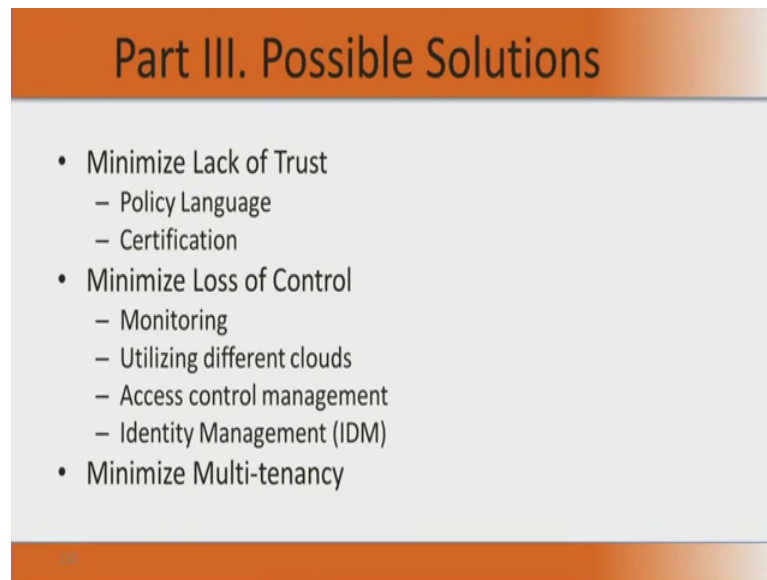
So, I am just reading it out. Suppose a hacker breaks into cloud provider A and steals data from company X who is who is customer of this A. Assume that the compromise server also contains data from companies Y and Z. So, these are all the question who investigates this crime? Is it the cloud provider even though company X may fear that the provider will try to absolve itself from responsibility right. So, if cloud provider is going to investigate this, then he will say “I have no problem with it because it is your problem”, he can blame X for that.

Like some end user of X has shared the password it is gone. So, company X would like to go and do this investigation, but when company X wants to do this investigation, on that physical server in which companies Y and Z also have the data. Obviously, it is start looking into logs and those logs will have data of companies Y and Z also. So, essentially the privacy are whatever the confidentiality of the logs of company Y and Z essentially gets violated. So, now, this is a peculiar scenario that a cloud provider A steals data of company X.

A hacker breaks into cloud provider A and steals have a date of company X. If company if the X will not want A to do it and A cannot permit X to do it. X does not want A to do it because A might will not if A alone does it then he will not project what went wrong with him. He may absolve himself, A will not allow X to do it because then it will see the data of Y and Z and there is a confidentiality clause that is signed as a cloud service provider A has signed confidentiality for privacy clause Y and z. So, he will not allow X to come and see the log because the privacy of a data Y and Z would be compromising.

So, it is a very very peculiar situation. So, that can be many such situations which make even investigations into crimes, more difficult and more transparent from the difference stake holders point of view. So, now, we have talked about all threats threat models etcetera on the cloud. Now, in the remaining part of this session we will know start looking at possible solutions. So, we have seen so far we have seen cloud as a infrastructure, we have seen the different fears of lack of trusted comes. And then in the next part we did see some of the privacy and threat issues security issues in the cloud environment. The last part now part three of cloud and related security we will see what are the possible solutions.

(Refer Slide Time: 07:30)

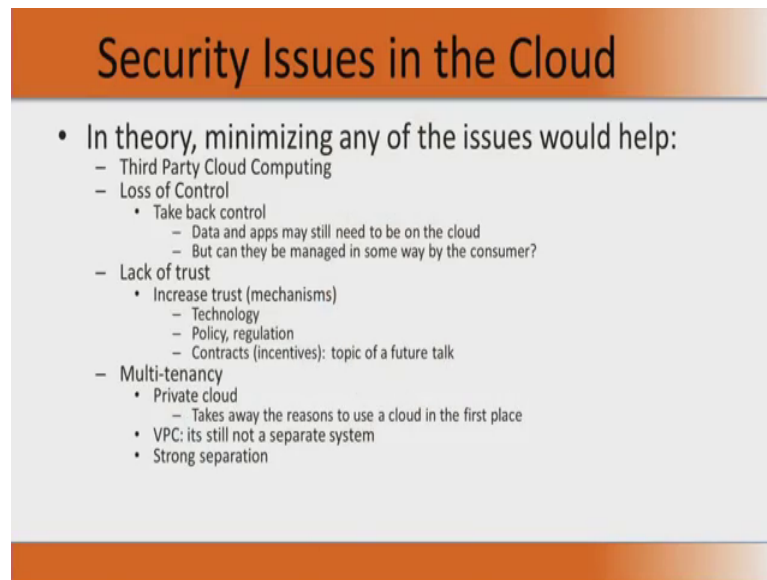


The solutions could be actually in three parts and we will cover the first part in this session while will cover the remaining two parts in the next session. So, the first part would be to minimize lack of trust. The second thing is to minimize loss of control and the third thing is to minimize multi tenancy. So, we have to look at all these three. If I minimize lack of trust I start trust in the cloud service provider, certainly this the fears would reduce. Now, what are the different of ways which I could minimize lack of trust.

Similarly, when I what I mean by minimizing loss of control is that, I keep monitoring and I can also utilize different clouds; if one cloud fails, I can go to another cloud. And I need to have lot of access controls mechanism and manage the access control. And I also manage identity. So, if I am going to do all these things, then the of course, my I do not loss control. I basically can have control over what I am trying to do on a cloud. And of course, minimizing multi tenancy.

So, these are all some possible solutions let us go and look at the pros and cons of the solutions, to start with and then we will look in this session we will talk about minimizing lack of trust. In the sub sequent session will talk about the other two in detail.

(Refer Slide Time: 09:02)



Security Issues in the Cloud

- In theory, minimizing any of the issues would help:
 - Third Party Cloud Computing
 - Loss of Control
 - Take back control
 - Data and apps may still need to be on the cloud
 - But can they be managed in some way by the consumer?
 - Lack of trust
 - Increase trust (mechanisms)
 - Technology
 - Policy, regulation
 - Contracts (incentives): topic of a future talk
 - Multi-tenancy
 - Private cloud
 - Takes away the reasons to use a cloud in the first place
 - VPC: its still not a separate system
 - Strong separation

Now, first thing is that we are looking at in theory minimizing any of the issues given below would help. Specifically when I am looking at third party cloud computing. What are the things that I need to go and minimize? First thing is I want to go and improve the trust right as we. So, I want to minimize lack of trust. How will I go and minimize lack of trust? That means, I want to go and increase the trust, one thing is I will put lot more technology there.

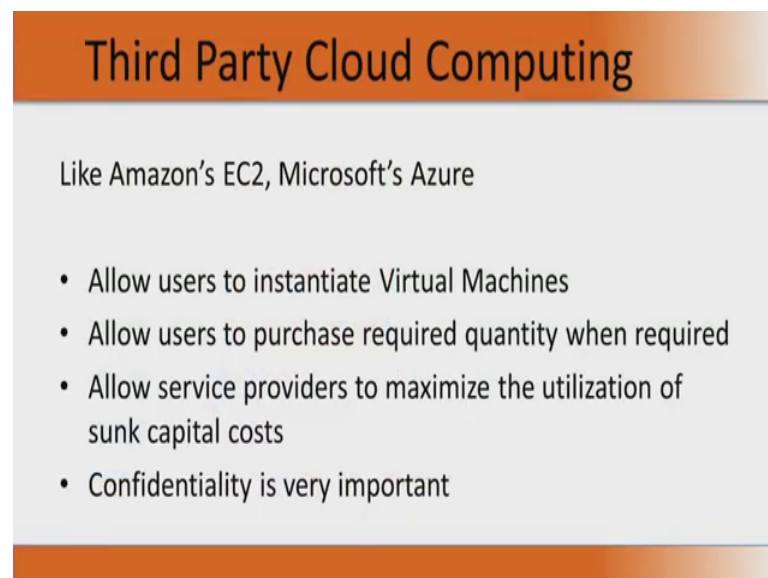
I will also put lot more policies and regulation and technology to go and say that these policies and regulations are adhere to. We will also have contracts with some incentives. So, these are some things we will discuss in in our future talks. Now, by doing all these things you can increase the level of trust. The second thing that we are looking at these loss of control, when there is a control loss when there is a server that fail, we need to take back control.

Your data and applications may still need to be on this cloud. So, we have to shift it to another cloud, what it means shift it to another cloud? Can they be managed in some way by the customer consumer. So, can I have multiple clouds once fails again go to another cloud. So, these type of issues are very important when we look at loss of control. Loss of control is even that a data center essentially becomes not accessible. Now, how quickly can I go to another dead cloud with all the necessary information and I can seamless the start running the show.

The next thing is about multi tenancy. If I say I want a private cloud then the reasons of a cloud itself is lost. A cloud is to share the infrastructure. So, multi tenancy is important. We will now talk of this virtual private, virtual private cloud which is which again not in in again it is a same thing even in a VPC, there will be servers in which physical servers in which applications or virtual machines and applications of several other uses should be as of different customer will be in the same place.

So, one of that thing we need to ensure is there is a strong separation between any two virtual machines that are running on the same physical server. So, these are all the broadly how we go and handle these security issues, but we will go into depth it for each one of them here.

(Refer Slide Time: 12:12)



The slide features a title bar with a gradient from orange to white. Below the title, the text 'Like Amazon's EC2, Microsoft's Azure' is centered. A bulleted list follows, detailing user and provider capabilities and the importance of confidentiality.

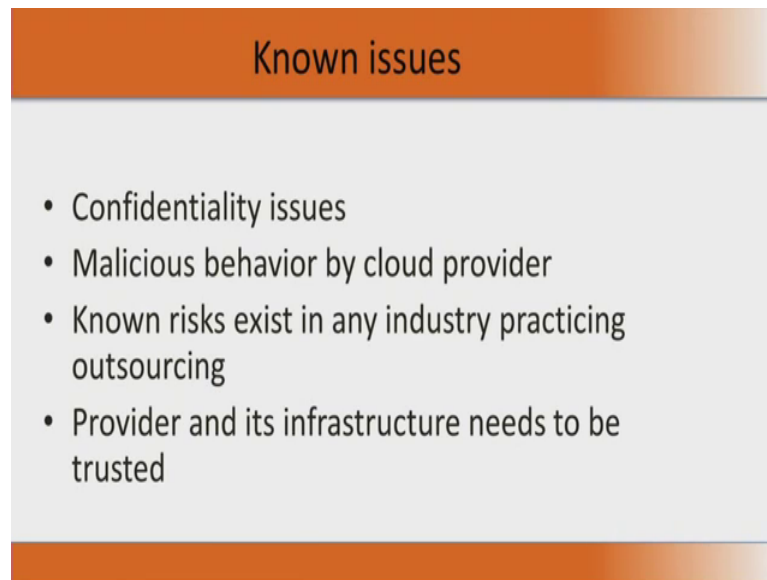
Third Party Cloud Computing

Like Amazon's EC2, Microsoft's Azure

- Allow users to instantiate Virtual Machines
- Allow users to purchase required quantity when required
- Allow service providers to maximize the utilization of sunk capital costs
- Confidentiality is very important

When I will talk about third party cloud computing like amazon's EC2 or the Microsoft azure, what do they provide? They allow users to instantiate virtual machines they allow user to purchase required quantity of resources whenever they required. And allows service providers to maximize the utilization of sunk capital costs and they also confidentiality is very important. So, third party cloud computing at least for not very very sensitive applications has been a good success of today.

(Refer Slide Time: 12:46)



Known issues

- Confidentiality issues
- Malicious behavior by cloud provider
- Known risks exist in any industry practicing outsourcing
- Provider and its infrastructure needs to be trusted

So, what are the known issues when you go for third party computing? Of course, confidentiality issues are important and we are going on a third party. So, that could be malicious behavior by cloud provider itself. And there could be some other customer of the cloud provider who could have a malicious a behavior. And of course, there are this is this are out sourced model I am actually getting this the cloud being maintained by the third party. So, it is an outsourcing and so, there are known risks for outsourcing.

Ultimately the important thing is that are the cloud service provider and his infrastructure that us deployed for us to use that needs to be trusted. So, this is the main thing when we look at third party.

(Refer Slide Time: 13:43)

New Vulnerabilities & Attacks

- Threats arise from other consumers
- Due to the subtleties of how physical resources can be transparently shared between VMs
- Such attacks are based on placement and extraction
- A customer VM and its adversary can be assigned to the same physical server
- Adversary can penetrate the VM and violate customer confidentiality

We have seen in the previous session many many vulnerabilities new vulnerabilities in addition to a old vulnerabilities that we see. Conventional vulnerabilities of some buddy trying to hack into your system it is that physical resources are shared between virtual machines. So, an adversary can have more physical can have an application legal application running on the same physical server which can basically go and sneak into it, sneak into your application illegally are sneak into your data. So, the notion of multi tenancy give out a set of new vulnerabilities and attacks.

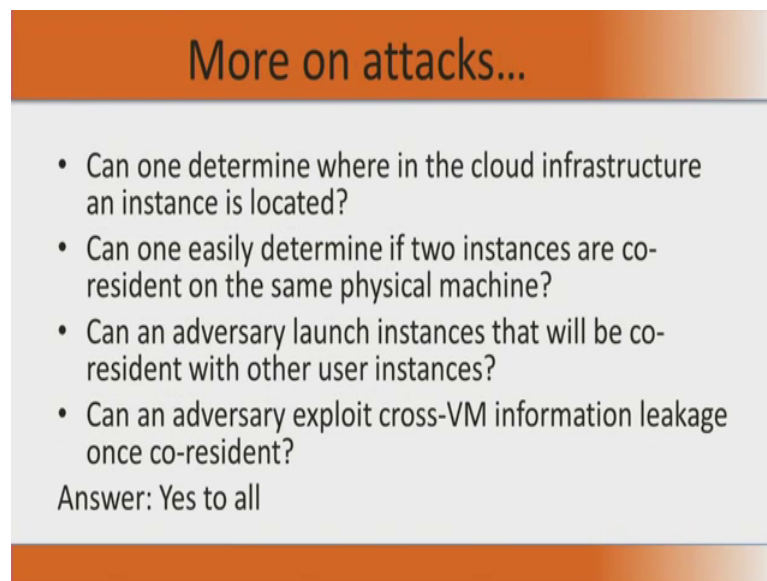
(Refer Slide Time: 14:28)

More on attacks...

- Collaborative attacks
- Mapping of internal cloud infrastructure
- Identifying likely residence of a target VM
- Instantiating new VMs until one gets co-resident with the target
- Cross-VM side-channel attacks
- Extract information from target VM on the same machine

Then we could have because of this multi tenancy you could have of some collaborative attacks. And another thing is I could map the internal cloud infrastructure and based on that I could go and position my attack. And there can also be the cross virtual machine side channel attacks which can extract information from the target virtual machine on the same machine. So, all these things come because of many many softwares trying to run on the same physical hardware.

(Refer Slide Time: 15:03)



More on attacks...

- Can one determine where in the cloud infrastructure an instance is located?
- Can one easily determine if two instances are co-resident on the same physical machine?
- Can an adversary launch instances that will be co-resident with other user instances?
- Can an adversary exploit cross-VM information leakage once co-resident?

Answer: Yes to all

So, to just look into this, to summarize this can one determine where in the cloud infrastructure an instance is located? Can one easily determine if two instances are co resident on the same physical machine? Where one incident is a normal instance, one incident normal instance another is actually a malicious instance. Can an adversary launch instances that will be co resident with other user instances of his choices? Can an adversary exploit cross virtual machine information leakage once he is a co resident?

The answer to all this things unfortunately is yes to all. And that makes security on cloud a very important aspect. So, in the so to sum up what we have done so far, we have look that different security issues on the cloud and we are looking at many important privacy issues there. And we looked at the data cycle and at different data life cycle and a different points we are looking privacy of this data life cycle.

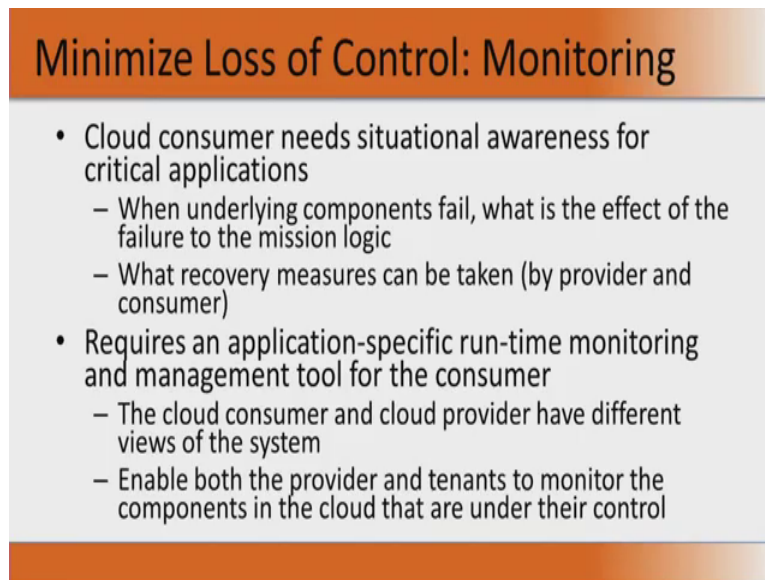
(Refer Slide Time: 16:25)



What we really find is that, to actually go and address many of the security and privacy concerns we need to have certain good policies and we need to have reduce the lack of trust and also minimize loss of control and minimize multi tenancy. Now, what it means to minimize loss of control? The thing is that loss of control, there are four important points. One thing is I need to keep consistently monitoring whether I have control or not. And when I lose control I should that there should be a provision by which loss control means that one particular thing is not available to me because of whatever be the reason.

Now, have to move entire thing into another cloud and starting executing. And when we move when we access a single cloud on move from one cloud to another cloud, then there is an access control management and that access control management seamlessly take care of these issues. There is an access control management for me access to one cloud when that cloud fails, I need to go and access another cloud. So, how do we extend this access control management for the next cloud? Then there is of course, something like identity management. How do we manage identity across clouds? So, all this things come as a point when I say when I want to minimize loss of control.

(Refer Slide Time: 18:10)



Minimize Loss of Control: Monitoring

- Cloud consumer needs situational awareness for critical applications
 - When underlying components fail, what is the effect of the failure to the mission logic
 - What recovery measures can be taken (by provider and consumer)
- Requires an application-specific run-time monitoring and management tool for the consumer
 - The cloud consumer and cloud provider have different views of the system
 - Enable both the provider and tenants to monitor the components in the cloud that are under their control

First look at monitoring, so whenever there is a situation where there is an incident, some component failed. We need to clearly understand what is the effect of the failure on the machine logic and what sort of recovery mechanism measure should be taken, what type of recovery machine measurement to the measures to be taken by the provider cloud and also the consumer. This requires an application specific run time monitoring and management tool for the consumer because ultimately the consumer needs the control right.

So, the consumer consistently observes every application and so, for every application he like to have a lock and he would like to keep monitoring whether there is a component failure and this is how we go in for minimizing loss of control from the monitoring point of view. So, now, what is the challenge here, if I allow a consumer to monitor what is happening on my server in a multi tenant model, especially when there are more than one tenants sitting on the same physical infrastructure giving out such type of monitoring facility to the consumer can lead to privacy violation. So, there is some point that we need to take care that. And when there is an attack we need to provide a mechanisms that enabled the provider to act on attacks that he can handle.

(Refer Slide Time: 19:56)

Minimize Loss of Control: Monitoring (Cont.)

- Provide mechanisms that enable the provider to act on attacks he can handle.
 - infrastructure remapping (create new or move existing fault domains)
 - shutting down offending components or targets (and assisting tenants with porting if necessary)
 - Repairs
- Provide mechanisms that enable the consumer to act on attacks that he can handle (application-level monitoring).
 - RAdAC (Risk-adaptable Access Control)
 - VM porting with remote attestation of target physical host
 - <http://www.faqs.org/patents/app/20100031047>
 - Provide ability to move the user's application to another cloud

For example, somebody has I have a software X and there is another fellow was instantiated, another virtual machine on the same server where X is running with in a intention to attack X. So, the immediately that should be infrastructure remapping where I move this particular, create new or moving existing fall domains out and creating or moving this virtual machine to a better system. Similarly, shutting down some offending components are targets this provider needs.

So, in some sense even if I have I am using the cloud as an infrastructure as a service model, still the provider the cloud service provider should be given control to move the virtual machine that I am using along with operating system in the software, he should be in position to move the virtual machine to some other server or some other physical server. So, that is the other thing is that we should provide mechanisms that enable the consumer to act on attacks, that he can handle right.

So, this is what we call is risk adaptable access control. So, there is a very clear there is even a patent, you can look at the website there where this gives a way by which I find, I as a consumer not as a cloud service provider I as a consumer find the there is an attack on the system on the cloud. So, I now want to move it to another virtual, the virtual machine that is running on one physical server, I want to move it another server. Now, there is a clear cut way by which I need to go and appraise that.

So, now, the I am appraiser, I send an attestation request and then the system actually takes it to an attester who will now go and certify this target server that physical server is good it does not have something. So, I get an attestation and then now I am go and spawn. So, in some essence if you look at the very broad of perspective in this cloud, I would like to monitor whether there is an attack.

In case there is an attack I would like to move this machine, virtual machine to a new machine, new physical server with in that cloud. And before I move I would like to have more information about that machine. And how do I get this machine information? I basically send some attestation and I get then attestation based on which I make a decision. So, how does a consumer go and ask for this attestation and get back and attestation. There are some patents with very interesting things.