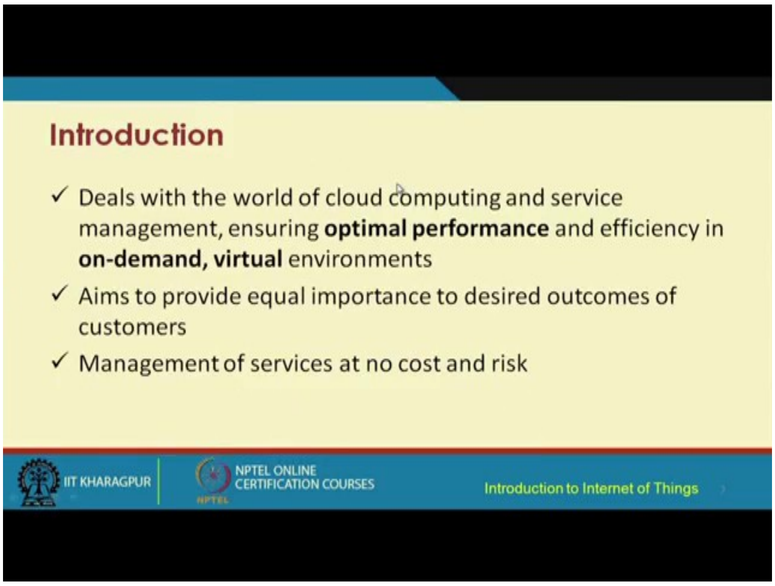
Introduction to Internet of Things
Prof. Sudip Misra
Department of Computer Science and Engineering
Indian Institute of Technology, Kharagpur

Lecture - 39
Cloud Computing - Service Management and Security

In this lecture which is the third in the series on cloud computing for internet of things we are going to specifically focus on issues of service management and security. So, we will look at some of the issues with service management and security in this lecture and we will not specifically get get too much deep into how to offer the service management and how to secure the systems that will be basically you know out of the scope of this introductory course on internet of things. So, we will simply try to focus on the issues that are there and which have to be taken care of while dealing with cloud computing and particularly more specifically of cloud computing for IoT.

(Refer Slide Time: 01:13)



Introduction

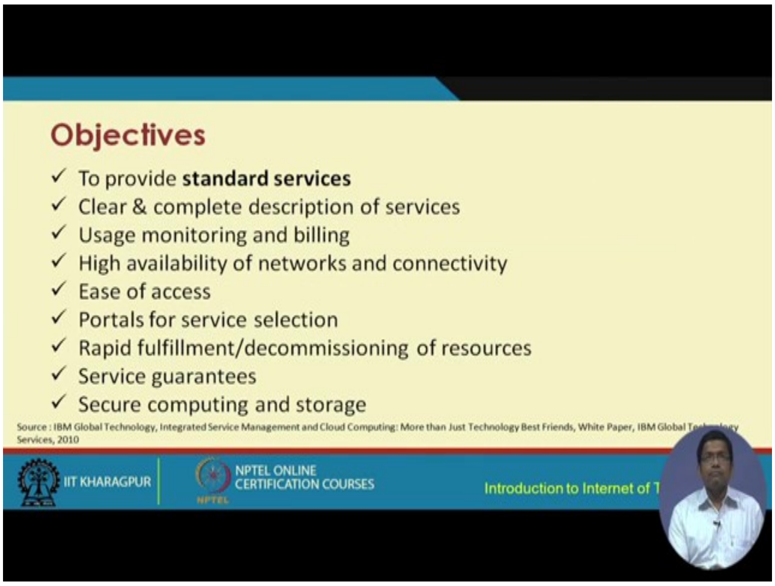
- ✓ Deals with the world of cloud computing and service management, ensuring **optimal performance** and efficiency in **on-demand, virtual** environments
- ✓ Aims to provide equal importance to desired outcomes of customers
- ✓ Management of services at no cost and risk

IIT KHARAGPUR
NPTEL ONLINE CERTIFICATION COURSES
Introduction to Internet of Things

So, let us look at some of these different issues. So, before that we have to be careful about few things. So, when we are talking about cloud computing we are essentially talking about service offerings computing services being offered and when we talk about service offerings we have to ensure that there is optimal performance that is delivered to the intended customers or the end users and there is on demand whenever there is required, the services are offered in an efficient manner in a virtual environment because as we saw in the previous lectures on cloud computing these are environments which are virtual. Cloud is essentially a virtual environment where you know computing resources are offered through the through the use or through the help of virtualization technologies.

So, basically the aim is to provide equal importance to desired outcomes of customers through service management. So, that the customers are satisfied and so, that there you know the customers get the services in an; in you know in a good way at no extra cost and with minimum risk. So, minimum risk means I will give you an example over here cost is understandable, but risk basically refers to that let us say that customer was using some computing resource and if due to some reason that resource becomes unavailable there should be the risk mitigation technique should ensure that there is some additional physical resource which will be mapped to the virtual one that the customer was using.

(Refer Slide Time: 03:19)



Objectives

- ✓ To provide **standard services**
- ✓ Clear & complete description of services
- ✓ Usage monitoring and billing
- ✓ High availability of networks and connectivity
- ✓ Ease of access
- ✓ Portals for service selection
- ✓ Rapid fulfillment/decommissioning of resources
- ✓ Service guarantees
- ✓ Secure computing and storage

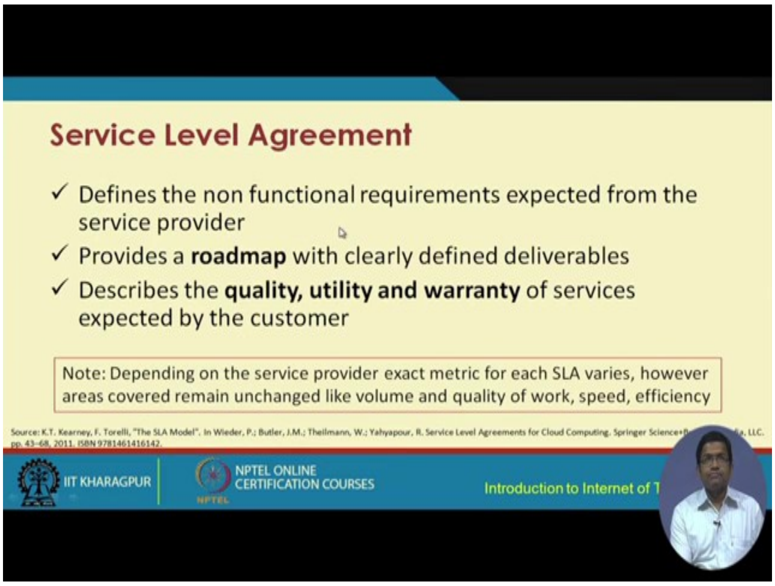
Source : IBM Global Technology, Integrated Service Management and Cloud Computing: More than Just Technology Best Friends, White Paper, IBM Global Technology Services, 2010

IIT KHARAGPUR
NPTEL ONLINE CERTIFICATION COURSES
NPTEL
Introduction to Internet of T

So that provisioning has to be done dynamically and the customer should not feel that something was has had gone wrong and because of which this change happened in the background. So, basically it is required to offer different types of services and services including usage monitoring and billing there should be complete description of clear and complete description of the services that the customer is going to get. Then issues with respect to availability of networks and connectivity and it should be available continuously high availability of networks and connectivity should be there; there should be ease of access to these resources and and it should be managed the services should be managed in such a manner that the customer will not be able to get any get any feeling of any under or you know underperformed computing environment.

There should be portals for service selection there should be service guarantees and rapid fulfillment of resources or decommissioning of resources should should be there and it should be a secure environment where securely computing and storage facilities are made available to the users.

(Refer Slide Time: 04:34)



Service Level Agreement

- ✓ Defines the non functional requirements expected from the service provider
- ✓ Provides a **roadmap** with clearly defined deliverables
- ✓ Describes the **quality, utility and warranty** of services expected by the customer

Note: Depending on the service provider exact metric for each SLA varies, however areas covered remain unchanged like volume and quality of work, speed, efficiency

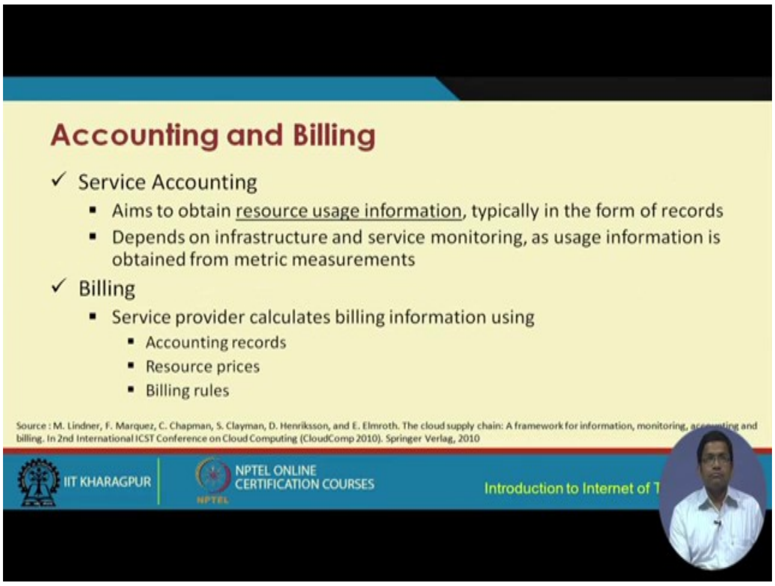
Source: K.T. Kearney, F. Torelli, "The SLA Model". In Wieder, P.; Butler, J.M.; Theilmann, W.; Yahyapour, R. Service Level Agreements for Cloud Computing. Springer Science+B a, LLC. pp. 43–68, 2011. ISBN 9781461416142.

IIT KHARAGPUR
NPTEL ONLINE CERTIFICATION COURSES
NPTEL
Introduction to Internet of T

So, what is this service level agreement? So, service level agreement as per definition is about non functional requirements that are expected from the service provider more specifically the cloud service provider and this service level agreement in short in the industry it is known as SLA this SLA basically is required to provide a roadmap which will give clearly defined deliverables

So, this SLA will typically describe the quality, the utility, the warranty of services that are expected by the customer. So, this SLA will be some sort of an agreement and handshaking platform between the service providers and the customers.

(Refer Slide Time: 05:35)



Accounting and Billing

- ✓ Service Accounting
  - Aims to obtain resource usage information, typically in the form of records
  - Depends on infrastructure and service monitoring, as usage information is obtained from metric measurements
- ✓ Billing
  - Service provider calculates billing information using
    - Accounting records
    - Resource prices
    - Billing rules

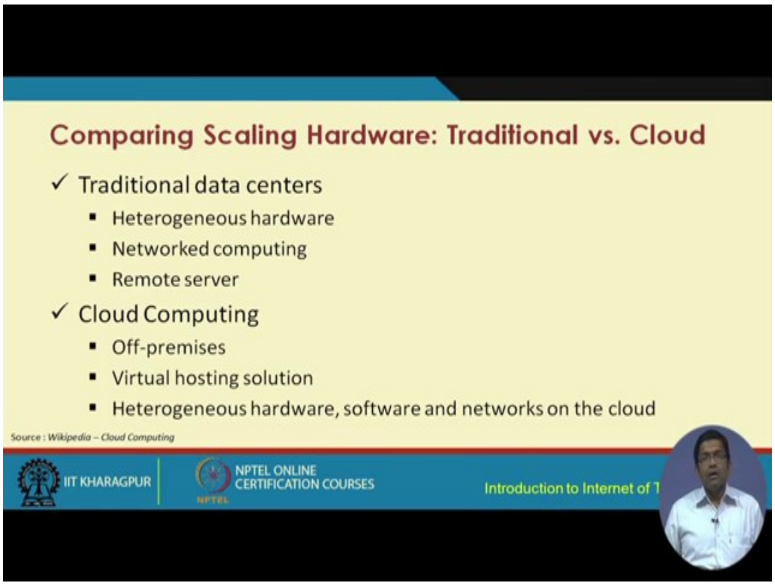
Source : M. Lindner, F. Marquez, C. Chapman, S. Clayman, D. Henriksson, and E. Elmroth. The cloud supply chain: A framework for information, monitoring, accounting and billing. In 2nd International ICST Conference on Cloud Computing (CloudComp 2010). Springer Verlag, 2010

IIT KHARAGPUR
NPTEL ONLINE CERTIFICATION COURSES
NPTEL
Introduction to Internet of T

So, that the customers know what level of services the customer is going to get from the service provider. Accounting and billing which go hand in hand are very important. So, basically based on the resources the use of the resources and the information about such an such use it is required to bill the customers it is required to bill the customers and keeping track of this information about the resource. Resource use which is typically in the form of records the customers will be billed and the customers will be having you know it they will billed based on the accounting records, the resource prices and the billing rules. There has to be some rules based on which the customer is going to be billed maybe this much unit of resource consumption will lead to this much you know billing rate a higher amount will lead to another higher rate and so on.

So like this there has to be slabs or some billing policy some billing rules which has to be agreed upon by between the customers and the service provider. So, accounting records which has to be kept track of which is a core component of the accounting module the resource prices; that means, you know what is the unit cost of each of these different resources and the billing rules; that means, what is the policy by which the customer is going to be billed. So, all these taken together will be used for billing purpose.

(Refer Slide Time: 07:21)



Comparing Scaling Hardware: Traditional vs. Cloud

✓ Traditional data centers

- Heterogeneous hardware
- Networked computing
- Remote server

✓ Cloud Computing

- Off-premises
- Virtual hosting solution
- Heterogeneous hardware, software and networks on the cloud

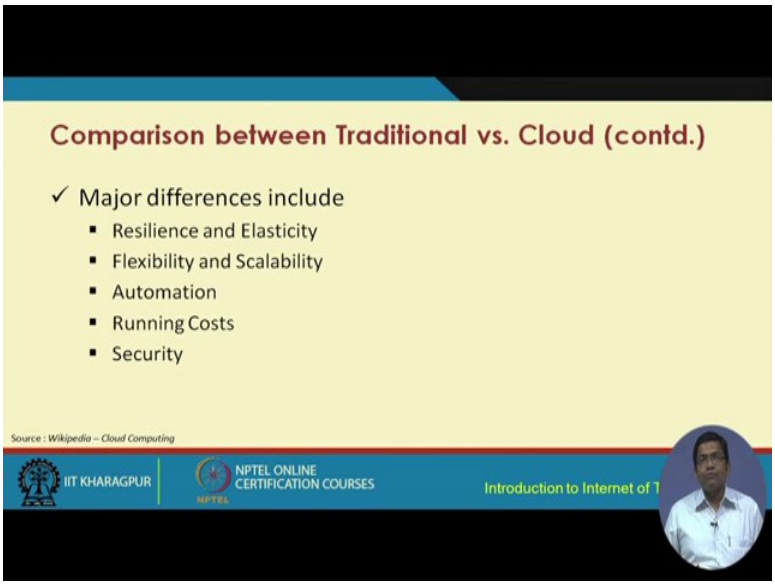
Source : Wikipedia – Cloud Computing

IIT KHARAGPUR
NPTEL ONLINE CERTIFICATION COURSES
NPTEL
Introduction to Internet of T

Now traditionally data centers were used or even simple IT infrastructure used to be used in the companies in the organizations now we are talking about replacing such things or supplementing such traditional regular IT infrastructure based or data center based platforms with cloud. So, we are talking about that. So, let us compare with respect to different criteria now for example, with respect to the hardware the traditional data centers used to use heterogeneous hardware different types of hardware purchase through different means you know different groups purchasing and so on and so forth heterogeneous hardware with network computing and remote server.

So typically what would happen through a remote environment these remote network environment these heterogeneous hardware would get access to a server get access to the server and that used to be the traditional way of getting access to different computing resources getting access to remote server. Means like data centers would be hosted remotely and through this hardware and the network environment the users are going to get access to the servers and computing needs etcetera, etcetera that used to be traditional in cloud computing we are talking about off-premise resources with virtually hosted solutions with heterogeneous hardware software and networks everything available on the cloud whenever things are required, whenever users have requirements they can easily scale up or down the resources the resources are going to be made available to the users as per the requirement through a virtualized platform.

(Refer Slide Time: 09:39)



Comparison between Traditional vs. Cloud (contd.)

✓ Major differences include
- Resilience and Elasticity
- Flexibility and Scalability
- Automation
- Running Costs
- Security

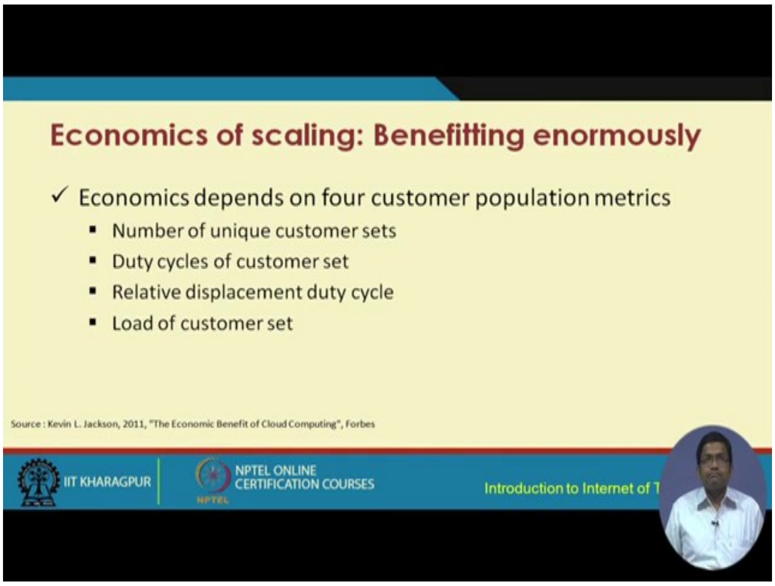
Source : Wikipedia – Cloud Computing

IIT KHARAGPUR
NPTEL ONLINE CERTIFICATION COURSES
Introduction to Internet of T

So, there is some difference as you can understand between the traditional data centers traditional IT infrastructure in the companies and the cloud computing environment there are different other differences as well which we have already understood in different perspective in the previous 2 lectures on cloud computing. One is the differences in resilience and elasticity you know. So, cloud resources cloud platforms are available you know in an elastic manner resilient manner resilience means that something going wrong users will not have a clue of it you know and it is taken care of the problem is taken care of its resilient to different kinds of failures and so on.

Flexibility and scalability you know you need more resources you just pay for it you have the resources with you whenever you need automation is understood running costs security; security is very important security is you know in the cloud environment you have more security compared to the traditional data center or regular IT infrastructure based environment and with respect to running costs I have already explained before. So, I do not need to explain further. So, the running you know. So, here actually you have running costs compared to the traditional onetime cost or periodic costs in on the traditional data center environment. So, here you have running costs. So, you need you need more resources you pay for it you need even more you pay even more and so on. So, running costs have to be taken care of in the cloud computing model.

(Refer Slide Time: 11:07)



Economics of scaling: Benefitting enormously

✓ Economics depends on four customer population metrics

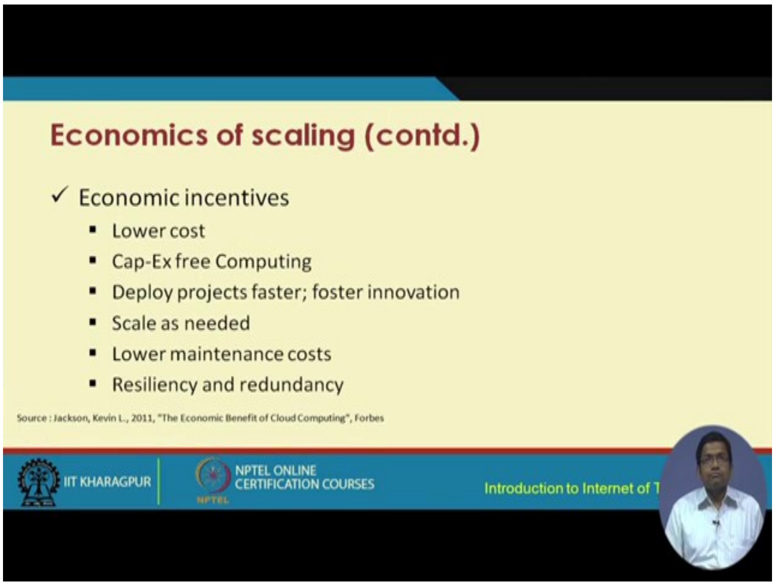
- Number of unique customer sets
- Duty cycles of customer set
- Relative displacement duty cycle
- Load of customer set

Source : Kevin L. Jackson, 2011, "The Economic Benefit of Cloud Computing", Forbes

IIT KHARAGPUR
NPTEL ONLINE CERTIFICATION COURSES
Introduction to Internet of T

Now the economics of scaling which basically benefits the users enormously and the economics basically depends on 4 customer population metrics number one the number of unique customer sets, number 2 is the duty cycle of the customer set, number three is the relative displacement duty cycle and number 4 is the load of the customer set. So, all these basically factors all these factors basically help in coming up with ideas of economics of scaling.

(Refer Slide Time: 11:47)



Economics of scaling (contd.)

✓ Economic incentives

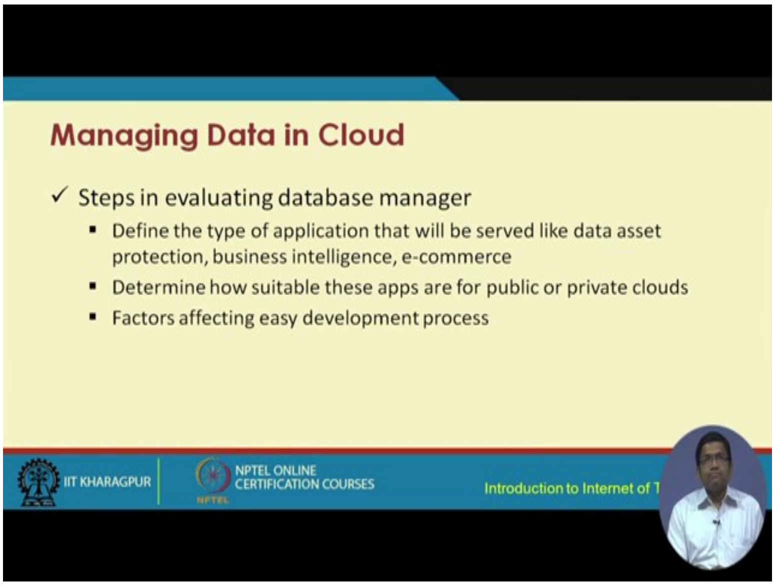
- Lower cost
- Cap-Ex free Computing
- Deploy projects faster; foster innovation
- Scale as needed
- Lower maintenance costs
- Resiliency and redundancy

Source : Jackson, Kevin L., 2011, "The Economic Benefit of Cloud Computing", Forbes

IIT KHARAGPUR
NPTEL ONLINE CERTIFICATION COURSES
Introduction to Internet of T

There are different economic incentives for cloud computing lowering the cost behind infrastructure and computing required in the organization then you know cap-ex free computing you know cap free computing you know exclusively made available to the customers deployment of projects faster that will foster innovation as well then you know scaling up or down as an when required lower maintenance costs resiliency and redundancy.

(Refer Slide Time: 12:21)



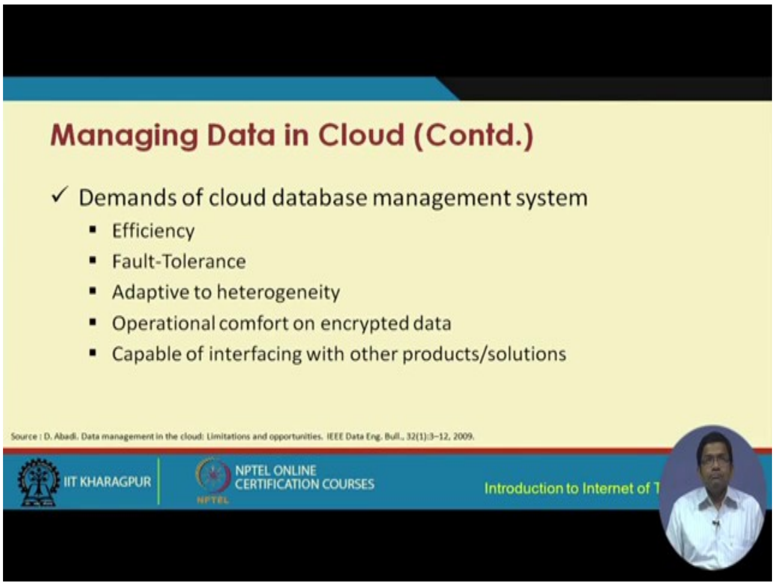
Managing Data in Cloud

✓ Steps in evaluating database manager
- Define the type of application that will be served like data asset protection, business intelligence, e-commerce
- Determine how suitable these apps are for public or private clouds
- Factors affecting easy development process

IIT KHARAGPUR
NPTEL ONLINE CERTIFICATION COURSES
Introduction to Internet of T

Steps in evaluating the database manager; so, database management is very important you need to manage the data in the cloud. So, there are different ways of doing it. So, will not get into too much of thing, but we need to understand the saliency behind this particular issue. So, it is required to define the type of application that will be served like the data asset protection, business intelligence, e-commerce etcetera and determine how suitable these applications are for public and private clouds and the factors that are affecting the easy deployment process.

(Refer Slide Time: 13:01)



Managing Data in Cloud (Contd.)

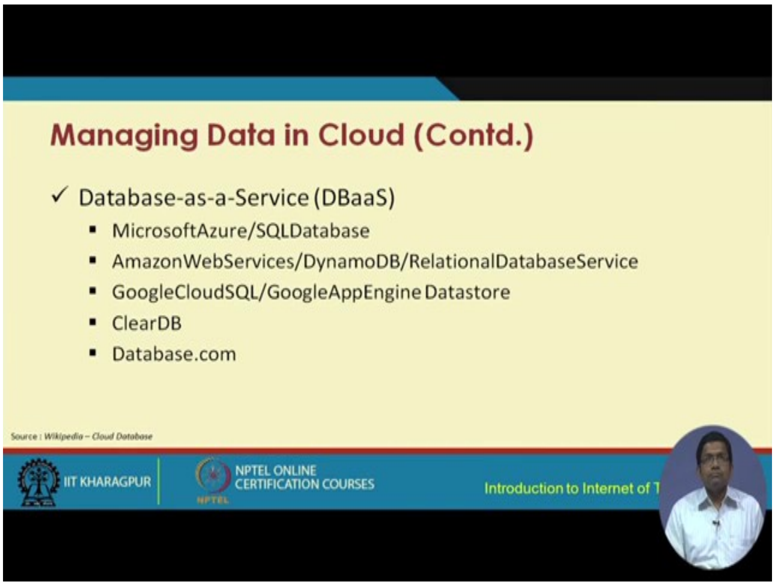
- ✓ Demands of cloud database management system
  - Efficiency
  - Fault-Tolerance
  - Adaptive to heterogeneity
  - Operational comfort on encrypted data
  - Capable of interfacing with other products/solutions

Source : D. Abadi. Data management in the cloud: Limitations and opportunities. IEEE Data Eng. Bull., 32(1):3–12, 2009.

IIT KHARAGPUR
NPTEL ONLINE CERTIFICATION COURSES
NPTEL
Introduction to Internet of T

The demands of cloud database management system include efficiency fault tolerance adaptive; adaptivity to heterogeneity operational comfort on encrypted data and keep and the ability of interfacing with different products and solutions.

(Refer Slide Time: 13:32)



Managing Data in Cloud (Contd.)

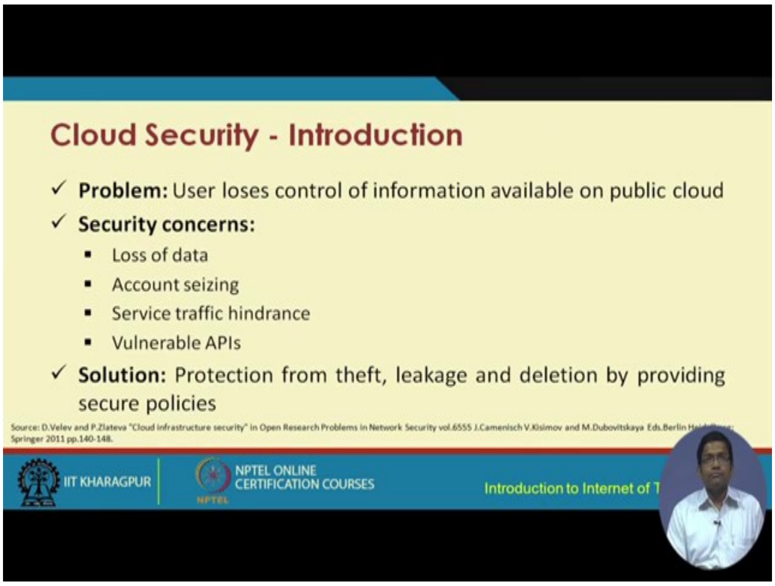
- ✓ Database-as-a-Service (DBaaS)
  - MicrosoftAzure/SQLDatabase
  - AmazonWebServices/DynamoDB/RelationalDatabaseService
  - GoogleCloudSQL/GoogleAppEngine Datastore
  - ClearDB
  - Database.com

Source : *Wikipedia – Cloud Database*

IIT KHARAGPUR
NPTEL ONLINE CERTIFICATION COURSES
NPTEL
Introduction to Internet of T

So this basically is quite you know explicit it is quite understandable each of these. So, we do not need to really dig into them in further detail. So, for managing data in the cloud we need some kind of service like database as a service DBaaS we need something like that and that has to be integrated with the cloud platforms like Microsoft azure or SQL database. So, SQL database basically comes with Microsoft azure or with Amazon web services with the help of DynamoDB relational database service and so on or in the case of Google cloud SQL taking help of database as a service like platforms like Google app engine data store, clearDB database dot com and so on.

(Refer Slide Time: 14:29)



Cloud Security - Introduction

- ✓ **Problem:** User loses control of information available on public cloud
- ✓ **Security concerns:**
  - Loss of data
  - Account seizing
  - Service traffic hindrance
  - Vulnerable APIs
- ✓ **Solution:** Protection from theft, leakage and deletion by providing secure policies

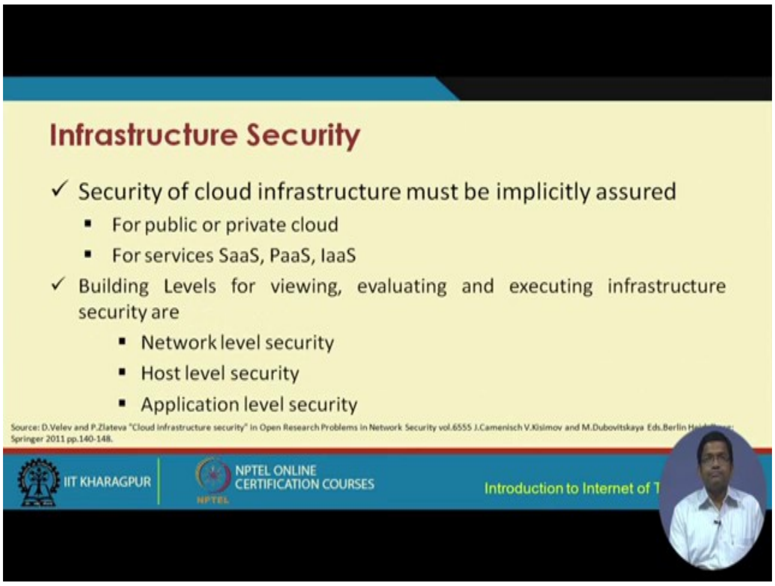
Source: D.Velev and P.Zlateva "Cloud infrastructure security" in Open Research Problems in Network Security vol.6555 J.Camenisch V.Kisimov and M.Dubovitskaya Eds.Berlin Heidelberg: Springer 2011 pp.140-148.

IIT KHARAGPUR
NPTEL ONLINE CERTIFICATION COURSES
NPTEL
Introduction to Internet of T

So these are the different platforms database as a service platforms that are available through commercial or open source mechanisms for use with cloud. Now let us come to the issue of security which is the second part of the lecture and here basically we have to be careful because when you are talking about cloud you are essentially handling different types of data and not only different types of data this data are going to be stored in different servers different platforms which may be geographically distributed without the cloud user even having a clue about what is going on behind the scene where physically the data is going to decide the cloud user does not know. So, data security is very important and overall the security of the cloud platform is very important because otherwise the customers will have lot of concerns which will affect directly or indirectly their use of cloud services.

So, the problem is that the user in a cloud platform would essentially lose control of the information that is available on the public cloud. So, concerns more specifically about the loss of data seizing of the account service traffic hindrance vulnerability of APIs are paramount in the case of cloud and the security of cloud. So, these security concerns have to be taken care of in addition to any other IT security issues that you already know. So, the solution is to have counter security solutions, platforms APIs you know applications software etcetera, etcetera which will protect from theft leakage of data deletion of data accidentally by providing security policies by providing security policies.

(Refer Slide Time: 16:32)



Infrastructure Security

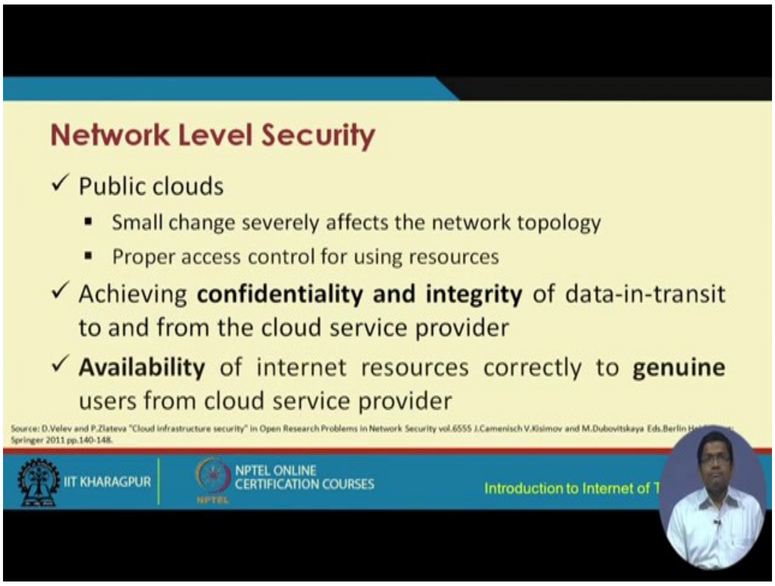
- ✓ Security of cloud infrastructure must be implicitly assured
  - For public or private cloud
  - For services SaaS, PaaS, IaaS
- ✓ Building Levels for viewing, evaluating and executing infrastructure security are
  - Network level security
  - Host level security
  - Application level security

Source: D.Velev and P.Zlateva "Cloud infrastructure security" in Open Research Problems in Network Security vol.6555 J.Camenisch V.Kisimov and M.Dubovitskaya Eds.Berlin Heidelberg: Springer 2011 pp.140-148.

IIT KHARAGPUR
NPTEL ONLINE CERTIFICATION COURSES
NPTEL
Introduction to Internet of T

So, security of cloud infrastructure must be implicitly assured for public or private cloud for services such as SaaS, PaaS and IaaS building levels of viewing evaluating and executing infrastructure security include network level security host level security and application level security.

(Refer Slide Time: 16:54)



Network Level Security

- ✓ Public clouds
  - Small change severely affects the network topology
  - Proper access control for using resources
- ✓ Achieving **confidentiality and integrity** of data-in-transit to and from the cloud service provider
- ✓ **Availability** of internet resources correctly to **genuine** users from cloud service provider

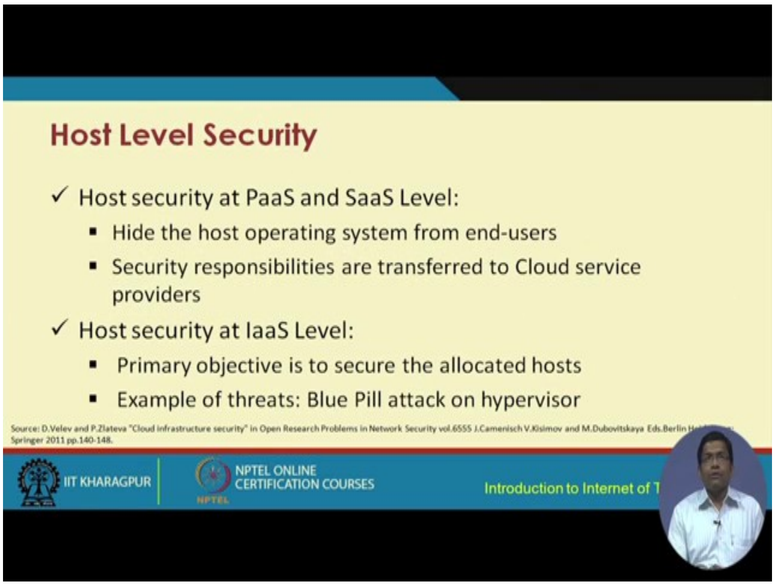
Source: D.Velev and P.Zlateva "Cloud infrastructure security" in Open Research Problems in Network Security vol.6555 J.Camenisch V.Kisimov and M.Dubovitskaya Eds.Berlin Heidelberg: Springer 2011 pp.140-148.

IIT KHARAGPUR
NPTEL ONLINE CERTIFICATION COURSES
NPTEL
Introduction to Internet of T

In the case of public cloud we have to ensure that the small change does not severely affect the network topology and there has to be proper access control for using resources. So, this is a network level issue and that has to be ensured. Second thing is achieving you know character traits like confidentiality and integrity of data in transit to and from cloud service provider.

So confidentiality of data see as you know that data confidentiality integrity availability and non repudiation are very much important issues in the context of security. So, achieving at the network level achieving confidentiality and integrity of data in transit data flowing into the cloud and coming out of the cloud has to be insured by the cloud service provider and the security rather the confidentiality.

(Refer Slide Time: 18:13)



Host Level Security

✓ Host security at PaaS and SaaS Level:
- Hide the host operating system from end-users
- Security responsibilities are transferred to Cloud service providers

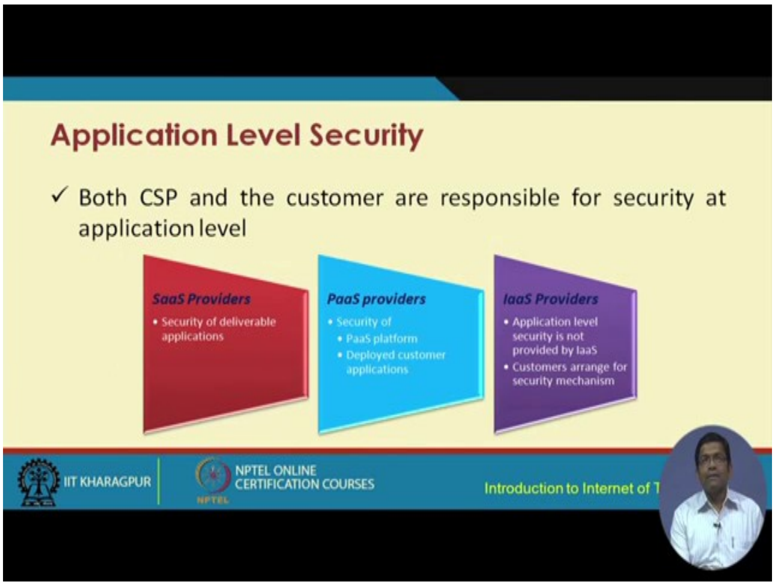
✓ Host security at IaaS Level:
- Primary objective is to secure the allocated hosts
- Example of threats: Blue Pill attack on hypervisor

Source: D.Velev and P.Zlateva "Cloud infrastructure security" in Open Research Problems in Network Security vol.6555 J.Camenisch V.Kisimov and M.Dubovitskaya Eds.Berlin He
Springer 2011 pp.140-148.

IIT KHARAGPUR
NPTEL ONLINE CERTIFICATION COURSES
NPTEL
Introduction to Internet of T

And integrity of it availability of internet resources correctly to genuine users from the cloud service provider is another issue of concern at the network layer at the host layer issues particularly at the PaaS and the SaaS level include hiding the host operating system from the end users and ensuring to delegate security responsibilities to the cloud service providers. Host security at IaaS level include the objective of securing the allocated hosts with the help of different software etcetera to ensure that attacks such as the blue pill attack on the hypervisor which is a core component of IaaS platforms is mitigated or is taken care of blue pill attack as you may be already aware is a specific type of attack on the hypervisor and hypervisor is what I have already explained in the previous lecture on cloud. So, hypervisor you know the virtual machines sit on top of the hypervisor; hypervisor is tasked to manage these virtual machines.

(Refer Slide Time: 19:31)



Application Level Security

✓ Both CSP and the customer are responsible for security at application level

SaaS Providers

- Security of deliverable applications

PaaS providers

- Security of
  - PaaS platform
  - Deployed customer applications

IaaS Providers

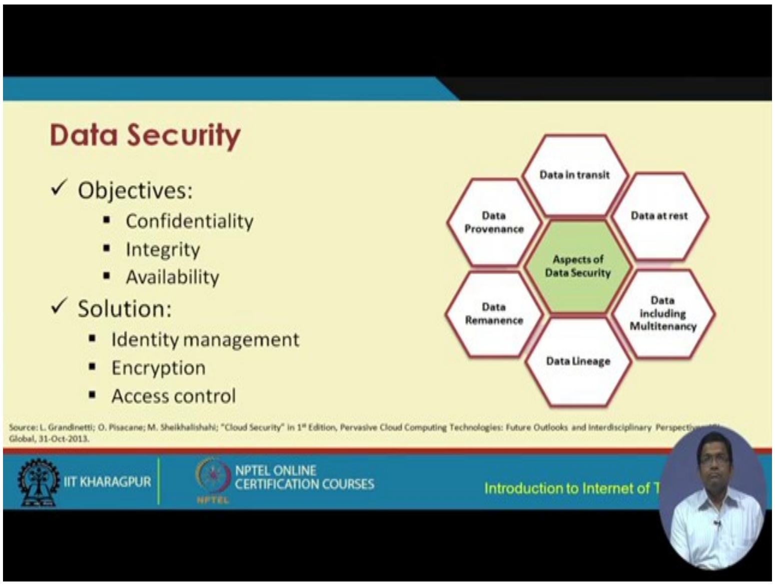
- Application level security is not provided by IaaS
- Customers arrange for security mechanism

IIT KHARAGPUR
NPTEL ONLINE CERTIFICATION COURSES
NPTEL
Introduction to Internet of T

So, blue pill attack is a very popular form of attack on the hypervisor and that kind of threat has to be taken care of at the host level. At the application level both the CSP and the customer are responsible for security at the application level. So, it is you know here specifically the application at the application level not just the CSP the customer also has to take care.

so if it is a SaaS provider SaaS cloud service provider taken care of the security of deliverable applications is there you know should be their main focus from a security perspective from for PaaS providers security of the PaaS PaaS platform; that means, the platform which is offered as a service for development it is a Google app engine kind of environment you know its security etcetera has to be taken care of and the deployed customer applications security of the deployed customer applications. So, that is also another concern at the IaaS level IaaS providers level the application level security is not provided by IaaS customers arrange for the security mechanism themselves.

(Refer Slide Time: 20:47)



Data Security

- ✓ Objectives:
  - Confidentiality
  - Integrity
  - Availability
- ✓ Solution:
  - Identity management
  - Encryption
  - Access control

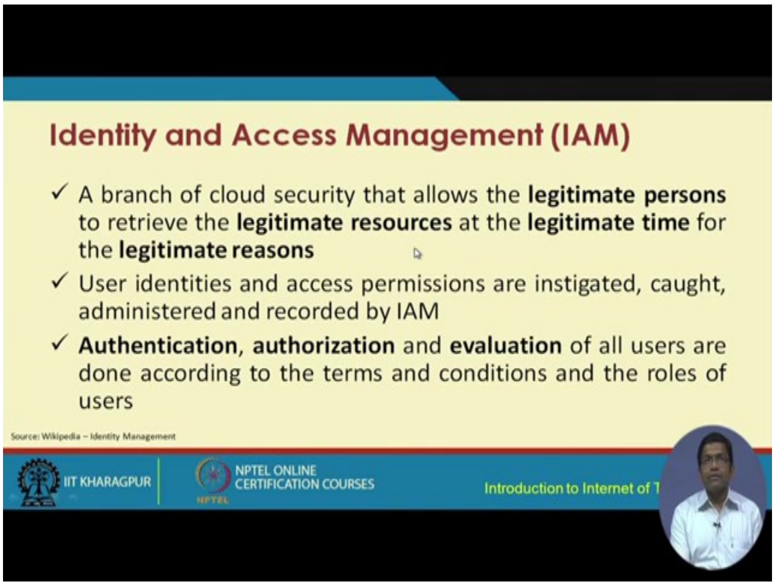
Source: L. Grandinetti; O. Pisacane; M. Sheikhalishahi; "Cloud Security" in 1st Edition, Pervasive Cloud Computing Technologies: Future Outlooks and Interdisciplinary Perspectiv... Global, 31-Oct-2013.

IIT KHARAGPUR
NPTEL ONLINE CERTIFICATION COURSES
NPTEL
Introduction to Internet of T

So customer has to take care of the security themselves data security has different objectives and the corresponding issues objectives include confide ensuring confidentiality of the data integrity of the data and availability what does confidentiality means that the data should be confidential and should be made available to only the intended stakeholder integrity means that the data should not be tampered with in between. That means, when it is flowing into the cloud or coming out of the cloud and availability means that the data should be made available as per the service level agreement to the intended customers in a secured manner.

So that different solutions include you know using identity management techniques encryption access control and so on. So, there are different aspects of data security data provenance, data in transit, data at rest data at rest means the data that is used for long term use that is data at rest I mean which does not change to fast and it will be there in the server for long term use you know in the future and so, on data including multi tenancy and the data lineage. So, data lineage means data lineage data remanence and data provenance these are the issues with the data. So, data lineage means like from the start you know the from the source till the data is used you know ensuring the security of it and you know similarly the data remanence basically takes care of that whenever the residual data etcetera, etcetera you know securing that data you know keeping track of the data that basically has to be taken care of.

(Refer Slide Time: 22:45)



Identity and Access Management (IAM)

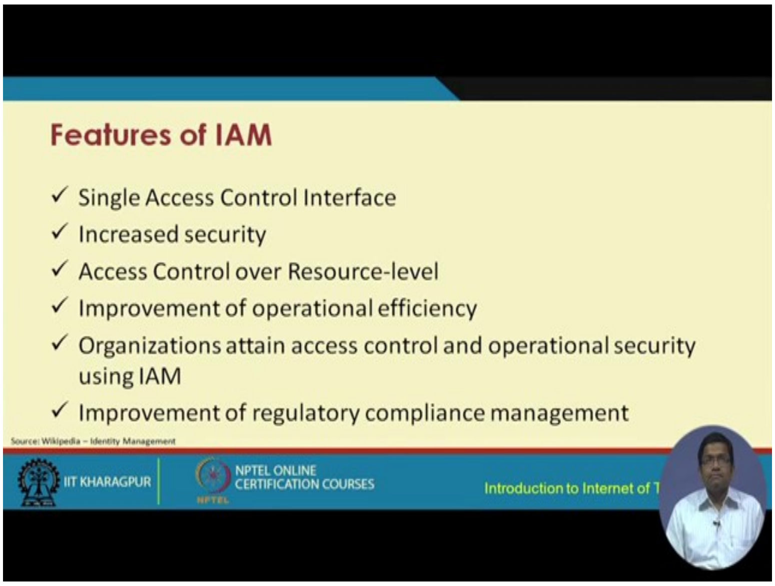
- ✓ A branch of cloud security that allows the **legitimate persons** to retrieve the **legitimate resources** at the **legitimate time** for the **legitimate reasons**
- ✓ User identities and access permissions are instigated, caught, administered and recorded by IAM
- ✓ **Authentication**, **authorization** and **evaluation** of all users are done according to the terms and conditions and the roles of users

Source: Wikipedia – Identity Management

IIT KHARAGPUR
NPTEL ONLINE CERTIFICATION COURSES
NPTEL
Introduction to Internet of T

So like these actually these are the different issues of data security. So, let us first talk about identity and access management IAM which is basically a branch of cloud security that allows the legitimate persons to retrieve the legitimate resources at legitimate time for legitimate reasons. So, legitimate persons retrieving legitimate resources at legitimate time for legitimate reasons is basically the issue the main issue behind identity and access management in cloud security here the users the user identities and the access permissions are instigated caught administered.

(Refer Slide Time: 23:38)



Features of IAM

- ✓ Single Access Control Interface
- ✓ Increased security
- ✓ Access Control over Resource-level
- ✓ Improvement of operational efficiency
- ✓ Organizations attain access control and operational security using IAM
- ✓ Improvement of regulatory compliance management

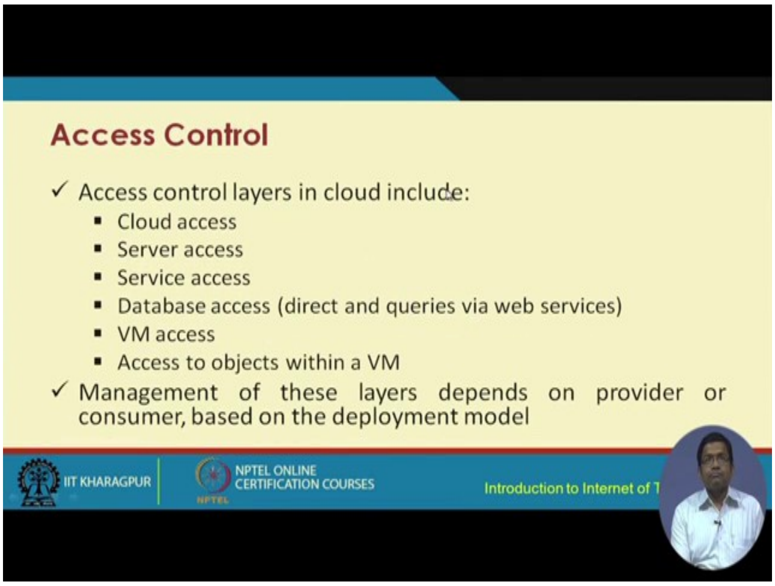
Source: Wikipedia – Identity Management

IIT KHARAGPUR
NPTEL ONLINE CERTIFICATION COURSES
NPTEL
Introduction to Internet of T

And located recorded by IAM; that means, the identity and access management module authentication authorization and evaluation of all resources are done according to the terms and conditions and the roles of the users.

Features of this module include single access control interface, increased security, access control over resource level, improvement of operational efficiency organizations attaining access control and operation security using this module and improvement of regulatory compliance management access control is very important in cloud.

(Refer Slide Time: 24:02)



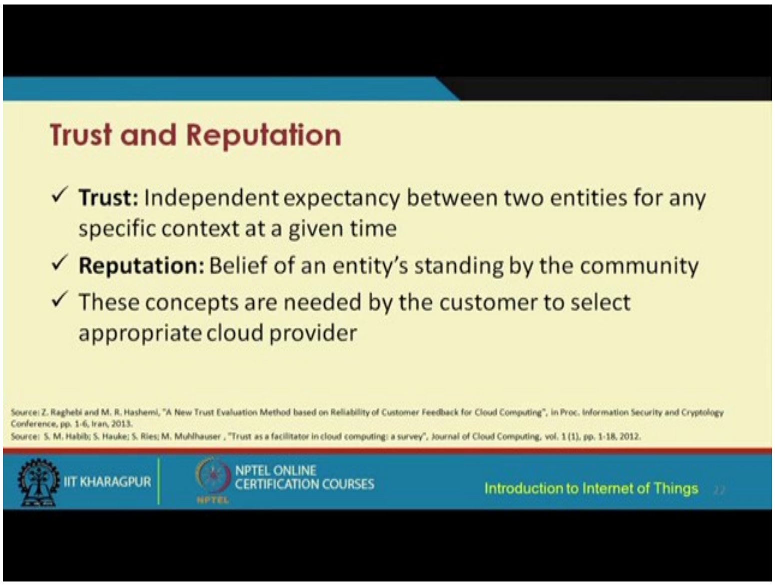
Access Control

- ✓ Access control layers in cloud include:
  - Cloud access
  - Server access
  - Service access
  - Database access (direct and queries via web services)
  - VM access
  - Access to objects within a VM
- ✓ Management of these layers depends on provider or consumer, based on the deployment model

IIT KHARAGPUR
NPTEL ONLINE CERTIFICATION COURSES
Introduction to Internet of T

So, service providers have to take care of it explicitly. So, access control layers in cloud include cloud access server level access service level access database access both directly and indirectly directly the queries should be sent via web services. So, taking care of that and VM access virtual machine level access to objects within a virtual machine.

(Refer Slide Time: 24:49)



Trust and Reputation

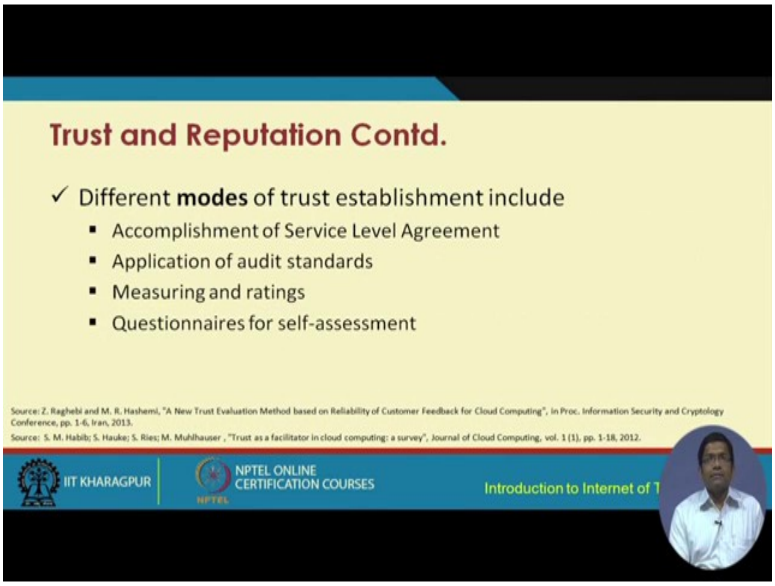
- ✓ **Trust:** Independent expectancy between two entities for any specific context at a given time
- ✓ **Reputation:** Belief of an entity's standing by the community
- ✓ These concepts are needed by the customer to select appropriate cloud provider

Source: Z. Raghebi and M. R. Hashemi, "A New Trust Evaluation Method based on Reliability of Customer Feedback for Cloud Computing", in Proc. Information Security and Cryptology Conference, pp. 1-6, Iran, 2013.
Source: S. M. Habib; S. Hauke; S. Ries; M. Muhlhauser , "Trust as a facilitator in cloud computing: a survey", Journal of Cloud Computing, vol. 1 (1), pp. 1-18, 2012.

IIT KHARAGPUR
NPTEL ONLINE CERTIFICATION COURSES
NPTEL
Introduction to Internet of Things
22

So these are the different levels of access and the control of access to these differently layers has to be taken care of management of these layers depends on the provider or the consumer based on the deployment model. Trust and reputation are very important trust basically takes care of issue of independent expectancy between 2 entities for any specific context at a given time independent expectancy; expectancy between 2 entities. So, they have to trust each other and at the same time hand in hand comes the issue of reputation and reputation is about the belief of an entity; entities standing on the community you know what does the entity have you know what is its reputation in the community.

(Refer Slide Time: 25:37)



Trust and Reputation Contd.

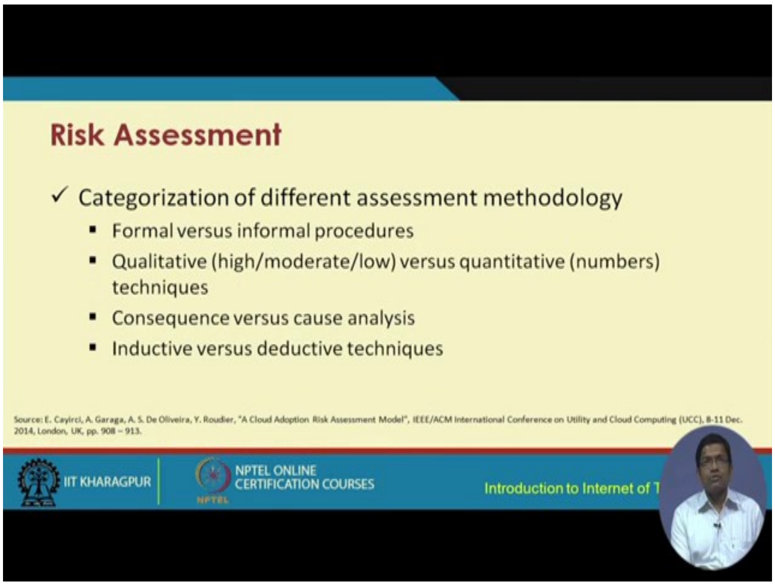
- ✓ Different **modes** of trust establishment include
  - Accomplishment of Service Level Agreement
  - Application of audit standards
  - Measuring and ratings
  - Questionnaires for self-assessment

Source: Z. Raghebi and M. R. Hashemi, "A New Trust Evaluation Method based on Reliability of Customer Feedback for Cloud Computing", in Proc. Information Security and Cryptology Conference, pp. 1-6, Iran, 2013.
Source: S. M. Habib; S. Hauke; S. Ries; M. Muhlhauser , "Trust as a facilitator in cloud computing: a survey", Journal of Cloud Computing, vol. 1 (1), pp. 1-18, 2012.

IIT KHARAGPUR
NPTEL ONLINE CERTIFICATION COURSES
NPTEL
Introduction to Internet of T

So these are the 2 different issues that that goes hand in hand. So, these concepts are needed by the customer to select appropriate cloud provider. So, there are different models or sorry rather different modes of trust establishment. So, these include accomplishment of service level agreement. So, whatever service level agreement exists you know accomplishing it then application of the audit standards that are out there you know whether the audit standards have been adequately applied or not measuring and rating and questionnaire for self assessment.

(Refer Slide Time: 26:11)



Risk Assessment

✓ Categorization of different assessment methodology

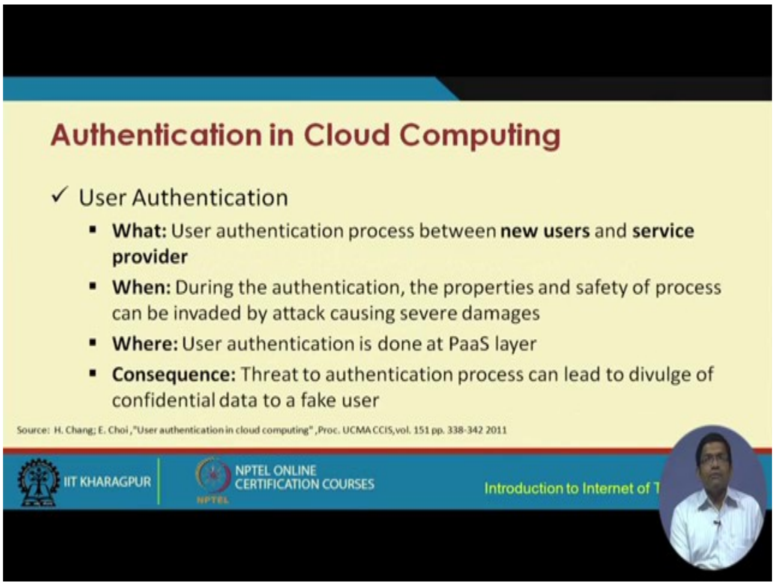
- Formal versus informal procedures
- Qualitative (high/moderate/low) versus quantitative (numbers) techniques
- Consequence versus cause analysis
- Inductive versus deductive techniques

Source: E. Cayirci, A. Garaga, A. S. De Oliveira, Y. Roudier, "A Cloud Adoption Risk Assessment Model", IEEE/ACM International Conference on Utility and Cloud Computing (UCC), 8-11 Dec. 2014, London, UK, pp. 908 – 913.

IIT KHARAGPUR
NPTEL ONLINE CERTIFICATION COURSES
NPTEL
Introduction to Internet of T

So, these are the different levels of trust access trust establishment that has to be there there. Risk assessment categorization of different assessment methodology formal versus informal procedures of risk assessment qualitative versus quantitative methods of risk assessment qualitative means that high risk moderate risk low risk versus quantitative means numeric risk figures consequence versus cause analysis. So, whether the risk is due to a consequence of something or what is the cause behind the risk and inductive versus deductive techniques.

(Refer Slide Time: 26:50)



Authentication in Cloud Computing

✓ User Authentication

- **What:** User authentication process between **new users** and **service provider**
- **When:** During the authentication, the properties and safety of process can be invaded by attack causing severe damages
- **Where:** User authentication is done at PaaS layer
- **Consequence:** Threat to authentication process can lead to divulge of confidential data to a fake user

Source: H. Chang; E. Choi ,"User authentication in cloud computing" ,Proc. UCMA CCIS,vol. 151 pp. 338-342 2011

IIT KHARAGPUR
NPTEL ONLINE CERTIFICATION COURSES
NPTEL
Introduction to Internet of T

So, these are the different categories of risk assessment in cloud authentication in cloud computing user authentication. So, there are different aspects like what where user authentication process which takes care of the user authentication process between the new users and the service provider when during the authentication the properties and the safety of process which can be invaded by attacks causing severe damages and where the user authentication is done at the PaaS layer and the consequence is threat to authentication process can lead to divulge; divulge divulgation divulging of confidential data to a fake user.

So, with this we come to 2 broad main issues in cloud computing one is taking care of the service management with the help of SLAs between the customers and the service providers, number 2 is this issue of security; security of infrastructure, security of the platform, security of the software and the data security data security is very much important. Customers did not know really that where their data is going to reside how the data is going to flow around in the system and that has to be assured to the customer that their data is going to be safe. So, taking care of measures to ensure that there is enough security of the data and the parties can trust each other you know that also has to be ensured through the process of some kind of reputation tracking and ensuring that those reputation measures are basically disseminated for you know developing trust between these different parties. So, these all these things have to be ensured in order to meaningfully use cloud in a commercial or any any kind of environment.

Thank you.