

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

Lecture – 24

Loss of control in the cloud. Always the consumer fields is losing control when he gives the data this software and other things to the third party. Why is the feeling coming up?

(Refer Slide Time: 00:28)



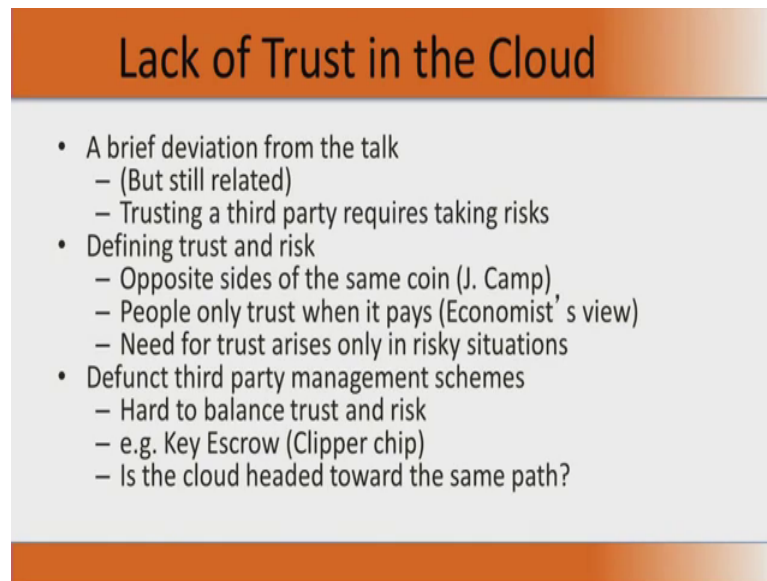
Loss of Control in the Cloud

- Consumer's loss of control
 - Data, applications, resources are located with provider
 - User identity management is handled by the cloud
 - User access control rules, security policies and enforcement are managed by the cloud provider
 - Consumer relies on provider to ensure
 - Data security and privacy
 - Resource availability
 - Monitoring and repairing of services/resources

The feeling is coming up because all the data application resources are located with the provider. He manages who can enter who cannot enter and he has you though you put lot of controls, you do not know the whether the control. You do not have final control of, whether the controls that you have stated to the third party he is maintaining it or not. All your security policies everything is maintained by the cloud provider and you rely on that provider for data security and privacy your resource availability and also your monitoring and repairing of services resources.

So, all these things are completely under the third parties' control. So, that the third party may give you access to this, but you really do not know whether the third party can access and change any of your data in your absence. So, that is the main field of loss of control from the customer end, from the consumer end in using a cloud.

(Refer Slide Time: 01:45)



Lack of Trust in the Cloud

- A brief deviation from the talk
 - (But still related)
 - Trusting a third party requires taking risks
- Defining trust and risk
 - Opposite sides of the same coin (J. Camp)
 - People only trust when it pays (Economist's view)
 - Need for trust arises only in risky situations
- Defunct third party management schemes
 - Hard to balance trust and risk
 - e.g. Key Escrow (Clipper chip)
 - Is the cloud headed toward the same path?

The lack of trust in the cloud. Again we it is a slightly the deviation from original import of this course, but then we need to go and define trust which we actually failed mathematical definition of trust as I explained in the previous session is not possible. I also suggest that you could look at a book on an Trust and Risk as Jeanne Camp. Trust and Risk are actually opposite sides of the same coin. And the basically when you look at trust that we start where is trust becoming very important.

It actually becomes important from the notion of accountability and verifiability. If something goes wrong who has done it and how do I go and prove that he has done it. And can the third party something which is not in there your control can they I go and cover it up. So, these are some of the major issues that come with trust. And what is risk?

Risk is a measure of what how much you are vulnerable. Risk is a measure of vulnerability. Vulnerability, when vulnerable, so when I want to do a risk assessment the way we go about doing this is, when there is a situation where in for an adversary there is an opportunity to do some action within your system, in which the cost that you get because of the action is much more the cost that you that the amount you lose because of that action is much more than the amount you spend in controlling that action.

Let me let me give you a example let me repeat that statement. Risk is a measure of the vulnerability and the vulnerability is measured in situations where, you want to there is a loss of control there is someone who comes in to your system, in an opportune moment wherein he does something to the system and the cost that you incur because that action

is much more than the cost that you have you would have actually invested, if you want to have that control. And not allow that fellow to enter. So, this is what I mean by vulnerability.

Putting down into very very raw terms, if I give it to you I have some cost benefit. If I make all my things if I shift all the things, all my software or hardware and infrastructure in to the cloud I have certainly lot of cost benefit, but the amount of cost I save versus the amount I may lose because I lost control of my data and a deployment extra. In case of some vulnerability if that cost is going to be much higher than the cost benefit that I am going to get by moving my infrastructure to cloud. Then I am vulnerable, then I have taken a huge risk. So, risk is...

So, people have been trying to define risk, but this is the way we I find risk to be, I find this is a better definition for risk it is the again I repeat, this the vulnerability it is the measure of vulnerability for an attacker to attack at an opportunity where in there is a loss of control due to cost and the amount of cost I gain by losing that control to it is a third party is much lesser then the amount of cost I pay because somebody exploited that loss of control and enter the system and damage the system.

So, trust and risk are very very hard to balance and that makes this entire, there is a need for search courses. We go we are going to a have six levels of courses as we are now in level one of this course and a level one of the course and then we have five more levels spread over next year and the two. And what will we talking there always one important point that will come at every point down in the remaining five levels. And this level would be how do you balance trust and risk.

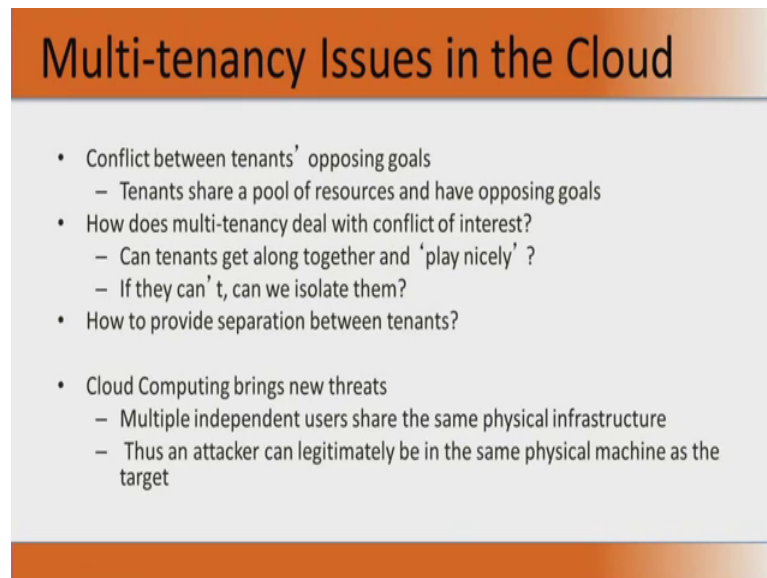
The most important thing is whenever we go an adopt a new technology, then there is lot of trust and risk related issues to be addressed. Cloud is a new technology right is the cloud actually heading towards extension because of the trust. If it is going towards extinction, then there is no point in anybody moving towards it because again they have to come back and already I mentioned in the previous module. In the previous session that especially for an in industry where there inner and business is not IT right say banking. Now, you move all the infrastructure to cloud and tomorrow when you want to bring it back into your own fold, you may not have the talent with in your organization to support it. So, this cloud business is much more trickier than previous things. One very interesting thing was that clipper chip is also called key's crow. These was at the chip

given by the government for many many many appliances which will have it shown encryption and that encryption was a classified encryption.

So, this this was issued by the government in something like 1993 in the western world. And it completely became defunct in 1996. There was a big hype 1993, but in 1994 if I remember right, there was a paper that was published which stated many vulnerability is in this chip, it was basically an encryption a chip which will take your data and encrypt and sent. You can go to web and look at clipper chip and it will give you many more details, but in 1994 there was a paper which talked about some vulnerability there.

Then a many things went unaddressed. And the adoption of this became a very serious concern. And the whole effort died in within three to four years. So, is cloud going for that? will security be such an important concern that crowd may fall down as a as a paradigm.

(Refer Slide Time: 09:32)



The slide features a title bar at the top with a gradient from orange to white, containing the text "Multi-tenancy Issues in the Cloud". Below the title bar is a light gray rectangular area containing a bulleted list of issues. The list is as follows:

- Conflict between tenants' opposing goals
 - Tenants share a pool of resources and have opposing goals
- How does multi-tenancy deal with conflict of interest?
 - Can tenants get along together and 'play nicely' ?
 - If they can't, can we isolate them?
- How to provide separation between tenants?

- Cloud Computing brings new threats
 - Multiple independent users share the same physical infrastructure
 - Thus an attacker can legitimately be in the same physical machine as the target

So, these are the important questions that need to be answered here. The other major a factor of for this thing is multi tenency. So, suppose I am going to go in to a flat right, my moving from home one home to another home. I am shifting my residence what are the questions you will ask. Who are my neighbors? What do they eat? Right if you are pure vegetarian and they are neighbor eats non veg every day morning you may not like it right.

Similarly, when I am going to a cloud environment and say the same server some ten fellows ten software of ten different organization would be executing when will ask who

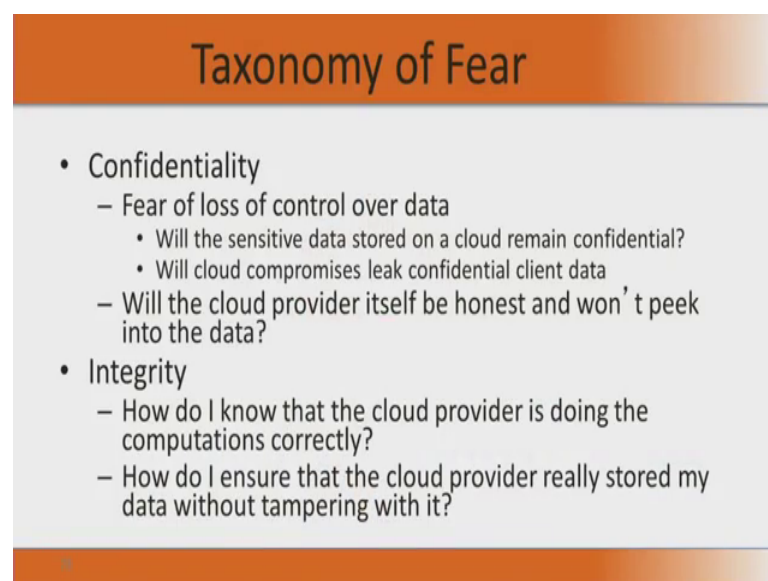
are these a tenants, who are these fellows. And you will also start asking question whether some mistake of that fellow will upset your security work CIA your confidentiality integrity availability. How would as the fellow provide that separation between these tenants. So, I have the some fellow in the same server another fellow is executing is using the same memory is using the same peripherals.

Now, my data my password everything is going to be in that memory and sometime later his possible is going to be in the same memory. So, will he not looking to data wily not a touch me. So, what permission he will have? Can he have a legitimate access to my data as for as; legitimate in the sense from the system is point of view. He is also a root you are also a root and this has root privileges and since he is a root, he is accessing you.

Can such type of statement can be made. So, all these things come up. Can all the tenantsb; they are they are good neighbors. Will they come and steal my house will they drill hole from the next door and come into the house and steal. So, these are all questions that need to be answered. These are all questions at need to be sufficiently powerfully answered, satisfactory answer itself is not suffice in need a powerful answer.

So, multi tenancy is a very big issue in clouds. The moment I say I cannot have multi tenancy give me a separate server then is not a cloud. So, there is no resource pooling and all those essential characteristics of a cloud it is lost. And you will not get that economic benefit then it becomes your own data center.

(Refer Slide Time: 12:02)



Taxonomy of Fear

- Confidentiality
 - Fear of loss of control over data
 - Will the sensitive data stored on a cloud remain confidential?
 - Will cloud compromises leak confidential client 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?

Now, comes fear. I did mention about that Tamil movie Thenali where Kamal Hasan list

set of fear in a doctor question scene. So, what are the fear here let me talking Tamil (using foreign language) come. So, many fears come when you go into cloud. Let us list all those fears let me talk about those fears. Confidentiality, yes you have fear of loss of control over data right. Will the sensitive data remain confidential when I put on the cloud especially in a multi tenant environment. Will this data be leaked who leak this data it is not that tenant is intelligent, another fellow executing, my own service provider how good he is? Will he leak my data will he not ping into peek into my data. Is he honest? right.

The second thing is integrity. Can somebody go an change; all the computations are they happening correctly are they using the same software right. Specifically I do not know, this is more on the engineering side. There are some floating point program which you have personally or executed say two decade or one decade down the line and some embedded processors, where if I used different optimization levels for my compiler I get different answers.

The answer will be correct up to two to there decimal, but beyond 3 decimal it might be different. And if I am looking at very high accuracy like I am computing in multi crores an then I am looking at 4th digit or 5th digit. In my computation we correct if my rounding of correct what short of optimization they are using. Especially when we starting using cloud in a manufacturing infrastructure, where I want to do a large scale collaborative manufacturing between countries pan earth, pan universe manufacturing of say some auto component right.

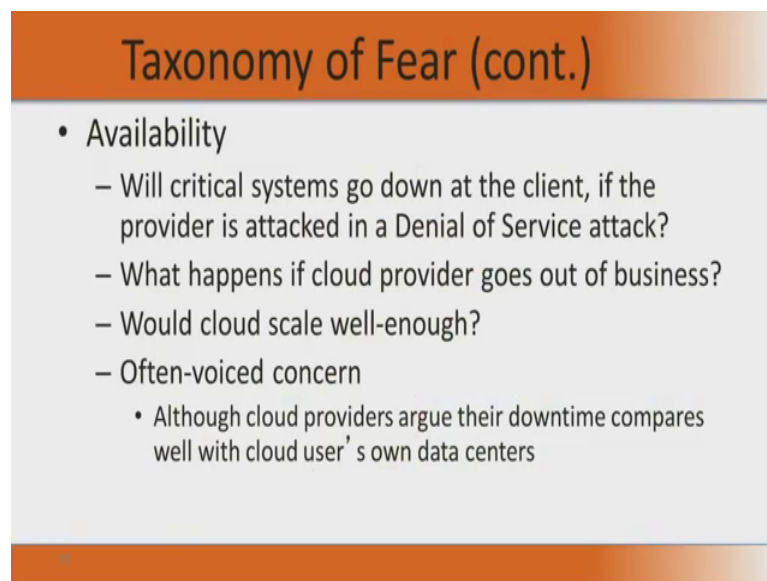
So, will the computations are they done correctly what software they use. Is my data that is stored it is not tempered or is not changed. These are all some very important integrity issues right. I fear those things. I need to get much more powerful answers about confidentiality and integrity. Third thing is about availability. I may ensure that on a real day I am opening up say something on my quarter end, will the critical system we available or it will suddenly go off. Will there be a denial of service attack as you put the latest virus. I do not have any control.

Suddenly what happens if the cloud fellow nobody, it somebody all of them vacated and they move to a new cloud what will happen if his business goes down he winds up shop. Then I have to bring back it or I have to look at another cloud; what it means and specifically when we look at say banking as a very important at thing. So, we need

continued support right. If my server for example if my doing my research and server is gone for say two days, but if a bank closes for do this I do not know, it is to be very difficult and will this clouds scale enough.

So, I have looked say hundred branches two hundred branches three hundred branches. Tomorrow I am going to three thousand branches, we will scale enough. I am looking at a research center research organization which all its a thing or put on cloud. Tomorrow I am looking at the hundred employees, tomorrow ten thousand employees will scale enough?

(Refer Slide Time: 16:07)



The slide has an orange header with the title "Taxonomy of Fear (cont.)". Below the header is a light gray area containing a bulleted list of concerns related to availability. The list includes four main points, with the last one having a sub-bullet.

- 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?
 - Would cloud scale well-enough?
 - Often-voiced concern
 - Although cloud providers argue their downtime compares well with cloud user's own data centers

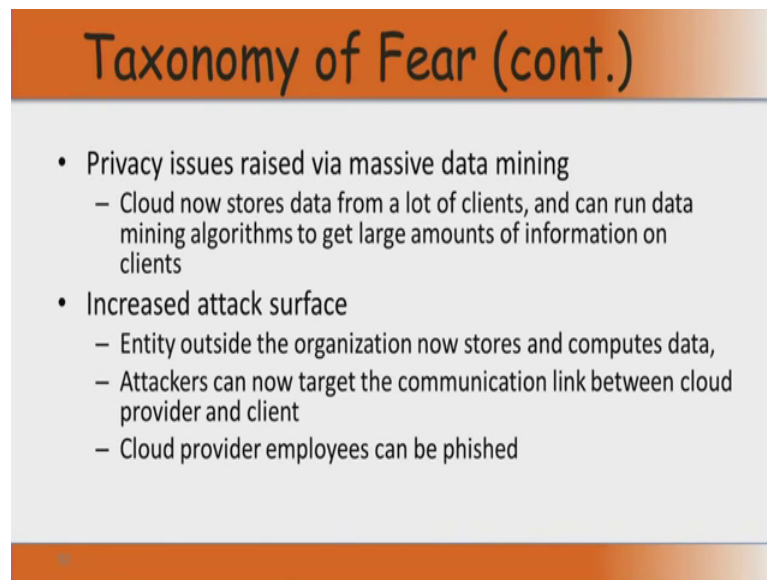
So, the cloud people now come out with are argument, your down time is much comparatively less than my down time right. This down time itself is a misnomer. So, I. So, misnomer in the sense you say the down time is in percentage, in the next five years I will give you 99 percent up time. So, one percent down time. Now, what is this one percent in say 1500 days, 15 days right. So, we can go and say 15 days then close you close a bank. So, suppose it happens that in say two years down the line 15 days it got closed.

Now, you go and look at the 5 year period and remaining time it was all working fine. So, in a 5 year period fifteen days it got closed. Let as say 4 years 350 days it was running and the last fifteen days it closed. Still by your service level agreement 99 percent it was up time, but can your bank close completely for 15 days there gone, we go out of business right. So, these are all very very important thing. Availability again when

you sign in a SLA and say some percentage of availability, it does not mean what a duration I may not even want my customer to have one hour, the bank goes because and may be somebody who is critically ill. They need money need they need cash right.

So, this is service. So, this very very important this very important fear. So, when you guys sign SLA, look at somebody says 99 percent up time in what duration that is very important.

(Refer Slide Time: 18:01)



The slide features a title 'Taxonomy of Fear (cont.)' in a dark orange header. Below the title, on a light gray background, is a bulleted list of security concerns. The list includes two main categories: 'Privacy issues raised via massive data mining' and 'Increased attack surface'. Each category has several sub-points detailing specific risks like data mining by cloud providers, external entities storing data, attackers targeting communication links, and phishing of cloud provider employees.

Taxonomy of Fear (cont.)

- 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
- Increased attack surface
 - Entity outside the organization now stores and computes data,
 - Attackers can now target the communication link between cloud provider and client
 - Cloud provider employees can be phished

Privacy issues, you go to some important mails and your typing something. So, put some verb or some noun there. You see lot of advertisement coming on the side which are related to your words. So, I say some something then I say some cloth some nearby cloths stores address comes here. That means, there mining your data. So, what is it that what is the guarantee that massive data mining is not happening and the. So, they may say that I mining data to see your basic usage pattern. So, that I could give you more effective service, but it is not necessary that this mined data is just go into stop at mining. Or they may use it for some other purpose.

And more importantly your attack surface is now increased. What you mean by the attack surface increase? Now, I have many organizations which are much more even physically or electronically closer to your data and storage. So, now, the attackers can now start targeting the communication link between the cloud provider and the clients. It is not just within the client it is between the client and we cloud provider right. So, between the cloud provider and the client I can start attacking in the communication.

The cloud provider and it is not just I am looking at the public. I am also my own people, but now have to look at the data center people also. If some employee of the data center is phished I am gone. So, now, the people whom I am looking at the process I am looked at and technology one of the three important things when I talk about ppt right, it is people, process and technology. The people, process and technology as not just ended that people, process and technology as not ended with my organization alone. When I out source it to a cloud then my people, process technology now expands to the cloud.

So, I have to move be concern about it processes and people and the technology used by the cloud. I should go an give information security awareness to the cloud service provider. I should ensure that a enough information security education he has done to the people of those organization otherwise my whole infrastructure is gone.

(Refer Slide Time: 20:58)

The slide is titled "Taxonomy of Fear (cont.)" and contains a bulleted list of concerns. The first bullet point is "Auditability and forensics (out of control of data)", which includes two sub-points: "Difficult to audit data held outside organization in a cloud" and "Forensics also made difficult since now clients don't maintain data locally". The second bullet point is "Legal quagmire and transitive trust issues", which includes two sub-points: "Who is responsible for complying with regulations?" (with a sub-bullet "e.g., SOX, HIPAA, GLBA ?") and "If cloud provider subcontracts to third party clouds, will the data still be secure?".

So, this increased attack surface is another important aspect of fear.

The next two important things is auditability, is very difficult to go and audit an outside organization especially inside a cloud because logs for example, if I want audit logs of servers I need logs of a virtual machines. I cannot look at what the other fellow did not do or what he has done. Suppose I want to go and find out he has peeked into my data? he is just a passive observer. I need to go and see his log, but his log will not available to me if I insist on that then my loge will be available to him and then there we a confidentiality breach.

In the same sense even forensics is going to be a extremely difficult and the other

important thing we talked about transitivity in trust A trust B, B trust C, A need not trust C the same thing happens here. I give my thing to your cloud vendor. So, the cloud service provider the cloud service provider would have another through who is going to maintain its storage. Now, I try it I certainly trust cloud service provider, but and the cloud service provider trust the disc vendor or, but I may not trust the disc vendor. So, there is a transitive trust issues here. And then of course, the legal quagmire. So, somebody can ask me they will ask me from a medical person. They will ask me about Hippa. I am maintaining this hippa regulation right. Thethe organization is going to be questioned not the cloud service provider. So, it is my responsibility to see that the cloud service provider who is maintaining my data in the processees and programs adhere to the standard which I should we theory.

So, this is this is another very important thing. So, these are all that we fear about this.

(Refer Slide Time: 22:54)

The slide has an orange header with the text "Taxonomy of Fear (cont.)". Below the header, on the left, is a small photo of John Chambers, Cisco CEO, with a speech bubble containing the quote: "Cloud Computing is a security nightmare and it can't be handled in traditional ways. John Chambers, CISCO CEO". To the right of the quote is a small blue line graph. Below these elements is a bulleted list of security challenges in cloud computing.

- Security is one of the most difficult task to implement in cloud computing.
 - Different forms of attacks in the application side and in the hardware components
- Attacks with catastrophic effects only needs one security flaw

So, to conclude it is famous statement by Cisco CEO of this report at well reported. Cloud computing is a security nightmare and it cannot be handled in traditional ways. So, security is one of the most difficult task to implement in cloud computing. And even if there is a single flaw here it could have catastrophic effects which will go an effect not just a single organizations, but it will go and effect if set of organizations. So, in the next session we will now go and talk more about what are all the threats.

Thank you.