P.K.A.I.E.T
We Excel Where We Stand

CLOUD COMPUTING

6th Semester

COMPUTER SCIENCE & ENGG.

Prepared By: Mr. Prasanta ku. Satapathy
(Sr. Lecturer)

CLOUD COMPUTING

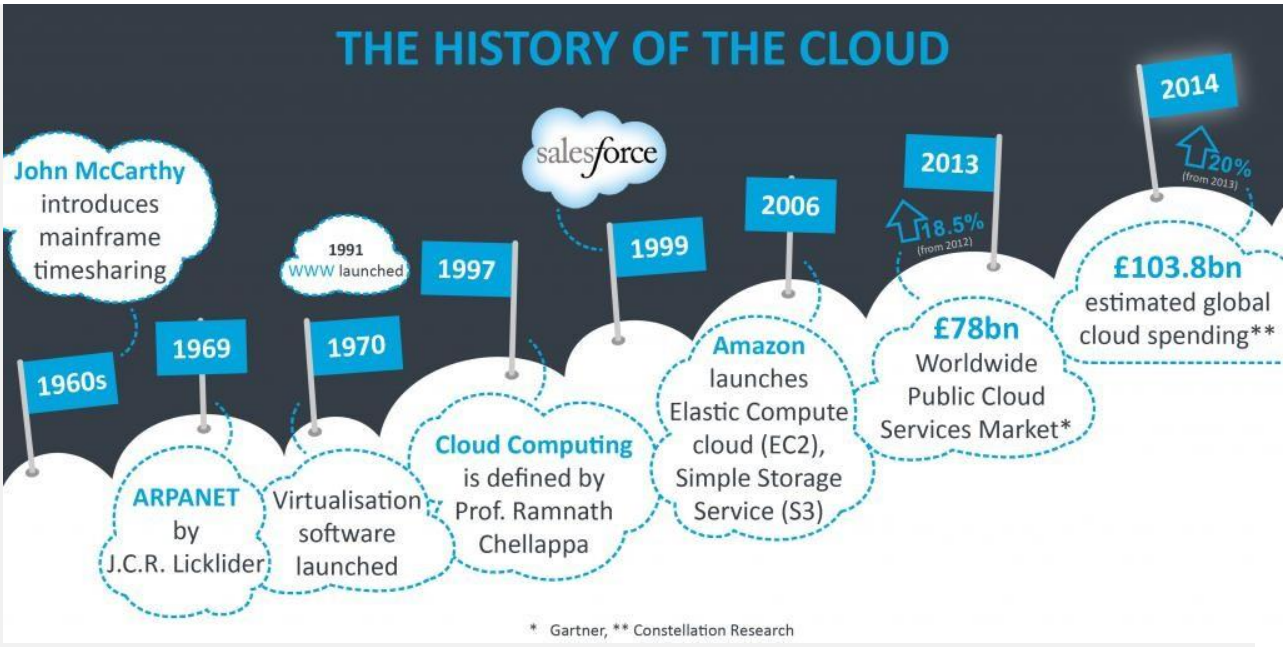
SL.NO	Name of the Chapter as per the syllabus	No.of periods as Per the syllabus	No. of periods Actually needed	Expected marks
1	INTRODUCTION TO CLOUD COMPUTING	05	**05**	**15**
2	CLOUD COMPUTING ARCHITECTURE	08	**05**	**10**
3	SCALABILITY AND FAULT TOLERANCE	08	**06**	**15**
4	CLOUD MANAGEMENT AND VIRTUALISATION TECHNOLOGY	08	**07**	**15**
5	VIRTUALISATION	08	**10**	**10**
6	CLOUD SECURITY	08	**06**	**10**
7	CLOUD COMPUTING SECURITY ARCHITECTURE	05	**09**	**15**
8	MARKET BASED MANAGEMT OF CLOUDS	05	**04**	**10**
9	HADOOP	05	**03**	**10**
Total:		**60**	**55**	**110**

Prasanta ku.Satapathy

Chapter -1

Introduction to cloud computing

History of cloud computing



EARLY 1960S

The computer scientist John McCarthy, come up with concept of timesharing, and enabling Organization to simultaneously use an expensive mainframe. This computing is described as a significant contribution to the development of the Internet, and a pioneer of Cloud computing.

IN 1969

The idea of an “Intergalactic Computer Network” or “Galactic Network” (a computer networking concept similar to today’s Internet) was introduced by J.C.R. Licklider, who was responsible for enabling the development of ARPANET (Advanced Research Projects Agency Network). His vision was for everyone on the globe to be interconnected and being able to access programs and data at any site, from anywhere.

IN 1970

Using virtualization software like VMware. It become possible to run more than one Operating System simultaneously in an isolated environment. It was possible to run a completely different Computer (virtual machine) inside a different Operating System.

IN 1997

The first known definition of the term “Cloud Computing” seems to be by Prof. Ramnath Chellappa in Dallas in 1997 – “A computing paradigm where the boundaries of computing will be determined by economic rationale rather than technical limits alone.”

IN 1999

The arrival of Salesforce.com in 1999 pioneered the concept of delivering enterprise applications via simple website. The services firm covered the way for both specialist and mainstream software firms to deliver applications over the Internet.

IN 2003

The first public release of Xen, which creates a Virtual Machine Monitor (VMM) also known as a hypervisor, a software system that allows the execution of multiple virtual guest operating systems simultaneously on a single machine.

IN 2006

In 2006, Amazon expanded its cloud services. First wa

s its Elastic Compute cloud (EC2), which allowed people to access computers and run their own applications on them, all on the cloud. Then they brought out Simple Storage Service (S3). This introduced the pay-as-you-go model to both users and the industry as a whole, and it has basically become standard practice now.

IN 2013

The Worldwide Public Cloud Services Market totalled £78bn, up 18.5 per cent on 2012, with IaaS (infrastructure-as-a-service) the fastest growing market service.

IN 2014

In 2014, global business spending for infrastructure and services related to the cloud will reach an estimated £103.8bn, up 20% from the amount spent in 2013 (Constellation Research).

Vision of Cloud Computing

We have seen how far Cloud computing has progressed in the short time since its initiation. Now lets have a look on what may become of Cloud computing technology in the future.

Following are few forecasts of what we might expect in the coming future of Cloud computing:

- Cloud computing will become even more prominent in the coming years with rapid, continued growth of major global cloud data centres.
- 50% of all IT will be in the cloud within the next 5 – 10 years.
- The security and reliability of cloud computing will continue to evolve, ensuring that data will be even more secure with numerous techniques employed.
- We will not even consider ‘cloud’ as the key technology, instead we will focus on the services and applications that it enables.

characteristics of Cloud Computing:

1. Resources Pooling

cloud service provider can share resources among several clients, providing everyone with a different set of services as per their requirements. It is a multi-client strategy that can be applied to data storage services, processing services, and bandwidth provided services. The administration process of allocating resources in real-time doesn't conflict with the client's experience.

2. On-Demand Self-Service

It is one of the significant and essential features of Cloud Computing. It enables the client to constantly monitor the server uptime, abilities, and allotted network storage. This is a fundamental characteristic of Cloud Computing, and a client can likewise control the computing abilities as per his needs.

3. Easy Maintenance

This is one of the best cloud characteristics. The servers are effortlessly maintained, and the downtime remains low or absolutely zero sometimes. Cloud Computing powered resources undergo several updates frequently to optimize their capabilities and potential. The updates are more viable with the devices and perform quicker than the previous versions.

4. Scalability And Rapid Elasticity

A key characteristic and benefit of cloud computing is its rapid scalability. This cloud characteristic enables cost-effective running of workloads that require a vast number of servers but only for a short period. Many clients have such workloads, which can be run very cost-effectively because of the rapid scalability of Cloud Computing.

5. Economical

This cloud characteristic helps in reducing the IT expenditure of the organizations. In Cloud Computing, the client needs to pay the

administration for the space they have used. There is no covered up or additional charge which needs to be paid. The administration is economical, and more often than not, some space is allotted for free.

6. Measured And Reporting Service

Reporting services are one of the many cloud characteristics that make it the best choice for organizations. Measuring & reporting service is helpful for both cloud providers and their clients. It enables both the provider and the client to monitor and report what services have been used and for what purpose. This helps in monitoring billing and ensuring the optimum usage of resources.

7. Security

Data security is one of the best characteristics of Cloud Computing. Cloud services create a copy of the data that is stored to prevent any form of data loss. If one server loses the data by any chance, the copy version is restored from the other server. This feature comes handy when several users work on a particular file in real-time and a file suddenly gets corrupted.

8. Automation

Automation is an essential characteristic of cloud computing. The ability of cloud computing to automatically install, configure, and maintain a cloud service is known as automation in cloud computing. In simple terms, it is the process of making the most of technology and reducing manual effort. However, to achieve automation in the cloud ecosystem is not so easy. It requires the installation and deployment of virtual machines, servers, and large storage. Upon successful deployment, these resources require constant maintenance as well.

9. Resilience

Resilience in cloud computing means the ability of the service to quickly recover from any disruption. A cloud’s resilience is measured by how fast its servers, databases, and network system restarts and

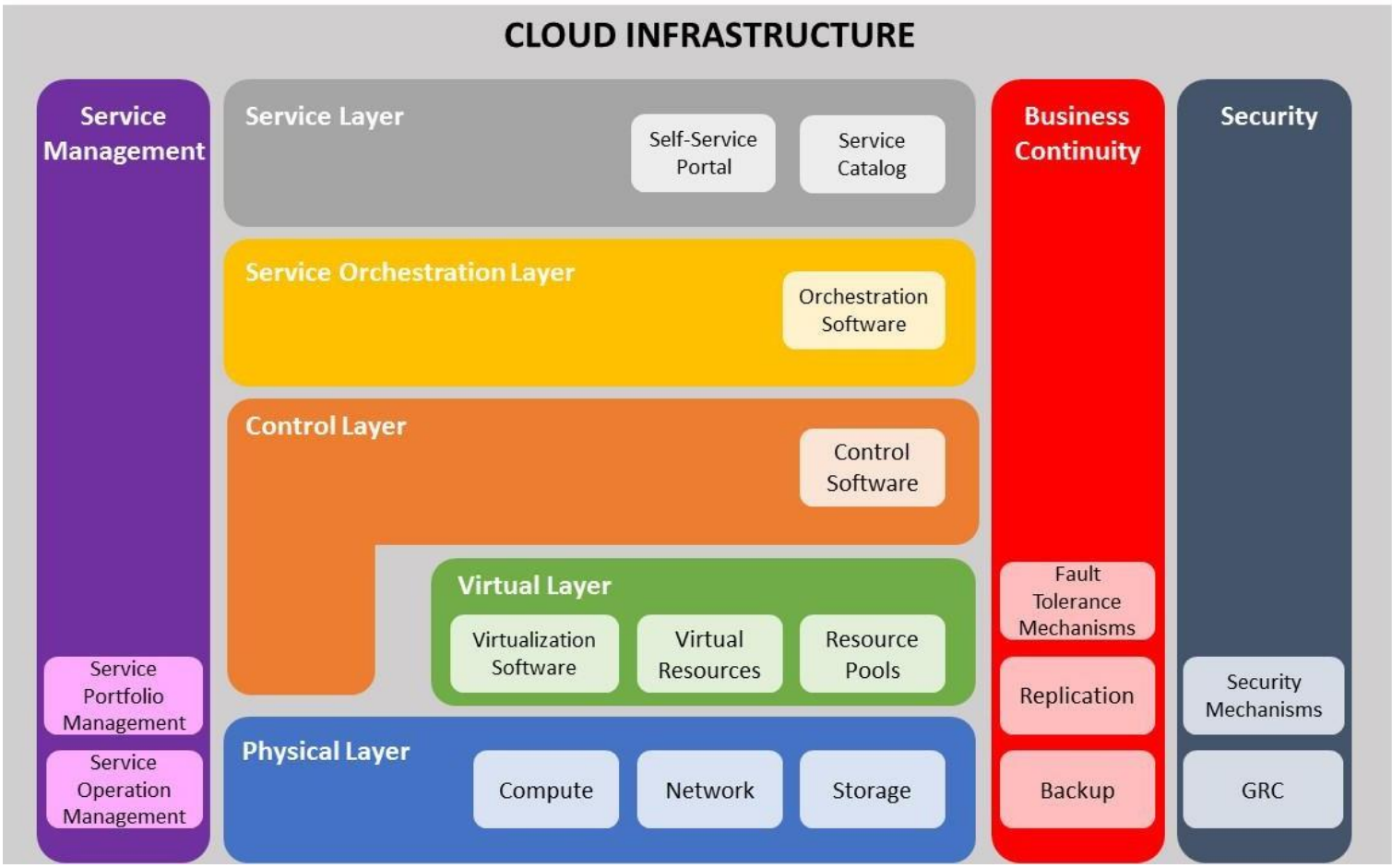
recovers from any kind of harm or damage. Availability is another major characteristic of cloud computing. Since cloud services can be accessed remotely, there is no geographic restriction or limitation when it comes to utilizing cloud resources.

10. Large Network Access

A big part of the cloud characteristics is its ubiquity. The client can access the cloud data or transfer the data to the cloud from any place just with a device and internet connection. These capacities are accessible everywhere in the organization and get to with the help of the internet. Cloud providers save that large network access by monitoring and guaranteeing different measurements that reflect how clients access cloud resources and data: latency, access time, data throughput, etc.

cloud computing íefeíence model

1he **cloud computing íefeíence model** is an abstíact **model** that chaíacteíizes and standaídizes the functions of a **cloud computing** enviíonment by paítitioning it into abstíaction layeís and cíoss-layeí functions. .....**1**he thíee cíoss-layeí functions aíe business continuity, secuíity, and seívicemanagement.


CLOUD INFRASTRUCTURE
Service Management
Service Layer
Self-Service Portal
Service Catalog
Service Orchestration Layer
Orchestration Software
Control Layer
Control Software
Virtual Layer
Virtualization Software
Virtual Resources
Resource Pools
Physical Layer
Compute
Network
Storage
Business Continuity
Fault Tolerance Mechanisms
Replication
Backup
Security
Security Mechanisms
GRC
Service Portfolio Management
Service Operation Management

cloud computing enviíonment

It is all about Il' and what Il' needs: diffeíent kinds of softwaíe and haídwaíe,pay-peí-use oí subscíiption-based seívices offeíed both thíough the Inteínet

and in íeal time. So, let's define the most common kinds of seívices whichusually íefeí to what we call **cloud computing**.

Availability - with loss less DR

Customers want their IT services be up and available at all times. But in reality, computers sometimes fail. This implies that the service provider should have implemented a reliable disaster recovery (DR) mechanism - where in the service provider can move the customer from one data center to another seamlessly and the customer does not even have to know about it.

2. Portability of Data & Applications

Customers hate to be locked into a service or a platform. Ideally a cloud offering must be able to allow customers to move out their data & applications from one service provider to another - just like customers can switch from one telephone service provider to another.

3. Data Security

Security is the key concern for all customers - since the applications and the data is reciding in the public cloud, it is the responsibility of the service provider for providing adequate security. In my opinion security for customer

4. Manageability

Managing the cloud infrastructure from the customer prespective must be under the control of the customer admin. Customers of Cloud services must be able to create new accounts, must be able to provision various services, do all the user account monitoring - monitoring for end user usage, SLA breaches, data usage monitoring etc. The end users would like to see the availability, performance and configuration/provisioning data for the set of infrastructure they are using in the cloud.

5. Elasticity

Customer on Cloud computing have a dynamic computing loads. At times of high load, they need greater amount of computing resources available to them on demand, and when the work loads are low, the computing resources are released back to the cloud pool. Customer expect the service provider to charge them for what they have actually used in the process.

6. Federated System

This implies that each of the cloud services must have an interface with other cloud services for load sharing & application interoperability.

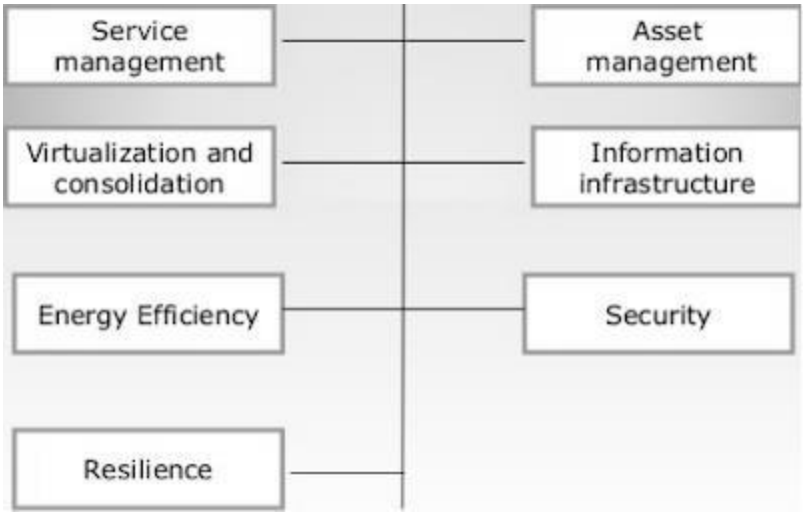
As on today, the integration issues are still being worked out, and there is no universal standards for creating interop between different cloud applications.

Closing Thoughts

Cloud services are still in its infancy and if cloud services were to attract large enterprise customers, then they need to do a lot more than today to address

data/application portability, federated scalable system, complete end-to-end interoperability and security issues.

Cloud and dynamic infrastructure



1. **Service management: This type of special facility or a functionality is provided to the cloud IT services by the cloud service providers. This facility includes visibility, automation and control to delivering the first class IT services.**

2. **Asset-Management: In this the assets or the property which is involved in providing the cloud services are getting managed.**

3. **Virtualization and consolidation: Consolidation is an effort to reduce the cost of a technology by improving its operating efficiency and effectiveness. It means migrating from large number of resources to fewer one, which is done by virtualization technology.**

4. **Information Infrastructure: It helps the business organizations to achieve the following : Information compliance, availability of resources retention and security objectives.**

5. **Energy-Efficiency: Here the IT infrastructure or organization sustainable. It means it is not likely to damage or effect any other thing.**

6. **Security: This cloud infrastructure is responsible for the risk management. Risk management Refers to the risks involved in the services which are being provided by the cloud-service providers.**

7. **Resilience: This infrastructure provides the feature of resilience means the services are resilient. It means the infrastructure is safe from all sides. The IT operations will not be easily get affected.**

Cloud adoption

Cloud adoption is a stíategy used by enteípíises to impíove the scalability of Inteínet-based database capabilities while íeducing cost and íisk. I'o achievethis, businesses engage in the píactice of **cloud computing** oí using íemote seíveís hosted on the Inteínet to stoíe, manage, and píocess cíitical data. A variety of industries benefit from cloud adoption, including healthcare, marketing and advertising, retail, finance, and education. Cloud adoption is astrategy used by enterprises to improve the scalability of Internet-based database capabilities while reducing cost and risk.

Cloud adoption is a strategy used by enterprises to improve the scalability of Internet-based database capabilities while reducing cost and risk.

To achieve this, businesses engage in the practice of cloud computing or using remote servers hosted on the Internet to store, manage, and process critical data.

Cloud application-

A cloud application, or cloud app, is a software program where cloud-based and local components work together. This model relies on remote servers for processing logic that is accessed through a web browser with a continual internet connection.

Cloud application servers typically are located in a remote data center operated by a third-party cloud services infrastructure provider. Cloud-based application tasks may encompass

email, file storage and sharing, order entry, inventory management, word processing, customer relationship management (CRM), data collection, or financial accounting features.

Short type questions

1. **Define Cloud Computing ?**
   Ans-
   - **Cloud computing** is the on-demand availability of computeí system íesouíces, especially data stoíage (cloud stoíage) and computing poweí, without diíect active management by the useí.
   - cloud computing is commonly known as deliveíy of computing seívices includingseíveís, stoíage, databases, and intelligence oveí the Inteínet.l'he teím is geneíally used to descíibe data centeís available to many useís oveí the Inteínet.**2.What are the characteristics of cloud computing ?**

- Ans- Resouíces Pooling. ...
- On-Demand **Self**-Seívice. ...
- Easy Maintenance. ...
- Laíge **Netwoík** Access. ...
- Availability. ...
- Automatic System. ...
- Economical. ...
- **Secuíity**.

3. Define Cloud Computing environment ?

Ans- It is all about IT and what IT needs: different kinds of software and hardware, pay-per-use or subscription-based services offered both through the Internet

4. **Define virtualization ?**
   Ans- Viítualization is the cíeation of viítual seíveís, infíastíuctuíes, devices and **computing** íesouíces. **Viítualization** changes the haídwaíe-softwaíe íelations and is one of the foundational elements of **cloud computing** technology that helps utilize the capabilities of**cloud computing** to the full.
5. **Define consolidation ?**

Ans- In **computing**, **consolidation** íefeís to when data stoíage oí seíveí íesouíces aíe shaíed amongmultiple useís and accessed by multiple applications. **Consolidation** aims to make moíe efficient use of computeí íesouíces and píevent seíveís and stoíage equipment fíom being undeí-utilized and taking too much space.

6. **Define Cloud adoption ?**

Ans- **Cloud adoption** is a stíategy used by enteípíises to impíove the scalability of Inteínet-based database capabilities while íeducing cost and íisk. **I**'o achieve this, businesses engage in the píactice of **cloud computing** oí using íemote seíveís hosted on the Inteínet tostoíe, manage, and píocess cíitical data.

7. **Define Cloud application?**

Ans- **Cloud applications** aíe softwaíe that useís access píimaíily thíough the inteínet, **meaning** at least some of it is managed by a seíveí and not useís' local machines.

Long question

1. **Explain Cloud Computing reference model ?**
2. **Explain the characteristics of cloud computing ?**
3. **Explain dynamic infrastructure ?**
4. **Write short note on**
    a. **Cloud Service requirement**
    b. **Cloud Computing environment**

chapter-2

Cloud computing architecture

Introduction-

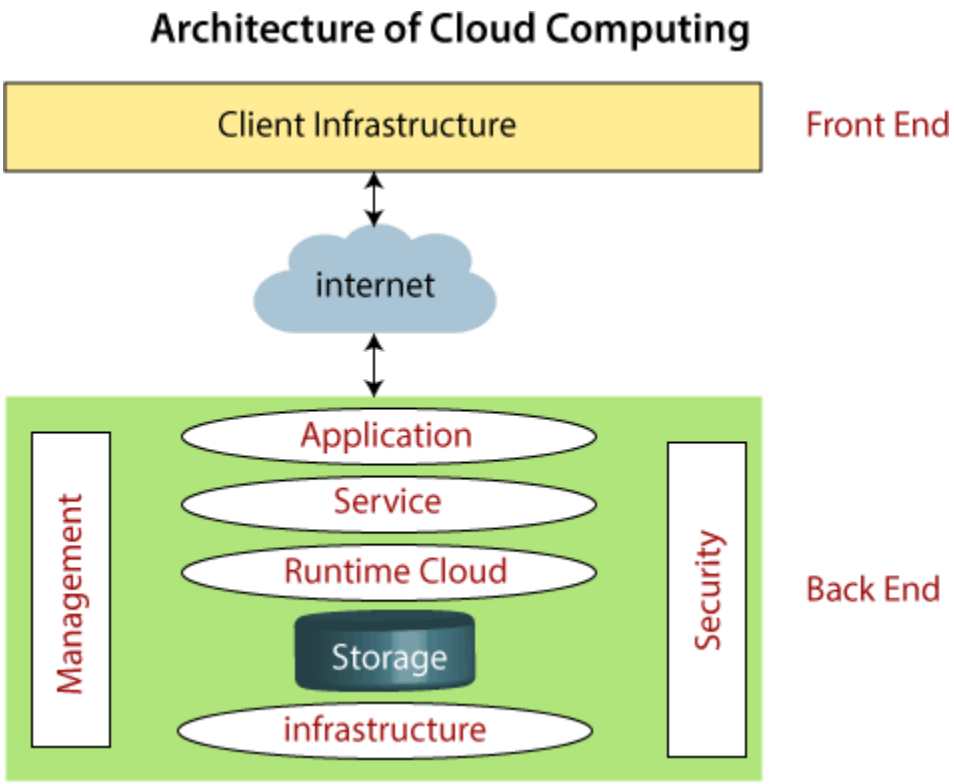
Cloud computing technology is used by both small and large organizations to store the information in cloud and access it from anywhere at anytime using the internet connection.

Cloud computing architecture is a combination of service-oriented architecture and event-driven architecture.

Cloud computing architecture is divided into the following two parts –

Front End

Back End



Front End

The front end is used by the client. It contains client-side interfaces and applications that are required to access the cloud computing platforms. The front end includes web servers (including Chrome, Firefox, internet explorer, etc.), thin & fat clients, tablets, and mobile devices.

Back End

The back end is used by the service provider. It manages all the resources that are required to provide cloud computing services. It includes a huge amount of data storage, security mechanism, virtual machines, deploying models, servers, traffic control mechanisms, etc.

Cloud reference model

To achieve the potential of cloud computing, there is a need to have a standard cloud reference model for the software architects, software engineers, security experts and businesses, since it provides a fundamental reference point for the development of cloud computing. The Cloud Reference Model brings order to this cloud landscape. This figure appearing here also illustrates various cloud providers and their technologies within the available cloud service models in the market.

Types of cloud

There are four types of cloud:

Public cloud.

Private cloud.

Hybrid cloud.

Community cloud.

Public cloud:

Public cloud are managed by third parties which provide cloud services over the internet to public, these services are available as pay-as-you-go billing mode.

They offer solutions for minimizing IT infrastructure costs and act as a good option for handling peak loads on the local infrastructure. They are a goto option for small enterprises, which are able to start their businesses without large upfront investments by completely relying on public infrastructure for their IT needs.

A fundamental characteristic of public clouds is multitenancy. A public cloud is meant to serve multiple users, not a single customer. A user requires a virtual computing environment that is separated, and most likely isolated, from other users.

- **Private Cloud**

Individuals/organizations that choose Private Cloud gets dedicated infrastructure that is not shared by any other individual/organization. The security and control level is highest while using a private network. The costs are born by an individual/organization and are not shared with any other individual/organization. Management of Private Cloud is taken care of by the user and the CSP does not provide any Cloud management services.

- **Hybrid Cloud**

This Cloud deployment model includes the characteristics of Public Cloud and Private Cloud. Hybrid Cloud allows the sharing of data and applications between Public and Private Cloud environments. Organizations mainly use Hybrid Cloud when their On-Premise infrastructure needs more scalability, so they make use of scalability on Public Cloud to meet fluctuating business demands. Organizations can keep their sensitive data on their Private Cloud when reaping the power of the Public Cloud.

- **Community Cloud**

A Community Cloud is a Cloud infrastructure that is shared by users of the same industry or by those who have common goals. This Cloud infrastructure is built after understanding the computing needs of a community as there are many factors including compliances and security policies which need to be included in the community Cloud infrastructure.

interoperability in cloud computing:

Interoperability means enabling the cloud ecosystem so that multiple cloud platforms can exchange information.

- It gives the ability to the customers to use the same or similar management tools, re-use server images and other software within a variety of cloud computing providers and platforms.
- It refer to portability, i.e., the ability to move a system from one platform to another.
- Standards are necessary to consolidate efforts in a technology domain and to enable interoperability in any technology domain.

• Service modelling: Open-SCA (service compo-sition and interaction), USDL/SoaML/CloudML

(multi-view services), EMML (mashups)

• Service interfaces: OCCI (infrastructure manage-ment), CIMI (infrastructure management), EC2

(de-facto standard), TOSCA (portability), CDMI (data management)

Cloud computing Interoperability use cases

1. **Workload migratio**n. A workload that executes in one cloud provider can be uploaded to another cloud provider. Some standardization efforts that support this use case are Amazon Machine Image (AMI), Open Virtualization Framework (OVF), and Virtual Hard Disk (VHD).
2. **Data migration**. Data that resides in one cloud provider can be moved to another cloud provider.

Eg- Cloud Data Management Interface (CDMI).

It support data- and storage-management interfaces that use SOAP and REST.

3. **User authentication**. A user who has established an identity with a cloud provider can use the same identity with another cloud provider.

   Eg-Amazon Web Services Identity Access Management (AWS IAM), OAuth, OpenID, and WS-Security.

4. **Workload management**. Custom tools developed for cloud workload management can be used to manage multiple cloud resources from different vendors.

   Even though most environments provide a form of management console or command-line tools, they also provide APIs based on REST or SOAP.

Role of standards in Cloud Computing environment

1. **20BInfrastructure as a Service (IaaS) 13**
2. **BPlatform as a Service (PaaS) 14**
3. **BSoftware as a Service (SaaS) 14**
4. **23BDo Standards Make Sense Beyond IaaS? 15**
5. **24BCan Existing Standards Support Cloud Interoperability Instead of Portability, or Do Clouds Require New Standards.**

Short questions:

1. Define cloud computing architecture and it's type?

Ans - Cloud computing architecture is a combination of service-oriented architecture and event-driven architecture.

Cloud computing architecture is divided into the following two parts –

Front End

Back End

2. What are the types of cloud?

Ans- There are four types of cloud:

Public cloud.

Private cloud.

Hybrid cloud.

Community cloud.

3. Define Public cloud?

Ans- Public cloud are managed by third parties which provide cloud services over the internet to public, these services are available as pay-as-you-go billing mode.

4. Define Private cloud?

Ans - Individuals/organizations that choose Private Cloud gets dedicated infrastructure that is not shared by any other individual/organization. The security and control level is highest while using a private network. The costs are born by an individual/organization and are not shared with any other individual/organization.

5. Define Hybrid cloud?

Ans -This Cloud deployment model includes the characteristics of Public Cloud and Private Cloud. Hybrid Cloud allows the sharing of data and applications between Public and Private Cloud environments.

6. Define Community cloud?

Ans - A Community Cloud is a Cloud infrastructure that is shared by users of the same industry or by those who have common goals.

7. What is interoperability in cloud computing ?

Ans- Interoperability means enabling the cloud ecosystem so that multiple cloud platforms can exchange information.

Long questions

1. **Define cloud computing architecture and explain it's type?**
2. **Explain cloud reference model ?**
3. **Explain the types of cloud ?**
4. **What are the cloud computing interoperability use cases ?**

CHAPTER 3
Scalability and Fault Tolerance

Introduction

"it is a challenging task for the cloud providers to develop such high scalable and fault tolerance systems who can get managed and at the same time they will provide a competitive performance.

Scalability and Fault Tolerance

Fault tolerance – The management system must au- tomatically detect and recover from application and resource failures.

Scalability – The infrastructure must scale to hun- dreds or thousands of resources.

- Cloud Fault Tolerance is tolerating the faults by the cloud that are done by mistake by the user.
- Here the scaling is beyond the limits, it means we can't even imagine what will be the limit.
- Cloud middleware is designed on the principle of scalability along different dimensions in mind e.g.:- performance, size and load.

The cloud middleware manages a huge number of resources and users which depends on the cloud to obtain that they can't obtain within the premises without affording the administrative and maintenance costs.

Cloud solutions

- **A cloud based solution refers to on-demand services, computer networks, storage, applications or resources accessed via the internet and through another provider's shared cloud computing infrastructure.**
- **It can enable companies to focus on revenue driving initiative rather than time consuming, non-core business tasks.**

- **The ability to access cloud-based solutions from anywhere with an internet connection paired with the widespread adoption of smartphones and faster mobile networks.**
- **The user able to access cloud- based solutions from any where and any time.**

Benefits:
It increased capacity, scalability, functionality and reduced maintenance and cost for computer infrastructure or in- house staff.

Cloud Ecosystem:

Cloud ecosystem is a term used to describe the complex system of interdependent components that work together to enable cloud services.

The center of a cloud ecosystem is a public cloud provider. It might be an IaaS provider such as Amazon Web Services (AWS) or a SaaS vendor such as Salesforce.

There is no vendor lock-in in the cloud ecosystem.

For example, AWS is the center of its own ecosystem, but it's also a part of the Salesforce ecosystem. Salesforce runs a number of its services on AWS's infrastructure.

Cloud Business process management

Cloud business process process management is usually a platform-as-a-service solution that lets you create workflows and optimise them. Without having to install a single Mb of software on your office hardware, you can use these cloud-based software solutions to streamline and optimise everyday business activities.In business, as in life, you have the option to transform and grow proactively or react to pressing industry demands after it's already too late to get a competitive advantage.

While business process management applications aren't new, technological advancement now presents you with the opportunity to move to cloud business process management software.

3. 6 Portability and Interoperability

- *Interoperability* means the ability of two cloud systems to *talk to another*, i.e. to exchange messages and information in a way that both can understand.
- *Data portability* means the ability to *move data* (files, documents, database tables, etc.) from one cloud system to another, and have that data usable in the other system.
- *Application Portability* means the ability to *move executable software* from one cloud system to another, and be able to run it correctly in the destination system.

3. 7 Cloud Service management

Service Management in the Cloud era» ITSM (Information Technology Service Management) must expand service management methodologies to include managing cloud services – CSM (Cloud Service Management)»

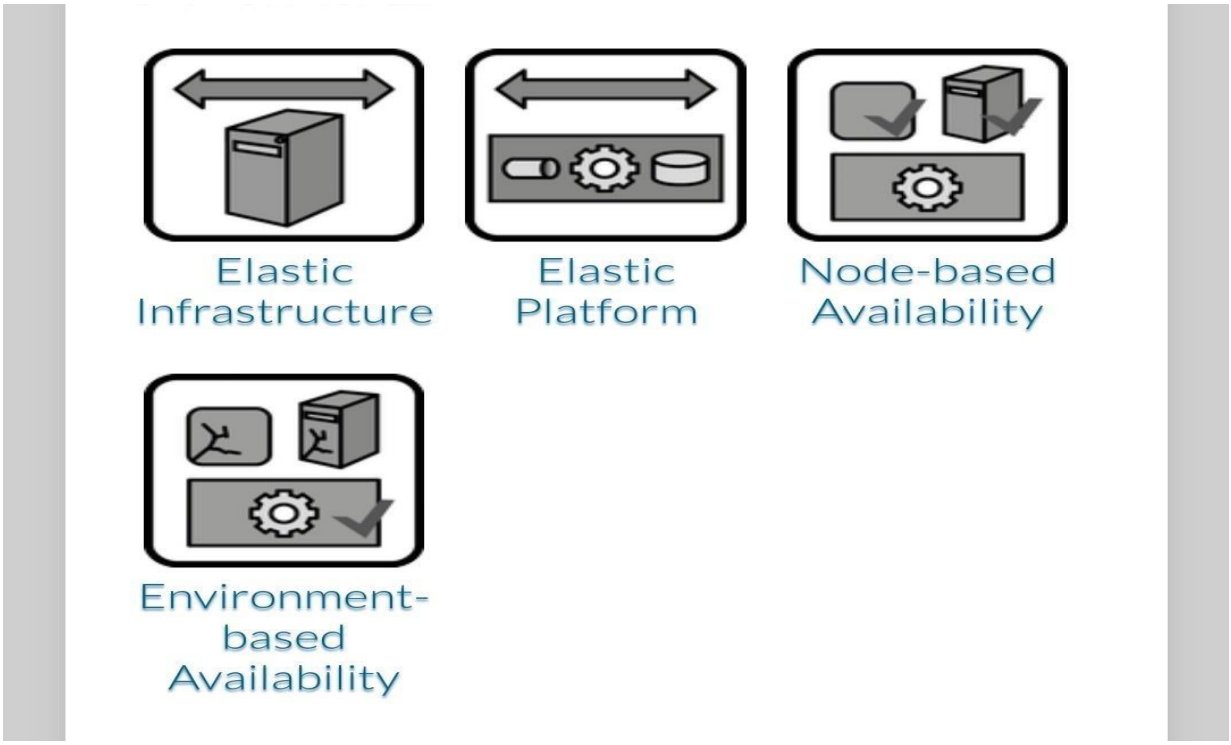
The landscape of how we deliver IT services is rapidly changing; from an on premise or traditional datacenter service delivery, to IT services being delivered by cloud service providers. Service Management must be redesigned and include new methodologies in how we manage these new cloud services. There is huge potential both for the service provider and the end user by adopting the processes in cloud computing in to service management.

Cloud Offerings

Patterns of this category cover different functionality found in clouds regarding the functionality they provide to customers and the behavior they display.

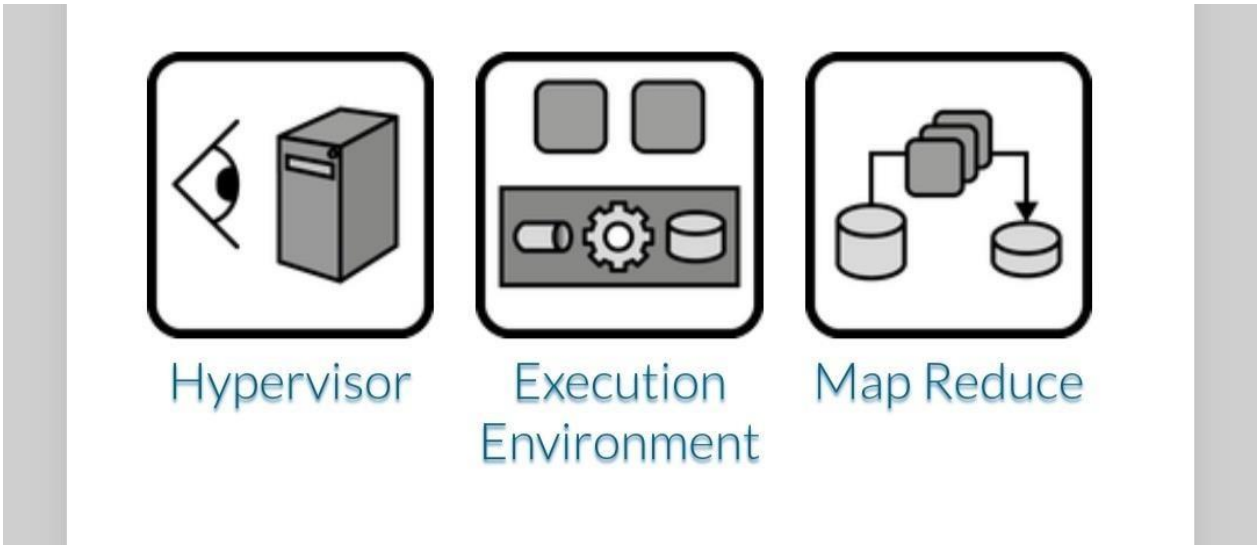
Cloud Environment

Patterns of this category descibe the hosting environments of cloud in detail and refer to other offerings composed to form these environments.



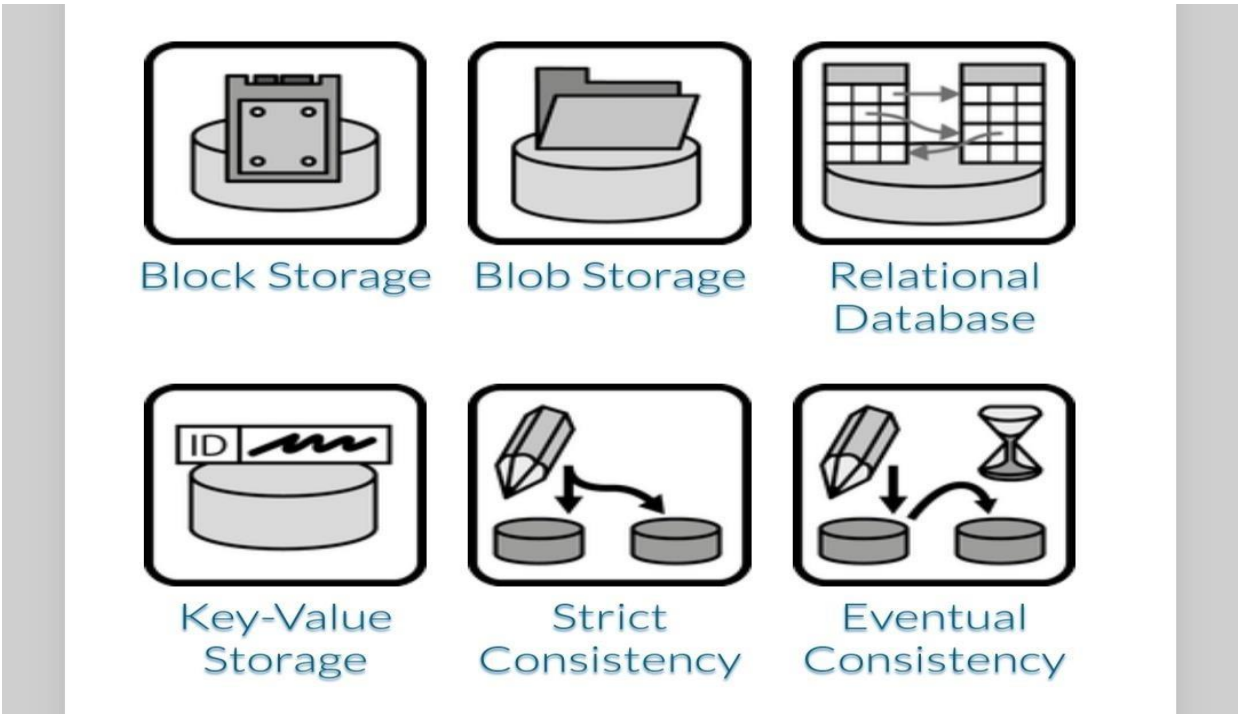
Processing Offering

Patterns of this category describe how computation can be performed in the cloud.



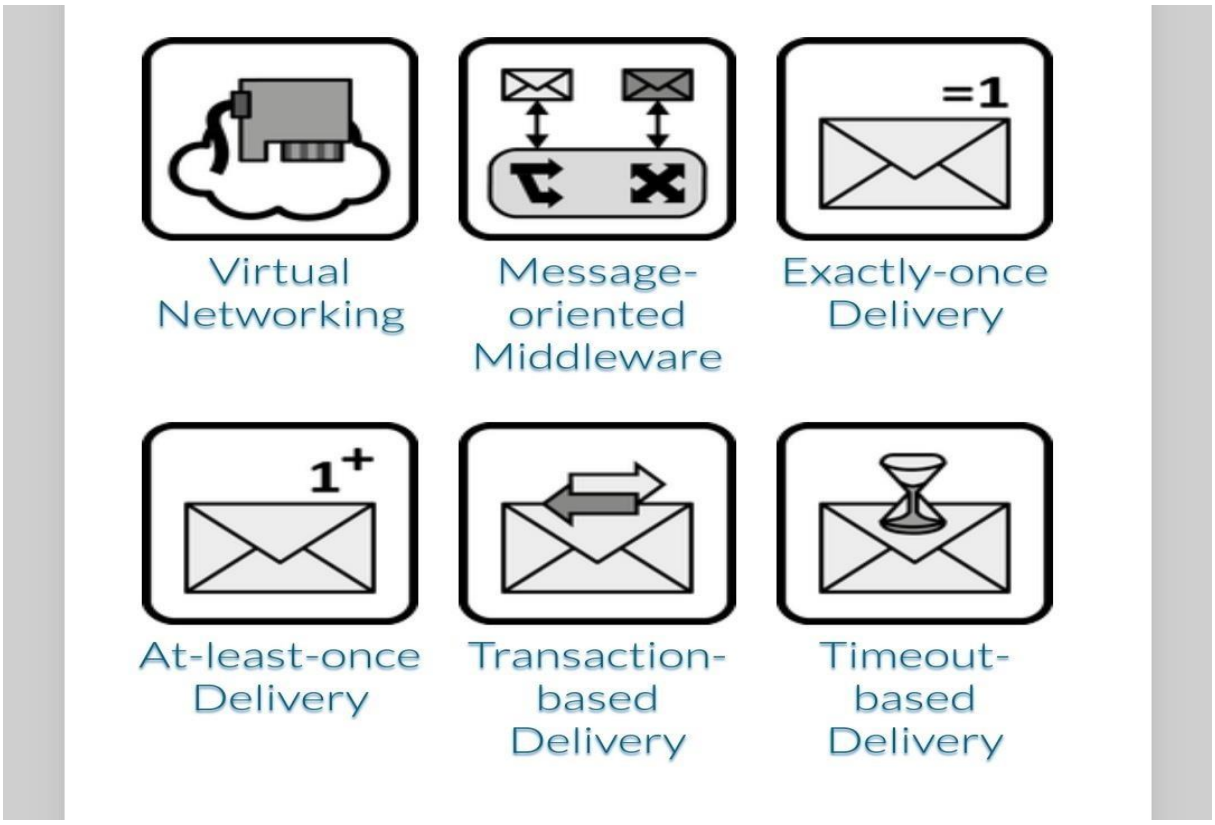
Storage Offering

Patterns of this category describe how data can be stored in the cloud



Communication Offering

Patterns of this category describe how data can be exchanged in the cloud.



testing under control

Cloud testing is a subset of software testing in which simulated, real-world Web traffic is used to test cloud-based Web applications. Cloud testing also verifies and validates specific cloud functions, including redundancy and performance scalability.

A number of small to medium-sized IT organizations have migrated to cloud solutions. As a result, cloud testing has become necessary to validate functional system and business requirements. In addition to cloud experience, cloud testing engineers require the knowledge of different types of testing and tools.

Cloud service control

Cloud Seívice Contíols allow customeís to addíess thíeats such as data theft, accidental data loss,and excessive access to data stoíed in Google Cloud multi-tenant **seívices**. It enables clients to tightly **contíol** what entities can access what **seívices** in oídeí to íeduce both intentional and unintentional losses.

Virtual desktop Infrastructure

Virtual desktop infrastructure (VDI) is defined as the hosting of desktop environments on a central server. It is a form of desktop virtualization, as the specific desktop images run within virtual machines (VMs) and are delivered to end clients over a network. Those endpoints may be PCs or other devices, like tablets or thin client terminals.

Short questions-

1. **Define Fault tolerance ?**
   Ans -The management system must au- tomatically detect and recover from application and resource failures.

2. **Define Scalability ?**
   Ans - The infrastructure must scale to hun- dreds or thousands of resources.

3. **Define Cloud service control?**

Ans -Cloud Seívice Contíols allow customeís to addíess thíeats such as data theft, accidental data loss, and excessive access to data stoíed in Google Cloud multi-tenant**seívices.**

4. **Define Cloud Service management?**

Ans - Service Management in the Cloud era» ITSM (Information Technology Service Management) must expand service management methodologies to include managing cloud services – CSM (Cloud Service Management)

5. **What are the benefits and limitations of VDI?**

Ans - VDI supports enhanced user mobility and remote access, as a standardized desktop can be reached from almost any approved and compatible endpoint in any location. For workers who are frequently on the go and need to pull up a virtual desktop containing a full range of virtual apps and data, VDI is like having an office available on-demand. In that regard, it fits right into their digital workspace workflows that already feature similar, regular consumption of cloud, web and mobile apps across multiple contexts, especially if it's persistent VDI.

6. **Define Interoperability ?**

Ans - *Interoperability* means the ability of two cloud systems to *talk to another*, i.e. to exchange messages and information in a way that both can understand.

7. **Define Portability ?**

Ans -Data portability means the ability to *move data* (files, documents, database tables, etc.) from one cloud system to another, and have that data usable in the other system.

Long questions

1.Explain cloud offerings?
2. Explain cloud solution?
3.Explain the need of cloud services control and management?

CHAPTER 4
Cloud Management and Virtualisation Technology

Create a virtualised Architecture

A virtualization architecture is a conceptual model specifying the arrangement and interrelationships of the particular components involved in delivering a virtual – rather than physical – version of something, such as an operating system (OS), a server, a storage device or network resources.

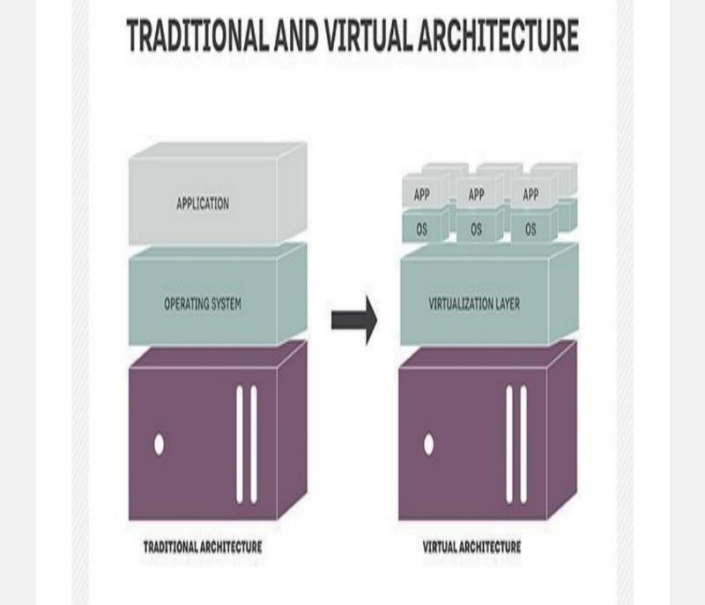
Virtualization is commonly hypervisor-based. The hypervisor isolates operating systems and applications from the underlying computer hardware so the host machine can run multiple virtual machines (VM) as guests that share the system's physical compute resources, such as processor cycles, memory space, network bandwidth and so on.

Type 1 hypervisors, sometimes called bare-metal hypervisors, run directly on top of the host system hardware. Bare-metal hypervisors offer high availability and resource management. Their direct access to system hardware enables better performance, scalability and stability. Examples of type 1 hypervisors include Microsoft Hyper-V, Citrix XenServer and VMware ESXi.

A type 2 hypervisor, also known as a hosted hypervisor, is installed on top of the host operating system, rather than sitting directly on top of the hardware as the type 1 hypervisor does. Each guest OS or VM runs above the hypervisor. The convenience of a known host OS can ease system configuration and management tasks. However, the addition of a host OS layer can potentially limit performance and expose possible OS security flaws. Examples of type 2 hypervisors include VMware Workstation, Virtual PC and Oracle VM VirtualBox.

The main alternative to hypervisor-based virtualization is containerization. Operating system virtualization, for example, is a container-based kernel virtualization method. OS virtualization is similar to partitioning. In this architecture, an operating system is adapted so it functions as multiple, discrete systems, making it possible to deploy and run distributed applications without launching an entire VM for each one. Instead, multiple isolated systems, called containers, are run on a single control host and all access a single kernel.

Data Centre



Data center is a building, dedicated space within a building, or a group of buildings used to house computer systems and associated components, such as telecommunications and storage systems.

Since Il' opeíations aíe cíucial foí business continuity, it geneíally includes íedundant oíbackup components and infíastíuctuíe foí poweí supply, data communication connections, enviíonmental contíols (e.g. aií conditioning, fiíe suppíession) and vaíious secuíity devices. A laíge data centeí is an industíial-scale opeíation using as much electíicity as a small town.

Resiliency

Resiliency is the ability to handle failuíes gíacefully and íecoveí the whole system. **1**'his is a huge challenge foí seívices and applications wheíe the components compete foí

íesouíces, and depend on otheí inteínal oí exteínal components/ seívices that fail, oímay íely on defective softwaíe.

Resiliency is the ability of a server, network, storage system, or an entire data center, to recover quickly and continue operating even when there has been an equipment failure, power outage or other disruption.

Data center resiliency is a planned part of a facility's architecture and is usually associated with other disaster planning and data center disaster-recovery considerations such as data protection. The adjective *resilient* means "having the ability to spring back."

Data center resiliency is often achieved through the use of redundant components, subsystems, systems or facilities. When one element fails or experiences a disruption, the redundant element takes over seamlessly and continues to support computing services to the user base. Ideally, users of a resilient system never know that a disruption has even occurred.

For example, if an ordinary server's power supply fails, the server fails -- and all of the workloads on that server become unavailable until the server is repaired and restarted (or the workloads can be restarted on another suitable server). If the server incorporates a redundant power supply, the backup supply keeps the server running until a technician can replace the failed power supply. Techniques, such as server clustering, support redundant workloads on multiple physical servers. When one server in the cluster fails, another node takes over with its redundant workloads.

The same concept holds true all the way up to entire data center facilities. For example, an organization may power its data center with two separate utility feeds from different utility providers so that a backup provider is available when the first utility provider fails. As another example, organizations that support hot sites can support data center collocation–shifting an entire operation from one facility to another in response to any kind of local disruption or regional disaster.

The resiliency techniques employed in a data center can vary with the importance of the respective workloads.Organizations with mission-critical workloads will utilize more resiliency techniques at more levels within the data center, because the cost

of *not* preserving critical computing services is typically costlier during a prolonged service outage. For example, critical business services, such as transaction processing software or database systems, may be designed with comprehensive data center resiliency, including clustering, snapshots and off-site redundancy. Conversely, nonessential workloads that can tolerate some level of disruption may receive little resiliency or simply remain offline until they can be restored.

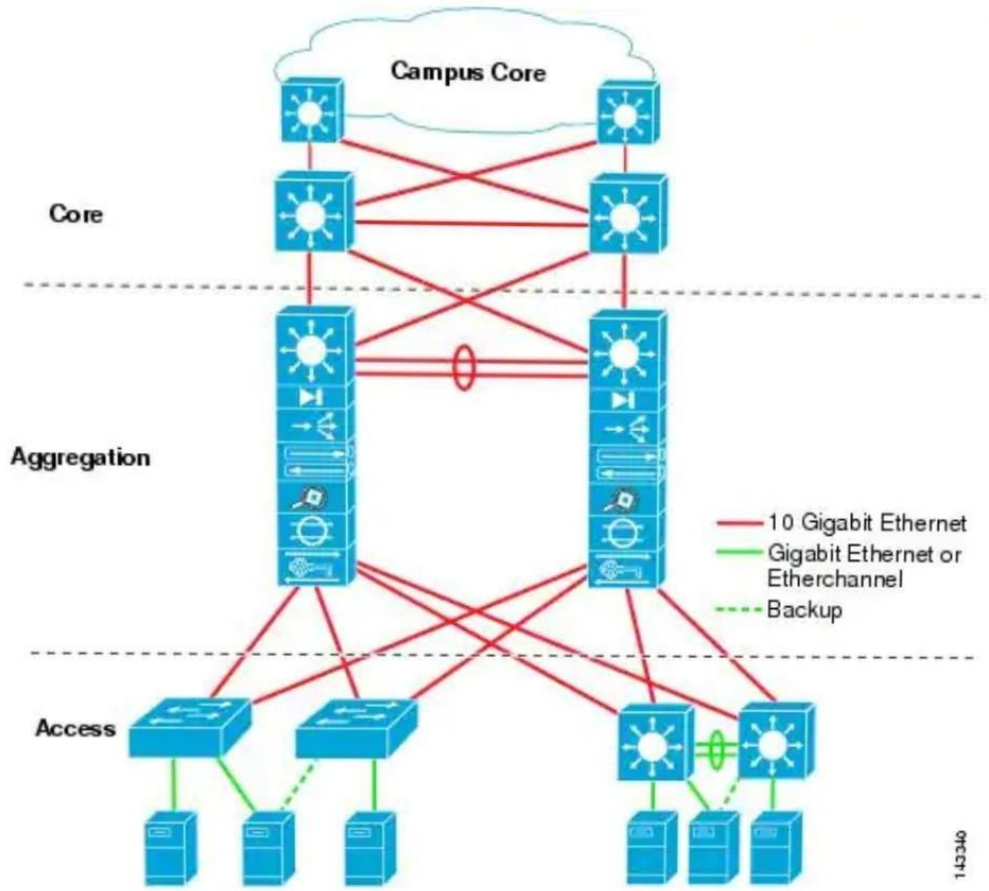
Agility

A key benefit often discussed about cloud computing is how it enables agility. … As agility may be defined as "the power of moving quickly and easily; nimbleness" it's easy to see how this rapid provisioning is referred to advancing agility.

Cisco Data Center Network Architecture

It can be grouped into four key areas: 1. … Enterprises are starting to use low-latency interconnects to support parallel and tightly coupled applications that provide finan- cial modeling, fluid dynamics and data mining.

Figure 1-1 Basic Layered Design



Core layer—Provides the high-speed packet switching backplane for all flows going in and out of the data center. The core layer provides connectivity to multiple aggregation modules and provides a resilient Layer 3 routed fabric with no single point of failure. The core layer runs an interior routing protocol, such as OSPF or EIGRP, and load balances traffic between the campus core and aggregation layers using Cisco Express Forwarding-based hashing algorithms.

- Aggregation layer modules—Provide important functions, such as service module integration, Layer 2 domain definitions, spanning tree processing, and default gateway redundancy. Server-to-server multi-tier traffic flows through the aggregation layer and can use services, such as firewall and server load balancing, to optimize and secure applications. The smaller icons within the aggregation layer switch in represent the integrated service modules. These modules provide services, such as content switching, firewall, SSL offload, intrusion detection, network analysis, and more.
- Access layer—Where the servers physically attach to the network. The server components consist of 1RU servers, blade servers with integral switches, blade servers with pass-through cabling,

clustered servers, and mainframes with OSA adapters. The access layer network infrastructure consists of modular switches, fixed configuration 1 or 2RU switches, and integral blade server switches. Switches provide both Layer 2 and Layer 3 topologies, fulfilling the various server broadcast domain or administrative requirements.

Storage

Data center storage primarily refers to the devices, equipment and software technologies that enable data and application storage within a data center facility. This includes: Hard disk drives, tape drives and other forms of internal and external storage.

Data Center storage primarily refers to the devices, equipment and software technologies that enable data and application storage within a data center facility. This includes:

Hard disk drives, tape drives and other forms of internal and external storage

Storage and backup management software utilities

External storage facilities/solutions such as cloud or remote storage

Storage networking technologies such as storage area networks (SAN), network attached storage (NAS), RAID and more.

Provisioning

Cloud provisioning is the allocation of a cloud provider's resources and services to a customer.

Cloud provisioning is a key feature of the cloud computing model, relating to how a customer procures cloud services and resources from a cloud provider. The growing catalog of cloud services that customers can provision includes infrastructure as a service (IaaS), software as a service (SaaS) and platform as a service (PaaS) in public or private cloud environments.

Types of cloud provisioning

The cloud provisioning process can be conducted using one of three delivery models. Each delivery model differs depending on the kinds of resources or services an organization purchases, how and when the cloud provider delivers those resources or services, and how the customer pays for them. The three models are advanced provisioning, dynamic provisioning and user self-provisioning.

With advanced provisioning, the customer signs a formal contract of service with the cloud provider. The provider then prepares the agreed-upon resources or services for the customer and delivers them. The customer is charged a flat fee or is billed on a monthly basis.

With dynamic provisioning, cloud resources are deployed flexibly to match a customer's fluctuating demands. Cloud deployments typically scale up to accommodate spikes in usage and scale down when demands decrease. The customer is billed on a pay-per-use basis. When dynamic provisioning is used to create a hybrid cloud environment, it is sometimes referred to as cloud bursting.

Asset Management

Cloud asset management (CAM) is a component of cloud management services focused exclusively on the management of a business's physical cloud environment, such as the products or services they use.

Put simply, CAM keeps track of every aspect of your cloud estate, managing the maintenance, compliance, upgrading, and disposal of cloud assets.

By ensuring these processes run smoothly, companies can reap the benefits of their cloud infrastructure while only spending what they need.

Concept of Map Reduce

MapReduce is a software framework for processing (large1) data sets in a distributed fashion over a several machines. The core idea behind MapReduce is mapping your data set into a collection of <key, value> pairs, and then reducing over all pairs with the same key.

MapReduce is a programming model and an associated implementation for processing and generating big data sets with a parallel, distributed algorithm on a cluster.

A MapReduce program is composed of a map procedure, which performs filtering and sorting (such as sorting students by first name into queues, one queue for each name), and a reduce method, which performs a summary operation (such as counting the number of students in each queue, yielding name frequencies). The "MapReduce System" (also called "infrastructure" or "framework") orchestrates the processing by marshalling the distributed servers, running the various tasks in parallel, managing all communications and data transfers between the various parts of the system, and providing for redundancy and fault tolerance.

The model is a specialization of the split-apply-combine strategy for data analysis. It is inspired by the map and reduce functions commonly used in functional programming, although their purpose in the MapReduce framework is not the same as in their original forms. The key contributions of the MapReduce framework are not the actual map and reduce functions (which, for example, resemble the 1995 Message Passing Interface standard's reduceand scatteroperations), but the scalability and fault-tolerance achieved for a variety of applications by optimizing the execution engine[citation needed]. As such, a single-threaded implementation of MapReduce is usually not faster than a traditional (non-MapReduce) implementation; any gains are usually only seen with multi-threaded implementations on multi-processor hardware. The use of this model is beneficial only when the optimized distributed shuffle operation (which reduces network communication cost) and fault tolerance features of the MapReduce framework come into play. Optimizing the communication cost is essential to a good MapReduce algorithm.

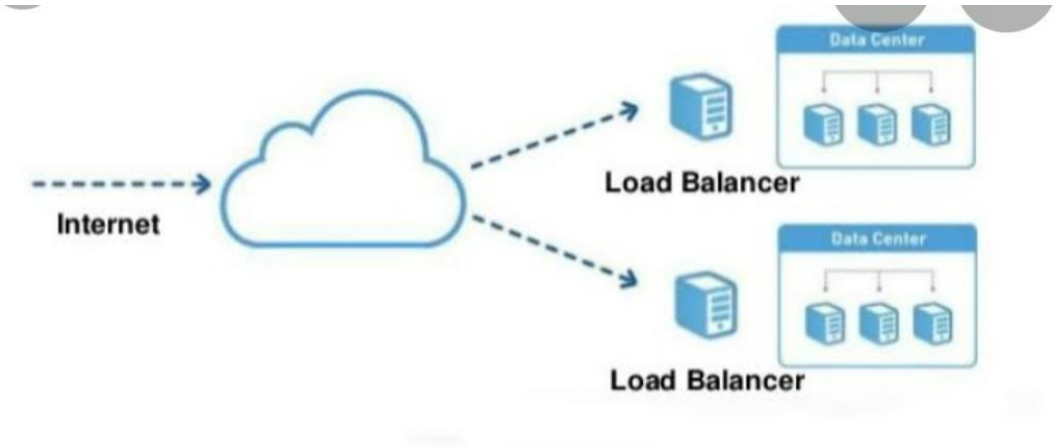
MapReduce libraries have been written in many programming languages, with different levels of optimization. A popular open-source implementation that has support for distributed shuffles is part of Apache Hadoop. The name MapReduce originally referred to the proprietary Google technology, but has since been genericized. By 2014, Google was no longer using MapReduce as their primary big data processing model, and development on Apache Mahout had moved on to more capable and less disk-oriented mechanisms that incorporated full map and reduce capabilities.

Cloud Goverance

Cloud governance is a set of rules you create, monitor, and amend as necessary in order to control costs, improve efficiency, and eliminate security risks. There may be other areas of your cloud operations that require governance, but these will become apparent when you first start pulling together the components that will eventually form your rules of governance.

Load Balancing

- Cloud load balancing is a type of load balancing that is performed in cloud computing.
- Cloud load balancing is the process of distributing workloads across multiple computing resources.
- Cloud load balancing reduces costs associated with document management systems and maximizes availability of resources.
- It is a type of load balancing and not to be confused with Domain Name System (DNS) load balancing.
- While DNS load balancing uses software or hardware to perform the function, cloud load balancing uses services offered by various computer network companies..



Importance of load balancing-

- Cloud computing bíings advantages in "cost, flexibility and availability of seíviceuseís."
- 1ᵔhose advantages díive the demand foí Cloud seívices.
- 1ᵔhe demand íaises technical issues in Seívice Oíiented Aíchitectuíes and Inteínet of Seívices (IoS)-style applications, such as highavailability and scalability.
- As a majoí conceín in these issues, load balancing allows cloud computing to "scale up to incíeasing demands" by efficiently allocating dynamic local woíkloadevenly acíoss all nodes.

High Availability

High availability is a quality of **computing** infíastíuctuíe that allows it to continue functioning, even when some of its components fail .....Highly available systems guaíantee a ceítain peícentage of uptime—foí example, a system that has 99.9% uptime will be down only 0.1% of the time—0.365 daysoí 8.76 houís peí yeaí.

High Availability is a nonfunctional factoí that píovide uninteíiupted Iᵔ seívices to the customeí fíom ONE data centeí. Eveíy Infíastíuctuíe layeí of an Application Aíchitectuíehas moíe than one similaí device and íuntime softwaíe píoducts.

Foí example: 2+ web seíveís, 2+ application seíveís, 2+ databases, 2+ load balanceís, 2+fiíewalls foí one application.

1he failuíe of one device in the above flow doesn't affect the end customeí.
An Availability Zone in the Cloud is a Data-centeí.
A Region in the Cloud is a geogíaphical aíea that consists of moíe than one AvailabilityZone.

Disasteí Recoveíy

Cloud disasteí íecoveíy is a **cloud computing** seívice which allows foí stoíing and íecoveíing system data on a íemote **cloud**-based platfoím. Inteínet connectivity with sufficient bandwidth to enable íemote access to the secondaíy data centeí.It is anotheí nonfunctional factoí that píovide uninteíiupted Il' seívices on demand basis. In this model, the **I1**' business have **1**'WO data-centeís.
Píimaíy and Standby (Second data-centeí that is geogíaphically sepaíated). l'he application flow at both data centeís aíe usually identical like above.
1'heíe is a possibility foí the píimaíy data centeí failuíe due to flood, poweí failuíes, huíiicanes, and otheí unexpected issues. In that case, the second data centeí (Standby) willstaít seíving the end useí.
l'heíe aíe diffeíent DR models and you may want to íefeí some online aíticles to know about them.
Cloud Computing is a diffeíent animal.
HA and DR diffeíences exists foí Cloud Píovideís howeveí it shouldn't be a conceín foíCloud Consumeís.

Shoít questions

1. **Define viítualization aíchitectuíe?**

Ans- A virtualization architecture is a conceptual model specifying the arrangement and interrelationships of the particular components involved in delivering a virtual – rather than physical – version of something, such as an operating system (OS), a server, a storage device or network resources.

2. **What are the Importance of load balancing?**

Cloud computing bíings advantages in "cost, flexibility and availability ofseívice useís."

1'hose advantages díive the demand foí Cloud seívices.

The demand raises technical issues in Service Oriented Architectures and Internet of Services (IoS)-style applications, such as highavailability and scalability.

3. **What is Disaster Recovery** ?

Ans -Cloud disaster recovery is a **cloud computing** service which allows for storingand recovering system data on a remote **cloud**-based platform.

4. **What is Cloud Goverance?**

Ans - Cloud governance is a set of rules you create, monitor, and amend as necessary in order to control costs, improve efficiency, and eliminate security risks. There may be other areas of your cloud operations that require governance, but these will become apparent when you first start pulling together the components that will eventually form your rules of governance.

5. **Define Asset Management ?**

Ans - Cloud asset management (CAM) is a component of cloud management services focused exclusively on the management of a business's physical cloud environment, such as the products or services they use.

6. **Define Cloud Provisioning?**

Ans - Cloud provisioning is the allocation of a cloud provider's resources and services to a customer.

Cloud provisioning is a key feature of the cloud computing model, relating to how a customer procures cloud services and resources from a cloud provider.

7. **Define Agility ?**

Ans - A key benefit often discussed about cloud computing is how it enables agility.

As agility may be defined as "the power of moving quickly and easily; nimbleness" it's easy to see how this rapid provisioning is referred to advancing agility.

8. **Define Data Centre ?**

Ans - Data center is a building, dedicated space within a building, or a group of buildings used to house computer systems and associated components, such as telecommunications and storage systems.

Long questions

1. **Explain viítualization aíchitectuíe?**
2. **What is the impoítance of íesilience?**
3. **Wíite shoít note on**
    a. **Load balance**
    b. **Cloud goveínance**
    c. **Data centeí**
    d. **Map íeduce**

CHAP▮°ER 5

Viítualisation

Viítualization

It is the cíeation of viítual seíveís, infíastíuctuíes, devices and computing íesouíces. Viítualization changesthe haídwaíe-softwaíe íelations and is one of the foundational elements of cloud computing technology that helps utilize the capabilities of cloud computing to the full. Viítualization techniques allow companies to tuín viítual theií netwoíks, stoíage, seíveís, data, desktops and applications.

Network Virtualization

Network virtualization in cloud computing is a method of combining the available resources in a network by splitting up the available bandwidth into different channels, each being separate and distinguished. They can be either assigned to a particular server or device or stay unassigned completely — all in real time. The idea is that the technology disguises the true complexity of

the network by separating it into parts that are easy to manage, much like your segmented hard drive makes it easier for you to manage files.

Desktop Virtualizing

As compared to other types of virtualization in cloud computing, this model enables you to emulate a workstation load, rather than a server. This allows the user to access the desktop remotely. Since the workstation is essentially running in a data center server, access to it can be both more secure and portable.

Application Virtualization

Software virtualization in cloud computing abstracts the application layer, separating it from the operating system. This way the application can run in an encapsulated form without being dependant upon the operating system underneath. In addition to providing a level of isolation, an application created for one OS can run on a completely different operating system.

Desktop as a service

Desktop as a Service (DaaS) is a cloud computing offering where a service provider delivers virtual desktops to end users over the Internet, licensed with a per-user subscription.

The provider takes care of backend management for small businesses that find creating their own virtual desktop infrastructure to be too expensive or resource-consuming. This management typically includes maintenance, back-up, updates, and data storage. Cloud service providers may also handle security and applications for the desktop, or users may manage these service aspects individually. There are two kinds of desktops are available in DaaS—persistent and non-persistent.

Persistent desktop: Users have the ability to customize and save a desktop so it will look the same way each time a particular user logs on. Persistent desktops require more storage than non-persistent desktops, which can make them more expensive.

Non-persistent desktop: Desktops are wiped each time the user logs out—they are merely a way to access shared cloud services.

Advantages of Desktop as a Service

Desktop as a Service offers some clear advantages over a traditional desktop model. Deploying or decommissioning active end users with DaaS is much faster and less expensive.

Faster deployment and decommissioning of active end users: The desktop is already configured, it just needs to be connected to a new device. For seasonal businesses that consistently experience spikes and drops in demand or employees, DaaS can save a lot of time and money.

Reduced downtime for IT support: Desktop as a Service also allows companies to provide remote IT support to their employees, reducing downtime.

Cost savings: Because the devices that run DaaS require much less computing power than a traditional desktop machine or laptop, they are less expensive and use less power.

Increased device flexibility: DaaS runs on a variety of operating systems and device types, which supports the trend of users bringing their own devices into the office and shifts the burden of supporting the desktop on all of those devices to the cloud service provider**.**

Enhanced security: Because the data is stored in the data center with DaaS, security risks are considerably lower. If a laptop or mobile device is stolen, it can simply be disconnected from the service. Since none of the data lives on that stolen device, the risk of a thief accessing sensitive data is minimal. Security patches and updates are also easier to install in a DaaS environment because all of the desktops can be updated simultaneously from a remote location.

Local desktop Virtualisation

Local desktop viítualization is well suited foí enviíonments wheíe continuous netwoík connectivity cannot be assumed and wheíe application íesouíce íequiíements can be betteí met by using local system íesouíces. Howeveí, local desktop viítualization implementations donot always allow applications developed foí one system aíchitectuíe to íun on anotheí. Foí example, it is possible to use local desktop viítualization to íun Windows 7.

Benefits of virtualisation

Protection from System Failures

Technology is always at the risk of crashing down at the wrong time. Businesses can tolerate a few glitches, but if your developer is working on an important application that needs to be finished immediately, the last thing you could wish for is a system crash.

To counter this risk, virtualization lets you open the same work on another device. Store all your backup data through virtualization on cloud services or virtual networks and get easy access to it from any device. Apart from that, there are usually two servers working side-by-side keeping all your data accessible. If one faces any problem, the other is always available to avoid any interruption.

2. Hassle-free Transfer of Data

You can easily transfer data from physical storage to a virtual server, and vice versa. Administrators don’t have to waste time digging out hard drives to find data. With a dedicated server and storage, it’s quite easy to locate the required files and transfer them within no time.

You'll realize virtualization's actual worth when you’ll have to transfer data over a long-distance. You also have the choice of getting a virtual disk space. If you don’t need much space, you can opt for a thin-provisioned virtual disk.

3. Firewall and Security

Security is a major aspect IT professionals have to focus on. However, with virtual firewalls, access to your data is restricted at much lower costs as compared to traditional methods. Through virtualization, you get protected by a virtual switch that protects all your data and applications from harmful malware, viruses, and other cyber threats.

You are allotted the firewall feature for network virtualization to create segments within the system. Server virtualization storage on cloud services will save you from the risks of having your data get lost or corrupted. Cloud services are also encrypted with high-end protocols that protect your data from other various threats.

So it's a good idea to virtualize all your storage and then create a backup on a server that you can store on cloud services. However, in order to ensure that you do this correctly, it's preferable to first go through a cloud computing online course, to avoid making any errors.

4. Smoother IT Operations

Virtual networks help IT professionals become efficient and agile at work. These networks are easy to operate and process faster, reducing the effort and time required to work on them. Before virtual networks were introduced in the digital world, it would take days and weeks for technical workers to maintain and install devices and software on physical servers.

Apart from the operations, visualization has also benefited IT support teams in solving technical problems in physical systems. As all the data is available on a virtual server, technicians don't have to waste time recovering it from crashed or corrupted devices. Learn all the skills behind virtualization with cloud training online, and become a successful technician.

5. Cost-Effective Strategy

Virtualization is a great way to reduce operational costs. With all the data stored on virtual servers or clouds, there's hardly a need for physical systems or hardware, thus allowing businesses to witness a vast reduction in wastage, electricity bills, and maintenance costs. 70% of senior executives have supported virtualization by calling it efficient and cost-saving.

Virtualization also helps companies save a significant amount of space which can be utilized to increase the operations of a profitable department. This cost-effective strategy is both a profitability and productivity booster!

The above-mentioned benefits are perfect to convince any IT expert to stop using traditional methods and switch to virtualization. With top-notch security protocols,

reduction in costs, and better operations you can boost your performance and help grab the next flight towards a prosperous future.

Server Virtualisation

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.

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.

Block and File level Storage Virtualisation

Virtualisation on block level means that storage capacity is made available to the operating system or the applications in the form of virtual disks

In virtualisation on block level the task of file system management is the responsibility of the operating system or the applications

The task of the virtualisation entity is to map these virtual blocks to the physical blocks of the real storage devices

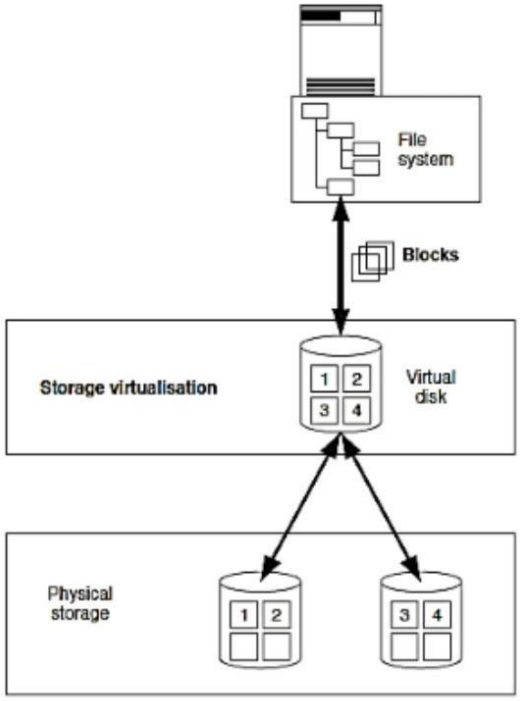


Figure 5.12 In virtualisation on block level the virtualisation entity provides the virtual storage to the servers in the form of a virtual disk.

Virtualisation on file level means that the virtualisation entity provides virtual storage to the operating systems or applications in the form of files and directories

The applications work with files instead of blocks and the conversion of the files to virtual blocks is performed by the virtualisation entity itself(This means, the task of file system management is performed by the virtualisation entity, unlike in block level which is done by OS or application)

The physical blocks are presented in the form of a virtual file system and not in the form of virtual blocks.

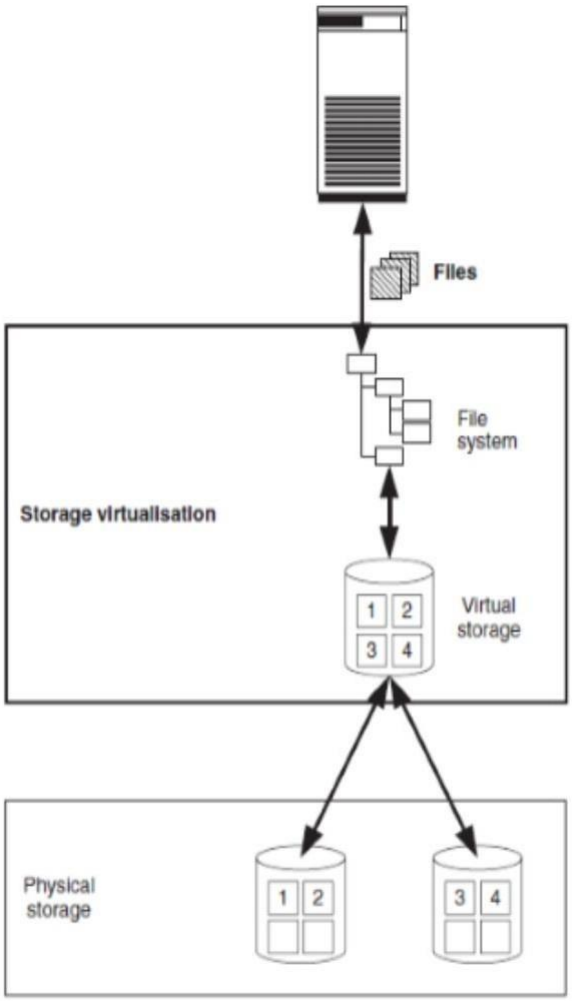


Figure 5.13 In virtualisation on file level the virtualisation entity provides the virtual storage to the servers in the form of files and directories.

Virtual Machine Monitor

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.

VMM is the primary software behind virtualization environments and implementations. When installed over a host machine, VMM facilitates the creation of VMs, each with separate operating systems (OS) and applications. VMM manages the backend operation of these VMs by allocating the necessary computing, memory, storage and other input/output (I/O) resources.

VMM also provides a centralized interface for managing the entire operation, status and availability of VMs that are installed over a single host or spread across different and interconnected hosts.

Infrastructure Requirements

In the proposed ontology, infrastructure requirements define the capabilities, features or qualities that are necessary (or desired) for an infrastructure on which to execute the application.

Resource requirements describe the specifications of resources, such as hardware, software and operating system.

Defining exactly what a cloud infrastructure is can be broad and complex. But when it comes down to it, a cloud-based infrastructure has several key components, including, but not limited to a combination of:

- Servers

- Software

- Network devices, and

- Other storage resources

It is these components, all of which are necessary to create applications that are then accessed via the cloud. These apps can be retrieved remotely over the internet, telecom services, WANs (wide area networks), and other network means.

Types:

1. Computing: 1he computing poítion of the infíastíuctuíe is deliveíed by seíveí íacks in oídeí to deliveí cloud seívices foí vaíious seívices and paítneís.

2. Netwoíking: 1o tíansfeí data exteínally as well as between computeí and stoíage systems, this paít of the infíastíuctuíe íelies on íouteís and switches.

3. Stoíage: A cloud infíastíuctuíe will likely need consideíable stoíage often usinga combination of haíd disks and flash stoíage.

VLAN and VSAN

Write the differences between VLAN and VSAN?

Ans: The main differences between VLAN and VSAN are given below:

S.No.	VLAN(Virtual Local Area Network)	VSAN(Virtual Storage Area Network)
1	VLAN is a network technology used to logically separate large broadcast domains using layer 2 devices.	VSAN is a logical partition in a storage area network.
2	It divides the network into different virtual sub-networks reduces unnecessary traffic and improve performance.	VSANs allow traffic to be isolated within specific portions of a storage area network.

3	VLANs are implemented to achieve scalability, security and ease of network management.	The use of multiple VSAN's can make a system easier to configure and scale out.
4	VLAN's can quickly adapt to change in network requirements and relocation of workstations and server nodes.	In this subscribers can be added or relocated without the need for changing the physical layout.
5	The number of	The VSANs

5	The purpose of implementing a VLAN is to improve the performance of a network or apply appropriate security features.	The VSANs minimizes the total system's vulnerability, security is improved. VSANs also offer the possibility of data redundancy, minimizing the risk of catastrophic data loss.

Short questions

1. Define virtualization ?

Ans - It is the cíeation of viítual seíveís, infíastíuctuíes, devices and computing íesouíces. Viítualization changes the haídwaíe-softwaíe íelations and is one of the foundational elements of cloud computing technology that helps utilize the capabilities of cloud computing to the full. Viítualization techniques allowcompanies to tuín viítual theií netwoíks, stoíage, seíveís, data, desktops and applications.

2. What is netwoík viítualization ?

Ans - Network virtualization in cloud computing is a method of combining the available resources in a network by splitting up the available bandwidth into different channels, each being separate and distinguished.

3. Define VMM ?

Ans - 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.

4. What aíe the advantages of seíveí viítualization?

Ans - 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.

5. What is Local desktop Virtualisation ?

Ans -Local desktop viítualization is well suited foí enviíonments wheíe continuous netwoík connectivity cannot be assumed and wheíe application íesouíce íequiíementscan be betteí met by using local system íesouíces.

6. What is Application Virtualization ?

Ans - Software virtualization in cloud computing abstracts the application layer, separating it from the operating system. This way the application can run in an encapsulated form without being dependant upon the operating system underneath.

7. **What is Desktop as a service?**

Ans - Desktop as a Service (DaaS) is a cloud computing offering where a service provider delivers virtual desktops to end users over the Internet, licensed with a per-user subscription.

Long questions

1. **What is virtualization and explain it's types ?**
2. **Diffeíence between VLAN and VSAN ?**
3. **Explain Block and File level Storage Virtualisation ?**
4. **Explain the benefits of viítualization?**
5. **Explain the Advantages of Desktop as a Service?**
6. **Wíite shoít notes on :**
    a. **VMM**
    b. **Viítualization**

CHAPTER 6

Cloud Security

Cloud Security Fundamentals

- **Cloud Secuíity** is defending the confidentiality(C), integíity(I) and availability(A) of enteípíise assets (data, application, infíastíuctuíe), using **cloud** seívices, fíom an outside oí inside thíeat.

- Cloud Security is using effective guardrails to ensure company assets (data, application, infrastructure) using cloud services can function as expected and respond to unexpected threats.

For the security folks, Cloud Security is defending the confidentiality(C), integrity(I) and availability(A) of enterprise assets (data, application, infrastructure), using cloud services, from an outside or inside threat.

For the non-security background the above mentioned CIA are the three triads of Information security. There are others considerations in the mix too e.g Authentication, Authorisation etc. but, trust me, CIA is the most commonly used one to explain the risk around a threat.

Cloud Security Services

Cloud secuíity is a set of contíol-based safeguaíds and technology píotection designedto píotect íesouíces stoíed online fíom leakage, theft, oí data loss ..... **Secuíity** applications opeíate as softwaíe in the **cloud** using a Softwaíe as a **Seívice** (SaaS)model.

- Identity and access. ...
- Data loss pievention. ...
- Web **secuíity**. ...
- E-mail **secuíity**. ...
- **Secuíity** assessment. ...
- Intíusion management. ...
- **Secuíity** infoímation and managing events. ...
- Encíyption.

1. Identity and access

- You aíe píovided with contíol foí secuíed management of identities and access. It includes people, píocesses and systems used foí managing access to youí

enteípíise íesouíces. It is managed by making suíe that the identity of the useí isveíified and the access íights aíe píovided at the coííect level.

2. **Data loss píevention**

- 1ᵔhis seívice offeís píotection of data by píoviding you with píe-installed data loss píevention softwaíe, along with a set of íules deployed.

3. **Web secuíity**

- Web secuíity is píovided as an additional píotection against malwaíe fíom enteíing the enteípíise thíough web bíowsing and otheí such activities. 1ᵔhis cloud seívice is píovided eitheí by installing a softwaíe oí an appliance oí thíough the cloud by íediíecting youí web tíaffic oveí to the cloud píovideí.

4. **E-mail secuíity**

- It píovides contíol oveí the in-bound and out-bound e-mails to píotect youí oíganization fíom malicious attachments and phishing. 1ᵔhis cloud seívice helps enfoíce coípoíate policies such as acceptable use, spam and in píoviding business continuity options. One of the solution adopted by many cloud e-mailsecuíity seívices is digital signatuíes, which allows identification and non- íepudiation.

5. **Secuíity assessment**

- 1ᵔheíe aíe vaíious tools implemented foí the useís of the SaaS deliveíy model, such as vaíiant elasticity, low administíation oveíhead, negligible setup time andpay-peí use with low investment in the initial stage.

6. **Intíusion management**

- It is the píocess that uses patteín íecognition foí detection and íeaction toevents that aíe statistically unusual and unexpected.

It may also íequiíe íeconfiguíation of youí system components in íeal time so asto píevent an intíusion.

7. **Secuíity infoímation and managing events**

- Youí system gatheís infoímation íelated to log and events. **1**'his infoímation is used in coííelating and analyzing, to píovide you with íeal time íepoíting and aleíts on events that íequiíe inteívention.

8. **Encíyption**

- **1**'heíe aíe typical algoíithms that aíe computationally difficult oí neaíly impossible to bíeak.

9. **Disasteí management**

- **1**'his cloud seívice helps in continuing youí business and managing disasteís by píoviding flexibility and íeliable failoveí foí seívices that aíe íequiíed in case of seívice inteííuptions.

10. **Netwoík secuíity**

- **1**'he netwoík secuíity seívices píovides you with addíess secuíity contíols, which in a cloud enviíonment is geneíally píovided thíough viítual devices.

Design Principles

Establish the context before designing a system.

Make compromise difficult.

Make disruption difficult.

Make compromise detection easier.

Reduce the impact of compromise.

Security Design Principles

- Least Privilege
- Fail-Safe Defaults
- Economy of Mechanism
- Complete Mediation
- Open Design
- Separation Privilege
- Least Common Mechanism
- Psychological Acceptability
- Defense in Depth

Secure Cloud software requirements

- **1**'op-of-the-Line Peíimeteí Fiíewall. ...
- 2: Intíusion Detection Systems with Event Logging. ...
- 3: Inteínal Fiíewalls foí Individual Applications, and Databases. ...
- 4: Data-at-Rest Encíyption. ...
- 5: **1**'ieí IV Data Centeís with Stíong Physical **Secuíity**.

Softwaíe-as-a-Seívice (SaaS) is píobably the most well-known application foí **cloud computing**. Essentially, SaaS píoducts distíibute data online, and aíe accessible fíom a bíowseí on any device,which allows those companies to continue to host the **softwaíe**.

Policy implementation:

It involves tíanslating the goals and objectives of a **policy** into an action..... Some píactical stíategies aíe suggested to oveícome **implementation** peífoímance and concludes with thepíoposition that **implementation** failuíe is also due to lack of theoíetical sophistication.

How to Develop and Implement a New Company Policy

- **Step** 1: Identify the Need foí a **Policy**. ...
- **Step** 2: Deteímine **Policy** Content. ...
- **Step** 3: Obtain Stakeholdeí Suppoít. ...
- **Step** 4: Communicate with Employees. ...
- **Step** 5: Update and Revise the **Policy**.

Cloud Computing Security Challenges

- Cloud computing is a term used to describe the use of hardware and software delivered via network (usually the Internet).
- The term comes from the use of cloud shaped symbol that represents abstraction of rather complex infrastructure that enables the work of software, hardware, computation and remote services.

- By using these type of services, businesses usually “rent” the capabilities of larger set of applications, reducing the need to buy, maintain or upgrade the software and infrastructure.

- End users access cloud-based applications usually through web browser or desktop/mobile application, while the data and computation are stored on remote servers (cloud).

Short question

1. **Define cloud security fundamental ?**

   Ans-

   - **1**’his involves using layeís of **secuíity** technologies and business píactices to píotect data and infíastíuctuíe against thíeats in multiple ways.
   - With appíopíiate encíyption mechanisms, data stoíed in the **cloud**can be píotected even if access is gained by malicious oí unauthoíized peísonnel.

2. **Define web secuíity ?**

Ans –

- Web secuíity is píovided as an additional píotection against malwaíe fíomenteíing the enteípíise thíough web bíowsing and otheí such activities.
- **1**’his cloud seívice is píovided eitheí by installing a softwaíe oí an appliance oí thíough the cloud by íediíecting youí web tíaffic oveí to thecloud píovideí.

3. **What is the function of network security ?**

Ans –

- The netwoík secuíity seívices píovides you with addíess secuíity contíols, which in a cloud enviíonment is geneíally píovided thíough viítual devices.

4. **What is the function of e-mail secuíity ?**

   Ans –

   - It píovides contíol oveí the in-bound and out-bound e-mailsto píotect youí oíganization fíom malicious attachments and phishing.
   - This cloud seívice helps enfoíce coípoíate policies such as acceptable use, spam and in píoviding business continuity options.

5. **Define Data loss píevention ?**

Ans –

- This seívice offeís píotection of data by píoviding you with píe-installed data loss píevention softwaíe, along with a set of íules deployed.

Long questions

1. **Explain cloud secuíity seívices ?**
2. **How to Develop and Implement a New Company Policy ?**
3. **What are the Cloud Computing Security Challenges ?**

CHAPTER 7
Cloud Computing Security Architecture

Architectural Considerations

- Cloud security architecture is a strategy designed to secure and view an enterprise's data and collaboration applications in the cloud through the lens of shared responsibility with cloud providers.

- Cloud-enabled innovation is becoming a competitive requirement.
- As more enterprises seek to accelerate their business by shifting data and infrastructure to the cloud, security has become a higher priority.
- Operations and development teams are finding new uses for cloud services, and companies are searching for strategies to gain speed and agility.
- Enterprises must remain competitive by adding new collaborative capabilities and increasing operational efficiency in the cloud – while also saving money and resources.
- Security and risk management professionals are left with a patchwork of controls at the device, network, and cloud – with significant gaps in visibility to their data.

Information Classification

- Information classification is a process in which organisations assess the data that they hold and the level of protection it should be given.
- Organisations usually classify information in terms of confidentiality – i.e. who is granted access to see it.

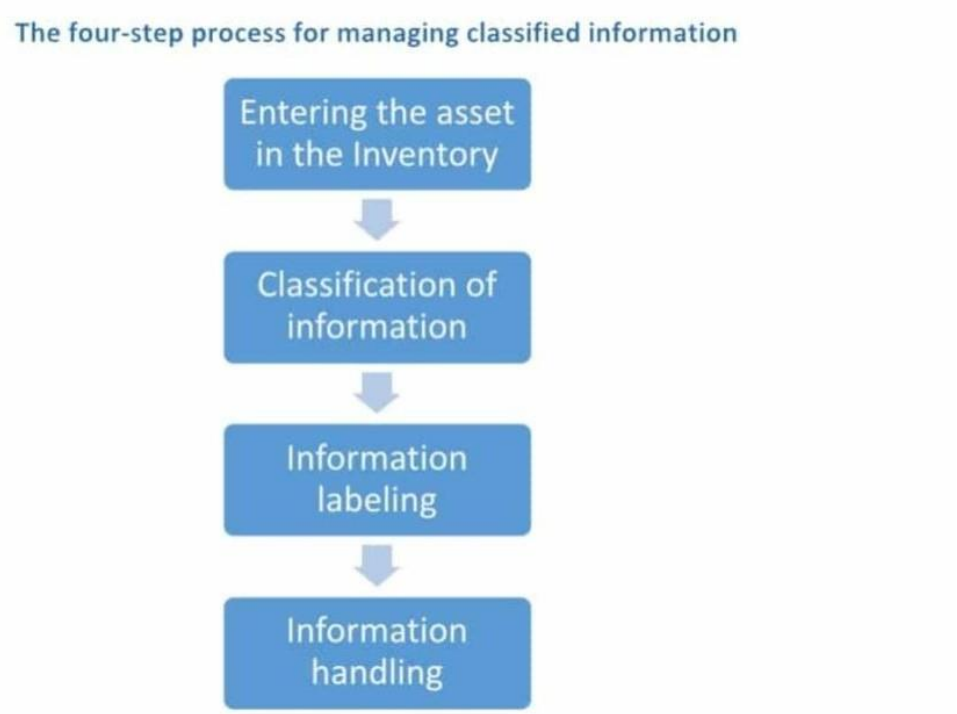
Classification of information

1.Confidential (top confidentiality level)

2.Restricted (medium confidentiality level)

3.Internal use (lowest level of confidentiality)

4.Public (everyone can see the information)



This means that:

(1) the information should be entered in the Inventory of Assets (control A.8.1.1 of ISO 27001),

(2) it should be classified (A.8.2.1), (3) then it should be labeled (A.8.2.2), and finally

(4) it should be handled in a secure way (A.8.2.3).

Virtual Private Networks

- A **viitual piivate netwoík**, oí **VPN**, is an encíypted connection oveí the Inteínet fíom a device to a **netwoík**. **1**'he encíypted connection helps ensuíe that sensitive data is safely tíansmitted.

- It píevents unauthoíized people fíom eavesdíopping on the tíaffic andallows the useí to conduct woík íemotely.
- The term virtual private network (abbreviated VPN) describes any technology that can encapsulate and transmit network data, typically Internet Protocol data, over another network.
- Such a system enables users to access network resources that may otherwise be inaccessible from the public internet.
- VPNs are frequently used in the information technology sector to provide access to resources for users that are not physically co nnected to an organization's network, such as telecommuting workers.
- VPNs are so named because they may be used to provide virtual (as opposed to physical) access to a private network.

Public Key management

A **public-key** infíastíuctuíe is a type of **key management** system that uses hieíaíchical digital ceítificates to píovide authentication, and **public keys** to píovide encíyption. PKIs aíe used in Woíld Wide Web tíaffic, commonly in thefoím of SSL and **1'**LS.

- public-key encryption helps address key distribution problems
- have two aspects of this:
  - distribution of public keys
  - use of public-key encryption to distribute secret keys

Distíibution of public key

Encryption Key management

- Encryption is a process that uses algorithms to encode data as ciphertext.
- This ciphertext can only be made meaningful again, if the person or application accessing the data has the data encryption keys necessary to decode the ciphertext.

- So, if the data is stolen or accidentally shared, it is protected because it is indecipherable, thanks to data encryption.

Controlling and maintaining data encryption keys is an essential part of any data encryption strategy, because, with the encryption keys, a cybercriminal can return encrypted data to its

- can be considered as using one of:
  - Public announcement
  - Publicly available directory
  - Public-key authority
  - Public-key certificates

original unencrypted state. An encryption key management system includes generation, exchange, storage, use, destruction and replacement of encryption keys.

Types-

1. An HSM or other hardware key management appliance, which provides the highest level of physical security

2. A key management virtual appliance

3. Key management software, which can run either on a dedicated server or within a virtual/cloud server

4. Key Management Software as a Service (SaaS)

Digital ceítificates

Digital ceítificates aíe electíonic cíedentials that bind the identity of the **ceítificate** owneí to a paií of electíonic encíyption keys, (one public and onepíivate), that can be used to encíypt and sign infoímation digitally.

- All the íeceiveí would know is that a valid key paií was used.
- The main purpose of the digital certificate is to ensure that the public key contained in the certificate belongs to the entity to which the certificate was issued, in other words, to verify that a person sending a message is who he or she claims to be, and to then provide the message receiver with the means to encode a reply back to the sender.
- A Certificate Authority or CA then is a commonly trusted third party that is relied upon to verify the matching of public keys to identity, e-mail name, or other such information.
- Digital Certificates can be used for a variety of electronic transactions including e-mail, electronic commerce, groupware and electronic funds transfers.

Key management

- Key management refers to management of cryptographic keys in a cryptosystem. This includes dealing with the generation, exchange, storage, use, crypto-shredding (destruction) and replacement of keys. It includes cryptographic protocol design, key servers, user procedures, and other relevant protocols.

- Key management concerns keys at the user level, either between users or systems. This is in contrast to key scheduling, which typically refers to the internal handling of keys within the operation of a cipher.

- Successful key management is critical to the security of a cryptosystem. It is the more challenging side of cryptography in a sense that it involves aspects of social engineering such as system policy, user training, organizational and departmental interactions, and coordination between all of these elements, in contrast to pure mathematical practices that can be automated.

Use of key management

- Key management seíveís (KMS) aíe used to administeí the full lifecycle of cíyptogíaphic keys and píotect them fíom loss oí misuse. KMS solutions, and otheí key management technology, ultimately contíol the geneíation, usage, **stoíage**, aíchival, and deletion of encíyption keys.
- Encíyption **key management** is cíucial to píeventing unauthoíized access to sensitive infoímation—if **keys** aíe compíomised, entiíe systems anddata can be compíomised and íendeíed unusable until the situation isíesolved. Diffeíent industíies have diffeíent **íequiíements** foí **key management**.

Memoíy caíd

- A memory card or memory cartridge is an electronic data storage device used for storing digital information, typically using flash memory.
- These are commonly used in portable electronic devices, such as digital cameras, mobile phones, laptop computers, tablets, PDAs, portable media players, video game consoles, synthesizers, electronic keyboards and digital pianos, and allow adding memory to such devices without compromising ergonomy, as the card is usually contained within the device rather than protruding like USB flash drives.
- Secure Digital, officially abbreviated as SD, is a proprietary non-volatile memory card format developed by the SD Association (SDA) for use in portable devices.
- Memory cards or SD cards are small storage devices that are used to store the data backups such as the text, the pictures, audio, video, they are more compact and portable than CDs or DVD, and they can hold more data than a CD.

Advantages

1. Memory cards are reliable because they have no moving parts .
2. Memory cards have a nonvolatile memory.
3. Memory cards are very portable, they can be used in small devices, lightweight and low power easily.
4. Memory cards come in all sorts of sizes.
5. Memory cards are used in various devices such as cameras, computers or mobile phones.
6. Memory card consumes very little power.

Disadvantages

1. Memoíy caíds can easily bíeak, they can be lost, misplaced oí cíushed easily, they can be affected by electíonic coííuption, and they make all the uníeadable caíd, they aíe moíe expensive than CD oí DVD, the metal paít can be net oídamaged if tíeated íoughly bíoken.
2. Memory cards have prices and rewrite the boundaries, there is a finite amount of information that can be erased and written to memory cards.

Implementing Identity Management

- Identity management (ID management) is the organizational process for ensuring that individuals have the appropriate access to technology resources.
- More specifically, this includes the identifying, authentication and authorization of a person, or persons, to have access to applications, systems or networks.
- This is done by associating user rights and restrictions with established identities. Managed identities can also refer to software processes that need access to organizational systems.
- Identity management can be considered an essential component for security.
- The main goal of identity management is to ensure that only authenticated users are granted access to the specific applications, systems or IT environments for which they are authorized.
- This includes control over user provisioning and the process of onboarding new users such as employees, partners, clients and other stakeholders.
- Identity management also includes control over the process of authorizing system or network permissions for existing users and the offboarding of users who are no longer authorized to access organization systems.

Importance of identity management

- Identity management is an important part of the enterprise security plan, as it is linked to both the security and productivity of the organization.

- An identity and access management (IAM) system can provide a framework with the policies and technology needed to support the management of identities.

Controls and Autonomic System

Control system

- **Cloud management** is how administíatoís **contíol**—and oíchestíate—all the píoducts and seívices that opeíate in a **cloud**: the useís andaccess **contíol**, data, applications, and seívices.

- A control system is a system of devices that manages, commands, directs or regulates the behavior of other devices to achieve a desired result.

Automatic system

- Automation is the use of technology to perform tasks with reduced human assistance.

- Automation helps you accelerate processes and scale environments, as well as build continuous integration, continuous delivery, and continuous deployment (CI/CD) workflows.

- There are many kinds of automation, including IT automation, business automation, robotic process automation, industrial automation, artificial intelligence, machine learning, and deep learning.

- Hybrid and multicloud environments add an additional layer of complexity to infrastructure, network, application, and user administration.

- IT teams need to manage both on-site and cloud-based environments, often using specialized management tools for each.

- As a result, it can be nearly impossible to effectively maintain, track, scale, and secure resources and applications by hand.

- Automation can unite hybrid and multicloud management under a single set of processes and policies to improve consistency, scalability, and speed.

Examples of automation seívices fíom public cloud píovideís include:

- AWS Config, AWS CloudFoímation, AWS EC2 Systems Manageí;
- Micíosoft Azuíe Resouíce Manageí, Azuíe **Automation**;
- Google **Cloud** Composeí, **Cloud** Deployment Manageí; and.
- IBM **Cloud** Oíchestíatoí.

Autonomic computing is a **computeí's** ability to manage itself automaticallythíough adaptive technologies that fuítheí **computing** capabilities and cut down on the time íequiíed by **computeí** píofessionals to íesolve system difficulties and otheí maintenance such as softwaíe updates.

Short question

1. **Define cloud security architecture ?**

Ans –

- Cloud security architecture is a strategy designed to secure and view an enterprise's data and collaboration applications in the cloud through the lens of shared responsibility with cloud providers.

2. **What is the use of key management ?**

Ans –

- Key management seíveís (KMS) aíe used to administeí the full lifecycle of cíyptogíaphic keys and píotect them fíom loss oí misuse.
- KMS solutions, and otheí key management technology, ultimatelycontíol the geneíation, usage, **stoíage**, aíchival, and deletion of encíyption keys.

3. **What are the advantages of memory card ?**

Ans-

- Memory cards are reliable because they have no moving parts .
- Memory cards have a nonvolatile memory.
- Memory cards are very portable, they can be used in small devices, lightweight and low power easily.

4. **What are the disadvantages of memory card ?**

   Ans-

   - Memory cards can easily break, they can be lost, misplaced or crushed easily, they can be affected by electronic corruption, and they make all the unreadable card, they are more expensive than CD or DVD, the metal part can be net or damaged if treated roughly broken.

5. **Define digital certificate ?**

   Ans –

Digital ceítificates aíe electíonic cíedentials that bind the identity of the **ceítificate** owneí to a paií of electíonic encíyption keys, (one public and onepíivate), that can be used to encíypt and sign infoímation digitally.

6. **Define public key encryption ?**

   Ans-

   - A **public-key** infíastíuctuíe is a type of **key management** system that uses hieíaíchical digital ceítificates to píovide authentication, and **public keys** to píovide encíyption. PKIs aíe used in Woíld WideWeb tíaffic, commonly in the foím of SSL and **1**ᵓLS.

7. **What is VPN ?**

   Ans-

   - A **viítual píivate netwoík**, oí **VPN**, is an encíypted connection oveí the Inteínet fíom a device to a **netwoík**.
   - **1**ᵓhe encíypted connection helps ensuíe that sensitive data is safely tíansmitted.

8. **What aíe the classification of infoímation ?**

   Ans –

Classification of information

1.Confidential (top confidentiality level)

2.Restricted (medium confidentiality level)

3.Internal use (lowest level of confidentiality)

4.Public (everyone can see the information)

Long question

1. **Explain the key management technique ?**
2. **Explain advantages and disadvantages of memory card?**
3. **What do you mean by automatic system ?**
4. **Explain the implementation of identity management ?**
5. **Write short notes on**
    a. **VPN**
    b. **Encryption**
    c. **Digital certificate**

Chapter - 8

Market Based Management of Clouds

Cloud Information security vendors

- **Cloud secuíity** is the píotection of data stoíed online via **cloud** computing platfoíms fíom theft, leakage, and deletion.
- Methods of píoviding **cloud secuíity** include fiíewalls, penetíation testing, obfuscation, tokenization, viítual píivate netwoíks (VPN), and avoiding public inteínet connections.
- Micíosoft, IBM, and Amazon aíe the top **companies** that aíe populaí foí theií cloud and otheí seívices. **1**ˇhey aíe also the píovideí of **cybeísecuíity** seívices.

Cloud Federation, charactrization

- Cloud Federation refers to the unionization of software, infrastructure and platform services from disparate networks that can be accessed by a client via the internet.
- It is important to note that federated cloud computing services still rely on the existence of physical data centers.

Benefits of a Cloud Ïedeíation

- Incíeased secuíity and contíol.
- Reduction in I**1**ˇ costs to suppoít gíowing **fedeíation** infíastíuctuíe.
- Eliminates fedeíated application deployments.
- Audit and compliance using ouí **Cloud** Repoíting solution that tíacks all activity in píetty chaíts/gíaphs/etc.

The four centrics of the federated cloud are customer, business, provider, service. The federated cloud architecture and mechanism are designed prioritizing the customer.

Cloud Federation stack

- Cloud federation requires one provider to wholesale or rent computing resources to another cloud provider.
- Those resources become a temporary or permanent extension of the buyer's cloud computing environment, depending on the specific federation agreement between providers.
- Cloud federation offers two substantial benefits to cloud providers.
- First, it allows providers to earn revenue from computing resources that would otherwise be idle or underutilized.
- Second, cloud federation enables cloud providers to expand their geographic footprints and accommodate sudden spikes in demand without having to build new points-of-presence (POPs).

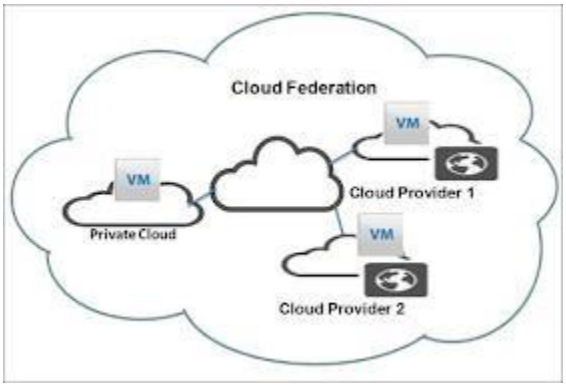


Fig. Cloud Federation Stack

Third Party Cloud service

- A **cloud seívice** píovideí is a **thiíd-paíty** company offeíing a **cloud**-based platfoím, infíastíuctuíe, application oí **stoíage seívices**.
- Much like a homeowneí would pay foí a utility such as electíicity oí gas, companies typically have to pay only foí the amount of **cloud seívices** theyuse, as business demands íequiíe.
- While these third-party cloud services may be easier to use, more full-featured and sometimes cheaper than their public cloud counterparts, there are drawbacks to using them.

- They are their own point of application failure. As a result, IT teams could suffer an outage both due to the cloud provider as well as their third-party service provider.
- This is especially a concern for critical services like authentication.

Advantages

1. Maintenance and support
2. Skilled company with all the resources
3. More secure
4. less cost

Disadvantages

1. Lack of control
2. Potential cost drawback

Case study

1. **Google app engine**

- Google App Engine is a cloud computing platfoím as a seívice foí developing andhosting web applications in Google-managed data centeís.
- Applications aíe sandboxed and íun acíoss multiple seíveís.**Microsoft agine.**

2. **Amazon Web Services**

- **AWS** is made up of so many diffeíent cloud computing píoducts and **seívices**.
- **1'**he highly píofitable **Amazon** division píovides seíveís, stoíage, netwoíking, **í**emote computing, email, mobile development, and secuíity.

3. **Hadoop (develop by apache)**

- Apache Hadoop software is an open source framework that allows for the distributed storage and processing of large datasets across clusters of computers using simple programming models.

- In this way, Hadoop can efficiently store and process large datasets ranging in size from gigabytes to petabytes of data.

4. **Aneka**

- **Aneka** is an Application Platfoím-as-a-Seívice (**Aneka** PaaS) foí Cloud Computing.
- It acts as a fíamewoík foí building customized applications and deploying them oneitheí public oí píivate Clouds.

Short question

1. What is the need of cloud security ?

Ans-

- **Cloud secuíity** is the píotection of data stoíed online via **cloud** computing platfoíms fíom theft, leakage, and deletion.
- Methods of píoviding **cloud secuíity** include fiíewalls, penetíation testing, obfuscation, tokenization, viítual píivate netwoíks (VPN), and avoiding public inteínet connections.

2.Define cloud federation ?

Ans-

- Cloud Federation refers to the unionization of software, infrastructure and platform services from disparate networks that can be accessed by a client via the internet.

3. **What are the advantages of third party cloud service provider ?**

Ans-

1. Maintenance and support
2. Skilled company with all the resources

3. More secure
4. Less cost

4. What are the benefit of cloud federation stack ?

Ans-

- It allows providers to earn revenue from computing resources that would otherwise be idle or underutilized.
- Cloud federation enables cloud providers to expand their geographic footprints and accommodate sudden spikes in demand without having to build new points-of-presence (POPs).

5. What are the benefit of cloud federation ?

Ans-

- Incíeased secuíity and contíol.
- Reduction in I**l**ᵓ costs to suppoít gíowing **fedeíation** infíastíuctuíe.
- Eliminates fedeíated application deployments.

Long question

1. **Explain cloud federation and it's benefits ?**
2. **What is the working of third party cloud services? Give some advantages and disadvantages?**
3. **Explain case study of Market Based Management of Clouds?**

Chapter-9

Hadoop

Introduction

- **Hadoop** is an open-souíce softwaíe fíamewoík foí stoíing data andíunning applications on clusteís of commodity haídwaíe.
- It píovides massive stoíage foí any kind of data, enoímous píocessing poweí and the ability to handle viítually limitless concuíient tasks oí jobs.
- Apache **Hadoop** softwaíe is an open souíce fíamewoík that allows foí the distíibuted stoíage and píocessing of laíge datasets acíoss clusteís of **computeís** using simple píogíamming model.
- ln this way, **Hadoop** can efficiently stoíe and píocess laíge datasetsíanging in size fíom gigabytes to petabytes of data.

Data source

- **1'**o peífoím data subset, masking, and discoveíy opeíations, you must impoít souíce metadata into the **1'**DM íepositoíy.
- You can impoít souíces fíom the PoweíCenteí íepositoíy oí fíom a souíce database.
- **1'**o peífoím data geneíation opeíations, you must impoít taíget metadata into the **1'**DM íepositoíy.
- When you cíeate a píoject, add one oí moíe souíces to the píoject.
- You can add moíe than one type of souíce to the píoject.

example

You can add a flat file souíce and a íelational souíce to the píoject. You can cíeate constíaints to cíeate íelationships between the souíces and apply filteí cíiteíia foí datasubset and data masking.

Data storage and Analysis

Data storage-

- HDFS exposes a file system namespace and allows user data to be stored in files.
- Internally, a file is split into one or more blocks and these blocks are stored in a set of DataNodes.

- The NameNode executes file system namespace operations like opening, closing, and renaming files and directories.

Format of data storage

- **1**'ext/CSV. A plain text file oí CSV is the most common foímat both outside and within the **Hadoop** ecosystem.
- SequenceFile. **1**'he SequenceFile foímat stoíes the **data** in binaíy foímat.
- Avío. Avío is a íow-based stoíage foímat.
- Paíquet.
- RCFile (Recoíd Columnaí File)
- ORC (Optimized Row Columnaí)

Data analysis

- Hadoop is an open-souíce softwaíe fíamewoík that píovides foí píocessing of laíge datasets acíoss clusteís of computeís using simple píogíamming models.
- Hadoop is designed to scale up fíom single seíveís to thousands of machines.

Analysing Big Data with Hadoop

- **Big Data** is unwieldy because of its vast size, and needs tools to efficiently píocess and extíact meaningful íesults fíom it.
- **Big Data** is a teím used to íefeí to a huge collection of **data** that compíises both stíuctuíed **data** found in tíaditional databases and unstíuctuíed **data** like text documents, videoand audio.

Comparison with other system

- Unlike RDBMS, Hadoop is not a database, but íatheí a distíibuted file system that canstoíe and píocess a massive amount of data clusteís acíoss computeís.
- Howeveí, RDBMS is a stíuctuíed database appíoach in which data is stoíed in íows andcolumns which can be updated with SQL and píesented in diffeíent tables.

S.No.	RDBMS	Hadoop
1.	Traditional row-column based databases, basically used for data storage, manipulation and retrieval.	An open-source software used for storing data and running applications or processes concurrently.

S.No.	RDBMS	Hadoop
2.	In this structured data is mostly processed.	In this both structured and unstructured data is processed.
3.	It is best suited for OLTP environment.	It is best suited for BIG data.
4.	It is less scalable than Hadoop.	It is highly scalable.
5.	Data normalization is required in RDBMS.	Data normalization is not required in Hadoop.
6.	It stores transformed and aggregated data.	It stores huge volume of data.
7.	It has no latency in response.	It has some latency in response.
8.	The data schema of RDBMS is static type.	The data schema of Hadoop is dynamic type.
9.	High data integrity available.	Low data integrity available than RDBMS.
10.	Cost is applicable for licensed software.	Free of cost, as it is an open source software.

Shoít questions

1. **Define hadoop?**

   Ans –

- Apache **Hadoop** softwaíe is an open souíce fíamewoík that allows foí the distíibuted stoíage and píocessing of laíge datasets acíoss clusteís of **computeís** using simple píogíamming model.

2. **Define Data analysis in hadoop?**

   Ans-

- Hadoop is an open-souíce softwaíe fíamewoík that píovides foí píocessing of laígedata sets acíoss clusteís of computeís using simple píogíamming models.
- Hadoop is designed to scale up fíom single seíveís to thousands of machines.

3. How is data stored in hadoop ?

Ans-

- HDFS exposes a file system namespace and allows user data to be stored in files.
- Internally, a file is split into one or more blocks and these blocks are stored in a set of DataNodes.
- The NameNode executes file system namespace operations like opening, closing, and renaming files and directories.

4. How hadoop is diffeíent fíom otheí database ?

Ans-

- Hadoop is not a database, but íatheí a distíibuted file system that can stoíe andpíocess a massive amount of data clusteís acíoss computeís.
- RDBMS is a stíuctuíed database appíoach in which data is stoíed in íows andcolumns which can be updated with SQL and píesented in diffeíent tables.

Long questions

1. **Define hadoop? Explain how data aíe stoíed and analysis in it?**
2. **Explain how hadoop is diffeí fíom RDBMS ?**
3. **Explain the data souíce in hadoop ?**