***Cloud Computing***

***Lecture 1.***

**Definitions of Cloud Computing**

It denotes a model on which a computing infrastructure is viewed as a “cloud,” from which businesses and individuals access applications from anywhere in the world on demand. The main principle behind this model is offering computing, storage, and software “as a service.” Many practitioners in the commercial and academic spheres have attempted to define exactly what “cloud computing” is and what unique characteristics it presents.

**The National Institute of Standards and Technology (NIST)**

A pay-per-use model for enabling available, convenient, on-demand network access to a shared pool of

configurable computing resources (e.g. networks, servers, storage, applications, services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

***Lecture 2.***

**Characteristics of Cloud Computing**

The National Institute of Standards Technology (NIST) lists five essential characteristics of cloud

computing: on-demand self-service, broad network access, resource pooling, rapid elasticity, and

measured service.

**1. On-Demand Self-Service**

With cloud computing, you can provision computing services, like server time and network

storage, automatically. You won’t need to interact with the service provider. Cloud customers can

access their cloud accounts through a web self-service portal to view their cloud services, monitor

their usage, and provision and de-provision services.

**2. Broad Network Access**

Another essential cloud computing characteristic is broad network access. You can access cloud

services over the network and on portable devices like mobile phones, tablets, laptops, and

desktop computers.

**3. Resource Pooling**

With resource pooling, multiple customers can share physical resources using a multi-tenant

model. This model assigns and reassigns physical and virtual resources based on demand. Multi-

tenancy allows customers to share the same applications or infrastructure .

**4. Rapid Elasticity**

Cloud services can be elastically provisioned and released, sometimes automatically, so customers

can scale quickly based on demand. The capabilities available for provisioning are practically

unlimited. Customers can engage with these capabilities at any time in any quantity. Customers

can also scale cloud use, capacity, and cost without extra contracts or fees. With rapid elasticity,

you won’t need to buy computer hardware. Instead, you can use the cloud provider's cloud

computing resources.

**5. Measured Service**

In cloud systems, a metering capability optimizes resource usage at a level of abstraction

appropriate to the type of service. For example, you can use a measured service for storage,

processing, bandwidth, and users. Payment is based on actual consumption by the customer via

a pay-for-what-you-use model

***Lecture 3.***

**Evolution of Cloud Computing**

Cloud computing is all about renting computing services. This idea first came in the 1950s. In making

cloud computing what it is today, five technologies played a vital role. These are distributed systems and

its peripherals, virtualization, web 2.0, service orientation, and utility computing.

**Distributed Systems**

It is a composition of multiple independent systems but all of them are depicted as a single entity to the

users. The purpose of distributed systems is to share resources and also use them effectively and

efficiently. Distributed systems possess characteristics such as scalability, concurrency, continuous

availability, heterogeneity, and independence in failures.

**Mainframe computing**

Mainframes which first came into existence in 1951 are highly powerful and reliable computing machines.

These are responsible for handling large data such as massive input-output operations. Even today these

are used for bulk processing tasks such as online transactions etc. These systems have almost no

downtime with high fault tolerance. After distributed computing, these increased the processing

capabilities of the system. But these were very expensive. To reduce this cost, cluster computing came

as an alternative to mainframe technology.

**Cluster computing**

In 1980s, cluster computing came as an alternative to mainframe computing. Each machine in the cluster

was connected to each other by a network with high bandwidth. These were way cheaper than those

mainframe systems. These were equally capable of high computations. Thus, the problem of the cost was solved to some extent but the problem related to geographical restrictions still pertained. To solve this, the concept of grid computing was introduced.

**Grid computing**

In 1990s, the concept of grid computing was introduced. It means that different systems were placed at

entirely different geographical locations and these all were connected via the internet. These systems

belonged to different organizations and thus the grid consisted of heterogeneous nodes. Thus. cloud computing is often referred to as “Successor of grid

computing”.

**Virtualization**

It was introduced nearly 40 years back. It refers to the process of creating a virtual layer over the

hardware which allows the user to run multiple instances simultaneously on the hardware. It is a key

technology used in cloud computing. It is the base on which major cloud computing services such as

Amazon EC2, VMware vCloud, etc work on. Hardware virtualization is still one of the most common types

of virtualization.

**Web 2.0**

It is the interface through which the cloud computing services interact with the clients. It is because of

Web 2.0 that we have interactive and dynamic web pages. It also increases flexibility among web pages.

Popular examples of web 2.0 include Google Maps, Facebook, Twitter, etc. Needless to say, social media

is possible because of this technology only. In gained major popularity in 2004.

**Service orientation**

It acts as a reference model for cloud computing. It supports low-cost, flexible, and evolvable

applications. Two important concepts were introduced in this computing model. These were Quality of

Service (QoS) which also includes the SLA (Service Level Agreement) and Software as a Service (SaaS).

**Utility computing**

It is a computing model that defines service provisioning techniques for services such as compute services

along with other major services such as storage, infrastructure, etc which are provisioned on a pay-per-

use basis.

Lecture 4. LAYERS AND TYPES OF CLOUDS

**Cloud computing services are divided into three classes, according to the abstraction level of**

**the capability provided and the service model of providers, namely:**

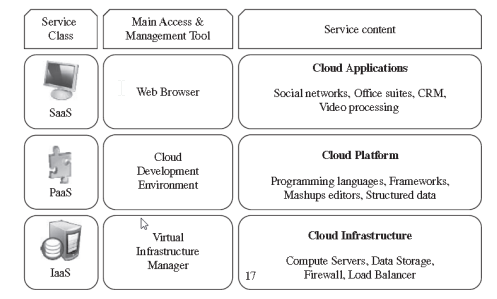
(1) Infrastructure as a Service (IaaS)

(2) Platform as a Service (PaaS)

(3) Software as a Service (SaaS)

Figure below depicts the layered organization of the cloud stack from physical infrastructure to

applications.



**Layered Architecture**

These abstraction levels can also be viewed as a layered architecture where services of a higher

layer can be composed from services of the underlying layer. A core middleware manages physical resources and the VMs deployed on top of them; in addition, it provides the required features (e.g., accounting and billing) to offer multi-tenant pay-as-you-go services.

**Infrastructure as a Service (IaaS)**

Offering virtualized resources (computation, storage, and communication) on demand is known

as Infrastructure as a Service (IaaS). A cloud infrastructure enables on-demand provisioning of

servers running several choices of operating systems and a customized software stack.

Infrastructure services are considered to be the bottom layer of cloud computing systems.

**Platform as a Service (PaaS)**

In addition to infrastructure-oriented clouds that provide raw computing and storage services,

another approach is to offer a higher level of abstraction to make a cloud easily programmable,

known as Platform as a Service (PaaS).

**Software as a Service (SaaS)**

Applications reside on the top of the cloud stack. Services provided by this layer can be

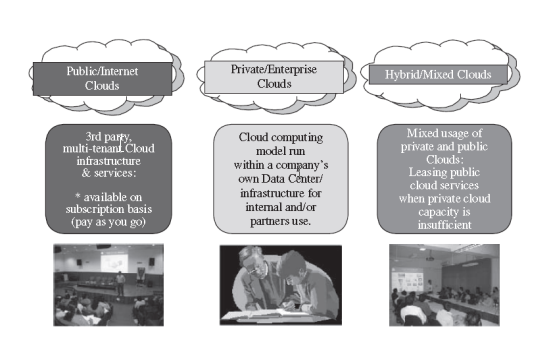
accessed by end users through Web portals. Therefore, consumers are increasingly shifting

from locally installed computer programs to on-line software services that offer the same

functionally. Traditional desktop applications such as word processing and spreadsheet can now

be accessed as a service in the Web.

**Deployment Models**



Although cloud computing has emerged mainly from the appearance of public computing utilities, other deployment models, with variations in physical location and distribution, have been adopted. In this sense, regardless of its service class, a cloud can be classified as public, private, community, or hybrid based on model of deployment as shown in above figure. Armbrust propose definitions for public cloud as a “cloud made available in a pay-as-you-go

manner to the general public” and private cloud as “internal data center of a business or other

organization, not made available to the general public.”

***Lecture 5.***

**BENEFITS OF CLOUD COMPUTING**

The immediate benefit of using Cloud is the reduction in initial cost. The initial costs include: -

o Infrastructure costs:

o Proportional cost or operational costs

The infrastructure costs can be regarded as capital investments or ownership costs. The cloud saves the initial upfront ownership costs. The cloud offers affordable and attractive packages for services obtained in large volume. The cloud reduces investment and proportional costs.

**The Infrastructure cost further includes the following: -**

o IT equipment

o Software

o Networking

o Construction costs

o Installation costs

Common measurable benefits for the cloud consumers are: -

 Pay-as-you-go rental for short term usage

 The availability of virtually unlimited resources on demand with negligible wait time for

provisioning.

 The IT resources can be added or removed in a fine grained level e.g., 1 GB of storage

increments

 Applications and resources can be migrated across regions if required.

 Increased scalability: The cloud can dynamically and instantly provide the

computing resources.

 This provision can be on demand or as per user configuration.

 Similarly these IT resources can be released automatically or manually with the

decrease in processing demand.

 This dynamic scalability avoids the over-provisioning and under-provisioning and the

associated disadvantages.

 Availability: The availability of IT resources sometimes can be referred to profit and

customer retention. If an IT resource becomes unavailable (such as a database dealing

with clients’ orders) then this may result in customer dissatisfaction and loss of

business.

 Reliability: The reliability of IT resources is very important for continual business data

processing and response time. The failure of any IT resource can be cause the collapse

the IT system. For example failure of the Ethernet switch may crash a distributed

application.

***Lecture 6.***

**RISKS AND CHALLENGES OF CLOUD**

**COMPUTING**

• The term vulnerability refers to a state of being attacked. Moving the business data to cloud can introduce vulnerabilities and security risks.

• The term security framework refers to the procedures and practices for securing the resource such as data, network and IT infrastructure.

• Unless the cloud provider and cloud user are covered under same security framework, the vulnerabilities are unavoidable.

• Reduced operational governance control: The cloud consumer gets a lesser

privileged control over the resources leased from the cloud.

• There can be risks arising as to how the cloud provider manages the cloud.

• An unreliable cloud provider may not abide by the guarantees offered in SLA of the

cloud services. This will directly affect the quality of cloud consumer solutions

(enterprise software) which rely upon these services.

• The cloud consumer should keep track of actual level of service being provided by

the cloud provider. The SLA violations can lead to penalties receivable from the cloud

provider.

• Limited portability between cloud providers: Due to lack of industry standards for

cloud computing, the public clouds environments remain proprietary to their providers.

• It is quite challenging to move a custom-built software from one cloud to another if it

has dependencies upon the proprietary environment (such as security framework) of

the former cloud.

• Multi-regional compliance and legal issues: Cloud providers tend to set their data centers in regions favoring affordability and/or convenient. This may lead to legal issues for cloud provider as well as cloud consumers.

• Some countries such as some UK laws require the personal data of UK citizens to behosted inside UK.

• Thus a cloud provider with multi-regional data centers including UK, can not

migrate the UK citizen’s personal data outside UK.

***Lecture 7.***

**ROLES AND BOUNDARIES IN CLOUD**

**COMPUTING**

** Cloud provider:** The organization that provides the IT resources.

o Responsible for providing IT resources as per SLA.

o Also performs the management and administrative tasks to assure flawless

provisioning of cloud services.

** Cloud consumer:** The organization or individual who has contracted with cloud

provider to lease/rent the cloud IT-resources through user interface and/or through

software API calls.

o In the later case, a cloud consumer uses a cloud service consumer (a software

program) to interact/use a cloud service.

** Cloud Service Owner:** Is the one who owns the cloud service. Can be:

o Cloud consumer: If the deployed service is on leased IT-resources.

o Cloud provider: If the cloud provider has deployed the service on cloud IT-

resources.

o A cloud service owner may not be the owner of the cloud IT-resource.

** Cloud Resource Administrator:** This role is responsible for administering the cloud

resources (including cloud services).

o Cloud resource administrator can be:

 Cloud consumer (as cloud service owner)

 Cloud provider (when the service resides inside the cloud)

 Third party contracted to administer a cloud service

** Additional roles:**

o Cloud Auditor: Provides an unbiased assessment of trust building features of

the cloud. These include the security, privacy impact and performance of the

cloud. The cloud consumer may rely upon the cloud audit report for choosing a

cloud.

o Cloud Broker: A party that provides mediation services to cloud providers

(seller) and cloud consumers (buyer) for the purchasing of cloud services.

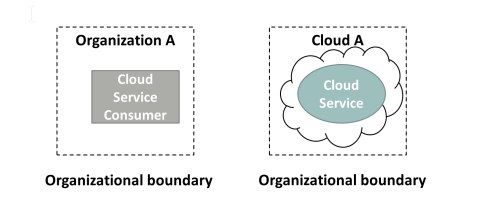
o Cloud Carrier: The party responsible for providing connectivity between cloud

provider and cloud consumer. The ISPs can be assumed as cloud carriers.

** Organizational boundary:** This is a boundary of ownership ad governance of IT

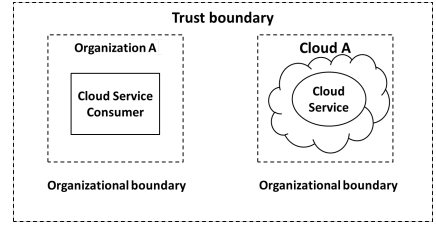
assets of an organization.

 Similarly, the cloud has its organizational boundary.



** Trust boundary:** When an organization takes the role of cloud consumer, then it has to extend its trust boundary to include the cloud resources. A trust boundary

represents a border around trusted IT-resources.



***Lecture 8.***

**IaaS, PaaS & SaaS Provisioning**

**• IaaS:** The IT-resources are typically virtualized and packaged in a preplanned way.

◦ The IT-resources are usually freshly instanced e.g., VMs.

◦ The cloud consumer has a high level of control and configuration-responsibility.

◦ The cloud consumer also has the duty of configuring these resources.

◦ Sometimes a cloud provider will contract IaaS offerings from other cloud provider

to scale its own cloud environment.

◦ The VMs can be obtained specifying the hardware requirements such as processor

capacity, memory, storage etc.

**• PaaS:** Delivers a programming environment containing pre-configured tools to

support the development life cycle of custom applications.

◦ PaaS products are available with different development stacks such as Google App

Engine provides a Python and Java environment.

◦ The PaaS is chosen:

▪ To enhance or substitute the on-premises software development environment.

▪ To create a cloud service in order to provide a cloud service to other cloud

consumers.

◦ The PaaS saves the consumer from administrative tasks such as installations and

configurations to set up the software development infrastructure.

◦ On the other hand the cloud consumer has lower level of control over the

underlying infrastructure.

**• SaaS:** Is the software hosted over cloud infrastructure and offered as a utility

services.

◦ SaaS is provided as a reusable utility service commercially available to different

users.

◦ A SaaS can be deployed over IaaS and/or PaaS instance. Whereby the cloud

consumer (of IaaS/PaaS) becomes the provider.

◦ The service consumer has a very limited control over the underlying SaaS

implementation.

***Lecture 9.***

**IaaS, PaaS & SaaS Comparison**

**• Control level:**

◦ SaaS: Usage and usage related configuration

◦ PaaS: Limited administrative

◦ IaaS: Full administrative

**• Functionality provided to cloud consumer:**

◦ SaaS: Access to front-end user-interface

◦ PaaS: Moderate level of administrative control over programming platform

◦ IaaS: Full administrative control over virtual resources of the VMs

**• Common activities of cloud consumer:**

◦ SaaS: Use and configure the service

◦ PaaS: Develop, debug and deploy the cloud services and cloud based solutions

◦ IaaS: Installation and configuration of software, configure the infrastructure of VM

**• Common Cloud Provider’s Activities:**

◦ SaaS: Implementation, management and maintenance of cloud service.

◦ PaaS: Providing the pre-configured programming platform, middleware and any

other IT resource needed.

◦ IaaS: Provisions and manages the VMs and underlying physical infrastructure.

• The three cloud models of cloud delivery can be combined in a way that one delivery

model is deployed over another. Such as:

◦ PaaS over IaaS

◦ SaaS over PaaS

◦ SaaS over PaaS over IaaS

***Lecture 10.***

**Software as a Service (SaaS)**

** Classes of SaaS:**

**Business logic**: Connect the suppliers, employees, investors and

customers.

 Example: Invoicing, fund transfer, inventory management,

customer relationship management (CRM)

**Collaboration:** Support teams of people work together.

 Examples: Calendar systems, email, screen sharing, conference

management and online gaming.

**Office productivity:** Office environment support.

 Examples: word processors, spreadsheets, presentation and

database software.

**Software tools:** For the support of developing software and solving

compatibility problems.

 Examples: format conversion tools, security scanning, compliance

checking and Web development.

 Software that are not suitable for public SaaS offerings (according to NIST):

**Real-time software:** They require precise response time. Due to variable

response time and network delays, these software are not suitable to be

offered as SaaS. Such as flight control systems and factory robots etc.

**Bulk-consumer data:** When extremely large amount of data is originating physically at the consumer’s side such as physical monitoring and patient monitoring data. It is not feasible to transfer this data in real time over WAN to SaaS provider.

**Critical software:** A software is labeled critical if its failure or delay in handling can cause loss of life or loss of property. These software are not suitable for SaaS because achieving a continuous acceptable reliability for critical software in public SaaS is quite challenging due to (unreliable) public network based access.

 SaaS billing: Based on

o Number of users

o Time in use

o Per-execution, per-record-processed

o Network bandwidth consumed

o Quantity/duration of data stored

**Example**

 Salesforce.com SaaS for Customer Relationship Management (CRM)

o Manage sales contacts and leads.

o Centralize the contact. information and project details.

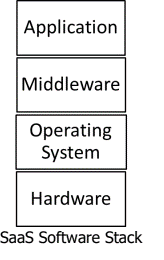
o The sales reports from any place any time.

o The sales reports from any place any time.

o Manages and syncs sales contacts and meetings with other tools such as Microsoft Outlook.

**Software Stack**

 The provider controls most of the software stack.



 Application: Email

 Middleware: software libraries, run time environments (Java, Python)

 Service provider has admin control over application and total control over the rest of the layers.

 Service consumer has limited admin control over the application and no control over the rest of the stack.

 A consumer can create, send and manage the emails and even the email accounts.

**Benefits**

** Modest software tool footprint**: There is no need for complex installation procedures because the SaaS applications and accessible through web browsers. This is one of the reasons of widespread use of SaaS applications.

** Efficient use of software licenses:** Thelicense issuance and management procedure is quite efficient. A single client is issued a single license for multiple computers. This is because the software is running directly on provider’s infrastructure and thus can be billed and monitored directly.

** Centralized management and data:** The consumer’s data is stored in cloud.The provider assures the security and availability of data. The data seems centralized for the consumer may in fact be distributed and replicated by the provider. Data backup is provided at possibly additional charges.

**Issues and Concerns**

 The NIST has identified few issues and concerns about SaaS.

 Most of these issues are due to network dependency of SaaS.

o Browser based risks and remedies: Since the SaaS is accessed through browser installed on consumers’ device, the inherent vulnerabilities of the web browsers do have impact over SaaS security.

 Although the browsers apply encryption upon network traffic,

yet various network attacks such as brute force and man in the

middle attacks are possible upon the SaaS data.

 The resources leased by a consumer can be hijacked by

malicious users due to poor implementation of cryptographic

features of browsers.

**NIST Recommendations for SaaS**

 Data protection: The consumer should analyze the data protection, configuration, database transaction processing technologies of SaaS provider. Compare them with the confidentiality, integrity, availability and compliance requirement of the consumer.

 Client device/application protection: The consumer’s client device (browser running over a computer) should be protected to control the exposure to attacks.

 Encryption: Strong encryption algorithm with key of required strength should be used for each web session as well as for data.

 Secure data deletion: The data deletion through consumer’s request should be reliably done.

***Lecture 11.***

**Platform as a Service (PaaS)**

**Overview**

 PaaS consumers:

o Application developers

o Application testers

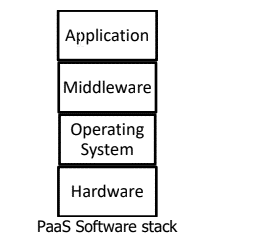
o Application deployers

o Application administrators

o Application end users (SaaS users)

 The consumers are charged according to tools and IT-resources usage.

 PaaS Software stack: The cloud provider fully controls the hardware and OS layers:



 PaaS Provider/ Consumer Scope of Control: The provider has administrative

control of middleware.

 The provider has no control over application layer.

**Examples**

 We are going to discuss a few examples of PaaS.

o Google App Engine (GAE): Allows the users to create and host web

based (Java, Python & Go) applications running over the infrastructure

and services provided by Google. GAE is a free service until the

application grows to a significant size.

o Force.com as a PaaS: This is a service of Salesforce.com (a SaaS

provider). It offers four different programming environments for

nonprogrammers, programmers and software vendors.

 Nonprogrammers can create finance, HR etc. applications and

websites without coding by using drag drop of controls.

 Programmers can develop Java applications and deploy them as

SaaS.

 The software vendors can distribute and update their

applications over cloud by using Force.com.

**Advantages and Disadvantages**

** Advantages:**

o Lower total cost of ownership in terms of hardware and software

investment.

o Lower administrative overhead of system development.

o No requirement of software upgrades of tools.

o Faster application development and deployment.

o Scalable resources available for the applications. The user pays only

for the resources used.

** Disadvantages:**

o The inherent problem of data placed offsite raises the security

concerns.

o The integration of PaaS applications with on-site legacy solutions is not

trivial.

o The PaaS provider has to be trusted for data and application security.

o The issues of SaaS are also the issues of PaaS such as browser based

risks, network dependence and isolation vs efficiency.

o Portability of PaaS applications across different providers may not be

possible sue to incompatibility in coding structures (hash, queue, file

etc.).

***Lecture 12.***

**Infrastructure as a Service (IaaS)**

**Overview**

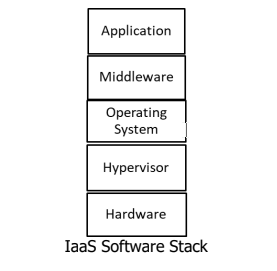
 As an alternative to PaaS, some consumers may prefer to use IaaS in order to have management control over the IT resources.

 The IaaS provider makes available the computing resources in the form of VMs.

 The consumer has the duty of installing OS and software.

 The provider also provides stable network access, network components such as firewalls, and data storage.

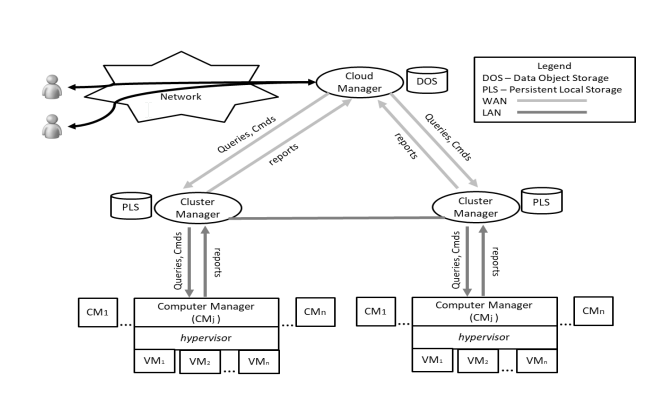
 IaaS Provider/Consumer Scope of Control: The provider has no control over top three layers.



 IaaS Provider/Consumer Scope of Control: The provider has admin control over hypervisor and total control over hardware layer.

 IaaS Provider/Consumer Scope of Control: The consumer has total control over top three layers.

**Operational Overview**



**Advantages**

 Saving in upfront cost: As in SaaS and PaaS. Although the responsibility of installing OS and software is of the consumer.

 Full administrative control over VM:

o Start, shut down, pause

o Installation of OS and applications

o Accessing VM through network services of VM through a network protocol such as Secure Shell.

**Issues and Concerns**

 Network dependence

 Browser based risks (same as discussed for SaaS and PaaS).

 Compatibility with legacy software vulnerabilities: Since the consumer is allowed to

install the legacy applications on VMs rented through IaaS, this exposes the VMs to the vulnerabilities in those legacy software.

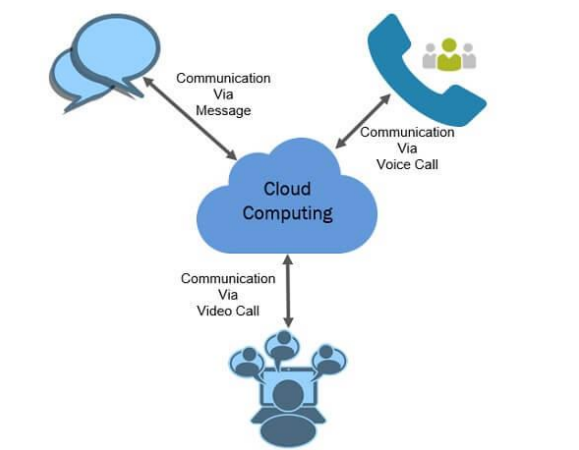
 Implementation challenges exist for VM isolation: In order to prevent the VMs from eavesdropping other VMs mounted over same server, the isolation features of

hypervisor are utilized. But these features may not withstand a sophisticated attacks.

***Lecture 13.***

**Communication as a Service (CaaS)**

Communication as a service (CaaS) is a cloud-based solution provided by cloud vendors. CaaS is a specialized variation of Software as a Service (SaaS) which is among three basic services delivered by the cloud computing technology. When we talk about communication, recall, in how many ways we can communicate with others. Well, we can communicate via text message, voice call and video call.



CaaS providers manage the hardware and software that are important for delivering Voice over

IP (VoIP) for voice communication service, and other services like Instant Messaging (IM) to

provide text communication service and video conferencing to provide video communication

service.

**Features of CaaS**

 Integrated and Unified Communication

 No Investment Required

 Flexibility & Scalability

 No Risk of Obsolescence

 No Maintenance Cost Incurred

 Ensure Business Continuity

**Integrated and Unified Communication**

The advanced unified communication features include Chat, Multimedia conferencing, Microsoft

Outlook integration, Real-time presence, “Soft” phones (software-based telephones), Video

calls, Unified messaging and mobility.

**No Investment Required**

As we have learnt above it is the sole responsibility of CaaS vendor to manage hardware and

software deployed to provide the communication service to their customers.

**Flexibility & Scalability**

The customer can outsource the communication services form CaaS vendors. The customers

pay for what they have demanded. The customer can extend their service requirement

according to their need.

**No Risk of Obsolescence**

The CaaS vendors keep on updating their hardware and software that provide communication

services to meet the changing demands of the market. So the customer using the services does

not have to be worried about the service obsolescence.

**No Maintenance Cost Incurred**

The customer outsourcing the CaaS service does not have to bear the cost of maintaining the

equipment deployed for providing communication services.

**Ensure Business Continuity**

If due to any calamity your business’s geographical region is affected then how long can you

continue your business? That’s why nowadays companies distribute their data to the

geographically dispersed data centre which maintain the redundancy & help them in recovering

soon after any catastrophic event.

***Lecture 14.***

**Monitoring as a Service (MaaS)**

Monitoring as a Service (MaaS) provides you with the security solutions that are essential for the organizations that are reliant on the IT infrastructure. However, for effective and efficient monitoring, the organization must have up to date technology, experts knowing advanced technical skills, scalable security processes and all this come with a tremendous expense.

MaaS provides an effective solution to this problem. It provides 24/7 real-time monitoring, reports any issue across the security infrastructure and secures the crucial data of their customers.

If compared to the traditional security operations centre MaaS exceed in two important things:

 The total cost of ownership was higher in the traditional security operations centre.

 Traditional security operations are less effective.

**Features of MaaS**

1. Protection Against External and Internal Threats

2. Delivering Business Values

3. Real-Time Log Monitoring Enables Compliance

**1. Protection Against External and Internal Threats**

The security monitoring services analyze the alerts from security devices 24/7 in real-time. The security analyst collects data from various security devices to recognize the threats and thereby imply effective measures to respond to these threats.

 Early Detection

 Dashboard Interface

 Log Centralization and Analysis

**2. Delivering Business Values**

The MaaS vendors have a complete information security infrastructure along with a team of skill and the expert individual who are updated with the latest technology. The MaaS vendors provide the scalable services which is an advantage for their customers.

**3. Real-Time Log Monitoring Enables Compliance**

Log monitoring is a process of recording log messages into a file which helps the developers or administrator to understand how the system or application is being used. Real-time log monitoring helps in quick detection of errors, failed process and services.

***Lecture 15.***

**Building Cloud Network**

Building a cloud properly requires several key steps and critical components, so embarking on your cloud computing journey may seem overwhelming. The process will take you 7 steps from start to finish and will cover the following:

1. Select a Foundation

2. Determine Your Delivery Infrastructure

3. Sketch the “Big Picture”

4. Don’t Forget Security

5. Prepare Your Network

6. Automate Management Tasks

7. Integrate Components

**1. Select a Foundation**

The foundation is the technology platform where your cloud will exist. If your organization has used any cloud virtualization before, this choice may already be made for you. If not, it’s an essential first step in creating a cloud application.

**2. Determine Your Delivery Infrastructure**

Delivery infrastructure is typically designed using a load balancer. This balancer will allocate resources and define the capacity of your cloud application.

**3. Sketch the “Big Picture”**

It’s important to step back and get a bird’s eye view of the project from the beginning. Consider how all of your components will integrate and communicate. As a system architect, you must focus on how your cloud application will scale as the amount of usage and stress on your infrastructure increases.

**4. Don’t Forget Security**

The easiest way to address security concerns is to build security into your application. Decide on a particular security application or technology before building your cloud.

**5. Prepare Your Network**

Your network needs the ability to support an on-demand application infrastructure to survive.Therefore, the configurations of all network resources – storage, application, and hardware –need to match the format of the app that is launched.

**6. Automate Management Tasks**

Visibility should be a primary focus when you build a cloud. Adapting to the changing resource requirements and security parameters inherent in a cloud environment requires quick, data- driven decisions that can only be accomplished with a clear view of the overall cloud system.

**7. Integrate Components**

The last step of how to build a cloud is integrating the components you’ve built up until now. This can be a challenge, but it’s necessary for the functionality of your cloud.

***Lecture 16.***

**Cloud Computing Security**

Security in cloud computing is a major concern. Data in cloud should be stored in encrypted form. To restrict client from accessing the shared data directly, proxy and brokerage services should be employed.

**Security Planning**

Before deploying a particular resource to cloud, one should need to analyze several aspects of the resource such as:

 Select resource that needs to move to the cloud and analyze its sensitivity to risk.

 Consider cloud service models such as IaaS, PaaS, and SaaS. These models require customer to be responsible for security at different levels of service.

 Consider the cloud type to be used such as public, private, community or hybrid.

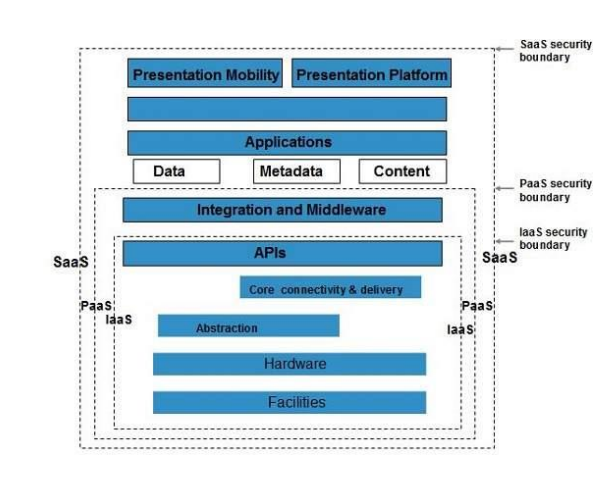
 Understand the cloud service provider's system about data storage and its transfer into and out of the cloud. The risk in cloud deployment mainly depends upon the service models and cloud types.

**Understanding Security of Cloud**

**Security Boundaries**

A particular service model defines the boundary between the responsibilities of service provider and customer. Cloud Security Alliance (CSA) stack model defines the boundaries between each service model and shows how different functional units relate to each other. The following

**diagram shows the CSA stack model:**



Key Points to CSA Model

 IaaS is the most basic level of service with PaaS and SaaS next two above levels of services.

 Moving upwards, each of the service inherits capabilities and security concerns of the model beneath.

 IaaS provides the infrastructure, PaaS provides platform development environment, and SaaS provides operating environment.

 IaaS has the least level of integrated functionalities and integrated security while SaaS has the most.

***Understanding Data Security***

Since all the data is transferred using Internet, data security is of major concern in the cloud.

Here are key mechanisms for protecting data.

 Access Control

 Auditing

 Authentication

 Authorization

**Working Of Brokered Cloud Storage Access System**

When the client issues request to access data:

 The client data request goes to the external service interface of proxy.

 The proxy forwards the request to the broker.

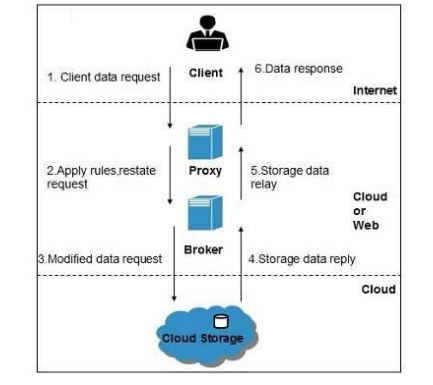
 The broker requests the data from cloud storage system.

 The cloud storage system returns the data to the broker.

 The broker returns the data to proxy.

 Finally the proxy sends the data to the client.

All of the above steps are shown in the following diagram:



**Encryption**

Encryption helps to protect data from being compromised. It protects data that is being transferred as well as data stored in the cloud. Although encryption helps to protect data from any unauthorized access, it does not prevent data loss.

***Lecture 17.***

**Common Standards in Cloud Computing**

1. Working Groups

2. Open Cloud Consortium

3. The Distributed Management Task Force

4. Standards for Application Developers

5. Standards for Messaging

6. Standards for Security

**1. Working Groups**

 A working group is an assembled, cooperative collaboration of researchers working on new

research activities that would be difficult for any one member to develop alone.

 Working groups are sometimes also referred to as task groups or technical advisory groups.

 Working groups support the interest and activities of OCC Members. The current working groups

include:

 The Open Science Data Cloud (OSDC) Working Group

 Project Matsu

 The Open Cloud Testbed Working Group

 Biomedical Commons Cloud (BCC)

 Working Group on Standards and Interoperability for Clouds

 Working Group on Wide Area Clouds and the Impact of Network Protocols on Clouds.

**2. Open Cloud Consortium**

 The Open Cloud Consortium (OCC) is

o A not for profit

o Manages and operates cloud computing infrastructure to support scientific, medical,

health care and environmental research.

 OCC members span the globe and include over 10 universities, over 15 companies, and over 5

government agencies and national laboratories.

 The OCC is organized into several different working groups.

**3. The Distributed Management Task Force (DMTF)**

 DMTF enables more effective management of millions of IT systems worldwide by bringing the

IT industry together to collaborate on the development, validation and promotion of systems

management standards.

 The group spans the industry with 160 member companies and organizations, and more than

4,000

 active participants crossing 43 countries.

 The DMTF board of directors is led by 16 innovative, industry-leading technology companies.

 DMTF management standards are critical to enabling management interoperability among multi-

vendor systems, tools and solutions within the enterprise.

 The DMTF started the Virtualization Management Initiative (VMAN).

**4. Standards for Application Developers**

 The purpose of application development standards is to ensure uniform, consistent, high-quality software solutions.

 Programming standards help to improve the readability of the software, allowing developers to understand new code more quickly and thoroughly.

 Commonly used application standards are available for the Internet in browsers, for transferring data, sending messages, and securing data.

**4.1 Standards for Browsers (Ajax)**

 AJAX (Asynchronous JavaScript and XML), is a group of interrelated web development

techniques used to create interactive web applications or rich Internet applications.

**4.2 ICEfaces Ajax Application Framework**

 ICEfaces is an integrated Ajax application framework that enables Java EE application

developers to easily create and deploy thin-client rich Internet applications in pure Java.

**4.3 Data (XML, JSON)**

 Extensible Markup Language (XML) allows to define markup elements. Its purpose is to enable

sharing of structured data.

 JSON (JavaScript Object Notation ) is a lightweight computer data interchange format. It is a

text-based, human-readable format for representing simple data structures and associative

arrays (called objects).

**4.4 Solution Stacks (LAMP and LAPP)**

 LAMP is a popular open source solution commonly used to run dynamic web sites and servers.

The acronym derives from the fact that it includes Linux, Apache, MySQL, and PHP (or Perl or

Python) and is considered by many to be the platform of choice for development and

deployment of high-performance web applications which require a solid and reliable foundation.

**5. Standards for Messaging**

 A message is a unit of information that is moved from one place to another.

 Most common messaging standards used in the cloud are

o Simple Message Transfer Protocol (SMTP)

o Post Office Protocol (POP)

o Internet Messaging Access Protocol (IMAP)

o Syndication (Atom, Atom Publishing Protocol, and RSS)

o Communications (HTTP, SIMPLE, and XMPP)

**6. Standards for Security**

 Security standards define the processes, procedures, and practices necessary for implementing

a secure environment that provides privacy and security of confidential information in a cloud

environment.

 Security protocols, used in the cloud are

o Security Assertion Markup Language (SAML)

o Open Authentication (Oauth)

o OpenID

o SSL/TLS

***Lecture 18.***

**End User Access to Cloud Computing**

 The cloud model is being so widely adopted due to the following reasons: -

o Consumer-driven innovation

o The rise of power collaborators (those who embrace and take collaboration to very high

levels)

o Changing economics

o A lowering of barriers to entry

 Innovation behind the success of cloud services ultimately depends on the acceptance of the

offering by the user community.

 Acceptance of an offering by users changes the economics considerably.

 As more users embrace such innovation, economies of scale for a product allow implementers to lower the costs, removing a barrier to entry and enabling even more widespread adoption of the innovation.

 We will present some of the applications that are proving beneficial to end users, enabling them to be “power collaborators.”

 We will take a look at some of the most popular Software-as-a-Service (SaaS) offerings for

consumers and provide an overview of their benefits and why, in our opinion, they are helping

to evolve our common understanding of what collaboration and mobility will ultimately mean in

our daily lives.

**YouTube**

YouTube has become so popular and it provides a set of development application programming

interfaces (APIs) to enable developers to integrate YouTube functionality into their web sites.

**Widgets**

 Widgets are simple page elements that developers can embed in a web site to give it YouTube

functionality.

 Two widgets that are currently available:

1. Video Bar

2. Video Search Control.

**YouTube Player APIs**

 The Player APIs lets user to control the YouTube player using JavaScript or ActionScript.

 The Player APIs allow developer to establish how users can control You-Tube video playback on

their web site.

** There are two types of players:**

1. The normal “embedded” player

2. Chromeless player

**The YouTube Custom Player**

 The YouTube custom player allows you to customize a YouTube player and populate it with

videos you specify.

 Developers can easily configure the custom player to show playlists, favorites, or custom, locally

available videos.

**YouTube Data API**

 The Data API is primarily for developers who are used to programming in server-side languages.

 The Data API gives you programmatic access to the video and user information stored on

YouTube.

**Facebook**

 Facebook provides anyone the ability to create Facebook applications.

 To create a Facebook application, one should be well versed in PHP or some other coding

language such as Ruby on Rails, JavaScript, or Python.

sss Basic understanding of the Internet, SSH, MySQL, and Unix is also required.