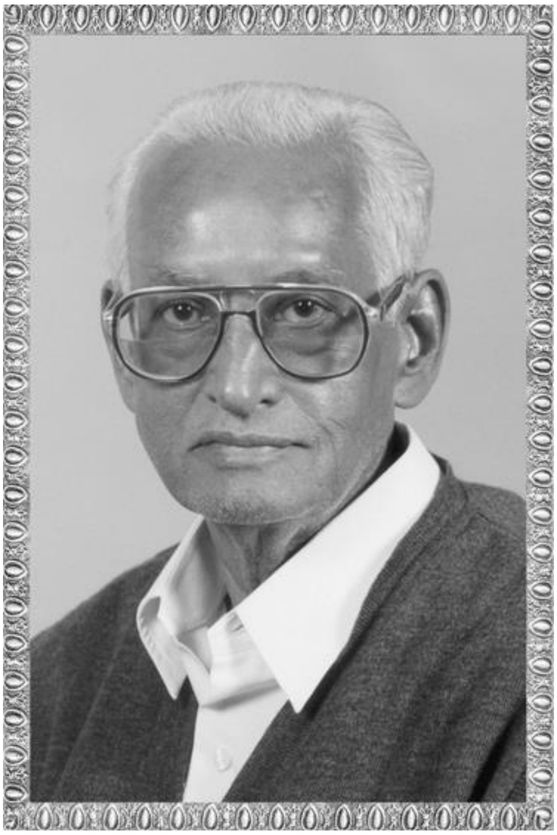
SHREE H. N. SHUKLA GROUP OF COLLEGES

(Affiliated to Saurashtra University & Gujarat Technological University)



Lt. Shree Chimanbhai Shukla

M.Sc I.T. SEM-2 - Cloud Computing

Shree H.N.Shukla College Campus,
Street No. 2, Vaishali Nagar,
Nr. Amrapali Railway Crossing,
Raiya Road, Rajkot.
Ph. (0281)2440478, 2472590

Shree H.N.Shukla College
Street No. 3, Vaishali Nagar,
Nr. Amrapali Railway Crossing,
Raiya Road, Rajkot.
Ph. (0281)2471645

Website: www.hnshukla.com
Email : hnsinfo@hnshukla.com

Index

Contents

UNIT -2

Unit – 2
Part -1 Infrastructure as a Service (IaaS)

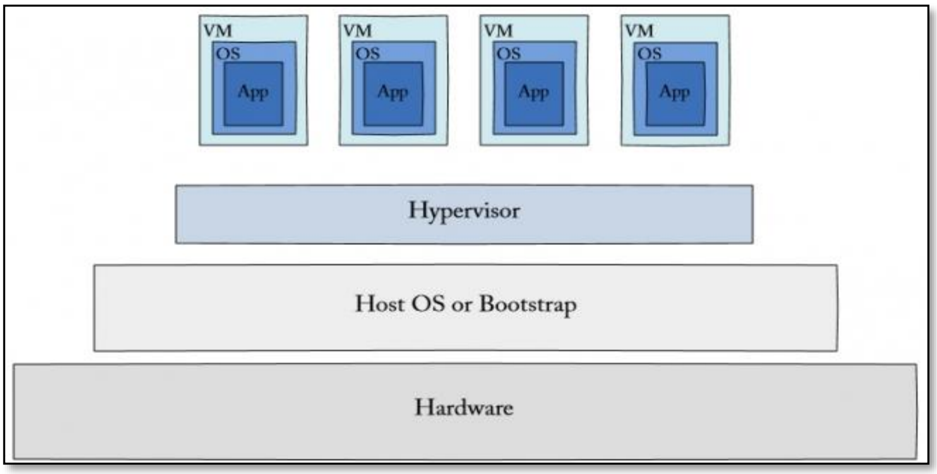
Introduction to IaaS

- Cloud infrastructure services, known as "Infrastructure as a Service" (IaaS), **deliver computer infrastructure, storage, and networking**.
- **IaaS**, as the name suggests, is a way of providing Cloud computing infrastructure such as virtual machines, storage drives, servers, operating systems & networks, which is also an on-demand service.
- Instead of purchasing servers or developing software, clients buy those resources as a fully outsourced service based on their requirement.
- "Public cloud" is considered as an infrastructure that consists of shared resources, based on a self-service over the Internet.
- In one word, it is the only layer of the cloud where the customer gets the platform for their organization to outsource IT infrastructure on a pay-per-use basis.
- IaaS provides users with:
  1. Load balancers
  2. Disk storage via virtual machines
  3. Software Packages
  4. IP address
  5. VLANs
- Advantages of IaaS are:
  1. **Dynamic:** Users can dynamically opt & configure devices such as CPU, storage drive, etc.
  2. **Easy Access:** Users can easily access the vast cloud computing power.
  3. **Renting:** Flexible and efficient while renting IT infrastructures.
  4. **Full control** of computer resources along with portability.
- Disadvantages of IaaS are as follows:
  1. Internet connection is a must.
  2. IaaS depends on virtualization services.
  3. This service restricts user-privacy & customization

Introduction to virtualization

- Virtualization is the ability which allows sharing the physical instance of a single application or resource among multiple organizations or users.
- This technique is done by assigning a name logically to all those physical resources & provides a pointer to those physical resources based on demand.

- Over an existing operating system & hardware, we generally create a virtual machine which and above it we run other operating systems or applications. This is called **Hardware Virtualization.**
- The virtual machine provides a separate environment that is logically distinct from its underlying hardware.
- Here, the system or the machine is the host & virtual machine is the guest machine. This virtual environment is managed by a firmware which is termed as a **hypervisor.**



- There are **several approaches** or ways to virtualizes cloud servers. These are:
  - **Grid Approach**: where the processing workloads are distributed among different physical servers, and their results are then collected as one.
  - **OS - Level Virtualization**: Here, multiple instances of an application can run in an isolated form on a single OS
  - **Hypervisor-based Virtualization**: which is currently the most widely used technique
- With hypervisor's virtualization, there are various sub-approaches to fulfill the goal to run multiple applications & other loads on a single physical host.
- A technique is used to allow virtual machines to move from one host to another without any requirement of shutting down. This technique is termed as **"Live Migration"**.
- Another technique is used to actively load balance among multiple hosts to efficiently utilize those resources available in a virtual machine, and the concept is termed as **Distributed Resource Scheduling or Dynamic Resource Scheduling.**

Types of Virtualization

- The virtualization of cloud has been categorized into four different types based on their characteristics. These are:
  1. Hardware Virtualization
  2. Full Virtualization
  3. Emulation Virtualization
  4. Para-virtualization
  5. Software Virtualization

6. OS Virtualization
7. Server Virtualization
8. Storage Virtualization

How Virtualization works in cloud?

- Virtualization plays a significant role in cloud technology and its working mechanism. Usually, what happens in the cloud - the users not only share the data that are located in the cloud like an application but also share their infrastructures with the help of virtualization.
- Virtualization is used mainly to provide applications with standard versions for the cloud customers & with the release of the latest version of an application the providers can efficiently provide that application to the cloud and its users and it is possible using virtualization only.
- By the use of this virtualization concept, all servers & software other cloud providers require those are maintained by a third-party, and the cloud provider pays them on a monthly or yearly basis.
- In reality, most of the today's hypervisor make use of a combination of different types of hardware virtualization. Mainly virtualization means running multiple systems on a single machine but sharing all resources (hardware) & it helps to share IT resources to get benefit in the business field.

Advantages of virtualization:

- The number of servers gets reduced by the use of virtualization concept
- Improve the ability of technology
- The business continuity also raised due to the use of virtualization
- It creates a mixed virtual environment
- Increase efficiency for development & test environment
- Lowers Total Cost of Ownership (TCO)

Features of virtualization:

1. Partitioning: Multiple virtual servers can run on a physical server at the same time
2. Encapsulation of data: All data on the virtual server including boot disks is encapsulated in a file format
3. Isolation: The Virtual server running on the physical server are safely separated & don't affect each other
4. Hardware Independence: When the virtual server runs, it can migrate to the different hardware platform

Different approaches to virtualization

- Server virtualization can be viewed as a part of overall virtualization trend in the IT companies that include network virtualization, storage virtualization & management of workload.
- This trend brings development in automatic computing.

For Server Virtualization, there are three popular approaches. These are:

1. Virtual Machine model
2. Para-virtual Machine model
3. Operating System (OS) layer Virtualization

1. **Virtual Machine model:**
    - It is based on host-guest paradigm, where each guest runs on a virtual replica of hardware layer.
    - This technique of virtualization provide guest OS to run without modification.
    - However it requires real computing resources from the host and for this a hypervisor or VM is required to coordinate instructions to CPU.
2. **Para-Virtual Machine model:**
    - It is also based on host-guest paradigm & uses virtual machine monitor too.
    - In this model the VMM modifies the guest operating system's code which is called 'porting'.
    - Like that of virtual machine, similarly the Para-virtual machine is also capable of executing multiple operating systems.
3. **Operating System Layer Virtualization**:
    - Virtualization at OS level functions in a different way and is not based on host-guest paradigm.
    - In this model the host runs a single operating system kernel as its main/core and transfers its functionality to each of the guests.
    - The guest must use the same operating system as the host.
    - This distributed nature of architecture eliminated system calls between layers and hence reduces overhead of CPU usage.
    - It is also a must that each partition remains strictly isolated from its neighbors because any failure or security breach of one partition won't be able to affect the other partitions.

Server Virtualization

- It is the division of physical server into several virtual servers and this division is mainly done to improvise the utility of server resource.
- In other word it is the masking of resources that are located in server which includes the number & identity of processors, physical servers & the operating system.
- This division of one physical server into multiple isolated virtual servers is done by server administrator using software.
- The virtual environment is sometimes called the **virtual private-servers**.
- In this process, the server resources are kept hidden from the user.
- This partitioning of physical server into several virtual environments; result in the dedication of one server to perform a single application or task.

Usage of Server Virtualization

- This technique is mainly used in web-servers which reduces the cost of web-hosting services.
- Instead of having separate system for each web-server, multiple virtual servers can run on the same system/computer.

The primary uses of server virtualization are:

- To centralize the server administration
- Improve the availability of server
- Helps in disaster recovery
- Ease in development & testing
- Make efficient use of server resources.

Advantages:

- **Cost Reduction:** Server virtualization reduces cost because less hardware is required.
- **Independent Restart:** Each server can be rebooted independently and that reboot won't affect the working of other virtual servers.

Types of Virtualization: Resource virtualization

1. Hardware Virtualization.
2. Operating system Virtualization.
3. Server Virtualization.
4. Storage Virtualization.

1. Hardware Virtualization:

- When the virtual machine software or virtual machine manager (VMM) is directly installed on the hardware system is known as hardware virtualization.
- The main job of hypervisor is to control and monitoring the processor, memory and other hardware resources.
- After virtualization of hardware system we can install different operating system on it and run different applications on those OS.

Usage:

- Hardware virtualization is mainly done for the server platforms, because controlling virtual machines is much easier than controlling a physical server.

2. Operating System Virtualization:

- When the virtual machine software or virtual machine manager (VMM) is installed on the Host operating system instead of directly on the hardware system is known as operating system virtualization.

Usage:

- Operating System Virtualization is mainly used for testing the applications on different platforms of OS.

3. Server Virtualization:

- When the virtual machine software or virtual machine manager (VMM) is directly installed on the Server system is known as server virtualization.

Usage:

- Server virtualization is done because a single physical server can be divided into multiple servers on the demand basis and for balancing the load.

4. Storage Virtualization:

- Storage virtualization is the process of grouping the physical storage from multiple network storage devices so that it looks like a single storage device.
- Storage virtualization is also implemented by using software applications.

Usage:

- Storage virtualization is mainly done for back-up and recovery purposes.

What does Virtual Provisioning mean?

- Virtual provisioning is a virtual storage network (VSAN)-based technology in which storage space is allocated on demand to devices.
- This process allows virtualized environments to control the allocation and management of physical disk storage connected with virtual machines (VM).
- Virtual provisioning is also known as **thin provisioning**. However, virtual provisioning is more relevant to a virtual environment, while thin provisioning is more relevant to physical computing implementations.

Hypervisor

- A **hypervisor**, also known as a virtual machine monitor, is a process that creates and runs virtual machines (VMs).
- A hypervisor allows one host computer to support multiple guest VMs by virtually sharing its resources, like memory and processing.
- There are two types of hypervisors.
- Type 1 hypervisors, called **"bare metal,"** run directly on the host's hardware.
- Type 2 hypervisors, called **"hosted,"** run as a software layer on an operating system, like other computer programs.
- Hypervisors make it possible to use more of a system's available resources and provide greater IT mobility since the guest VMs are independent of the host hardware. This means they can be easily moved between different servers.

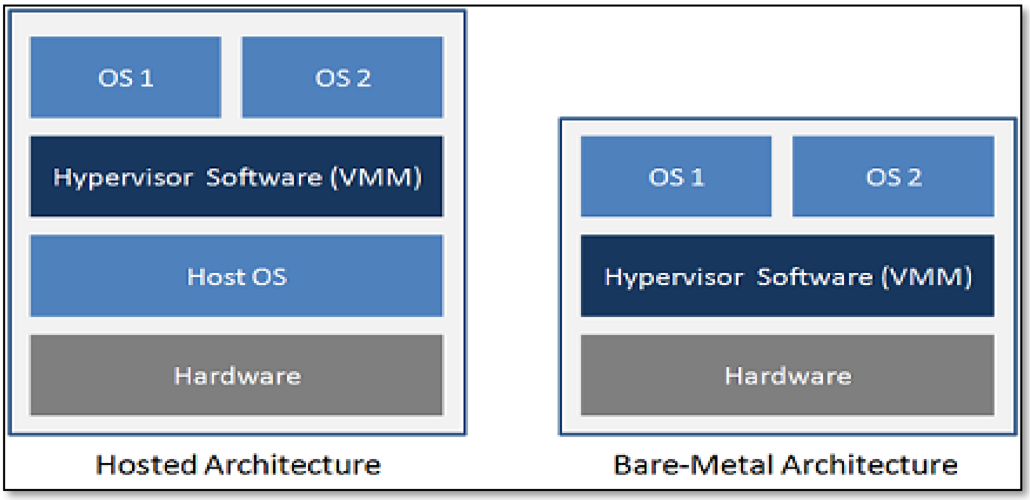
TYPE-1 Hypervisor:

- Hypervisor runs directly on underlying host system.
- It is also known as "**Native Hypervisor" or "Bare metal hypervisor**".
- It does not require any base server operating system.

- It has direct access to hardware resources.
- Examples of Type 1 hypervisors include **VMware ESXi, Citrix XenServer and Microsoft Hyper-V hypervisor.**

TYPE-2 Hypervisor:

- A Host operating system runs on underlying host system.
- It is also known as **'Hosted Hypervisor".**
- Basically a software installed on an operating system.
- Hypervisor asks operating system to make hardware calls.
- Example of Type 2 hypervisor include VMware Player or Parallels Desktop.
- Hosted hypervisors are often found on endpoints like PCs.



Machine Image

- Machine imaging is a process that is used to achieve the goal of system portability, provision, and deploy systems in the cloud through capturing the state of systems using a system image.
- A system image makes a copy or a clone of the entire computer system inside a single file.
- The image is made by using a program called system imaging program and can be used later to restore a system image.
- For example Amazon Machine Image (AMI) is a system image that is used in the cloud computing.
- The Amazon Web Services uses AMI to store copies of a virtual machine.
- An AMI is a file system image that contains an operating system, all device drivers, and any applications and state information that the working virtual machine would have.
- The AMI files are encrypted and compressed for security purpose and stored in Amazon S3 (Simple Storage System) buckets as a set of 10MB chunks.
- Machine imaging is mostly run on virtualization platform due to this it is also called as Virtual Appliances and running virtual machines are called instances.

- Because many users share clouds, the cloud helps you track information about images, such as ownership, history, and so on.
- The IBM Smart Cloud Enterprise knows what organization you belong to when you log in.
- You can choose whether to keep images private, exclusively for your own us e, or to share with other users in your organization.
- If you are an independent software vendor, you can also add your images to the public catalog.

Virtual Machine

- **A virtual machine**, known as a guest, is created within a computing environment, called a host.
- Multiple virtual machines can exist in one host at one time.
- Virtual machines are software computers that provide the same functionality as physical computers.
- Like physical computers, they run applications and an operating system.
- However, virtual machines are computer files that run on a physical computer and behave like a physical computer.
- In other words, virtual machines behave as separate computer systems.
- Virtual machines can also be used for other purposes such as server virtualization.
- Specialized software, called a hypervisor, emulates the PC client or server's CPU, memory, hard disk, network and other hardware resources completely, enabling virtual machines to share the resources.

Advantages of Virtual Machines:

- Provides disaster recovery and application provisioning options
- Virtual machines are simply managed, maintained, and are widely available
- Multiple operating system environments can be run on a single physical computer

Disadvantages of Virtual Machines:

- Running multiple virtual machines on one physical machine can cause unstable performance
- Virtual machines are less efficient and run slower than a physical computer.

Types of Virtual Machines:

1. **Process virtual machines**: Execute computer programs in a platform-independent environment. It masks the information of the underlying hardware or operating system. This allows the program to be executed in the same fashion on any platform.
2. **System virtual machines**: Support the sharing of a host computer’s physical resources between multiple virtual machines.

Data storage in cloud computing(storage as a service)

Introduction

- Cloud storage is a service which enables saving the data on offside storage system.
- This data is managed by third-party.
- This data is accessible by a web services API.
- **Cloud Storage** is technology that allows you to save files in storage, and then access those files via the Cloud.
- Let's break down this definition. First, storage is the computer's ability to save files and other resources for later use.
- When you restart a computer, the files that are still available after the computer turns back on are saved and read from storage.
- Such storage commonly consists of a hard drive, a USB Flash drive, or another type of drive.
- Because local data drives can be damaged or stolen, an idea was developed to use data drives over a network as storage.
- This allows the drives to be secured in a data center and backed up automatically.
- Initially, network storage required fast local networks (LAN), but today we have a ubiquitous network called the Internet.
- The second part of Cloud Storage, the Cloud, represents the Internet. Any service, including storage, available over the Internet, is called Cloud service.
- For ex: GMAIL it is email in the Cloud and An Amazon MP3 player, that's music in the Cloud.

Storage Devices

Following are the categories of storage devices:

1) **Block Storage Devices** – This type of devices provide raw storage to the clients. This raw storage is separated for creating volumes. A volume is a recognizable unit of data storage.
2) **File Storage Devices** – The file storage devices are provided to the client in the form of files for maintaining its file system. Storage data is accessed using the Network File System(NFS).

Storage Classes of cloud

Following are the categories of storage classes:

1. **Unmanaged Cloud Storage**
   - The storage is preconfigured for the customer, this is known as **unmanaged cloud storage.**
   - The customer cannot format or install his own file system or change drive properties.
2. **Managed Cloud Storage**
   - Managed cloud storage provides the online storage space on-demand.
   - This system shows the user like raw disk that the user can partition and format.

Amazon Elastic Compute Cloud (Amazon EC2)

- **Amazon EC2 (Elastic Compute Cloud)** is a web service interface that provides resizable compute capacity in the AWS cloud.
- It is designed for developers to have complete control over web-scaling and computing resources.
- Using Amazon EC2 eliminates your need to invest in hardware up front, so you can develop and deploy applications faster.
- You can use Amazon EC2 to launch as many or as few virtual servers as you need, configure security and networking, and manage storage.
- Amazon EC2 enables you to scale up or down to handle changes in requirements or spikes in popularity, reducing your need to forecast traffic.

Features of Amazon EC2

Amazon EC2 provides the following features:

- Virtual computing environments, known as **instances**
- Preconfigured templates for your instances, known as Amazon Machine Images (AMIs), that package the bits you need for your server
- Various configurations of CPU, memory, storage, and networking capacity for your instances, known as **instance types**.
- Secure login information for your instances using key pairs.
- Storage volumes for temporary data that's deleted when you stop or terminate your instance, known as **instance store volumes**
- Persistent storage volumes for your data using Amazon Elastic Block Store, known as **Amazon EBS volumes**
- Multiple physical locations for your resources, such as instances and Amazon EBS volumes, known as **Regions and Availability Zones**
- A firewall that enables you to specify the protocols, ports, and source IP ranges that can reach your instances using security groups
- Static IPv4 addresses for dynamic cloud computing, known as Elastic IP addresses
- Metadata, known as tags, that you can create and assign to your Amazon EC2 resources
- Virtual networks you can create that are logically isolated from the rest of the AWS cloud, and that you can optionally connect to your own network, known as *virtual private clouds* (VPCs)

Pricing for Amazon EC2

- When you sign up for AWS, you can get started with Amazon EC2 for free using the AWS Free Tier
- Generally, Amazon EC2 priced on per instance / per hour basis.
- However, any instance can be rented on per month basis as well. In such case, Reserved and Spot Instances pricing can be applied resulting in significant discount. Instances are priced depending on their "size", namely how much CPU and RAM included.

- Amazon EC2 provides the following purchasing options for instances:
  1. **On-Demand Instances**
     Pay for the instances that you use by the second, with no long-term commitments or upfront payments.
  2. **Savings Plans**
     You can reduce your Amazon EC2 costs by making a commitment to a consistent amount of usage, in USD per hour, for a term of 1 or 3 years.
  3. **Reserved Instances**
     You can reduce your Amazon EC2 costs by making a commitment to a specific instance configuration, including instance type and Region, for a term of 1 or 3 years.
  4. **Spot Instances**
     Request unused EC2 instances, which can reduce your Amazon EC2 costs significantly.

Amazon EC2 Compute Unit

- Amazon's EC2 in addition to being one of the oldest and most mature cloud server platforms, also provides clearly defined CPU tiers across its 8 different instance sizes.
- These are defined in terms of ECUs (EC2 Compute Unit) where 1 ECU is the equivalent CPU capacity of a 1.0-1.2 GHz 2007 Opteron or 2007 Xeon processor.
- Their instance sizes includes the following:
  - ✓ Small/m1.small (32-bit) = 1 ECU
  - ✓ Large/m1.large = 4 ECUs
  - ✓ High-CPU Medium/c1.medium (32-bit) = 5 ECUs
  - ✓ High-Memory Extra Large/m2.xlarge = 6.5 ECUs
  - ✓ Extra Large/m1.xlarge = 8 ECUs
  - ✓ High-Memory Double Extra Large/m2.2xlarge = 13 ECUs
  - ✓ High-CPU Extra Large/c1.xlarge = 20 ECUs
  - ✓ High-Memory Quadruple Extra Large/m2.4xlarge = 26 ECUs

Storage of Amazon EC2

Economical, High-Scale Storage Choices

1. **Amazon Glacier-** It is an extremely low-cost storage service. It offers secure and fast storage for data archiving and backup.
2. **Amazon Elastic Block Store (EBS)-** It provides block-level storage to use with Amazon EC2 instances. Amazon Elastic Block Store volumes are network-attached and remain independent from the life of an instance.
3. **AWS Storage Gateway-** This AWS service is connecting on-premises software applications with cloud-based storage. It offers secure integration between the company's on-premises and AWS's storage infrastructure.

Companies using AWS

- Instagram
- Zoopla
- Pinterest
- Netflix
- Dropbox
- Etsy
- Talkbox
- Playfish
- Ftopia

Eucalyptus

- Eucalyptus is open source software for building AWS-compatible private and hybrid clouds.
- As an Infrastructure as a Service (IaaS) product, Eucalyptus allows your users to provision your compute and storage resources on-demand.
- Amazon has partnered with Eucalyptus to deliver an Infrastructure as a Service (IaaS) product.
- As part of the deal, Amazon Web Services (AWS) is letting the IaaS provider tap into its application programming interfaces (APIs).
- Eucalyptus says it is now "fully compatible with the Amazon Web Services API, which means you can use or reuse your existing AWS-compatible tools, images (AMIs), and scripts to manage your own hybrid and on premise clouds."
- Eucalyptus's IaaS service is now compatible with the following AWS services: EC2, EBS, AMI, S3, and IAM.

Unit 2
Part -2 Cloud Security

Infrastructure Security

- Cloud computing utilizes three delivery models (SaaS, PaaS, and IaaS) to provide infrastructure resources, application platform and software as services to the consumer.
- These service models need different level of security in the cloud environment.
- Cloud service providers and customers are responsible for security and privacy in cloud computing environments but their level of responsibility will differ for different delivery models.
- Infrastructure as a Service (IaaS) serves as the foundation layer for the other delivery models, and a lack of security in this layer affects the other delivery models.
- In IaaS, although customers are responsible for protecting operating systems, applications, and content, the security of customer data is a significant responsibility for cloud providers.
- In Platform as a service (PaaS), users are responsible for protecting the applications that developers build and run on the platforms, while providers are responsible for taking care of the users' applications and workspaces from one another.
- In SaaS, cloud providers, particularly public cloud providers, have more responsibility than clients for enhancing the security of applications and achieving a successful data migration.
- In the SaaS model, data breaches, application vulnerabilities and availability are important issues that can lead to financial and legal liabilities.

INFRASTRUCTURE SECURITY: THE NETWORK LEVEL

- As network level of infrastructure security is concerned, it is important to distinguish between public clouds and private clouds.
- With private clouds, there are no new attacks, vulnerabilities, or changes in risk specific to this topology that information security personnel need to consider.
- If public cloud services, changing security requirements will require changes to the network topology and the manner in which the existing network topology interacts with the cloud provider's network topology should be taken into account.
- All data on the network need to be secured.
- Strong network traffic encryption techniques such as Secure Socket Layer (SSL) and the Transport Layer Security (TLS) can be used to prevent leakage of sensitive information.
- Several key security elements such as data security, data integrity, authentication and authorization, data confidentiality, web application security, virtualization vulnerability,

availability, backup, and data breaches should be carefully considered to keep the cloud up and running continuously.

- There are four significant risk factors in this use case:
  1. Ensuring the confidentiality and integrity of organization's data-in-transit to and from a public cloud provider
  2. Ensuring proper access control
  3. Ensuring the availability of the Internet-facing resources
  4. Replacing the established model of network zones and tiers with domains.

INFRASTRUCTURE SECURITY - THE HOST LEVEL

- When reviewing host security and assessing risks, the context of cloud services delivery models (SaaS, PaaS, and IaaS) and deployment models public, private, and hybrid) should be considered.
- The host security responsibilities in SaaS and PaaS services are transferred to the provider of cloud services.
- IaaS customers are primarily responsible for securing the hosts provisioned in the cloud in terms virtualization software security, customer guest OS or virtual server security.

INFRASTRUCTURE SECURITY - THE APPLICATION LEVEL

- Software security or applications should be a crucial element of a security program.
- Most enterprises with information security programs have yet to introduce an application security program to address this domain.
- Most websites are secured at the network level while there may be security loopholes at the application level which may allow information access to unauthorized users.
- Software and hardware resources can be used to provide security to applications. In this way, attackers will not be able to get control over these applications and change them.
- XSS attacks, Cookie Poisoning, Hidden field manipulation, SQL injection attacks, and Google Hacking are some examples of threats to application level security which resulting from the unauthorized usage of the applications.
- Designing and implementing applications aims at deployment on a cloud platform will require existing application security programs to reexamine current practices and standards. The application security spectrum ranges from single-user applications to multiuser e-commerce applications used by many users.

The level is responsible for managing

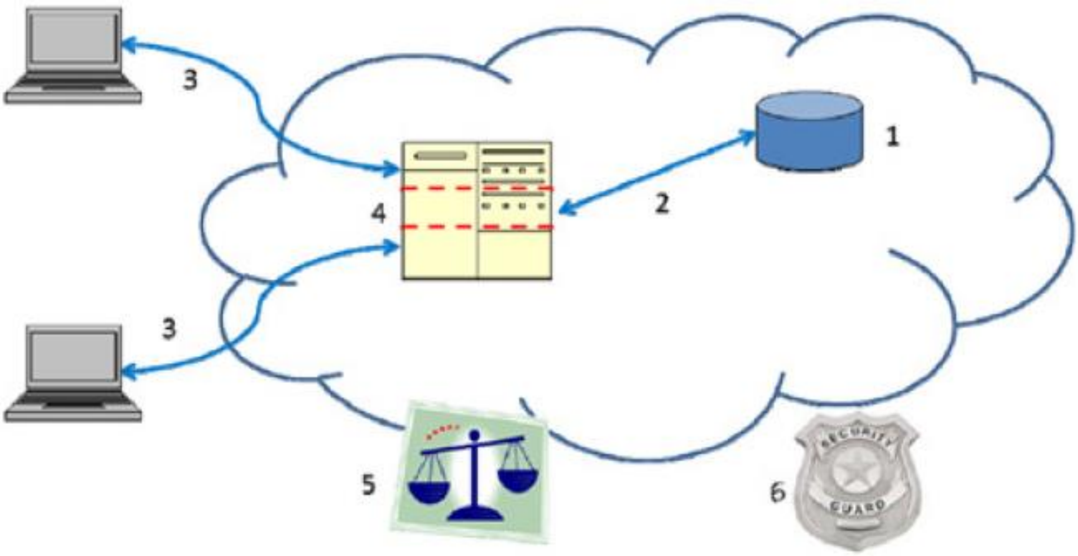
- Application-level security threats;
- End user security;
- SaaS application security;
- PaaS application security;
- Customer-deployed application security
- IaaS application security
- Public cloud security limitations

Data Security and Storage

- Majority of cloud service providers store customers' data on large data centers.
- Although cloud service providers say that data stored is secure and safe in the cloud, customers' data may be damaged during transition operations from or to the cloud storage provider.
- When multiple clients use cloud storage or when multiple devices are synchronized by one user, data corruption may happen.
- Different encryption techniques like public and private key encryption for data security can be used to control access to data.
- Backups or use of multiple providers can help companies to protect services from such failure and ensure data integrity in cloud storage.
- **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.

Data privacy and security Issues

- There are numerous security issues for cloud computing as it encompasses many technologies including networks, databases, operating systems, virtualization, resource scheduling, transaction management, load balancing, concurrency control and memory management.
- Therefore, security issues for many of these systems and technologies are applicable to cloud computing. For example, the network that interconnects the systems in a cloud has to be secure.
- Virtualization paradigm in cloud computing leads to several security concerns. For example, mapping the virtual machines to the physical machines has to be carried out securely.
- Data security involves encrypting the data as well as ensuring that appropriate policies are enforced for data sharing.
- In addition, resource allocation and memory management algorithms have to be secure.
- These six areas of security are:
  (1) security of data at rest,
  (2) security of data in transit,
  (3) authentication of users/applications/ processes,
  (4) robust separation between data belonging to different customers,
  (5) cloud legal and regulatory issues, and
  (6) incident response.



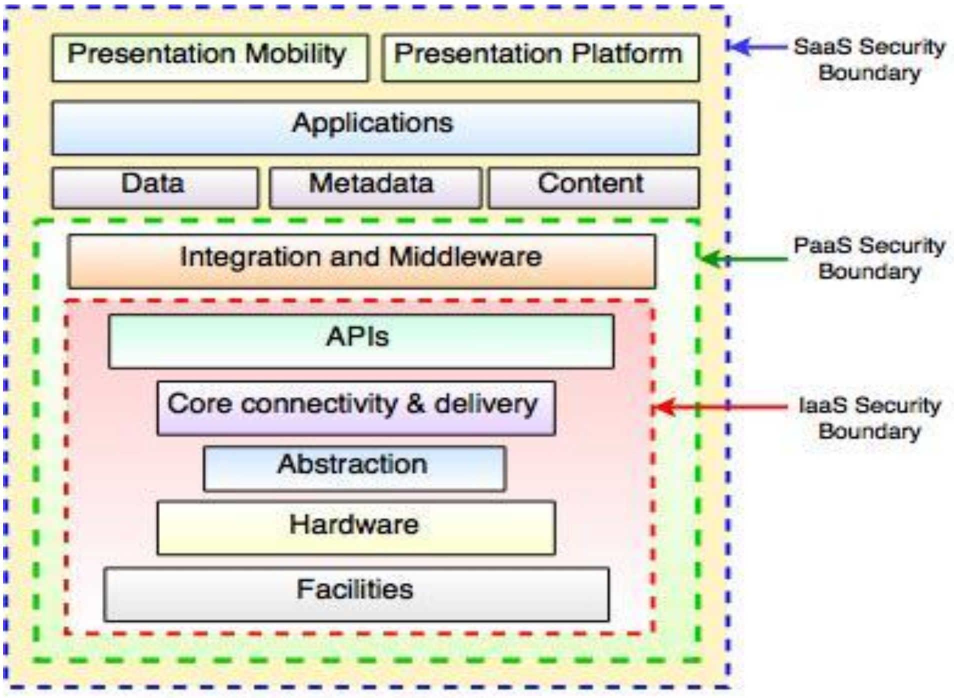
Security Planning

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 below.
- 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.
- This model describes the security boundaries at which cloud service provider's responsibilities end and the customer's responsibilities begin.
- Any security mechanism below the security boundary must be built into the system and should be maintained by the customer.
- Although each service model has security mechanism, the security needs also depend upon where these services are located, in private, public, hybrid or community cloud.

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

- All of the service models should incorporate security mechanism operating in all above-mentioned areas.

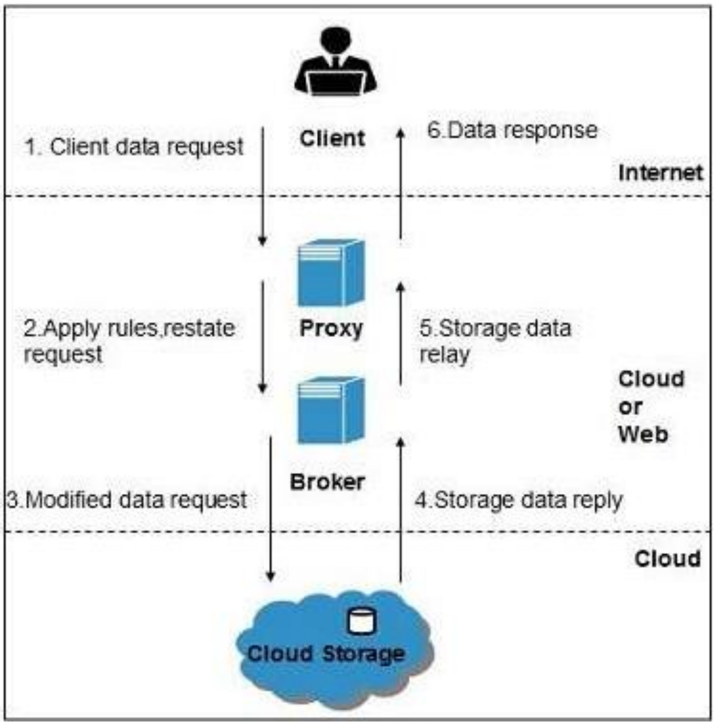
Isolated Access to Data

- Since data stored in cloud can be accessed from anywhere, we must have a mechanism to isolate data and protect it from client's direct access.
- Brokered Cloud Storage Access is an approach for isolating storage in the cloud. In this approach, two services are created:
  - A broker with full access to storage but no access to client.
  - A proxy with no access to storage but access to both client and broker.

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:



Authentication in cloud computing

- There are multiple methods to authenticate cloud users and many issues that come along with these methods.
- Cloud computing is helping businesses to store a large amount of data at relatively low costs but it is essential these service providers offer methods to ensure users are authenticated.
- There are multiple authentication techniques in cloud computing suited for different applications and use cases when it comes to the cloud.
- The best cloud authentication method depends on your preferences but each is a supported method.

Cloud Authentication Methods

1. **API Keys**
   - This method doesn't require client libraries and is transparent to the user.
   - This method identifies the project by creating a strong association between a key and a project.
   - API keys are less secure as they are vulnerable to man-in-the-middle attacks.
   - API keys can easily be added to any HTTP call as a query parameter in the header because they don't require a client library.
2. **Firebase Authentication**
   - This type of authentication provides backend services, app SDKs, and libraries to authenticate users to a mobile or web app.
   - This method authenticates users, using a variety of credentials like Google, Facebook, Twitter or GitHub.
   - The Firebase authentication method uses a client library to sign a JSON Web Token, JWT, with a private key after the user has successfully signed in.
   - This method then validates the JWT, through a proxy, was signed by Firebase and that the issuer matches the setting in API configuration.
3. **Auth0 Authentication**
   - This method not only authenticates and authorizes apps and APIs but it is also stack, device, and identity agnostic.
   - This method supports several providers and security assertion markup language specification.
   - Much like Firebase Authentication, this method also provides backend services, SDKs and user interface libraries for authenticating users in web and mobile apps.
   - Also, like Firebase Authentication, this method validates the JWT was signed and the issuer matches the API configuration.
4. **Google Authentication**
   - This authentication method allows users to authenticate by signing in with their Google account.

- Once the user is authenticated, they have access to all Google services and a Google ID token can be used to make calls to Google APIs and Cloud Endpoints APIs.
- This method also verifies that the JWT was signed by Google and the issuer is listed on the API configuration.

5. **Google Authorization and Service Accounts**
    - With this method, a JWT can be generated and signed using a service account and Google-provided client library for a Google Cloud Platform project.
    - This method uses the public key to validate a Google-signed JWT and to ensure that Google is listed as the issuer in the API configuration.
    - For this method, Google ID tokens are recommended for service accounts because the API producer only needs to white list Google as an issuer for all service accounts.

Cloud Computing Authentication Issues

1. Privacy Issues
2. Lack of Transparency
3. Security Issues
4. The Possibility of Exploitation of the Authentication Mechanism
5. Different Authentication Technologies Presents Challenges to Customers

- When it comes to cloud computing, service providers require customers to store their account information in the cloud, giving service providers access to this information.
- For many customers, this presents a privacy issue for them. The lack of transparency in the cloud makes it difficult for customers to ensure the proper rules are enforced.
- Customers using multiple cloud services have more copies of their information out there in the cloud. This causes security issues for customers and cloud service providers.
- Multiple copies of accounts lead to multiple authentication processes and provide the possibility to exploit the authentication mechanism.
- Cloud service providers use different authentication technologies for authenticating users and while this has less of an impact on SaaS than PaaS and IaaS, it presents challenges to customers.
- The major importance of authentication in cloud computing is for users to ensure their projects and information are safe and there when they need it.
- While there are still a few issues associated with cloud service providers being able to perform authentication methods without any challenges or security fears, it is important to remember just how new cloud computing is and the amount of room it has for progress.

Cloud contracting Model

1. **Selecting a cloud service:** Choosing the appropriate cloud service and deployment model is the critical first step in procuring cloud services.
2. **Cloud service provider and end-user agreements:** Terms of service and all CSP/customer-required agreements need to be integrated fully into cloud contracts.

3. **Service-level agreements:** SLAs need to define performance with clear terms and definitions, demonstrate how performance is being measured, and specify what enforcement mechanisms are in place to ensure that SLAs are met.
4. **CSP, agency, and integrator roles and responsibilities:** Careful delineation between the responsibilities and relationships among the federal agency, integrators and the CSP are needed in order to effectively manage cloud services.
5. **Standards:** The use of the National Institute of Standards and Technology's Cloud Computing Reference Architecture and agency involvement in standards are necessary for cloud procurements.
6. **Security:** Agencies must clearly detail the requirements for CSPs to maintain the security and integrity of data existing in a cloud environment.
7. **Privacy:** If cloud services host "privacy data," agencies must adequately identify potential privacy risks and responsibilities and address those needs in the contract.
8. **E-discovery:** Federal agencies must ensure that all data stored in a CSP environment is available for legal discovery by allowing all data to be located, preserved, collected, processed, reviewed and produced.
9. **Freedom of Information Act:** Federal agencies must ensure that all data stored in a CSP environment is available for appropriate handling under FOIA.
10. **E-records:** Agencies must ensure that CSPs understand and assist federal agencies in compliance with the Federal Records Act and obligations under that law.

COMMERCIAL AND BUSINESS CONSIDERATIONS

There are a number of contract types

Consumer to business:

- Typically these contracts relate to free cloud services, such as Facebook, where the cloud provider makes its money through advertising and/or the secondary processing of customer data.
- This type of contract has no scope for negotiation, and consumers generally have few rights under the contract.

Business to business:

- These contracts generally relate to services which an enterprise is paying for.
- There is usually little scope for negotiation, but the contract will usually vest more rights to the consumer – although the cloud provider's liability for service performance (including data damage and loss) may in some cases be very limited.
- The contract may also permit the cloud provider to unilaterally modify both the service and the contract, and place technical and contractual constraints on switching from one provider to another.

Bespoke (personalized) contracts:

- Cloud providers rarely offer scope for negotiation of their contracts, it is not correct to say that there is never any negotiation.

- Cloud providers have been known to negotiate specific agreements with those consuming organizations viewed as particularly influential or large volume.
- Cloud contracts vary: some are balanced and fair to both parties, and others are unbalanced, favoring the cloud provider.

Explain data privacy and security issues.

CLOUD SECURITY ISSUES

- Security is a major issue in IT business environment.
- Since customers and users shifted from Grid computing to Cloud computing in their business, many security issues appeared, which is a major concern for the Cloud provider due to the risk of losing customers.
- The Cloud Computing is mainly built on virtualization environment, that increase more risk of securing the cloud.

Virtual Security issues:

- The virtual environment area of the cloud computing is the most sensitive and important part of the cloud.
- This is because all the devices in the cloud are connected virtually through virtual networks that are running and managing the IT infrastructures and virtual servers in the cloud.
- In virtualization technology, multiple Virtual Machines (VM's) can run on top of a single physical machine, and can run on any OS within each VM's to manage the infrastructure.
- One of the main **virtual security issues** in the cloud are attacks on the network between VM's, and the trust between different VM's .
- There are others problems, such as non-secure Apps and vulnerability in VM's, which allow any unauthorized access.

1) Network Attacks in Virtual cloud:

- Running many different virtualization products increases the attackers (especially the hackers) perimeter.
- Amazon's cloud computing service (EC2), could be used to hack into other systems by using EC2 cloud service to allow a brute force attack, that will fire 400,000 passwords per second at a secured wireless network.
- Within a period of twenty minutes the system would had been attacked.

- The attackers hacked and shut down Sony's online customer networks in April 2011.
- Hackers used cloud based attacks to disrupt service to roughly 100 million
- users worldwide .

2) Distributed Denial of Service (DDOS) Attacks:

- This attack targets the networks and servers.
- It makes the network traffic and users being denied to access a certain Internet-based service in the cloud.
- In worst cases the attackers will use bonnets to perform DDOS. In order to stop hackers of attacking the network, face blackmail is provided.
- DDOS attacks should be considered as threats for cloud providers such AWS, Google Apps, and Microsoft Cloud.
- These scenarios show us that cloud computing network is still not secure, and this will drive us to non-secure applications.

3) Non-Secure Apps:

- Cloud applications security is a complicated issue for organizations and customers if they ignore securing their data before deploying it in the cloud.
- They need to consider the new threats and attacks spread
- Non-Secure applications opens the doors for further threats that could result in attacking the cloud through the network and Application Programming Interface (API).
- Man in The Middle attack is one of the problems for non-secure apps.
- This attack works as eavesdropping. Here, the attacker creates independent connections with the victims and transmits messages between them to make them believe that they are talking directly to each other over a private connection when in fact the entire conversation is run and controlled by the attacker.
- Facebook application is prone to Man- In -The -Middle attack (MITM) on users' data.

4) Domain Name Server (DNS) Attacks:

- It's easy for attackers to attack DNS in cloud computing when the users or customers try to call the server by name.
- Because, names are much easier to remember than Internet Protocol (IP) addresses, the attacker will create a temporary malicious cloud to fake the user or customers.

- Hence using IP address is not always feasible in DNS since customers will route malicious cloud.
- It may happen that even after all the DNS security procedures are implemented, security problems would exist based on the mode selected between the sender and the receiver.

Physical Security Issues

- Physical security issues are the other part of the cloud computing security.
- Although the data is stored in the virtual server in the cloud, it must also be stored in physical locations within physical hardware.
- Physical security in the cloud represents the physical machines and storage in the datacenter.
- Physical security issues shows as a loss of physical control, human attacks, power failure, access control, and third party trust.
- Those physical issues need to be protected also from any insider and outsider attackers.
- Usually the outside threats are easier to deal with than the inside threats because the outside attacks have been already prepared for through risk assessment plans.
- However, the internal physical security threats in cloud datacenter constitute the top risks in the cloud.

1) Loss of Physical Control:

- The loss of physical access control occurs when the customers join the cloud either by keeping their applications in the cloud, or using cloud storage for saving their data.
- This loss of control results in issues and concerns for the customers, such as trust and privacy of their data in the cloud provider's datacenter, control over their data in the cloud, and legal restrictions by cloud provider

a) Privacy and Data

- With private, public and community clouds, customer's data may not remain in the same system. In other words, it will not be located in the customer premises any more.

b) Control over Data

- Customers need to have a full control over their data, and not limited control and accountability within Public clouds such as (IAAS) implementation, and through (PAAS) operations.
- Customers need to have confidence that the provider will offer services with appropriate controls.

c) Legal and Regulatory Compliance

- It may be difficult or unrealistic for customers to utilize public clouds if their data need to be processed.
- This is a subject to legal restrictions or regulatory compliance.
- Customers should expect providers to build and certify their cloud to address the needs of regulated markets, and achieve certifications and trust confidentiality between customers and providers of the services.

2) Human Attacks:

- Human attacks happen when unauthorized personal tries to access the datacenter. This attack for datacenter could be man in the middle attack, or malicious insiders such as an employee of the datacenter.
- These kinds of attacks are examples of the cloud provider losing their significant control over securing datacenters and authorizing human attacker to enter their premises.

3) Power Failure:

- In the event that the datacenter of cloud providers is faced with any kind of problems which causes power failure, and the providers do not have any disaster recovery plan, then the data in the cloud is at risk if it is not saved by the customer and user during the downtime.
- This give rise to the possibility of attackers accessing the servers through the man in the middle attacks .
- Amazon’s cloud services infrastructure faced a power failure issue in their datacenter in August 2011 where many people who were using AWS were affected by such an outage because all the services were disconnect.