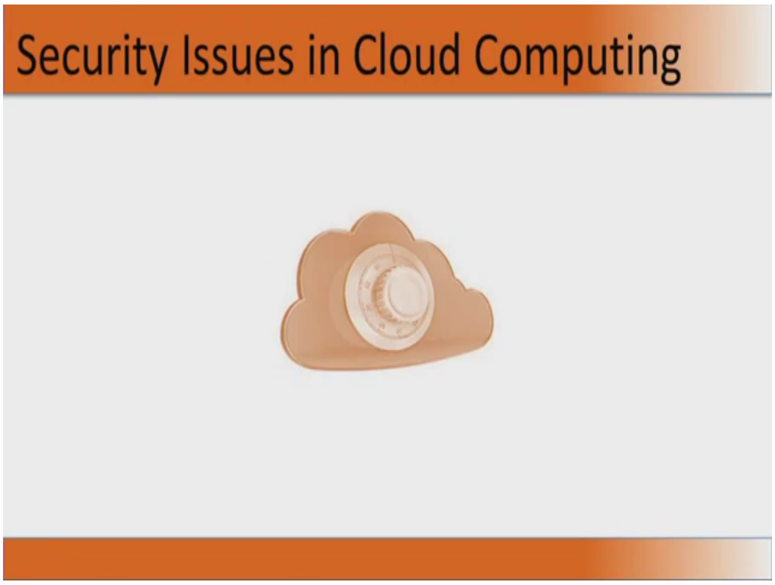
Introduction to Information Security
Prof. V. Kamakoti
Department of Computer Science and Engineering
Indian Institute of Technology, Madras

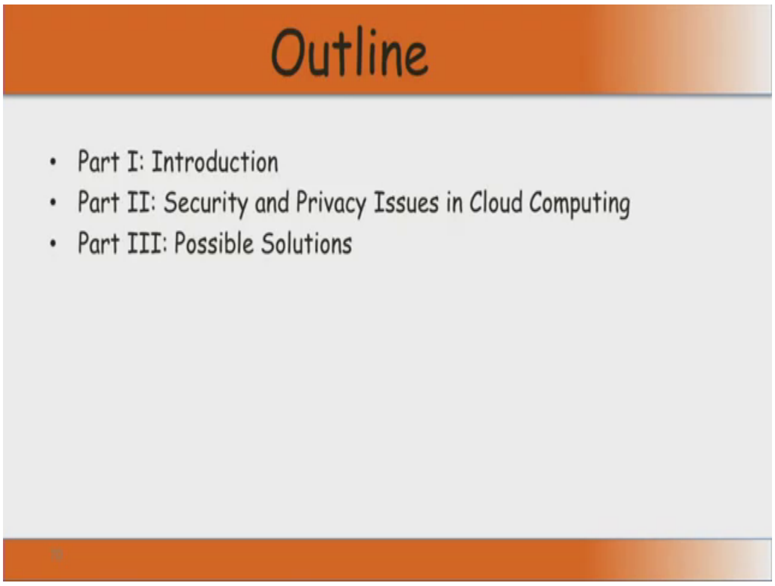
Lecture - 23

(Refer Slide Time: 00:11)



Security Issues in Cloud Computing

(Refer Slide Time: 00:19)

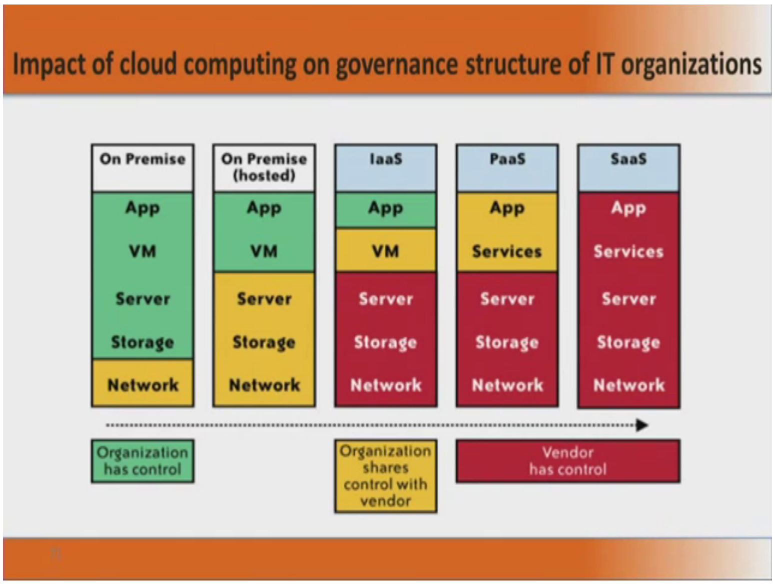


Outline

- Part I: Introduction
- Part II: Security and Privacy Issues in Cloud Computing
- Part III: Possible Solutions

We will look at security issues in cloud computing in 3 parts. Part 1 is introduction, we will talk about, what is security in the context of cloud computing. Then we will go into to the real security and privacy issues and part 3 will talk about possible solutions. now let us look at how the entire things runs.

(Refer Slide Time: 00:43)



Impact of cloud computing on governance structure of IT organizations

On Premise	On Premise (hosted)	IaaS	PaaS	SaaS
App	App	App	App	App
VM	VM	VM	Services	Services
Server	Server	Server	Server	Server
Storage	Storage	Storage	Storage	Storage
Network	Network	Network	Network	Network

Organization has control

Organization shares control with vendor

Vendor has control

So, there at least 5 different models that we are looking at. One thing is I have a data center in my in my premises, I have a bank I have the entire data center in the premises; that means, I will have I will own the storage, server, the virtual machine that is running on top of the server, just to remind you what is virtual machine. A virtual machine is a layer is a software layer that will basically run software. And it will give a view to the software that the entire machine belongs it belongs to the or entire machine is dedicated to running the software.

So, in a single server I could have several virtual machines, each virtual machine will running will be running it is own software or each virtual machine will be assign to a software. So, this one typical deployment scenario of a virtual machine and then there will be applications running on top. So, if you look at the left side of the corner it is basically that the organization for example, if you say bank, the bank as control complete control over what is stored what is the server they I use, the server, the passwords etcetera the admin privileges the virtual machine, the applications.

The network the organization actually shares control with some network vendor because the service providers will have their own hardware and necessary software infrastructure to monitor and manage the hardware. So, that is one the traditional model by which data centers work. I could have something called we could have something called a hosted model where in you go to somebody else premise or your allow somebody to come and setup everything in the in your premise.

So, here the control of your hardware, namely the server storage and network could have some share of control, but it is not the server and a storage will not be your exclusive control, but somebody else will be maintaining it for you. And then top of it would be the app and the virtual machines. So, today the model that many institutions especially banks will talk more about bank because your more worried about your money.

So, when I talk about information security the best case study that will appeal to everyman, who attends a course on information security would be a bank. So, that is why I am repeating bank because it is universally appealing to all. So, when you look at a typical banking institutions, today almost everything would be orange. In the sense there will be some system integrator who will be maintaining all the app, VM, servers, storage network, but organization will have some control over what is stored and what applications are running and what is the hardware that is executing these and the network right.

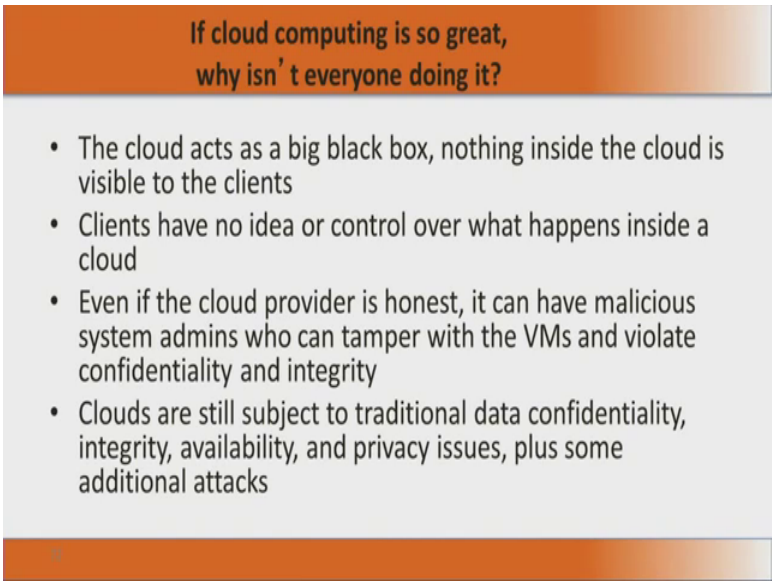
So, these two are traditional models which does not in my opinion does not come under the ambit it can be called us private clouds, the extremely private clouds. Now, the next model would be infrastructure as a service this is the real cloud that we are talking. Now, you see something in red. I am talking about the third block from the left I which is labelled IAAS, you are all the server you are hardware storage and network everything would be under the control of the vendor. So, is giving you as a service the infrastructure here. The VM will be a service which is shared between the organization and the vendor while app will be your own app.

Whatever shown in blue or green is the app is what belongs to the organization, you see the legend down organization has control, that is the legend for the green box and looking at the last row below the arrow mark in the slide. And then the orange box says organizations shares control with the vendor, while the red box says vendor alone as the control. So, when we move on to the PASS which is the, which is the platform as the service. Then you look again your app and service will become shared with the vendor the control of those will be shared with the vendor. And the and nothing is completely owned by the organization.

While we look at the last model everything the SAAS, were the software itself should be available as a service then everything is control by the vendor. So, as we move from left to right the control of the vendor becomes more than the control of the organization right.

So, in the first two there is there are parts where the organization has more control absolute control over certain layers and shared control in some layers. And as you move towards the right hand side the organization has no control over any layers at that point. So, there are very nice diagram that we that explains the changing control scenarios in organization is of today.

(Refer Slide Time: 06:39)



If cloud computing is so great, why isn't everyone doing it?

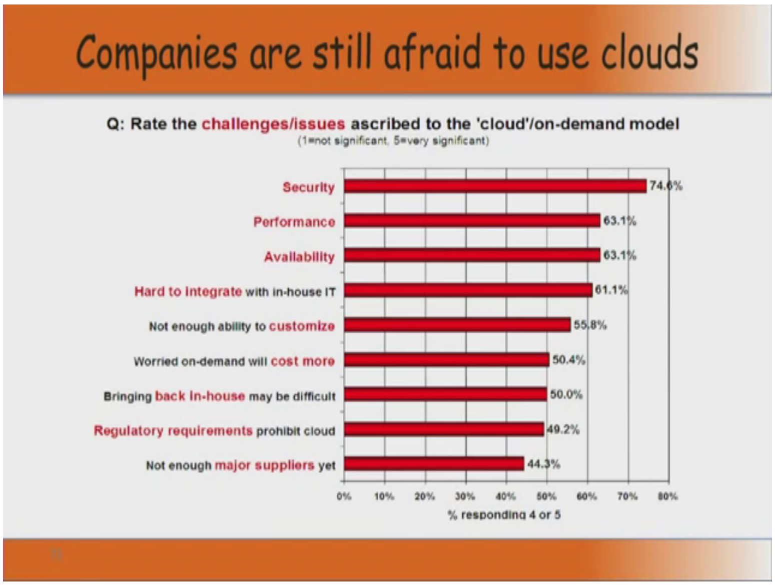
- The cloud acts as a big black box, nothing inside the cloud is visible to the clients
- Clients have no idea or control over what happens inside a cloud
- Even if the cloud provider is honest, it can have malicious system admins who can tamper with the VMs and violate confidentiality and integrity
- Clouds are still subject to traditional data confidentiality, integrity, availability, and privacy issues, plus some additional attacks

So, the now the question comes if cloud computing is so great you have seen so, many advantages technical benefits, administrative benefits, commercial benefits then why do not you use, why everyone is not using. The reason here is more of fear right when I look at looking at the list of fears, that could come I am always have reminded of one Tamil movie Tenali right and where in Doctor asks Kamal Hasan, what you fear in and gives one big list I fear of this I fear this.

Now, when you look at cloud computing also there is the very big list which organizations fears and that is the reason why it is not becoming popular. The first thing is that cloud access as a big black box. Nothing, is known to us what is inside. The clients whom you say should use the cloud as no idea and they come and start storing confidential private information. Now, you go back to our first module and say we want confidentiality, integrity, availability nobody knows what the cloud provider is going to provide you.

And we do not know whether the cloud providers is honest, whether the cloud providers can be trusted right. To a large extend I will go a little more deep down we really do not know whether he can provide as that CIA that we are looking for security. So, this is the first fear for me cloud is a black box. I do not know anything that is happening and now I am giving all the information right. Can I give can I not? if I give what will happens?. So, this this is how it is develops. We will now buildup this story in a more detailed fashion as you move now.

(Refer Slide Time: 08:44)



Companies are still afraid to use clouds

Q: Rate the challenges/issues ascribed to the 'cloud'/on-demand model

(1=not significant, 5=very significant)

Now, this is a very very interesting statistics I got it from internet, were in several questions were asked about cloud to many CTOS and CEOS and what and they were asked to grade in the range 1 to 5. 1 means your question is not very significant to us and 5 means your question is very significant to us.

All these questions were post and what you see here is the percentage of people who told the answer for those particular characteristics in the range of 4 or 5. Who mark did has 4 or 5. So, we went and ask say they asked hundred people about security security 74.6 percent of that people said that security on a cloud is a very significant factor. If a worry-some factors right. So, if you look at security 74.6 percent said it is very significant that is the rated in range 4 to 5.

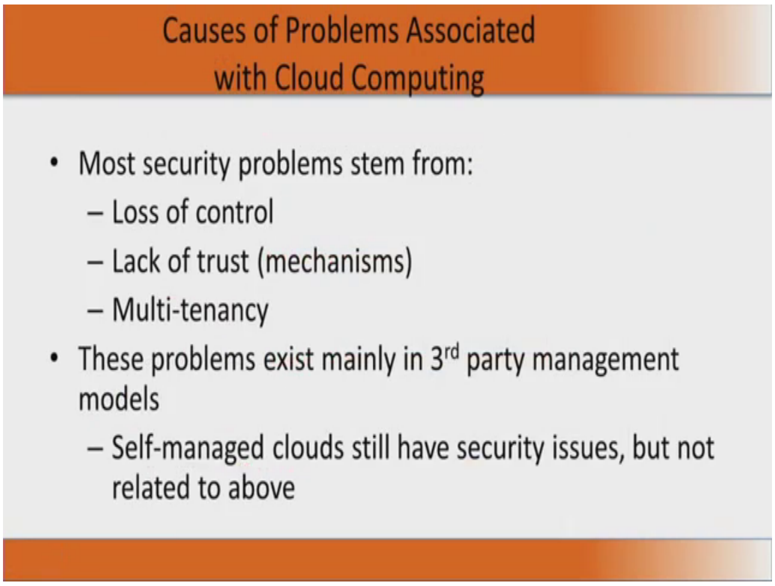
The remaining 20, 25 rated with value less than 4, but the major population 75 percent close to them self security is indeed a very significant concern. Similarly performance 63 percent said, availability 63 percent said. Hard to integrate with in house IT. I already have an in house IT now you want to move it a cloud, 61 percent. Not enough ability to customize right. I want some change right. So, you has let us take two bank model one bank is completely out sourced another is completely in house right. So, if a regulator wants a change the in house fellow will comes next day he can do it because he has a software development exclusively dedicated for it.

When you go for a out completely out source model when have to depend upon the system integrated to give you that change. And he may have n customer is we are not the only customer. So, he may take more time. So, that is another things. So, it more than 65.8 percent people fell felt that they were not able to customize it properly. And many thought that on demand it will cost more 50 percent thought and 50 percent it said. So, I go to that and suddenly I find it is not some some problem happens,for me to again restart this in house is going to be a herculean task. I think hundred percent should have told that bringing it back in house maybe difficult. Somehow 50 percent did not feel that right. Especially when your business is not IT and your business say banking. Now, you completely outsource and suddenly one day is a I want make it everything in house first time foremost I will not have inn innate talent within the organization to buildup an IT from scratch.

So, that is and the 49.2 percent told that regulatory retirements prohibit cloud. It is not really fully correct, but still there can be issues. And 44.3 percent said there are not big players already there. So, I may be left with one or choices and today I will be the first customer. So, I will be enjoying the first a groom bridegroom there, but tomorrow more on more bridegrooms come there, then I means loose that importance. So, that is a very very valid fear.

Now look at this, this is the very very important slide, which is talking lot about against cloud rather than for cloud and everything is a fear.

(Refer Slide Time: 12:46)



Causes of Problems Associated with Cloud Computing

- Most security problems stem from:
  - Loss of control
  - Lack of trust (mechanisms)
  - Multi-tenancy
- These problems exist mainly in 3rd party management models
  - Self-managed clouds still have security issues, but not related to above

So, now what is the, see there is some these are all broad things. So, why feel security is a fear. So, we are now talking about a course on information security. So, I will not talk about performance and other things, but we will now fully talk about security. The fears the we whatever we saw in the previous slide we have listed lot of fears. Let me talk about fears that are pertaining to security. The reason for this is I do not have control of my data. I do not have control of the processes. I do not have the control of the services this loss of control is one important thing.

Can I go and trust him what is the mechanism by which I can prove that the third party who is going to maintain all my data processes ectetera is trust worthy. And now more than one fellow will be using the servers. So, that adds more free up. Even if I am the only person using the server my organization alone then I am talking of several vulnerabilities and threads. Now, I am more than two fellows are running. So, what is the guaranty this multi tenancy model will my things may be will be will it be secured right.

So, these problem exist mainly in third party management models. When I manage the entire cloud, when the organization itself managers the cloud, it does not allow anybody else to come. That itself will have lot of vulnerabilities and security issues, but that does not actually has this type of these type of fears. So, what and try to tell through this slide is when you move from a data center which you may call us a private cloud for all practical purpose.

When you move to a public cloud a shared resource, what are what are the new types of fears that are going to come up. These are the things now why do we feel that I am loosing control what is control after all. One thing is for example, one of the control is data mobility what is the how can I share the data between the cloud services right. Now, there are there are many softwares at I want to deploy in the cloud. I really do not know where which software you will be running. I know that it will be running on different virtual machines. How do I securedly moves; and there can be software which interact which other right.

Your loan processing software has to go and look at the credit rating of your customer. Or it may be a reporting software; your loan processing has to look at a reporting software. So, how securedly data will be moving on one server one virtual machine to another right. I do not have any controls. So, this is some simple example of what I mean by what is loss of control really. I do not know where my data resides is it residing inside India are the outside India are inside your country are outside your country.

So, these are all very big issues and then very importantly some people now when suppose I am certified by certain agencies for example, there is there is of FISMA- federal information security management act right. There are several things that come out of that like your ISO27001 is your security concerns of the government which comes which reflects through these acts and these certifications can it be, you know maintained when I move from a a private standard alone infrastructure to a cloud infrastructure.

So, this is another short of things I trust. Suppose I have a FISMA or a certifications issued based on these acts I basically have a trust in my environment. And when I move to environment unless this type of certifications come up there. And they are also certified then the same trust cannot be gone. Now, this trust itself is sort of very subjective. One interesting thing is suppose you want to go and mathematically model trust. It is very very important to it is very important to look at a mathematical definition for trust because ultimately we are looking at a systems and trying to prove it is secured, formally prove it to be secured.

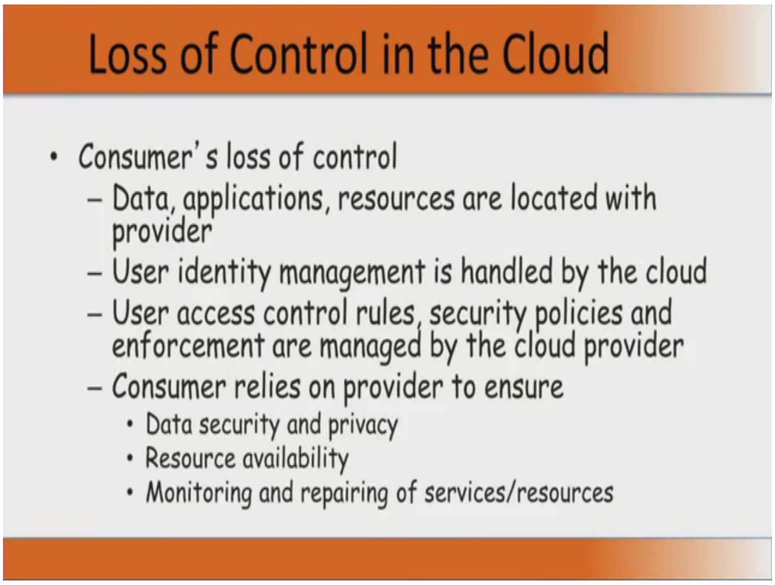
So, when we look at properties in mathematics, properties that are well defined in mathematics there should be some relations right. There are lot of mathematical relations for example, mathematical properties of relations. Trust is a relation between A and B, A trust B. In mathematics between entities you could define lot of relations, some of the relations very important relations are reflexive. A relation is reflexive on a set give every element is related itself. For example, if I trust myself and like that every individual in this well trust him selves, then then it is then it then trust is reflexive relation.

I do not trust myself many times. I do not trust in remembering my password I do not trust whether I will give a correct password that is why I have assistant tool which will tell whether my password is correct or not. There is another relation call symmetric if A is related to B then B should be related to A. I trust you, you may not trust me. So, trust is not symmetric, trust is not transitive also. A trust B, B trust C, A need not trust C. In one of this slide will talk about transitive relations about clouds specifically.

Trust is not transitive, trust is also not context independent. I trust you for something I do not trust for you something else right. Trust is also temporal morning I will trust you evening I may not trust you right. So, if you look at trust dose not satisfy any of the major mathematical properties that will helps someone to define a property. Trust as a property does not satisfy many mathematical many of the important mathematical relations.

So, it a very difficult to mathematically get a definition for trust, but ironically for several decades the whole world has been running on trust. And that mathematical. So, the lack of support from mathematics makes trust a very fear some property. A property that everybody fears of; quickly somebody will not trust especially when it comes to finance or economy it is very difficult for someone to trust another. So, for example, how many of you listening to me here will go and sign a security in a bank surety in a bank for a person whom you know for say one month, who me you know for say two months, we just go and see I do not know how many people will do that.

(Refer Slide Time: 20:35)



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

So, in the next session we will talk about more on this control aspect.

Thank you.

.