University of Technology
الجامعة التكنولوجية

Computer Science Department
قسم علوم الحاسوب

Cloud Computing Foundations
أساسيات الحوسبة السحابية

Asst. Lectur. Ghazwh Ghanim Jumaa
م.م غزوة غانم جمعة

cs.uotechnology.edu.iq

Lecture one

1- Introduction and Basic of Cloud Computing

Cloud computing is the delivery of computing services over the Internet. Cloud services allow individuals and businesses to use software and hardware that are managed by third parties at remote locations.

Why call it “cloud computing”?

Some say because the computing happens out there "in the clouds"

Examples of cloud services include online file storage, social networking sites, webmail, and online business applications.

The cloud computing model allows access to information and computer resources from anywhere that a network connection is available.

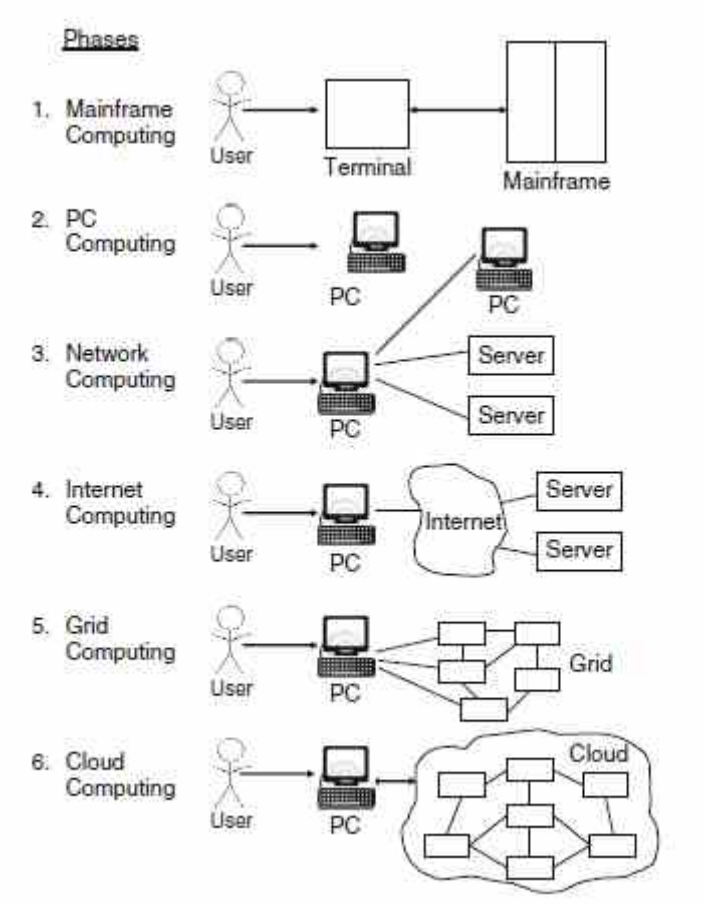
Cloud computing provides a shared pool of resources, including data storage space, networks, computer processing power, and specialized corporate and user applications.

We do not need to install the part of the software on the local computer, and we have this is the way, which overcomes the cloud computing platform they are operating completely independent of any does not depend on the type of device or system that is used by the user to gain access to the computerized cloud. Thus, cloud computing makes our mobile applications and effective.

So the Cloud Computing in a Nutshell

Computing itself, to be considered fully virtualized, must allow computers to be built from distributed components such as processing, storage, data, and software resources. Technologies such as cluster, grid, and now, cloud computing, have all aimed at allowing access to large amounts of computing power in a fully virtualized manner, by aggregating resources and offering a single system view. Utility computing describes a business model for on-demand delivery of computing power; consumers pay providers based on usage ("payas-you- go"), similar to the way in which we currently obtain services from traditional public utility services such as water, electricity, gas, and telephony. Cloud computing has been coined as an umbrella term to describe a category of sophisticated on-demand computing services initially offered by commercial providers, such as Amazon, Google, and Microsoft. 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."

Figure below, shows six phases of computing paradigms, from terminals/mainframes, to PCs, networking computing, to grid and cloud computing.



In phase 1, many users shared powerful mainframes using terminals.

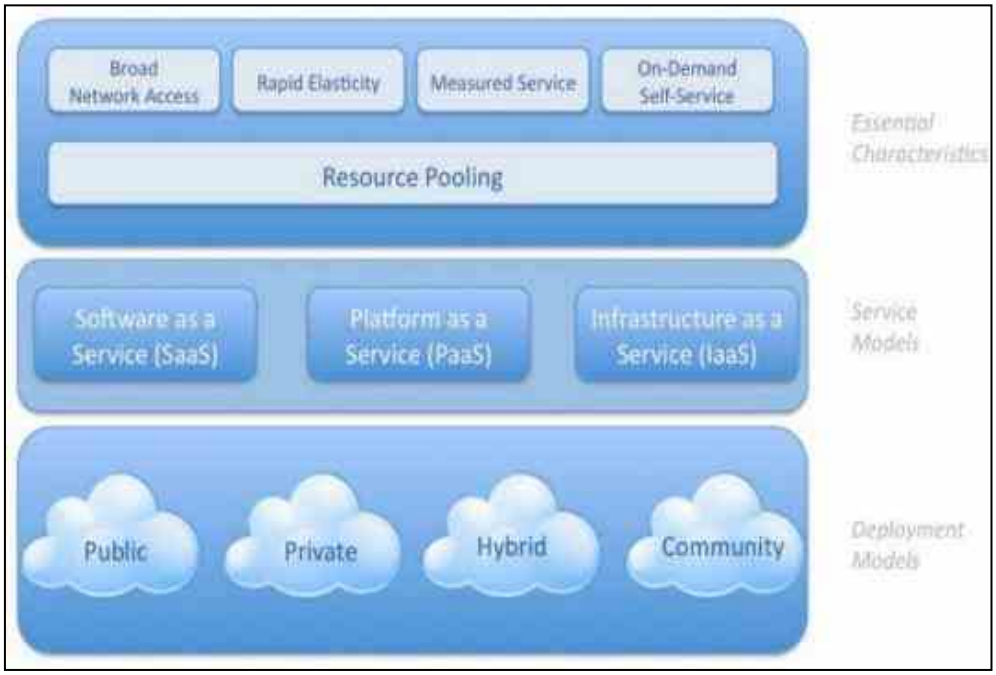
In phase 2, stand-alone PCs became powerful enough to meet the majority of users' needs.

In phase 3, PCs, laptops, and servers were connected together through local networks to share resources and increase performance.

In phase 4, local networks were connected to other local networks forming a global network such as the Internet to utilize remote applications and resources.

In phase 5, grid computing provides shared compute and storage resources distributed across different administrative domain, Grid Computing is the starting point and basis for Cloud Computing.

In phase 6, cloud computing further provides shared resources on the Internet in a scalable and simple way. The client gets all or part of it according Pay As You Go.



Overview of cloud computing model

2- The Traditional Software Model

Traditional software applications are based on a model with large, upfront licensing costs and annual support costs. Increasing the number of users can raise the base cost of the package due to the need for additional hardware server deployments and IT support. Licensing costs are often based on metrics that are not directly aligned with usage (server type, number of CPUs, etc., or some physical characteristic) and are not virtual. A typical enterprise software package requires hardware deployment, servers, and backup and network provisioning to accommodate the number of users on- and off-campus. Security architecture is also taxed in an effort to protect this valuable resource from unauthorized access.

Traditional software applications tend to be highly customizable, which comes at a cost—in both dollars and manpower.

3- Cloud Computing Benefits

Cloud computing benefits can be categorized into:

- **Cost Reduction**: The consumer does not need to take the stress of updating the software and hardware as they can get the latest and updated resources and services relatively in less time.
- **Power Management**: It is easier to manage virtual server as compared to physical server.
- **Scalability**: It is the one of the main positive aspects of cloud computing. If there is peak load or high traffic for a site, cloud can handle easily without need of any additional hardware infrastructure or equipments
- **Data Storage**: There are various data centers spread throughout the world and it makes easy for the businesses to choose the datacenter as per their convenience to get fast and easy access of services with unlimited data storage.
- **Trouble shooting and Backup (Disaster) recovery**: Hardware failure can also be easily traced out and corrected . the assessment of data can be done anytime and is highly beneficial for the IT industry in reducing workloads and whenever data needs to be recovered.
- **Efficiency and reliability**: To find efficiencies many organizations are moving towards cloud and backup is another significant advantage to the cloud and it maintains backup for all remote sites and branch offices.

4- Cloud Computing Attributes and Major Characteristics

Our definition of cloud computing is based on many attributes

1) Multitenancy (shared resources)

Unlike previous computing models, which assumed dedicated resources (i.e., computing facilities dedicated to a single user or owner), cloud computing is based on a business model in which resources are shared (i.e., multiple users use the same resource) at the network level, host level, and application level.

2) Massive scalability

Although organizations might have hundreds or thousands of systems, cloud computing provides the ability to scale to tens of thousands of systems, as well as the ability to massively scale bandwidth and storage space.

3) Elasticity

Users can rapidly increase and decrease their computing resources as needed, as well as release resources for other uses when they are no longer required.

4) Pay as you go

Users pay for only the resources they actually use and for only the time they require them.

5) Self-provisioning of resources

Users self-provision resources, such as additional systems (processing capability, software, storage) and network resources.

The Major Characteristics

- Virtualized: Resources (i.e. compute, storage and network capacity) in clouds are virtualized, and this is achieved at various levels including virtual machine (VM) and platform levels.

- Service oriented: Cloud is implemented using a service-oriented architecture model where all the capabilities or components are available over the network as a service. Whether it is software, a platform or infrastructure, everything is offered as a service.
- Elastic: Resources (i.e. compute, storage and network capacity) required for cloud applications can be dynamically provisioned and varied, that is, increased or decreased at runtime depending on user QoS requirements.
- Dynamic and distributed: Although cloud resources are virtualized, they are often distributed to enable the delivery of high-performance and/or reliable cloud services.These resources are flexible and can be adapted according to customer requirements such as software, network configuration and so on.
- Shared (economy of scale): Clouds are shared infrastructure where resources serve multiple customers with dynamic allocation according to their application's demand. This sharing model is also termed the multi-tenant model. In general, customers neither have any direct control over physical resources nor they are aware of the resource location and with whom resources are being shared.
- Market oriented (pay as you go): In cloud computing, customers pay for services on a pay-per-use (or pay-as-you-go) basis. The pricing model can vary depending on the QoS expectation of application. This characteristic addresses the utility dimension of cloud computing. That means that cloud services are offered as 'metered' services where providers have an accounting model for measuring the use of the services, which helps in the development of different pricing plans and models. The accounting model helps in the control and optimization of resource usage.

- Autonomic: To provide highly reliable services, clouds exhibit autonomic behavior by managing themselves in case of failures or performance degradation.

5- Limitations of Cloud Computing

Following are some limitations of cloud computing: -

- **Data segregation:** As data of many users are stored in same data center and same server or same hard disks it will raise the question from the users about the problem of mismatch. How cloud securely isolate users and differentiate the memory and storage of each users as this failure could lead to leakage of information from one customer to another
- **The Offline cloud:** As cloud computing is fully dependent upon internet connection. If the customer has a problem with internet connection, then he/she is unable to access the application or data from internet
- **Privacy:** Privacy is one of the major issues in cloud. Users are always concerned about their data so to overcome this issue provider should assure the users in following points. First, Employees are aware of their responsibilities related to the confidentiality, integrity, availability of data and information systems. Second, the confidential and/or personal client data including system access credentials are protected (e.g. encrypted) from unauthorized interception.

- **Software Licensing:** Many cloud providers relied heavily on open source software because the licensing model for commercial software is not a good match to Utility Computing.
- **Security :**Cloud computing providers support encryption and identity management but still people do not want to place secrets in to the cloud.

6- Cloud Computing Features

Cloud computing brings a number of new features compared to other computing paradigms. There are briefly described: -

•Scalability and on-demand services

Cloud computing provides resources and services for users on demand. The resources are scalable over several data centers.

•User-centric interface

Cloud interfaces are location independent and can be accesses by well established interfaces such as Web services and Internet browsers.

•Guaranteed Quality of Service (QoS)

Cloud computed can guarantee QoS for users in terms of hardware/CPU performance, bandwidth, and memory capacity.

•Autonomous system

The cloud computing systems are autonomous systems managed transparently to users. However, software and data inside clouds can be automatically reconfigured and consolidated to a simple platform depending on user's needs.

•Pricing

Cloud computing does not require up-from investment. No capital expenditure is required. Users pay for services and capacity as they need them.

Lecture Two

Cloud Services and Cloud Deployment

1. Cloud Services or Layers of clouds

Cloud computing can be viewed as a collection of services, which can be presented as a layered cloud computing architecture, as shown in Figure 1.

Cloud computing services are divided into five classes, according to the abstraction level of the capability provided and the service model of providers, namely: (1) Infrastructure as a Service, (2) Platform as a Service, and (3) Software as a Service (4) Virtualized computers (5) Data-Storage-as-a-Service

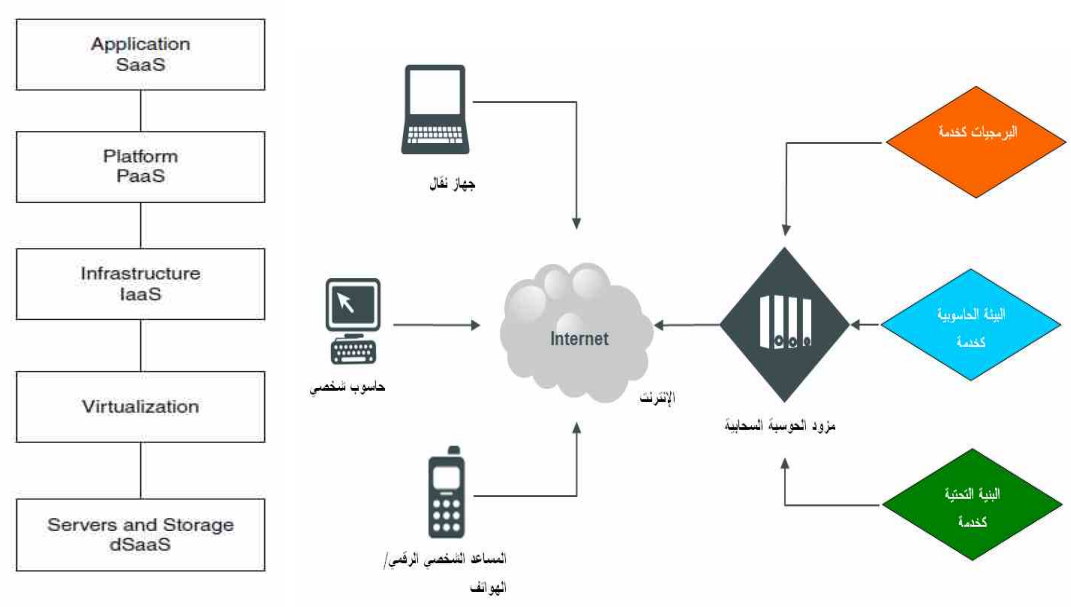


Figure1: layered of cloud computing

1- Software as a Service (SaaS):

Services offered through cloud computing usually include IT services, applications reside on the top of the cloud stack. Services 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. This model of delivering applications, know as software as a service, alleviates the burden of software maintenance for customers and simplifies development and testing for providers.**

Key benefits of a SaaS model include the following:

1- SaaS enables the organization to outsource the hosting and management of applications to a third party (software vendor and service provider) as a means of reducing the cost of application software licensing, servers, and other infrastructure and personnel required to host the application internally.

2- SaaS enables software vendors to control and limit use, prohibits copying and distribution, and facilitates the control of all derivative versions of their software. SaaS centralized control often allows the vendor or supplier to establish an ongoing revenue stream with multiple businesses and users without preloading software in each device in an organization.

3- Applications delivery using the SaaS model typically uses the one-to-many delivery approach, with the Web as the infrastructure. An end user can access a SaaS application via a web browser; some SaaS vendors provide their own interface that is designed to support features that are unique to their applications.

4- A typical SaaS deployment does not require any hardware and can run over the existing Internet access infrastructure. Sometimes changes to firewall rules and settings may be required to allow the SaaS application to run smoothly.

5- Management of a SaaS application is supported by the vendor from the end user perspective, whereby a SaaS application can be configured using an API, but SaaS applications cannot be completely customized.

Examples :Gmail , Photoshop online , Google Docs, Microsoft: office online.

2- Platform-as-a-Service (PaaS):

cloud platform offers an environment on which developers create and deploy applications and do **not necessarily need to know many processors or how much memory that applications will be using. In addition, multiple programming models and specialized services (e.g., data access, authentication) are offered as building blocks to new applications.** Paas, offers a scalable environment for developing and hosting web applications, which should be written in specific programming languages such as python or java, also includes operating systems and required services for a particular application.

PaaS platforms also have functional differences from traditional development platforms, including:

-Multitenant development tools

Traditional development tools are intended for a single user; a cloud-based studio must support multiple users, each with multiple active projects.

-Multitenant deployment architecture

Scalability is often not a concern of the initial development effort and is left instead for the system administrators to handle when the project deploys. In PaaS, scalability of the application and data tiers must be built-in (e.g., load balancing and failover should be basic elements of the developing platform).

-Integrated management

Traditional development solutions (usually) are not associated with runtime monitoring, but in PaaS the monitoring ability should be built into the development platform.

-Integrated billing

PaaS offerings require mechanisms for billing based on usage that are unique to the SaaS world.

Examples: Google AppEngine, window Azure, salesforce.com – Heroku.

3- Infrastructure-as-a-service (IaaS)

offering virtualized resources (computation, storage, network, and communication) on demand, cloud infrastructure enables on demand provisioning of servers running several choices of operating system and a customized software stack. Infrastructure services are considered to be the bottom layer of cloud computing systems.

Features available for a typical IaaS system include:

-Scalability

The ability to scale infrastructure requirements, such as computing resources, memory, and storage (in near-real-time speeds) based on usage requirements.

-Pay as you go

The ability to purchase the exact amount of infrastructure required at any specific time.

-Best-of-breed technology and resources

Access to best-of-breed technology solutions and superior IT talent for a fraction of the cost.

Examples: Amazon, windows Azure.

4- Virtualized Computers This layer forms the foundation of cloud technology. This enables user request for computing resources by accessing appropriate resources and deploy large numbers of virtual machines (VMs) on hardware (processors, memory, I/O devices).

5- Data-Storage-as-a-Service (dSaaS)

is a business model in which third-party providers rent space on their storage to end users. Provides storage that the consumer is used (bandwidth requirements).

2. Type or Deployment Models

Deployment models, with variation in physical location and distribution, a cloud can be classified as 4 main types:

• **Public Cloud** -The cloud infrastructure is available to the public on a commercial basis by a cloud service provider. This enables a consumer to develop and deploy a service in the cloud with very little financial outlay compared to the capital expenditure requirements normally associated with other deployment options.

Example: Amazon, Google Apps, Windows Azure

• **Private Cloud**-The cloud infrastructure has been deployed, and is maintained and operated for a specific organization. The operation may be in-house or with a third party on the premises. Computing architecture is dedicated to the customer and is not shared with other organizations. Example: eBay

TABLE: Public vs. private cloud

attributes	**public**	**private**
Infrastructure Owner	Third party (Cloud provider)	Enterprise
Scalability	Unlimited and On-Demand	Limited to the installed Infrastructure

Cost	Lower cost	High cost including: space, cooling, energy and hardware cost
Performance	Unpredictable guaranteed performance	Guaranteed performance
Security	Concerns regarding data privacy	Highly secure

Enterprise computing, we mean the use of computers for data processing in large organizations, also referred to as 'information systems' (IS), or even 'information technology' (IT) in general.

• Community Cloud

A Community Cloud is a semi private Cloud that is used by a defined group of enterprises with similar backgrounds and requirements can share their infrastructures, thus increasing their scale while sharing the cost**.**

• Hybrid Cloud

A composition of the two types (private and public) is called a Hybrid Cloud, where a private cloud is able to maintain high services availability by scaling up their system with externally provisioned resources from a public cloud when there are rapid workload actuations or hardware failures**.**

Lecture three

Cloud Computing Platforms

1- Infrastructure as A Service: AMAZON EC2

The Amazon cloud provides infrastructure as a service (IaaS), whereby computing infrastructure such as for servers, storage or network end points of a desired capacity are virtually provisioned in minutes through an automated web-based management console. This core IaaS service, called **Elastic Compute Cloud**, or EC2, is but **one** of a set of services that constitute the **Amazon cloud platform**, but the term **EC2 is also often used to describe the entire cloud offering**. **Amazon Elastic Compute Cloud (Amazon EC2) is a web service that provides resizable compute capacity in the cloud.** It is designed to make web-scale computing easier for developers. Amazon EC2's simple web service interface allows you to obtain and configure capacity with minimal friction. It provides you with complete control of your computing resources and lets you run on Amazon's proven computing environment. **Amazon EC2 reduces the time required to obtain and boot new server instances to minutes, allowing you to quickly scale capacity**, both up and down, as your computing requirements change. **Amazon EC2 changes the economics of computing by allowing you to pay only for capacity that you actually use**. Amazon EC2 provides developers the tools to build failure resilient applications and isolate themselves from common failure scenarios.

Amazon EC2 presents a true virtual computing environment, allowing you to use web service interfaces to launch instances with a variety of operating systems, load

them with your **custom application environment**, manage your network's access permissions, and run your image using as many or few systems as you desire.

To use Amazon EC2, you simply:

- Select a pre-configured, template image to get up and running immediately. Or create an **Amazon Machine Image (AMI)** containing your applications, libraries, data, and associated configuration settings.
- Configure security and network access on your Amazon EC2 instance.
- Choose which instance type(s) and operating system you want, then start, terminate, and monitor as many instances of your AMI as needed, using the web service APIs or the variety of management tools provided.
- Determine whether you want to run in multiple locations, utilize static IP endpoints, or attach persistent block storage to your instances.
- Pay only for the resources that you actually consume, like instance-hours or data transfer.

Characteristics of Amazon EC2

1- ELASTIC – Amazon EC2 enables you to increase or decrease capacity within minutes, not hours or days. You can commission one, hundreds or even thousands of server instances simultaneously. Of course, because this is all controlled with web service APIs, **your application can automatically scale itself up and down depending on its needs**. You have the choice of multiple instance types, operating systems, and software packages. Amazon EC2 allows you to select a configuration of memory, CPU, instance storage, and the boot partition size that is optimal for your choice of operating system and application.

2- RELIABLE – Amazon EC2 offers a highly reliable environment where replacement instances can be rapidly and predictably commissioned. The service runs within Amazon's proven network infrastructure and datacenters. The Amazon EC2 Service Level Agreement commitment is 99.95% availability for each Amazon EC2 Region.

3- SECURE – Amazon EC2 provides numerous mechanisms for securing your computer resources. Amazon EC2 includes web service interfaces to configure firewall settings that control network access to and between groups of instances.

4- INEXPENSIVE – Amazon EC2 passes on to you the financial benefits of Amazon's scale. You pay a very low rate for the compute capacity you actually consume.

2- Microsoft Azure

Azure is Microsoft's cloud computing solution. It consists of **three parts: storage, scalable computing, and the base fabric to hold everything together across a heterogeneous network Azure's storage service** allows the user to choose between **three storage formats: BLOBs, tables, and queues**. The BLOBs are essentially containers that can hold up to 5 GB of binary data.

The BLOB names have no restrictions. Tables in Azure are not true relational tables, but more like Big table – tables hold entities, and an entity is a list of named values. While you lose the ability to query Azure tables like a true relational database, it is able to scale effectively across many machines. Azures queues are primarily designed for use with the computing service. Queues are what allow different applications a user is running to communicate with each other. For example, a user may have designed a web front-end application that can

communicate with several worker applications to perform back-end processing. This application suite would use queues to exchange information between the web front-end and the various workers.

3- Open Source Cloud Platforms

An open source cloud is any ***cloud service or solution*** that is developed using open source technologies and software. This covers any public, private or hybrid cloud models providing SaaS, IaaS and PaaS that have been built and operate entirely on open source technologies.

Why an open-source cloud platform is a better option than a proprietary cloud platform. The most obvious answer is the cost: the licenses of proprietary solutions always involve higher price tags. Another important advantage is the flexibility and freedom to choose from a wide variety of frameworks, clouds, and services.

Proprietary platforms, on the other side, may tie you to the tools and services they own. In exchange, they offer certain advantages, such as commitment to SLAs (service-level agreements) and relieving you from hurdles such as testing and integration, but those advantages hardly overweight the benefits of openness.

The following many examples of **open-source cloud**:

Characteristics of the open source cloud

The open source cloud has the following characteristics:

- No vendor lock-in and there is seamless integration of the enterprise applications, products and systems developed/deployed by different organizations and vendors.
- The source code will be made available for the community, for adopters and end users to study and modify the software and to redistribute copies of either the original or the modified version. Source code will also be free from any royalty.
- With no vendor monopoly, the use of free and open standards is possible. With data transferability and open data formats, there are greater opportunities to share data across interoperable platforms.
- Adoption of open source software enhances the interoperability with other enterprise solutions because the reuse of recommended software stacks, libraries and components is possible.

4- Open Stack

What Is Open Stack?

OpenStack is a cloud operating system that controls large pools of compute, storage, and networking resources throughout a datacenter, all managed and provisioned through APIs with common authentication mechanisms.

A dashboard is also available, giving administrators control while empowering their users to provision resources through a web interface.

Beyond standard infrastructure-as-a-service functionality, additional components provide orchestration, fault management and service management amongst other services to ensure high availability of user applications.

- OpenStack is an open source project for creating and managing cloud infrastructure, including storage, compute power, and networking, as well as many related projects to help handle everything from identity management to database deployment.

- Big data and the Internet of Things are two users of cloud computing resources where many of the tools powering applications are being developed entirely in the open.

- And many more, from the traditional Linux / Apache / MySQL / PHP web server stack to everything from cloud storage applications to collaborative online editors.

Lecture Four

Virtualization

1- What is Virtualization?

One of the most important ideas behind cloud computing is scalability, and the key technology that makes that possible is virtualization. Virtualization, in its broadest sense, is the emulation (محاكاة) of one of more workstations/servers within a single physical computer. Put simply, virtualization is the emulation of hardware within a software platform. This allows a single computer to take on the role of multiple computers. This type of virtualization is often referred to as full virtualization, allowing one physical computer to share its resources across a multitude of environments. This means that a single computer can essentially take the role of multiple computers. However, virtualization is not limited to the simulation of entire machines. There are many different types of virtualization, each for varying purposes. Although the physical locations of data may be scattered across a computers RAM and Hard Drive, the process of virtual memory makes it appear that the data is stored contiguously and in order. RAID (Redundant Array of Independent Disks) is also a form of virtualization along with disk partitioning, processor virtualization and many other virtualization techniques.

Virtualization allows the simulation of hardware via software. For this to occur, some type of virtualization software is required on a physical machine. The most well known virtualization software in use today is VMware. VMware will simulate the hardware resources. An operating system and associated applications can then be installed on this virtual machine, just as would be done on a physical machine. Multiple virtual machines can be installed on a single physical machine, as separate entities. This eliminates any interference between the machines, each operating separately. Although virtualization technology has been around for many

years, it is only now beginning to be fully deployed. One of the reasons for this is the increase in processing power and advances in hardware technology. As the benefits of virtualization are realized, we can observe the benefits to a wide range of users, from IT professionals, to large businesses and government organizations.

There are four main objectives to virtualization:

• Increased use of hardware resources;

• Reduced management and resource costs;

• Improved business flexibility;

• Improved security and reduced downtime.

1- Increased use of Hardware Resources

With improvements in technology, typical server hardware resources are not being used to their full capacity. On average, only 5-15% of hardware resources are being utilized. One of the goals of virtualization is to resolve this problem. By allowing a physical server to run virtualization software, a server's resources are used much more efficiently. This can greatly reduce both management and operating costs. For example, if an organization used 5 different servers for 5 different services, instead of having 5 physical servers, these servers could be run on a single physical server operating as virtual servers.

2- Reduced Management and Resource Costs

Due to the sheer number of physical servers/workstations in use today, most organizations have to deal with issues such as space, power and cooling. Not only is this bad for the environment but, due to the increase in power demands, the construction of more buildings etc is also very costly for businesses. Using a virtualized infrastructure, businesses can save large amounts of money because they require far fewer physical machines.

3- Improved Business Flexibility

Whenever a business needs to expand its number of workstations or servers, it is often a lengthy and costly process. An organization first has to make room for the physical location of the machines. The new machines then have to be ordered in, setup, etc. This is a time consuming process and wastes a business's resources both directly and indirectly. Virtual machines can be easily setup. There are no additional hardware costs, no need for extra physical space and no need to wait around. Virtual machine management software also makes it easier for administrators to setup virtual machines and control access to particular resources, etc.

4- Improved Security and Reduced Downtime

When a physical machine fails, usually all of its software content becomes inaccessible. All the content of that machine becomes unavailable and there is often some downtime to go along with this, until the problem is fixed. Virtual machines are separate entities from one another. Therefore if one of them fails or has a virus, they are completely isolated from all the other software on that physical machine, including other virtual machines. This greatly increases security, because problems can be contained. Another great advantage of virtual machines is that they are not hardware dependent. What this means is that if a server fails due to a hardware fault, the virtual machines stored on that particular server can be migrated to another server. Functionality can then resume as though nothing has happened, even though the original server may no longer be working.

What is Virtualization in Cloud Computing?

Virtualization in Cloud Computing is making a virtual platform of server operating system and storage devices. This will help the user by providing multiple machines

at the same time it also allows sharing a single physical instance of resource or an application to multiple users. Cloud Virtualizations also manage the workload by transforming traditional computing and make it more scalable, economical and efficient. Virtualizations in Cloud Computing rapidly integrating the fundamental way of computing. One of the important features of virtualization is that it allows sharing of applications to multiple customers and companies.

2- Types of Virtualization in Cloud Computing

- **OS Virtualization**

  Operating system virtualization (OS virtualization) is a server virtualization technology that involves tailoring a standard operating system so that it can run different applications handled by multiple users on a single computer at a time. The operating systems do not interfere with each other even though they are on the same computer.

  In OS virtualization, the operating system is altered so that it operates like several different, individual systems. The virtualized environment accepts commands from different users running different applications on the same machine. The users and their requests are handled separately by the virtualized operating system.

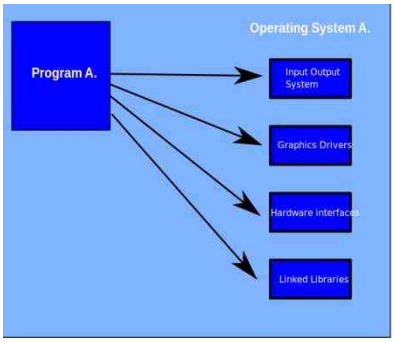
- **Application Server Virtualization**

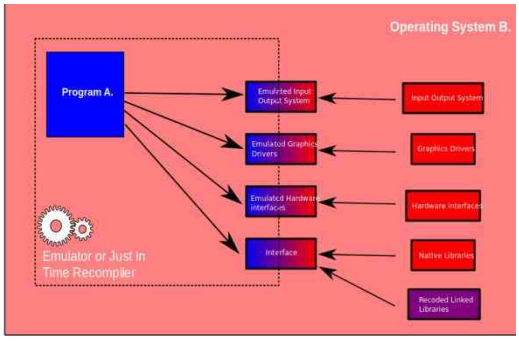
Application Server Virtualization also referred as 'Advanced Load Balancing' it enables IT departments to balance workloads of an application in an agile way. It spreads applications across servers and servers across applications. It also enables to manage the servers as a single instance. ASV gives a better network security compliance as only one server is visible to the public while the rest are hidden behind a reverse proxy network security appliance.

- **Application virtualization**

Application virtualization is the process by which a computer program is completely segregated(مفصول)from the underlying operating system. Whenever executed it behaves as

if it is directly interfacing with the original OS. Though it is not traditionally installed on the system hardware and can be isolated as per convenience.





- **Server Virtualization**

Server virtualization is the process of dividing a physical server into multiple unique and isolated virtual servers by means of a software application. Each virtual server can run its own operating systems independently.

- **Hardware Virtualization**

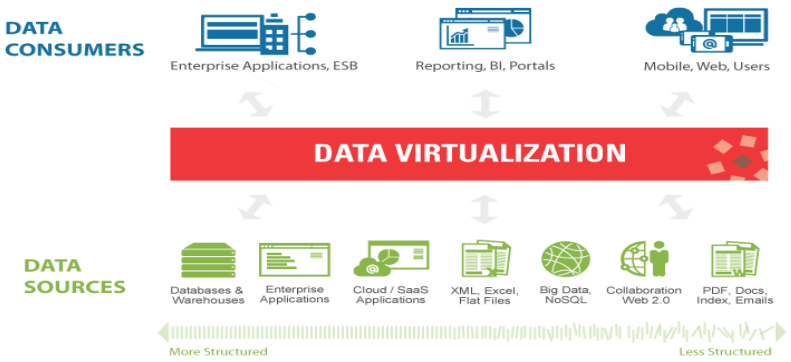
Hardware virtualization is the method used to create virtual versions of physical desktops and operating systems. It uses a virtual machine manager (VMM) called a hypervisor to provide abstracted hardware to multiple guest operating systems, which can then share the physical hardware resources more efficiently. Hardware virtualization offers many benefits, such as better performance and lower costs.

- **Storage Virtualization**

In storage virtualization in Cloud Computing, a grouping is done of physical storage which is from multiple network storage devices this is done so it looks like a single storage device. It can implement with the help of software applications and storage virtualization is done for the backup and recovery process. It is a sharing of the physical storage from multiple storage devices.

- **Data Virtualization**

Data virtualization enables to decrease the data errors and workloads. It also enables to simply manipulate data, where is it physically located and how is it formatted.

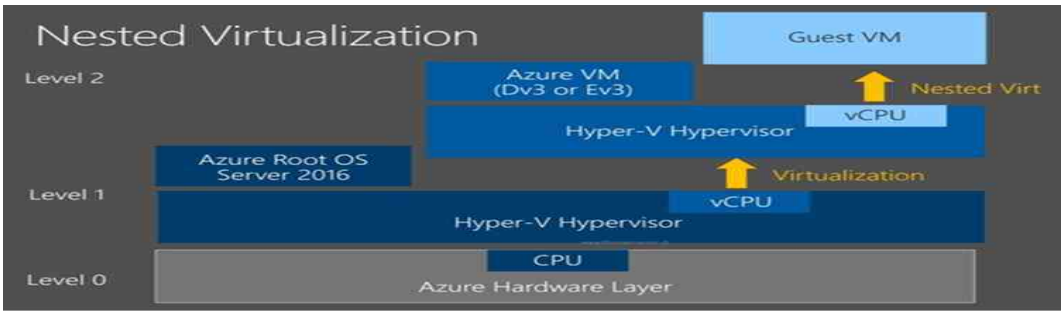


- **Desktop Virtualization**

The Phrase 'Work from Anywhere' is practically possible because of Desktop Virtualization it provides work convenience and security. It enables us to remotely access the data from anywhere and anytime through any device. It provides a lot of flexibility and feasibility for employees and the data is safe and secure as it is stored at a centralized location.

- **Nested Virtualization**

Nested Virtualization technology enables us to run one or more hypervisor within a virtual machine for e.g. we can create a virtual machine using hardware virtualization and deploy application virtualization within that virtual machine.



- **Network Virtualization**

What is network virtualization?

Network Virtualization (NV) refers to abstracting network resources that were traditionally delivered in hardware to software. NV can combine multiple physical networks to one virtual, software-based network, or it can divide one physical network into separate, independent virtual networks.

Network virtualization software allows network administrators to move virtual machines across different domains without reconfiguring the network. The software creates a network overlay that can run separate virtual network layers on top of the same physical network fabric.

Why network virtualization?

Network virtualization is rewriting the rules for the way services are delivered, from the software-defined data center (SDDC), to the cloud, to the edge. This approach moves networks from static, inflexible, and inefficient to dynamic, agile, and optimized. Modern networks must keep up with the demands for cloud-hosted, distributed apps, and the increasing threats of cybercriminals while delivering the speed and agility you need for faster time to market for your applications. With network virtualization, you can forget about spending days or weeks provisioning the infrastructure to support a new application. Apps can be deployed or updated in minutes for rapid time to value.

Benefits of Network Virtualization

Network virtualization helps organizations achieve major advances in speed, agility, and security by automating and simplifying many of the processes that go

into running a data center network and managing networking and security in the cloud. Here are some of the key benefits of network virtualization:

- Reduce network provisioning time from weeks to minutes
- Achieve greater operational efficiency by automating manual processes
- Place and move workloads independently of physical topology
- Improve network security within the data center

Types of network virtualization:

There are two types of network virtualization:

Internal network: Internal network virtualization: A virtualized internal network is a network that is restricted to one machine only. Hence it is also called "network in a box." It is essential to improve the efficiency of the network as communication over a network interface – which is also virtual – is allowed for communication.

External network: In the external network, at least one local network is subdivided or joined into the virtual network. To improve the effectiveness of big corporate networks or data center is the goal.

3- Virtualization of Resources

Anything required for the execution of a program is called a ***resource.*** The processor, memory, displays, mice, keyboards, disk storage, printers, and networks are all examples of resources. The primary functions of an operating system are management of resources and virtualization of resources. Part of the management is implicit in the virtualization.

This web presentation first takes a more careful look at the meaning of virtualization. Then it examines how the concept applies to various resources. Finally, it examines two principal mechanisms used in virtualization and how these mechanisms are used for various resources.

Virtualizing system specific resources such as "storage volumes, name spaces and the network resources" is known as resource virtualization.

There are various approaches to perform resource virtualization. Some of them are,

• Aggregating many individual components into larger resource pool.

• Grid computing or computer clusters where multiple discrete computers are combined to form a large supercomputer with enormous resources.

• partitioning a single resource such as disk space into number of smaller and easily accessible resources of same type.

4-Virtual Machine Monitor (VMM)

A Virtual Machine Monitor (VMM) is a software program that enables the creation, management and governance of virtual machines (VM) and manages the operation of a virtualized environment on top of a physical host machine.

VMM is also known as Virtual Machine Manager and Hypervisor. However, the provided architectural implementation and services differ by vendor product.

5- Virtual Machine (VM)

A virtual machine, commonly shortened to just VM, is no different than any other physical computer like a laptop, smart phone, or server. It has a CPU, memory, disks to store your files, and can connect to the internet if needed. While the parts that make up your computer (called hardware) are physical and tangible, VMs are often thought of as virtual computers or software-defined computers within physical servers, existing only as code.

6- What is a hypervisor?

A hypervisor is a software layer that creates and runs many isolated virtual machines (VMs) over single hardware, also known as a virtual machine monitor or VMM, is software that creates and runs virtual machines (VMs). A hypervisor allows one host computer to support multiple guest VMs by virtually sharing its resources, such as memory and processing.

There two major features of hypervisors:

1- Partitioning

Hypervisors partition the underlying hardware. Partitioning is a method for efficiently using an abundance of hardware resources by enabling multiple independent software payloads to run concurrently on the same hardware.

2- Resource Distribution

Hypervisors manage independent virtual machines by distributing resources like memory, network bandwidth, etc. among them.

7- The Xen Hypervisor:

The Xen hypervisor, sometimes simply called a virtual machine monitor, is an open source software program that coordinates the low-level interaction between virtual machines and physical hardware.

Para virtualization

is a virtualization technique that provides an interface to virtual machines that are similar to their underlying hardware. In para virtualization, the guest operating system is explicitly ported before installing a virtual machine because a non-tailored guest operating system cannot run on top of a virtual machine monitor (VMM).

8- What is VMware?

Virtualization software creates an abstraction layer over computer hardware that allows the hardware elements of a single computer— processors, memory, storage, and more— to be divided into multiple virtual computers, commonly called virtual machines (VMs). Each virtual machine runs its own operating system (OS) and behaves like an independent computer, even though it is running on a portion of the actual underlying computer hardware.

As you can imagine, virtualization enables more efficient utilization of computer hardware and enables a greater return on an organization’s hardware investment. It also enables cloud providers— public or private— to serve more users with their existing physical computer hardware.

VMware’s virtualization products are now a crucial part of many enterprises' IT infrastructures.

Lecture Five

Application and Programming of Cloud Computing

1- Applications of Cloud Computing

Cloud computing, in the simplest way, is said to be the next stage in the evolution of the Internet. Cloud computing can make it possible to access applications from anywhere. In cloud computing, the virtualization technique provides good support to resource utilization.

1) Mobile Cloud Computing

mobile cloud computing refers to an infrastructure where data storage and data processing happen outside the device. Mobile cloud application gives this kind of opportunity to computing power and storage of data away from mobile phones.

2) Healthcare or E-health

which employs wireless and mobile technologies for the attainment of healthrelated goals, can prove to be the next big thing in the field of delivering health services all over the world. A number of aspects are responsible for bringing about this transformation. These comprise rapid breakthrough in the field of mobile applications, the increase in opportunities for the amalgamation of present e-health services with mobile health, and persistent advancements in the expansion of mobile cellular network.

3) Cloud Gaming Cloud gaming

Also called gaming on demand, is a kind of online gaming. Presently, there are two varieties of cloud gaming: ***cloud gaming involving video streaming*** and ***cloud gaming involving file streaming.*** Cloud gaming focuses on providing continuous and undeviating play ability to end users across different devices. Cloud gaming

has superiority with respect to quality as well as economy. Cloud gaming employs a system in which the games execute on cloud servers, and the end users connect via networked slim clients. The slim clients are portable and are easily ported to resource-restricted platforms such as cellular devices. Cloud gaming makes gaming ubiquitous, and developers can improve the games according to varying configurations of PCs.

4) Storage APIs

provide easy access to cloud storage**,** but through superior features, power and flexibility can be attained. APIs can be accessed via XML or JSON or other programming languages. Cloud storage can be used to access static objects as well as for data storage. Big Query and App Engine are some of the popular cloud storage services. Authentication, speed, and flexibility are among the advantages of accessing data using cloud storage services.

2- Programming languages for cloud computing

Cloud computing is the provision of computing services, such as servers, storage, databases, networks, software, analysis, intelligence and more, over the Internet to deliver faster innovation, flexible resources, and economies of scale.

It consists of several technologies that currently have a great impact on the employability of software developers. The cloud can be exploited in countless ways: software as a service, platform as a service or infrastructure as a service, among others.

Cloud computing has meant a shift from the traditional way technology resources are used. Some of its advantages have to do with lower cost, increased speed, global scale, higher productivity, and enhanced security.

The following cloud programming languages will help you stand out in the field of cloud programming:

Java

Java is not only a general-purpose programming language, as it has also positioned itself in cloud computing. Its popularity among developers is overwhelming, as it is used by more than 10 million programmers and executed in more than 15 billion terminals worldwide.

The versatility of the Java language allows it to be used in the design of applications for Android, desktop computers, websites, and games. This makes it suitable for almost any programming task.

Among the advantages that can be mentioned, these stand out:

- It is easy to learn.
- It is designed to be used without complications.
- It is object-oriented to create modular programs and reusable codes.
- It is platform-independent, so it can be easily moved from one computer system to another.

The ability to run the same program on many different systems makes Java run smoothly when it comes to cloud computing. Due to its robustness, ease of use, multi-platform capabilities and security features, it occupies a privileged position among programmers who design Internet solutions.

ASP.NET

Asp.Net is a programming language designed by Microsoft to create websites and web applications with many functions. It is characterized by offering high-end solutions with dynamic web pages that can be viewed in different browsers.

It allows to design reliable and reusable applications, so its frame is very popular and relatively easy to use. Some of its benefits are the following:

- It secures applications using built-in Windows authentication.
- It reduces long lines of code in the development of large applications.
- It creates dynamic web pages without inconveniences.
- It is language-independent and easy to implement.
- Applications are highly monitored and managed.
- It has its own built-in caching functions.
- Content and logic are separated to reduce inconvenience.

PHP

PHP is a programming language widely used for web development and cloud computing because it is easy to learn and manipulate. It is therefore popular when it comes to automating websites and other functions.

This language can run on UNIX and Windows servers and has a powerful output buffer. Its dynamism stands out when designing applications with dynamic elements.

This language can run on UNIX and Windows servers and has a powerful output buffer. PHP can be used with a large number of database management systems, so it runs on the most popular web servers and is available for many different operating systems. It is a completely object-oriented language and helps to build large and complex web applications.

Why should you learn it? Because it is cheap, safe, fast and reliable to develop web applications.

Python

Python stands out as a high-level language created to be readable without difficulties, so any beginner can start programming with this tool. In its almost 30 years of existence in addition to evolving, it has remained among the preferences of software engineers!

It is known as an attractive programming language that supports development possibilities in various fields, thanks to elements that simplify the creation of web applications, API, academic programming and data science.

Python combines several features that improve programming, such as the presence of third-party modules, extensive support libraries, open source and community development, ease of learning and available support, easy-to-use data structures, productivity, and speed.

Its implementation is done, among others, in the following fields:

- GUI-based desktop applications.
- Image processing and graphic design applications.
- Scientific and computational applications.

- Games.
- Web Frames and Applications.
- Business applications.
- Operating systems.
- Language development.

Learning Python ensures the possibility of getting a job for a long time, as it has now also demonstrated its impact as a programming language for cloud computing.

Ruby

Ruby is an ideal cloud computing programming language for beginners because it is easy to use and to master. It also offers significant benefits because it is a huge ecosystem.

Mastering Ruby opens many possibilities in the field of cloud computing because this language has abundant resources to develop different applications, as well as more than 60,000 libraries and frameworks to choose from. In addition, there is an active community of developers who help in the event of problems.

Lecture Six

Cloud Storage

What Is Cloud Storage? There are many detention below:

Cloud storage is a data deposit model in which digital information such as documents, photos, videos and other forms of media are stored on virtual or cloud servers hosted by third parties. It allows you to transfer data on an offsite storage system and access them whenever needed.

Cloud storage is a cloud computing model that allows users to save important data or media files on remote, third-party servers. Users can access these servers at any time over the internet. Also known as utility storage, cloud storage is maintained and operated by a cloud-based service provider.

From greater accessibility to data backup, cloud storage offers a host of benefits. The most notable being large storage capacity and minimal costs. Cloud storage delivers on-demand and eliminates the need to purchase and manage your own data storage infrastructure. With "anytime, anywhere" data access, this gives you agility, global scale and durability.

How Cloud Storage Works

Cloud storage works as a virtual data center. It offers end users and applications virtual storage infrastructure that can be scaled to the application's requirements. It generally operates via a web-based API implemented remotely through its interaction with in-house cloud storage infrastructure.

Cloud storage includes at least one data server to which a user can connect via the internet. The user sends files to the data server, which forwards the message to

multiple servers, manually or in an automated manner, over the internet. The stored data can then be accessed via a web-based interface.

To ensure the constant availability of data, cloud storage systems involve large numbers of data servers. Therefore, if a server requires maintenance or fails, the user can be assured that the data has been moved elsewhere to ensure availability.

Types of Cloud Storage

Cloud services have made it possible for anyone to store digital data and access it from anywhere. This means that cloud storage is essentially a virtual hard drive. From saving important data such as word documents, and video files, to accessing the cloud to process complex data and run applications – cloud storage is a versatile system. To decide which is the best cloud storage, the user needs to determine their use case/s first. Let's look at the different types of cloud storage solutions:

1. Private cloud storage

Private cloud storage is also known as enterprise or internal cloud storage. Data is stored on the company or organization's intranet in this case. This data is protected by the company's own firewall. Private cloud storage is a great option for companies with expensive data centers and can manage data privacy in-house. A major advantage of saving data on a private cloud is that it offers complete control to the user. On the other hand, one of the major drawbacks of private cloud storage is the cost and effort of maintenance and updates. The responsibility of managing private cloud storage lies with the host company.

2. Public cloud storage

Public cloud storage requires few administrative controls and can be accessed online by the user and anyone else who the user authorizes. With public cloud storage, the user/company doesn't need to maintain the system. Public cloud

storage is hosted by different solution providers, so there's very little opportunity for customizing the security fields, as they are common for all users. Amazon Web Services (AWS), IBM Cloud, Google Cloud, and Microsoft Azure are a few popular public cloud storage solution providers. Public cloud storage is easily scalable, affordable, reliable and offers seamless monitoring and zero maintenance.

3. Hybrid cloud storage

Hybrid cloud storage is a combination of private and public cloud storage. As the name suggests, hybrid cloud storage offers the best of both worlds to the user – the security of a private cloud and the personalization of a public cloud. In a hybrid cloud, data can be stored on the private cloud, and information processing tasks can be assigned to the public cloud as well, with the help of cloud computing services. Hybrid cloud storage is affordable and offers easy customization and greater user control.

4. Community cloud storage

Community cloud storage is a variation of the private cloud storage model, which offers cloud solutions for specific businesses or communities. In this model, cloud storage providers offer their cloud architecture, software and other development tools to meet the community's requirements. Any data is stored on the community-owned private cloud storage to manage the community's security and compliance needs. Community cloud storage is a great option for health, financial or legal companies with strict compliance policies.

Benefits and Challenges of Cloud Storage Adoption

The cloud is rapidly becoming the storage environment of choice for enterprises. 30% of all corporate data was stored on the cloud in 2015, which increased to 50% in 2020. The cloud storage market has also grown in tandem and is expected to be worth $137.3 billion by 2025, as per Markets and Markets. This is because the cloud offers several benefits over traditional on-premise storage systems.

Benefits of cloud storage

- **Flexibility and ease of access**: Cloud storage means that your data is not tied down to any one location. Various stakeholders can access assets stored on the cloud from a location and device of their choice without any download or installation hassles.
- **Remote management support**: Cloud storage also paves the way for remote management either by internal IT teams or by managed service providers (MSPs). They can troubleshoot without being present on-site, speeding up issue resolution.
- **Fast scalability**: A major benefit of cloud storage is that you can provision new resources with only a few clicks without the need for any additional infrastructure. When faced with an unprecedented increase in data volumes, this feature aids business continuity.
- **Redundancy for backup**: Data redundancy (i.e., replicating the same data in multiple locations) is essential for an effective backup mechanism. The cloud ensures your data is kept secure in a remote location in case of a natural disaster, accident, or cyberattack.
- **Long-term cost savings**: In the long-term, cloud storage can save you significantly in the costs of hardware equipment, storage facilities, power supply, and personnel, which are sure to multiply as your organization grows.

Challenges of cloud storage

While there are undeniable advantages of adopting cloud storage, there are a few cons to remember as well. By navigating these cons or challenges, you can arrive at a pragmatic cloud storage strategy that maximizes its benefits.

- **Risk of vendor lock-in**: If all your data is stored in a single public cloud platform, there's a risk of vendor lock-in and potential inflexibilities. Address this with a hybrid or multi-cloud blueprint where there is sufficient interoperability between environments.

- **Security issues around multi-tenancy**: Public cloud environments are shared by multiple tenants, which can multiply your security vulnerabilities. You can prevent this through cloud data protection and by leveraging the private cloud for sensitive data.
- **Fragmentation of IT landscape**: Unplanned cloud storage adoption can cause your IT landscape to become fragmented over time. That's why you need a detailed strategic blueprint outlining your short, mid, and long-term cloud roadmap.
- **Outage and downtime risk**: Cloud platforms managed by external providers could suffer from an outage, rendering the data and applications stored in these environments inaccessible. Service level agreements should specify downtime metrics, and you need additional redundancy for your most critical data.
- **Short-term budget overruns**: Cloud cost worries are extremely common, where data storage and storage processes occupy more space than estimated. A cloud resource management tool can help address this, giving you visibility and control.

Selecting the right cloud storage provider

Let's look at the most critical aspects businesses need to consider when selecting a cloud storage provider.

- **Storage space:** The amount of data a business processes determines the requirement for storage space. A small organization (around 250 employees) could opt for public cloud storage services, which offer employees storage space of over 15 GB each. It is recommended to compare various public cloud storage pricing plans before signing the deal.
- **Maintenance & uptime:** Cloud servers need to be maintained to make sure the data stored is secure. However, downtimes and network failures can occur anytime. Therefore, understanding the maintenance and uptime needed by cloud service providers is essential. Organizations should ask their chosen cloud service providers to demonstrate their downtime plans and run checks before buying any cloud solution.
- **Security:** If data is compromised, then cloud storage comes in handy as a useful backup. There is no guarantee, however, that cloud storage

providers are safe from security threats. Understanding the security measures in place at the cloud storage provider is important. Two main factors need to be considered for security: the physical security of the cloud solution provider's servers and the level of encryption applied to the data stored.

- **Speed:** The speed of downloads from the cloud has a major impact on businesses and their ability to process critical data. If cloud storage providers place a cap on the download speed, retrieving data and running applications will take longer. Therefore, organizations need to gauge the cloud storage download speeds of a provider before buying any storage space.

Lecture Seven

Advanced Cloud Technologies

1- Green Cloud Computing

Green computing is the environmentally responsible and eco-friendly use of computers and their resources. In broader terms, it is also defined as the study of designing, manufacturing/engineering, using and disposing of computing devices in a way that reduces their environmental impact. Many IT manufacturers and vendors are continuously investing in designing energy efficient computing devices, reducing the use of dangerous materials and encouraging the recyclability of digital devices and paper. Green computing is also known as green information technology (green IT).

Green computing, or green IT, aims to attain economic viability and improve the way computing devices are used. Green IT practices include the development of environmentally sustainable production practices, energy efficient computers and improved disposal and recycling procedures.

Green Cloud Computing not only provides effective processing and infrastructure usage but also saves energy. Green computing is a method of reducing the consumption of computing resources as well as the negative consequences on the environment.

Green cloud computing is the process of implementing this architecture in data centers. Every field is reacting to rising energy usage and attempting to incorporate environmentally friendly ways in their fields. Given its numerous advantages, cloud computing was a welcome move for many IT organizations, and it also benefited the environment by lowering the energy consumption caused by the companies' data centers. Cloud computing, on the other hand, eliminates the necessity for a separate data center. It consolidated all processing and storage

requirements for a certain zone into a single data center with excellent security, decreasing data theft and loss.

Green Cloud Architecture is the result of these processes, which lead to both energy efficiency and a mindful understanding of carbon emissions. The purpose of constructing a Green Area is to reduce energy consumption.

Benefits of Green Cloud Computing

1- Reduced Cost 2- Automatic Updates 3- Green Benefits of Cloud computing 4- Remote Access 5- Disaster Relief 6- Self-service provisioning 7- Scalability 8- Reliability and fault-tolerance 9- Ease of Use 10- Skills and Proficiency 11- Response Time 12- Increased Storage 13 –Mobility.

2- Mobile cloud computing

uses cloud computing to deliver applications to mobile devices. These mobile apps can be deployed remotely using speed and flexibility and development tools. Mobile cloud applications can be built or revised quickly using cloud services. They can be delivered to many different devices with different operating systems, computing tasks, and data storage. Thus, users can access applications that could not otherwise be supported.

Mobile Cloud Computing applications have the following advantages:

1. Extended battery life.
2. Improvement in data storage capacity and processing power.
3. Improved synchronization of data due to “store in one place, accessible from anywhere” platform theme.
4. Improved reliability and scalability.
5. Ease of integration.

There are two types of applications of mobile cloud computing (MCC) that are almost similar. These are as follows:

1. Mobile Cloud application: It is defined as a model where processing is done in the cloud, and the storage is also in the cloud, and the presentation platform is the mobile device. For this, the internet connection should have to reliable and cell-phone to run a browser. It enables to use the smartphone with cloud technology with the following characteristics:

1. A smart-phone has a recognizable Operating System.
2. It provides advanced calling i.e. video calling and conferencing features.
3. Smart-phone must have the capability to run the installable application
4. Messaging features are available.
5. A smart-phone must have a persistent and proper internet connection.

2. Mobile Web Services:

In Mobile Web Services mobile devices consume more network traffic. It may lead to some challenges for web services such as mismatch of resolution and details of desktop computers. The device needs to know about that service and the way it can be accessed to use any web-service so that the mobile device can transmit specific information about the condition of the device and the user. Enabling Mobile Web Services are as follows:

1. Enables web-service systems with web services.
2. Enables in-built external services.
3. Enable the rest protocol.
4. Enables XML-RPC protocols.
5. Enables the capabilities to authenticate user roles.

2-Mobile Cloud Computing

Mobile cloud computing is the combination of cloud computing and mobile networks to bring benefits for mobile users, network operators, as well as cloud providers. Cloud computing exists when tasks and data are kept on the Internet rather than on individual devices, providing on-demand access.

Mobile apps may use the cloud for both app development as well as hosting. A number of unique characteristics of hosted apps make the mobile cloud different

from regular cloud computing. Mobile apps may be more reliant upon the cloud to provide much of the computing, storage, and communication fault tolerance than regular cloud computing does.

Benefits of Mobile Cloud Computing

1-Extending battery lifetime

2-Improving data storage capacity and processing power

3- Improving reliability.

Lecture Eight

Cloud Security

• Cloud Security Risks

1. Theft or loss of intellectual property

An outstanding 21% of data uploaded by companies to cloud-based file management services contain sensitive data. The analysis that was done by Skyhigh found that companies face the risk of having their intellectual property stolen.

Weak cloud security measures within an organization include storing data without encryption or failing to install multi-factor authentication to gain access to the service.

2. Compliance Violations

Organizations can quickly go into a state of non-compliance, which puts them in the risk of serious repercussions. BYOC is one of the ways companies often violate one of the tenets and regulations instituted by the government or Industrial Corporation. Whether it is FERPA for confidential student documents or HIPAA for private patient records, most firms operate under a regulatory body.

A state of non-compliance with any of these bodies lands companies in a lot of trouble. To mitigate this risk, companies should always use authentication systems for all the sensitive data in the firm.

Even tech giants like Facebook have been victims of resource exploitation due to user error or misconfigurations. Keeping employees informed about the dangers and risks of data sharing is of at most importance.

3. Malware attacks

Cloud services can be a vector for data exfiltration. As technology improves, and protection systems evolve, cyber-criminals have also come up with new techniques to deliver malware targets. Attackers encode sensitive data onto video files and upload them to YouTube.

Skyhigh reports that cyber-criminals use private twitter accounts to deliver the malware. The malware then exhilarates sensitive data a few characters at a time. Some have also been known to use phishing attacks through file-sharing services to deliver the malware.

4. End-user control

When a firm is unaware of the risk posed by workers using cloud services, the employees could be sharing just about anything without raising eyebrows. Insider threats have become common in the modern market. For instance, if a salesman is about to resign from one firm to join a competitor firm, they could upload customer contacts to cloud storage services and access them later. The example above is only one of the more common insider threats today.

Many more risks are involved with exposing private data to public servers.

5. Contract breaches with clients and/or business partners

Contracts restrict how business partners or clients use data and also who has the authorization to access it. Employees put both the firm and themselves at risk of legal action when they move restricted data into their cloud accounts without permission from the relevant authorities.

Violation of business contracts through breaching confidentiality agreements is common. This is especially when the cloud service maintains the right to share all data uploaded with third parties.

6. Shared vulnerabilities

Cloud security is the responsibility of all concerned parties in a business agreement. From the service provider to the client and business partners, every stakeholder shares responsibility in securing data. Every client should be inclined to take precautionary measures to protect their sensitive data.

While the major providers have already taken steps to secure their side, the more delicate control measures are for the client to take care of. Dropbox, Microsoft, Box, and Google, among many others, have adopted standardized procedures to secure your data. These measures can only be successful when you have also taken steps to secure your sensitive data.Key security protocols such as protection of user passwords and access restrictions are the client's responsibility.

7. Attacks to deny service to legitimate users

You are most likely well aware of cyber-attacks and how they can be used to hijack information and establish a foothold on the service provider's platform. Denial of service attacks, unlike cyber-attacks, does not attempt to bypass your security protocol. Instead, they make your servers unavailable to illegitimate users.

8. Insecure APIs

API or Application Programming Interfaces offer users the opportunity to customize their cloud service experience. APIs can, however, be a threat to cloud security due to their very nature. Apart from giving firms the ability to customize the features on their cloud service provider, they also provide access, authenticate, and effect encryption.

As APIs evolve to provide better service to users, they also increase their security risk on the data client's store. APIs provide programmers with the tools

to integrate their programs with job-critical applications. YouTube is one of the sites with an API that allows users to embed YouTube videos into their apps or websites. Despite of this great opportunity that the technology presents the user, it also increases the level of vulnerability to their data. Cyber-criminals have more opportunities to take advantage of thanks to these vulnerabilities.

9. Loss of data

Data stored on cloud servers can be lost through a natural disaster, malicious attacks, or a data wipe by the service provider. Losing sensitive data is devastating to firms, especially if they have no recovery plan. Google is an example of the big tech firms that have suffered permanent data loss after being struck by lightning four times in its power supply lines.

Amazon was another firm that lost its essential customer data back in 2011. An essential step in securing data is carefully reviewing the terms of service of your provider and their back up procedures. The backup protocol could relate to physical access, storage locations, and natural disasters.

10. Diminished customer trust

It is inevitable for customers to feel unsafe after data breach concerns at your firm. There have been massive security breaches that resulted in the theft of millions of customer credit and debit card numbers from data storage facilities.

The breaches reduce customer trust in the security of their data. A breach in an organization's data will inevitably lead to a loss of customers, which ultimately impacts the firm's revenue.

11. Increased customer agitation

A growing number of cloud service critics are keen to see which service providers have weak security protocols and encourage customers to avoid them. Most of these critics are popular around the internet and could lead to a poor impression of your firm in a few posts.
If your customers suspect that their data is not safe in your hands, they not only move to competitor firms but also damage your firm's reputation.

• Operating System Security

Security refers to providing a protection system to computer system resources such as CPU, memory, disk, software programs and most importantly data/information stored in the computer system. If a computer program is run by an unauthorized user, then he/she may cause severe damage to computer or data stored in it. So a computer system must be protected against unauthorized access, malicious access to system memory, viruses, worms etc.

OS security encompasses many different techniques and methods which ensure safety from threats and attacks. OS security allows different applications and programs to perform required tasks and stop unauthorized interference. OS security may be approached in many ways, including adherence to the following:

- Performing regular OS patch updates
- Installing updated antivirus engines and software
- Scrutinizing all incoming and outgoing network traffic through a firewall
- Creating secure accounts with required privileges only (i.e., user management)

- **Virtual Machine Security**

Virtualization - A technology that has an enormous effect in today's IT world. It is a technique that divides a physical computer into several partly or completely isolated machines commonly known as virtual machines (VM) or guest machines. Multiple of these virtual machines can run on a host computer, each possessing its own operating system and applications. This gives an illusion to the processes on these virtual machines as if they are running on a physical computer, but in reality they are sharing the physical hardware of the host machine. The software that allows multiple operating systems to use the hardware of the physical machine is called a hypervisor or a control program. Hypervisors sit between the operating system of the host machine and the virtual environment. There are various virtualization technologies available in the market, having their own merits and demerits. In non-virtual environment, the applications running on the machine can see each other, and in some cases can even communicate with each other, whereas in virtual environment the programs running in one guest machine are isolated from the programs running in another guest machine, in other words guest machines "provide what appear to be independent coexisting computers" to their running programs. The degree of isolation should be strong enough that the vulnerabilities in one virtual machine should not affect either the virtual machines or the underlying host machine. The computer that is being virtualized is of no difference from the computer that is not virtualized.

The virtualized environment is vulnerable to all the traditional attacks and exploits that are common to the normal environment. The case is even worse

in the virtualized environment, where there are several virtual computers running. The security expectations are higher in here because "there are more systems to protect", more possible points of entry, more holes to patch and there are more interconnection points in the virtualized environment. Attackers and Hackers are already been actively developing new malware programs for virtual machine environment. "Root kit infections, malware that detects a virtual environment and modifies itself accordingly" are some of them. "Low-level hypervisor attacks and deployment of malicious virtual systems" are few possible attacks that are unique to this environment. On the other hand new security protection programs are also emerging in the market every now and then from different vendors, but most of these security solutions are mainly focused on hypervisor. Since hypervisor is a new layer between the host's OS and virtual environment, it creates new opportunities for the malicious programs. And more over, hypervisor is basically a software program, so it has all the traditional software bugs and the security vulnerabilities as any software have. One of such product that hits the market recently is SHype, a new secure hypervisor that binds security policies to the virtual environment. A good debate on recent security solutions can be found on. However, virtual machine security is more than just deploying a secure hypervisor to the environment. Virtualization technologies are still evolving. Newer versions with added features are introduced before the security consequences of the older version has been fully studied. This work analyzes the general security threats in a virtual environment and suggests possible solutions for few of the mentioned threats.

- **Security Visualization**

The term *Security Visualization* refers to the concept of using visualization for security measures. For example, visualizing unauthorized access, information leakage, and tracking malicious web traffic. Other purposes include data visual analytics and threat intelligence, i.e., tracking and monitoring of security related events. For cloud technologies, adding the concept of security visualization to existing cloud services creates a "trust" relationship between the services used and the users. Although cloud technologies offer visualization features, it is for the purpose of analytics and reporting. The need for real-time security visualization framework to enable users to see and observe data movement and even being alerted by the service of a suspicious threat is crucial. Whether its public or private cloud, high-performance parallel computing with the cloud environment and cloud technologies by vendors allows users to provision large quantities of instances efficiently. Cloud technologies are expanding throughout the Internet realm, offering a wide range of services beginning from business management platforms, data analytics tools to facilitating efficient means for Internet of Things (IoT). However, security has become a major concern for every cloud provider and cloud user. For providers, implementing proper secure platforms is a priority whereas for users, the ever growing thoughts of how secure their data is on the cloud is their main concern. Therefore, there are always great needs to implement security applications, tools and techniques specifically targeting cloud providers and users, for example, secure tracking and monitoring of data movement and processes in SaaS infrastructure.