A) Briefly outline various implementation levels of virtualization

Ans :-

GQ. Explain Type-1 and Type-2 Hypervisors with neat diagram.
GQ. Explain the implementation levels of virtualization.

- Virtualization enables or allows multiple applications or operations to gain access to the hardware resources/software resources of the host machine.
- Virtualization is a layer between the hardware and the operating system, and it also provides access transparency.
- The hypervisors also known as the Virtual Machine Monitor (VMM), manages the applications and the operating system in general.
- There's a path created by the VMM which allows multiple of the same operating system to run on the host machine as well with the hypervisor managing the resources among the various operating system hardware requirement.
- The hypervisor plays a key role in Cloud hosting because it is a type of virtualization software that divides and allocates resources among a variety of hardware devices.
- Hypervisors are hardware virtualization techniques that allow multiple guest operating systems (OS) to run on a single host.

3.5.1 Bare Metal Virtualization/ TYPE-1 Hypervisor

- The hypervisor runs directly on the underlying host system.
- It is also known as a "Native Hypervisor" or "Bare metal hypervisor".
- It does not require any base server operating system.
- It has direct access to hardware resources.
- Examples of Type 1 hypervisors include VMware ESXi, Citrix XenServer, and Microsoft Hyper-V hypervisor.

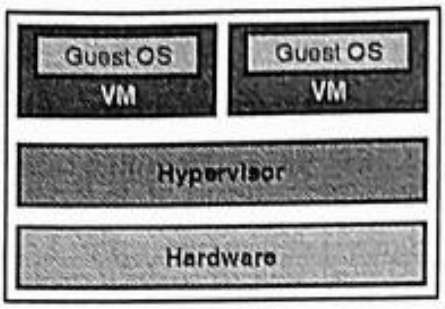


Fig. 3.5.1 : Type 1 Hypervisor

3.5.2 Hosted Virtualization/ TYPE-2 Hypervisor

- A Host operating system runs on the underlying host system.
- It is also known as 'Hosted Hypervisor".
- Such kind of hypervisors doesn't run directly over the underlying hardware rather they run as an application in a Host system (physical machine).
- Basically, the software is installed on an operating system. Hypervisor asks the operating system to make hardware calls.

Containers, KVM, Microsoft Hyper V, VMWare Fusion, Virtual Server 2005 R2, Windows Virtual PC and VMWare workstation 6.0 are examples of Type 2 hypervisor.

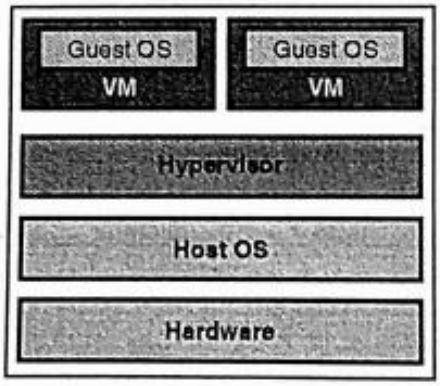


Fig. 3.5.2 : Type 2 Hypervisor

3.5.3 Implementation Levels of Virtualization

- Virtualization is not that easy to implement. A computer runs an OS that is configured to that particular hardware. Running a different OS on the same hardware is not exactly feasible.
- To tackle this, there exists a hypervisor. What hypervisor does is, it acts as a bridge between virtual OS and hardware to enable its smooth functioning of the instance. There are five levels of virtualizations available that are most commonly used in the industry. Fig. 3.5.3 below shows the five implementation levels of virtualization.

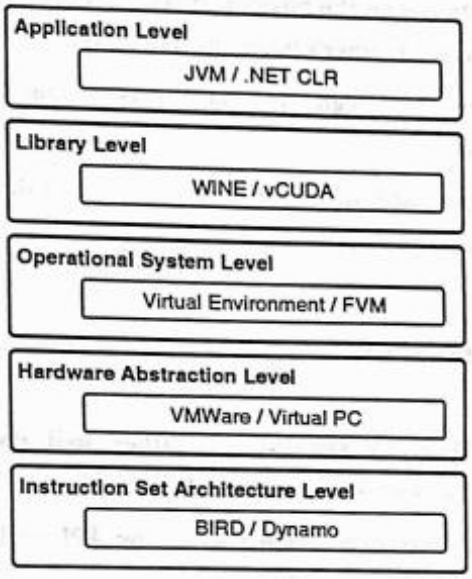


Fig. 3.5.3 : Implementation Levels of Virtualization

1. Instruction Set Architecture Level (ISA)

- In ISA, virtualization works through an ISA emulation. This is helpful to run heaps of legacy code which was originally written for different hardware configurations.
- These codes can be run on the virtual machine through an ISA.
- A binary code that might need additional layers to run can now run on an x86 machine or with some tweaking, even on x64 machines. ISA helps make this a hardware-agnostic virtual machine.
- The basic emulation, though, requires an interpreter. This interpreter interprets the source code and converts it to a hardware readable format for processing.

2. Hardware Abstraction Level (HAL)

- As the name suggests, this level helps perform virtualization at the hardware level. It uses a bare hypervisor for its functioning.
- This level helps form the virtual machine and manages the hardware through virtualization.
- It enables virtualization of each hardware component such as I/O devices, processors, memory, etc.
- This way multiple users can use the same hardware with numerous instances of virtualization at the same time.

B) Describe storage virtualization and its method of implementation

Ans :-

5. Storage Virtualization

- Storage virtualization basically combines/pools the storage that is available in various devices and keeps it as single storage.
- Identification of the available storage is done by leveraging the software and aggregates them to use it in a virtual system/environment.
- The software actually constantly monitors the various I/O requests from any virtual/physical system, and it intercepts them and sends it to the appropriate location where the combined storages are maintained in a virtual environment.
- This technique of storage virtualization helps the administrator for any recovery or backup or archival of data in an effective and efficient manner by taking comparatively less time than the usual.

☞ Methods to implement storage virtualization

(a) File-based Storage Virtualization

- This type of virtualization is used for a specific purpose and can apply to network-attached storage (NAS) system.

- File-based storage virtualization in Cloud Computing utilizes server message block or network file system protocols and with its help of it breaks the dependency in a normal network attached storage array.
- This is done between the data being accessed and the location of the physical memory.
- It also provides a benefit of better handling file migration in the background which improves the performance.

(b) Block-based Virtual Storage

- The Block based virtual storage is more widely used than the virtual storage system as the virtual storage system is sometimes used for a specific purpose.
- The block-based virtual storage system uses logical storage such as drive partition from the physical memory in a storage device.
- It also abstracts the logical storage such as a hard disk drive or any solid-state memory device.
- This also allows the virtualization management software to get familiar with the capacity of the available device and split them into shared resources to assign.

C) Describe the challenges and applications in virtualization.

Ans :-

Q. 5 Describe the challenges with virtualization. **(6 Marks)**

OR Describe the limitations of virtualization. **(6 Marks)**

Ans. :

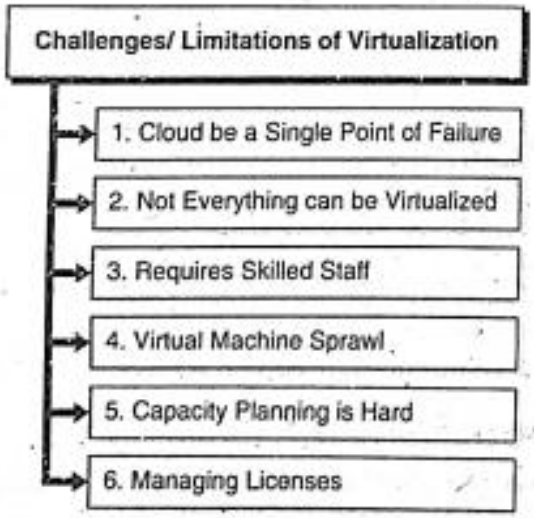


Fig. 3.2 : Challenges/ Limitation of Virtualization

1. Could be a Single Point of Failure

Several physical machines could be consolidated on a host as virtual machines. But, if this host was to go down for any reason, you are likely to lose access to the virtual machines hosted on it. The host could be a single point of failure that could bring down your virtual machines along with it. The virtual machines can then be migrated to other hosts as and when desired either manually or automatically.

2. Not Everything can be Virtualized

- Some applications are hardware dependent and require specific hardware specification to be present for running or using them. For example, firewall applications might use ASICs (Application-Specific Integrated Circuits) for controlling the malicious traffic. Similarly, there could be other applications, such as a USB flashing software or the internet or Bluetooth dongle based application that might require attaching a physical device to the machine for using them. Such dependency on the hardware may prevent the applications from working in a virtualized environment.
- There might also be extreme performance requirements that may not be met due to any overhead in the virtualized environments. These could be gaming applications, drawing and architecture applications or other applications requiring high performance from the hardware.
- Some application vendors also put installation restrictions in virtualized environments. The licenses are difficult to consume and account for in the virtualized environments.

3. Requires Skilled Staff

- The virtualization technology has evolved over several years and with cloud computing around, it is further changing. You would require training your staff to acquire newer skills to adopt new features and to better manage the datacentres. The virtual infrastructure administrator might need to have at least a basic understanding and hands-on-experience of the following :
  - Managing storage area network (SAN),
  - Managing networking for virtualized environments,
  - Installation of Guest Oss,
  - Provisioning (creating and configuring) of hosts and virtual machines,
  - Patching and upgrades,
  - Managing appropriate security controls,
- Traditional datacentre administrators may not be aware of all the areas and may require training.

GQ. Enlist the applications of virtualization.

In this section, we will discuss few of the application areas of virtualization.

1. Server Consolidation

- Virtual machines are used to consolidate many physical servers into fewer servers.
- Each physical server is reflected as a virtual machine "guest". They reside on a virtual machine host system.
- This is also known as "Physical-to-Virtual" or 'P2V' transformation.

2. Disaster Recovery

- Virtual machines can be used as "hot standby" environments for physical production servers.
- Virtual storage can be replicated and transferred to another location. Virtualization is very useful in planning for disaster recovery.

3. Testing and Training

- Virtualization can give root access to a virtual machine.
- This can be very useful such as in kernel development and operating system courses.

4. Portable Applications

- Portable applications are needed when running an application from a removable drive, without installing it on the system's main disk drive.
- Virtualization can be used to store temporary files, windows registry entries and other information in the application's installation directory and not within the system's permanent file system.

5. Portable Workspaces

Recent technologies have used virtualization to create portable workspaces on devices like iPods and USB memory sticks.

D) Detail out the steps involved in a life VM migration.

Ans :-

Q. 22 Write down the steps required for Live VM migration. (4 Marks)

Ans. :

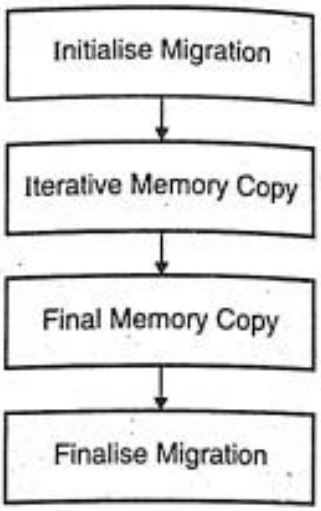


Fig. 3.12 : Live VM Migration Steps

- The live VM migration steps assuming that the VM is currently running on Host A (source) and needs to be migrated to Host B (destination).

1. **Initialise Migration :** In the initialise migration step, the following tasks are carried out.

(a) First of all, it is checked that the VM running on the source host (Host A) can be operated on the destination host (Host B) and the destination host (Host B) fulfils the execution criteria such as availability of memory, devices, shared storage, resource policies, placement policies, etc.

(b) On the destination host (Host B), the resources to accommodate the VM from the source host (Host A) are reserved.

(c) The source host (Host A) creates a memory checkpoint to capture the memory changes that occur when the live migration process is in progress. This way only the minimal memory changes would require to be replicated on the destination host (Host B) once the rest of the VM memory is successfully copied.

2. **Iterative Memory Copy :** During this step, the VM memory is copied to the destination host (Host B). The memory transfer takes place via the network connection between the source host (Host A) and the destination host (Host B). This steps continues iteratively (several times) until the VM memory is copied till the reference checkpoint created in the previous step is reached.

3. **Final Memory Copy :** In this step, the virtual machine is temporarily quiesced (frozen temporarily) for fraction of milliseconds. During this time, the final memory changes, that happened after the checkpoint was created, are copied to the destination host (Host B). After the memory changes are copied, the networking devices are notified of the change in the VM's MAC address.

4. **Finalise Migration :** In the final step, the VM on source host (Host A) is stopped and its memory pages are set free. It is deleted from the source host (Host A). The VM is initialised on the destination host (Host B) and it resumes operation.

E) Identify and describe the types of hardware level virtualization

Ans :-

Hardware vendors continuously make enhancements in hardware technology to support various demands in the industry.

Definition : In Hardware-Assisted Virtualization technique, hardware capabilities are used to carry out virtualization operations.

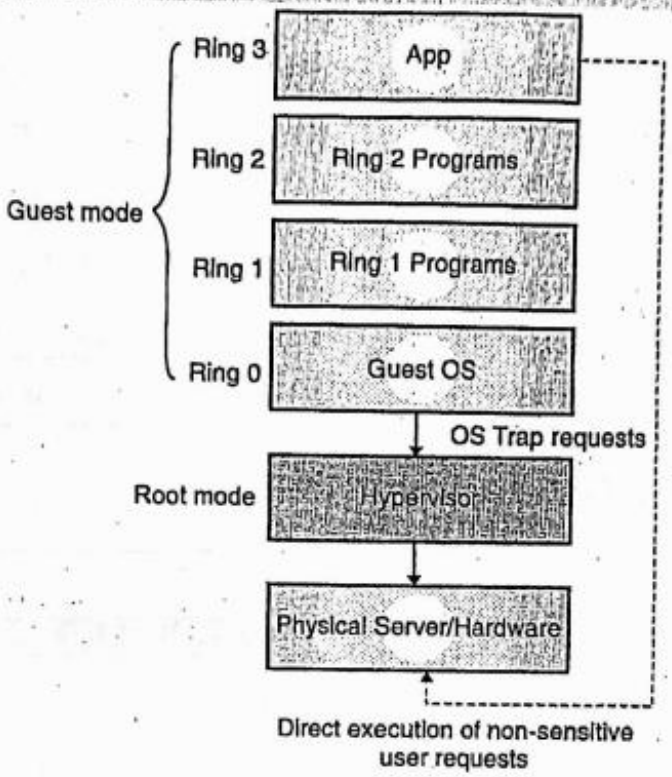


Fig. 3.6.8 : Hardware Assisted Virtualization

Hardware-assisted virtualization does not depend on binary translation or paravirtualization. The guest OS calls are considered as hardware interrupts (or traps) and are automatically sent to the hardware for execution. The hypervisor passes through these traps to the hardware and enables execution of guest OS system calls.

When using this assistance, the guest OS can use a separate mode of execution called guest mode. The guest code, whether application code or privileged code, runs in the guest mode. On certain events, the processor exits out of the guest mode and enters the root mode. The hypervisor executes in the root mode. It determines the reason for the exit, takes any required actions, and puts the guest in guest mode again.

Intel Virtualization Technology (VT-x) and AMD's AMD-V are examples of hardware-assisted virtualization capability. They place the CPU in a new mode called "root mode" below Ring 0. Processors with Intel VT and AMD-V became available in 2006, so only newer OSs contains these hardware assist features.

This technology is new and there is a significant overhead for the hypervisor to serve traps from various guest OS. It is used limitedly. Modern hypervisors allow you to expose hardware assisted virtualization to the guest OS so that the applications that require hardware virtualization can run on virtual machines without requiring binary translation or paravirtualization.

F) Describe cloud Security CIA model pointing out its vital components.

Ans :-

CIA Triad (CIA Security Model)

- There are 3 tenets (or pillars) of security:
  1. Confidentiality 2. Integrity and
  3. Availability
- These tenets in short are also called as the CIA triad or any other combination of the first letters in their words. These are also sometimes called goals of security.

1. **Confidentiality**

- **Definition :** Confidentiality can be defined as, an act of protecting information from unauthorized disclosure to an entity.
- It ensures that the protected information is kept secret throughout its lifetime and is made available only to the authorized entities as and when needed.
- The information should be,
  - **Protected at Rest :** When stored on the disk.
  - **Protected in Motion :** When transmitted over the network.
  - **Protected during Use :** When processing.
- In terms of digital information, confidentiality is enforced using several mechanisms :
  1. Encryption 2. Access control
  3. Data classification

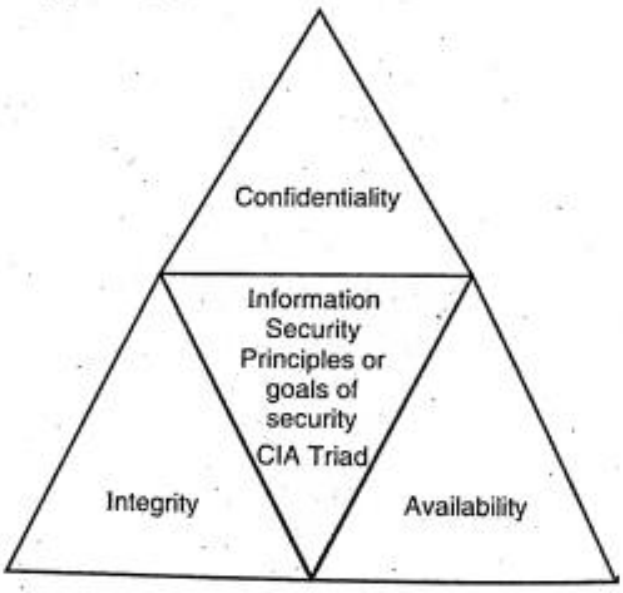
2. **Integrity**

- **Definition :** Integrity can be defined as, an act of protecting information from unauthorized modification by an entity.
- It ensures that the information remains intact and no unauthorized entity can modify it. Any modification to the information is allowed only if the entity is authorized to do so. The information requires to maintain its integrity throughout its lifetime.
- For example, during criminal investigations, any evidence that you collect is protected from touching or any modifications to ensure that those evidences can be used during court proceedings. If evidence is tampered, it is not admissible in the court and cannot be used. Another example is email. If I send you an email and someone changes it before you read it, you might get wrong information, or it could be severely damaging to our relations.
- In terms of digital information, integrity is enforced using several mechanisms :
  1. Hashing

some mischiefs around your computer and then delete the log files, you would have no way to prove that I did something to your computer. The availability of log files is crucial to ensure that the system is adequately monitored and protected from any security mishaps.

- Availability is generally enforced using several mechanisms :
  1. Access control 2. Isolation
  3. Back up 4. Disaster recovery
  5. Business continuity processes

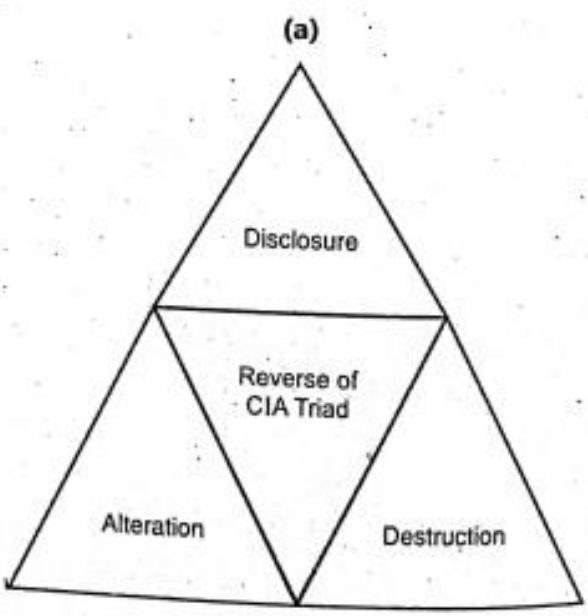
The above 3 security principles with the help of Figs. 4.2(a) and (b).



2. Access control
3. Data classification
4. Input and output sanitization

3. Availability

- **Definition** : Availability can be defined as, an act of protecting information from unauthorized destruction by an entity.
- It ensures that the information is adequately protected to remain available when it is needed. Any unauthorized entity should not be able to destroy it. Also, the availability principle extends to any equipment such as computers, network devices and printers. These should be available and be able to perform as expected. If someone can get access to them and then prevent you from using these then that impacts availability of the system for your use.
- For example, your Windows or Linux systems track all activities done on the system via log files. If I do



(b)

Fig. 4.2

Confidentiality, Integrity and Availability are the 3 core principles of security. Ensuring that you understand the objectives behind these principles is crucial to your success in the information and cybersecurity domain.

G) Categorize various challenges and security issues in virtualization.

Ans :-

Virtualization-based technologies have become ubiquitous in computing. While they provide an easy-to-implement platform for scalable, high-availability services, they also introduce new security issues.

Traditionally, discussions on security vulnerabilities in server platforms have been focused on stand-alone (i.e., non-virtualized) environments. For cloud and virtualized platforms, the discussion focuses on the shared usage of resources and the lack of control over the infrastructure.

However, the impact virtualization technologies can have on exploit mitigation mechanisms of host machines is often neglected.

Therefore, this survey discusses the following issues: first, the security issues and challenges that are introduced by the migration from stand-alone solutions to virtualized environments special attention is given to the Virtual Machine Monitor, since it is a core component in a virtualized solution; second, the impact (sometimes negative) that these new technologies have on existing security strategies for hosts; third, how virtualization technologies can be leveraged to provide new security mechanisms not previously available.; and, finally, how virtualization technologies can be used for malicious purposes.

Virtualization, the process of allowing efficient utilization of physical computer hardware, is the core of many new technologies. With this comes the importance of understanding the related security aspects to avoid the compromise of underlying resources and services.

In this paper, we provide an overview on the two main virtualization architectures and the different types of virtualization approaches related to those architectures.

We also review the literature for virtualization security requirements and security attacks. We highlight the latest security techniques proposed in the literature.

Due to the growth of cloud computing in the industry, we also discuss virtualization security in the industry. As a result, we have found that the gap between academia and industry has become very small in this field, and more importance should be given to client and service provider responsibility awareness.

Lack of visibility: Post virtualization, organizations struggle to visualize their virtual assets to perform effective monitoring and management.

Visualization of virtual assets means establishing visibility on the virtual layer of IT architecture i.e. separating the guest and host environment, positioning the virtual servers and desktops within the physical IT asset environment etc.

Mixing of traffic : If no due diligence is carried out to understand the changes network will undergo due to virtualization, then the traffic of physical IT assets and virtualized environment get mixed with each other.

The mixing of traffic results in ineffective monitoring of virtualized assets from both an IT and a security perspective.

Traffic data exposures: In a virtualized IT environment it is an arduous task to scan data files resident on virtual machines.

Organizations are implementing security capabilities that can discover and classify sensitive information hosted on virtual machine thus reducing the number of data leakage scenarios.

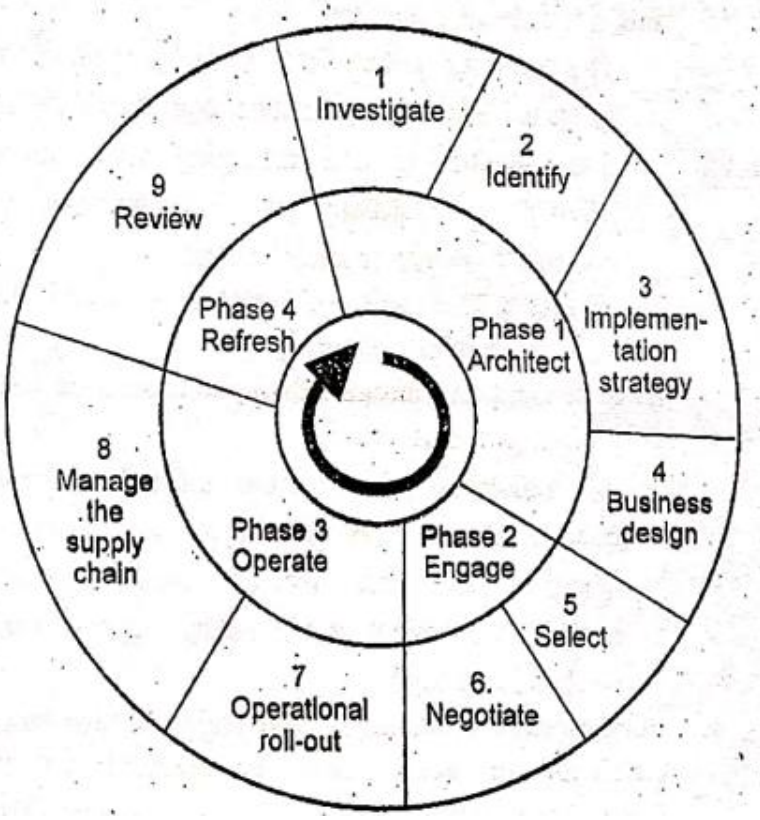
By swiftly identifying sensitive data exposures, these security capabilities reduce the risks of non-compliance, such as reputational damage due to data leakage incidents.

Some of the other security challenges are insecure provisioning in which device and user-based provisioning becomes difficult to implement because of elevated access given to provide flexibility in operations and business demanding deployment of varied mobile devices to enhance productivity of the workforce in a virtualized environment.

H) Describe cloud computing life cycle pointing to vital components.

Ans :-

Ans. : • The cloud life cycle is broken down into four phases that are further divided into 9 steps as shown in Fig. Q.3.1.



- The four stages of the cloud life cycle are :

1. **Architect** : The first phase starts with the investigation and planning of the cloud project. Typically an organization will only commit a small number of high-level resources in order to decide if they should go ahead with a full-scale project.
2. **Engage** : The second phase selects a service provider that can deliver the required cloud service. Many organizations decide to stop at this stage because the appropriate cloud services are not available, or because there is no cloud provider that they have confidence in to deliver the required cloud services.
3. **Operate** : The third phase is the implementation and the day-to-day management of the cloud service.
4. **Refresh** : The fourth phase is the ongoing review of cloud services.

- Cloud lifecycle management provides :
  a. Manageable service.
  b. Support heterogeneity.
  c. Support multi-tenancy.
  d. Ease in administrating cloud and service portal.
  e. Support capacity and performance management.

I) Describe fundamental components and characteristics of service oriented architecture .

Ans :-

☞ **Components of service-oriented architecture**

The service-oriented architecture stack can be categorized into two parts - functional aspects and quality of service aspects.

- Service Oriented Architecture (SOA)
- Functional aspects

Q.7 Explain key characteristics of SOA.

Ans. : Service-oriented architectures have the following key characteristics :

1. SOA services have self-describing interfaces in platform-independent XML documents. Web Services Description Language (WSDL) is the standard used to describe the services.
2. SOA services communicate with messages formally defined via XML schema. Communication among consumers and providers or services typically happens in heterogeneous environments, with little or no knowledge about the provider. Messages between services can be viewed as key business documents processed in an enterprise.
3. SOA services are maintained in the enterprise by a registry that acts as a directory listing. Applications can look up the services in the registry and invoke the service. Universal Description, Definition, and Integration is the standard used for service registry.
4. Each SOA service has a Quality of Service (QoS) associated with it. Some of the key QoS elements are security requirements, such as authentication and authorization, reliable messaging, and policies regarding who can invoke services.
5. Quality of service, security and performance are specified.
6. Software infrastructure is responsible for managing.
7. Services are cataloged and discoverable.
8. Data are cataloged and discoverable.
9. Protocols use only industry standards.

J) Classify Firewall best on the OSI layer

Ans :-

Firewalls can be classified based on various attributes. Let's learn about their types.

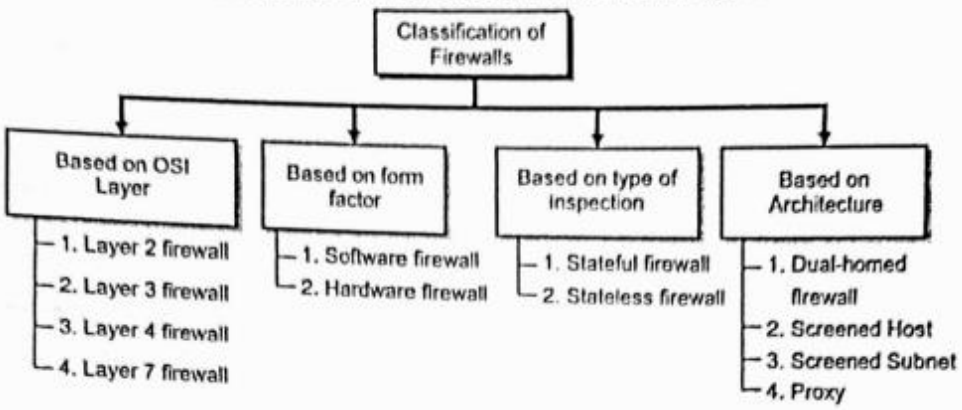


Fig. 4.11.1

A. Based on the OSI Layer

As you understand, OSI is a conceptual networking model. Based on the various layers, firewalls can be classified as following:

1. **Layer 2 Firewall :** These firewalls work at the "Data Link" layer of the OSI model. These firewalls require MAC, VLAN or device hardware level information to operate. One of the greatest advantage of these types of firewalls is that they are not IP dependent.
2. **Layer 3 Firewall :** These firewalls work at the "Network" layer of the OSI model. These filter traffic based on source/destination IP, port, and protocol. These are one of the most prevalent types of firewalls in use today. These are also called as Stateless firewalls. These are also called first-generation firewalls.
3. **Layer 4 Firewall :** These firewalls work at the "Transport" layer of the OSI model. These firewalls do everything that a Layer 3 firewall does and additionally track the active network connections and allow/deny traffic based on the state of those connections. These can effectively stop DoS attacks such as the ones based on TCP SYN/ACK as these are aware of the state of connection. These are also called as Stateful firewalls. These are also called second-generation firewalls.
4. **Layer 7 Firewall :** These firewalls are called Layer 7 but can work at three layers – Session, Presentation and Application. For simplicity, these are just called Layer 7 firewalls. Layer 7 firewalls do everything that a Layer 4 firewall does and additionally include the ability to intelligently inspect the contents of the network packets passing through them. For example, a Layer 7 firewall could deny all the HTTP requests from Korean IP addresses. They have the actual packet content level visibility and are the most advanced types of firewall in use today. These are also called third-generation firewalls.

K) Compare server side and client side encryption

Ans :-

Ans. :

Comparison Attribute	Server Side Encryption	Client Side Encryption
Keys managed at	Server	At each client
Encryption / Decryption Process	Carried out by server	Carried out by client
Complexity	Low	High
Data needs to be protected in-transit	Yes	No

L) Describe characteristics and features of Amazon EC2 Computer service

Ans :-

1. **IaaS**

EC2 is an example of an IaaS. You own the OS, networking, what is run on the machine and the responsibility to keep it protected. You are provided complete access to it as in a virtual machine running in your own datacentre. However, you do not have access to the underlying hypervisor on which your EC2 instance is running.

2. **Several instance types**

You can choose from a variety of instance types to match your computing requirements. Instance types define the hardware configuration of your EC2 instances. You are charged differently depending upon the instance type you choose. The higher is your hardware configuration, the costlier it is to run the corresponding EC2 instance. Table 5.3.1 gives a few examples of various instance types.

Table 5.3.1

Sr. No.	Instance Family	Instance Type Example	Hardware Configuration	Price per hour
1.	General Purpose	a1.medium	1 CPU, 2 GB RAM	$0.0255
2.	General Purpose	a1.4xlarge	16 CPU, 32 GB RAM	$0.408
3.	General Purpose	m5.24xlarge	96 CPU, 384 GB	$4.608
4.	Compute Optimized	c5d.18xlarge	72 CPU, 144 GB	$3.456
5.	Accelerated Computing	g3s.xlarge	4 CPU, 30.5 GB	$0.75
6.	Memory Optimized	x1e.32xlarge	128 CPU, 3,904 GB	$26.688
7.	Storage Optimized	i3.4xlarge	16 CPU, 122 GB	$1.248

- Imagine if you had to purchase a hardware having 3,900 GB RAM. Can you? The cloud really makes it cost effective and feasible to choose from various instance types depending on your computing requirements.
- Caution : The pricing is per region and is subject to change. Consider the instance family and their details for your reference only.

3. **Start and terminate instances as per your requirements**

You can start and terminate EC2 instances as per your requirement. Like typically happens in cloud environment, you only pay for what you use. EC2 instances are typically billed per hour.

4. **Elastic IP Addresses**

You can either assign a static or dynamic IP address for your EC2 instances. IP addresses are assigned based on the region.

5. **Auto Scaling**

Based on various conditions, such as CPU consumption, increased load, etc., you can automatically add more EC2 instances to support your computing requirements. Once the increased demand is taken care and you no more require as many EC2 instances, you can automatically terminate the extra instances.

6. **Multiple OS to choose from**

You can choose from a variety of Linux and Windows OS for your EC2 instances. You can also choose customised Amazon Machine Images (called AMI in short) from various vendors to support a particular use case or a specific computing requirement.

M) describe various cloud services offered by Microsoft Azur

Ans :-

GQ. What is Microsoft Azure Cloud Services ?

- Microsoft Azure is a cloud computing platform that provides a wide variety of services that we can use without purchasing and arranging our hardware. It enables the fast development of solutions and provides the resources to complete tasks that may not be achievable in an on-premises environment.
- Azure Services like compute, storage, network, and application services allow us to put our effort into building great solutions without worrying about the assembly of physical infrastructure.
- This tutorial covers the fundamentals of Azure, which will provide us the idea about all the Azure key services that we are most likely required to know to start developing solutions. After completing this tutorial, we can crack job interviews or able to get different Microsoft Azure certifications.

What is Azure

Microsoft Azure is a growing set of cloud computing services created by Microsoft that hosts your existing applications, streamline the development of a new application, and also enhances our on-premises applications. It helps the organizations in building, testing, deploying, and managing applications and services through Microsoft-managed data centers.

ces through Microsoft-managed data centers.

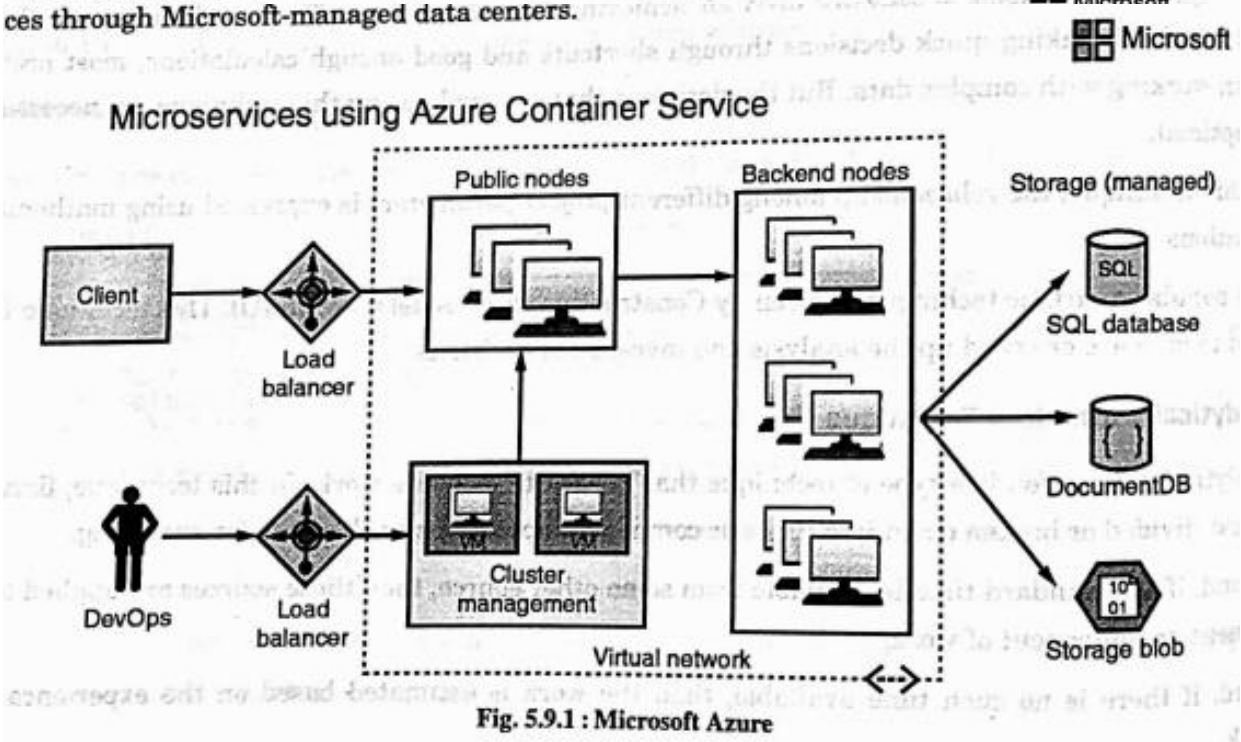


Fig. 5.9.1 : Microsoft Azure

Azure Services

- **Compute services :** It includes the Microsoft Azure Cloud Services, Azure Virtual Machines, Azure Website, and Azure Mobile Services, which processes the data on the cloud with the help of powerful processors.
- **Data services :** This service is used to store data over the cloud that can be scaled according to the requirements. It includes Microsoft Azure Storage (Blob, Queue Table, and Azure File services), Azure SQL Database, and the Redis Cache.
- **Application services :** It includes services, which help us to build and operate our application, like the Azure Active Directory, Service Bus for connecting distributed systems, HDInsight for processing big data, the Azure Scheduler, and the Azure Media Services.
- **Network services :** It helps you to connect with the cloud and on-premises infrastructure, which includes Virtual Networks, Azure Content Delivery Network, and the Azure Traffic Manager.

N) describe application life cycle management

Ans :-

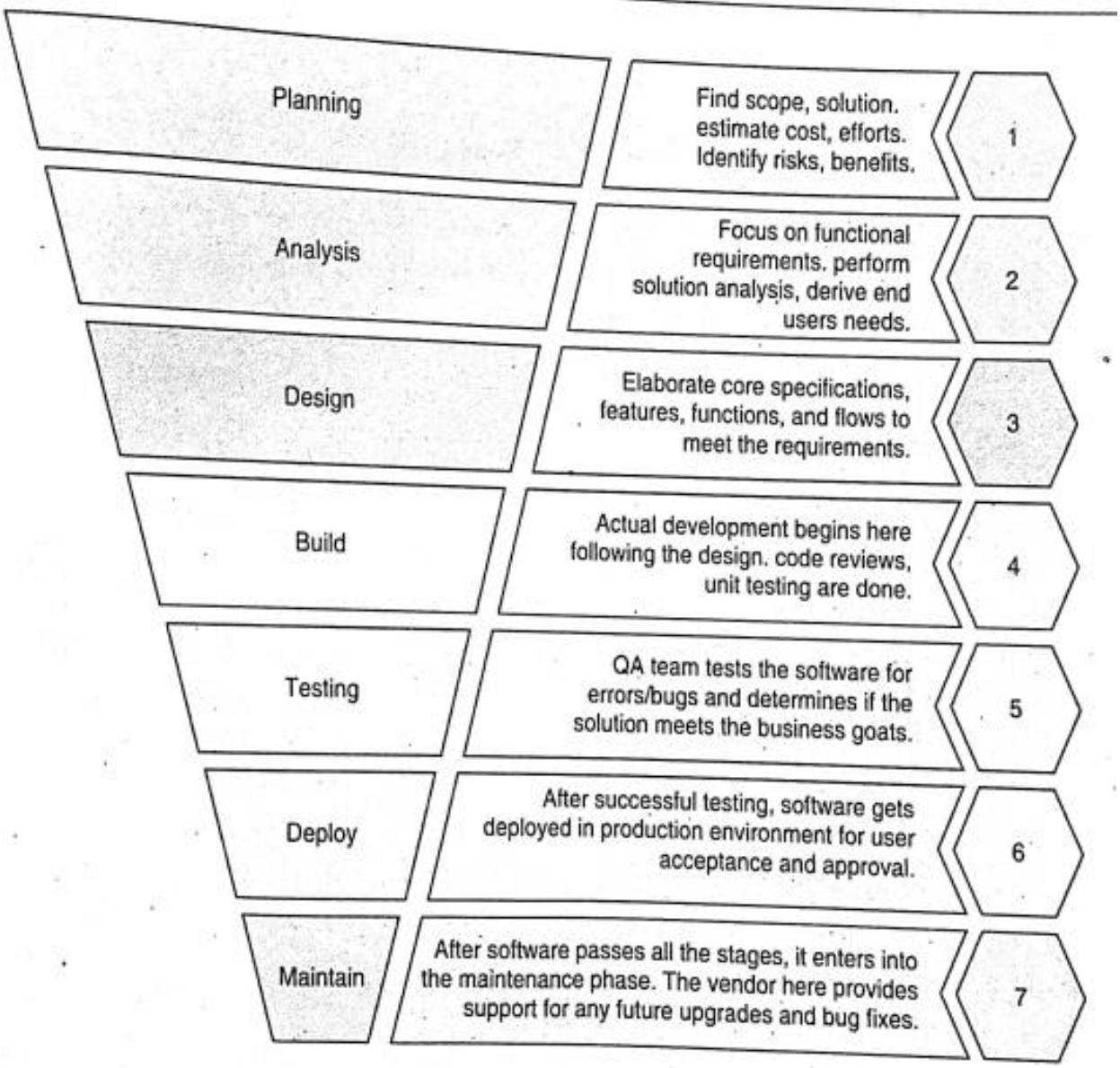
management (ALM). lifecycle

Ans. : **(4 Marks)**

- Application lifecycle management (ALM) encompasses all aspects of the application lifecycle, especially the usage, maintenance and servicing of the application after it has already been developed.

Application lifecycle management software tools help to provide visibility and transparency while promoting communication and collaboration throughout the application lifecycle.

- Application development typically follows software development lifecycle (SDLC) as shown following Fig. 5.4.



Cloud service providers provide several services and tools, for example, AWS Code Pipeline service, to automate build, test, stage, and finally move the application to production where it is continuously monitored for any performance issues.

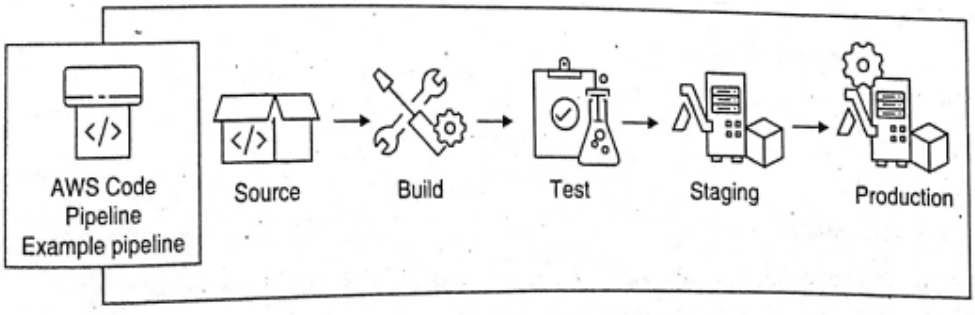


Fig. 5.4(b)

Characteristics of Application Lifecycle Management (ALM)

Application lifecycle management incorporates three closely connected aspects of management: governance, development, and operations. Each component plays a different role in effectively directing activities around the application throughout its life cycle and ensuring that the organisation is adequately positioned to create and derive value from its investments in technology.

1. Application Governance

- Governance describes the processes and activities used by the organisation to exercise decision-making control over applications that are being developed. The purpose of application governance is to ensure that the application consistently meets the needs of the business. Effective governance depends on a clear and efficient structure for decision-making, and on placing the right people in the right roles to make the best decisions about the application and its development and operation. Organisations must also ensure adequate transparency and flow of information such that project managers can make the most informed decisions to direct the lifecycle of the application.
- The activities typically carried out in application governance are as following.
  - Identifying key stakeholders
  - Assigning a sole point of accountability for the project
  - Establishing project ownership
  - Identifying decision-making teams
  - Ideation
  - Creating a business case for the project or application
  - Establishing requirements and user needs to inform the application development process
  - Project management and selection of working methods (agile, waterfall, DevOps, etc.)
  - Benefits management
  - Discontinuation

2. Application Development

- Application development includes the gathering and analysis of user requirements, the development, and testing of new code, building and testing new releases and the deployment of the application into the production environment. While application governance lasts for the entire application lifecycle, the application development process is not always active. Most application development may take place prior to the initial deployment, with additional development activities taking place post-deployment in response to changing user needs.
- The activities typically carried out in application development are as following.
  - Designing application according to user needs
  - Establishing software architecture
  - Application coding
  - Change management
  - Version control
  - Configuration management
  - Quality assurance and testing
  - Build management
  - Release management and deployment

3. Application Operations

- Application lifecycle management includes the operation of an application that has already been developed and deployed by the organisation. Applications operations includes the monitoring and performance measurement of applications in production, development, and implementation of appropriate monitoring tools, providing development teams with access to performance data, configuring application infrastructure, and coordinating the response to application issues such as performance faults or degradation. Application operations begin once an application has been deployed and continues through to the end of the application life cycle.
- The activities typically carried out in application operations are as following.
  - Customer support
  - Software maintenance
  - Software performance monitoring
  - Software security monitoring
  - Reporting

O) Describe key features and characteristics of Google App Engine

Ans :-

1. **Fully managed serverless application platform :** As a developer, you just need to bring your application code. Google App Engine manages the execution environment without you having to manage the underlying infrastructure. You don't need to,

   (a) Setup virtual machines (b) Install run time environments for your application

   (c) Configure infrastructure

   Google App Engine takes care of the infrastructure and application run time environment.

2. **Support for popular languages :** Google App Engine supports the popular application development languages such as Node.js, PHP, Python, Go, .NET, Java, Ruby, etc.

   It also provides options for bringing your own language runtimes and frameworks if you choose to do so.

3. **Auto Scaling :** Google App Engine automatically scales depending upon your application traffic. You don't need to worry about under provisioning or over provisioning your application resources.

4. **Monitoring, Logging and Diagnostics :** You can integrate with services such as Google Stackdriver to get powerful application diagnostics to debug and monitor the health and performance of your application.

5. **Application Versioning :** You can create and host different versions of your application and do user testing. You can also do intelligent traffic routing depending up on which application version you want users to use. For example, you can send 80% of application traffic to version 1, 15% to version 2 and 5% to version 3.

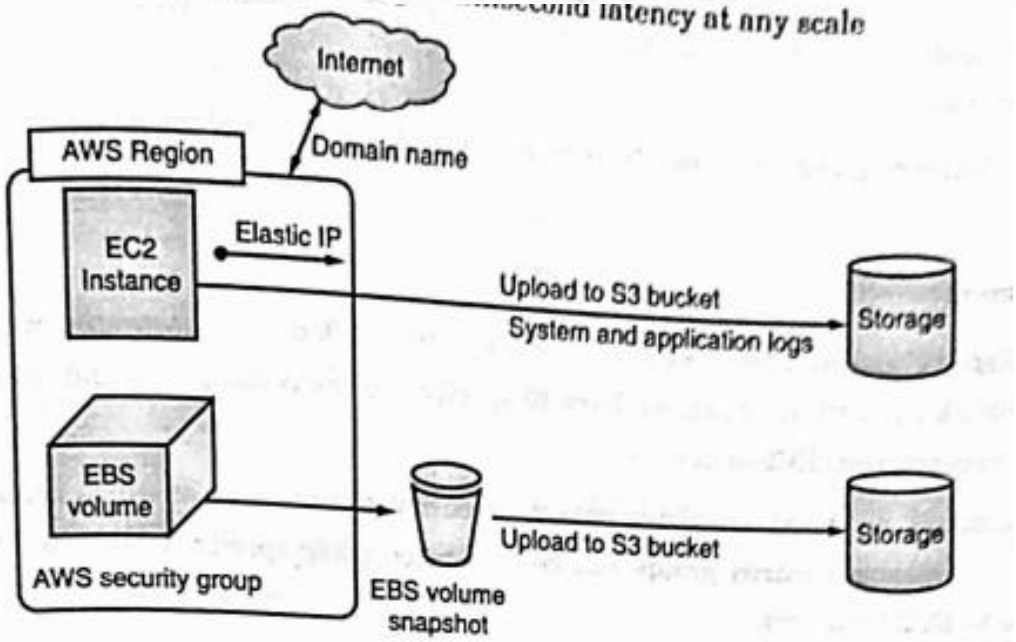
6. **Application Security :** You can protect your application by using App Engine Firewall. You can also use the TLS certificate service to encrypt the application traffic.

P) Identify and elaborate components of Amazon Web Service (AWS) architecture

Ans :-

AWS consists of many cloud services that you can use in combinations tailored to your business or organizational needs. This section introduces the major AWS services by category.

To access the services, you can use the AWS Management Console, the Command Line Interface, or Software Development Kits (SDKs).



☞ Security Management

- Amazon's Elastic Compute Cloud (EC2) provides a feature called security groups, which is similar to an inbound network firewall, in which we have to specify the protocols, ports, and source IP ranges that are allowed to reach your EC2 instances.
- Each EC2 instance can be assigned one or more security groups, each of which routes the appropriate traffic to each instance. Security groups can be configured using specific subnets or IP addresses which limits access to EC2 instances.

☞ Elastic Caches

- Amazon Elastic Cache is a web service that manages the memory cache in the cloud.
- In memory management, cache has a very important role and helps to reduce the load on the services, improves the performance and scalability on the database tier by caching frequently used information.

Q) Compare distributed computing and cloud computing.

Ans :-

Comparison Attribute	Distributed Computing	Cloud Computing
What it is?	Technology	Methodology and Principles
Purpose	Solve complex problems using network of computers	Deliver compute resources on demand
Lifespan	Years	Short-lived and on-demand
Expenditure	High	Low
Investment	Capital as well as Operational	Operational Investment only
Scalability	Up to aggregated hardware limit only	Nearly infinite
Innovation and changes	Slow	Rapid
Adopted by	Large enterprises only	Individuals, small to large enterprises
Skills required to operate	High	Low and specific to the consumed service
Shifting to another vendor	Complex and Costly	Comparatively easier and cheap
Primary consumption method	Direct interaction	Programmatic via APIs

R) Identify and elaborate different IoT enabling technologies

Ans :-

Ans. : The technology to build IOT infrastructure is divided into two categories as shown in Fig. Q.4.1.

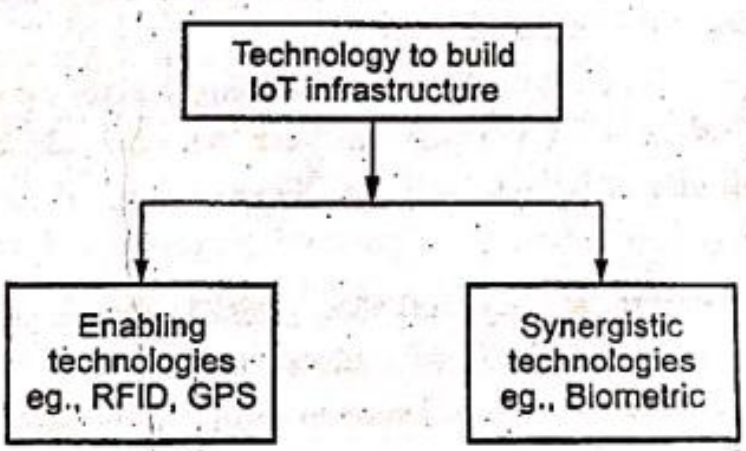


Fig. Q.4.1 Technologies to build IOT infrastructure

- Enabling technologies build up the foundations of the IoT. Among the enabling technologies, tracking (RFID), sensor networks, and GPS are critical.
- Synergistic technologies play supporting roles. For example, biometrics could be widely applied to personalize the interactions among humans, machines, and objects. Artificial intelligence, computer vision, robotics, and telepresence can make our lives more automated in the future.
- Fig. Q.4.2 shows various enabling and synergistic technologies to build IOT infrastructure

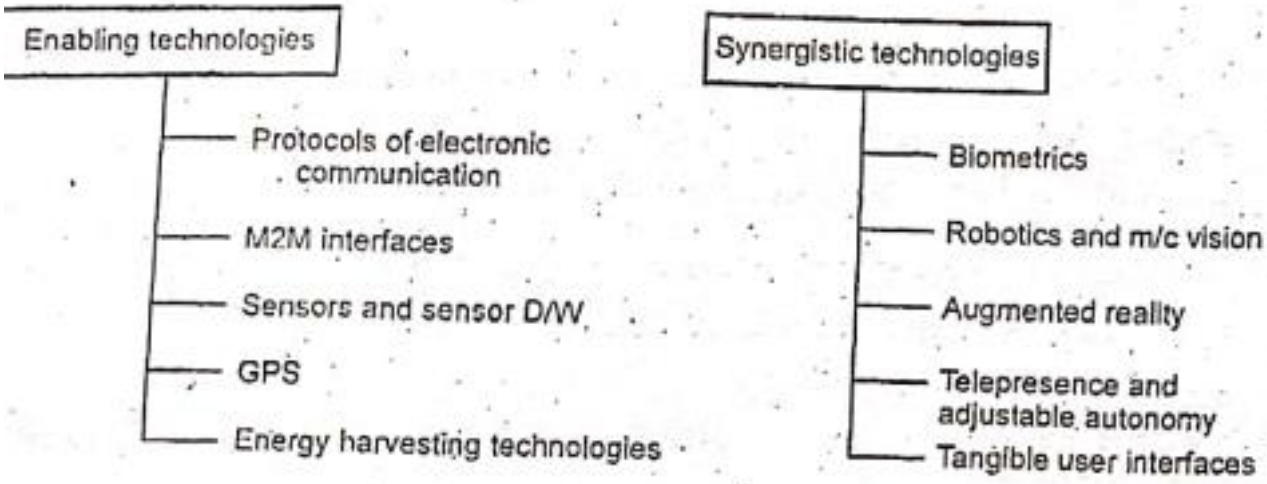


Fig. Q.4.2 Enabling and synergistic technologies

S) Illustrate the Iot application for online Social and professional networking the help of example.

Ans :-

- Social networking, as shown by the massive user groups, has become an everyday part of the lives of many people.
- Some groups also surpass the population of large nations, with more than 400 million active users on Facebook, for example.
- Social networks offer a medium to promote user contact and sharing, thus modeling relationships in the real world. For example, there is a multitude of integrated applications and some organizations now use the Facebook credentials of a user for authentication rather than requiring their credentials. Social networking has now expanded beyond contact between friends.
- Via storing heavy multimedia content in cloud storage systems, social networks help improves Internet usability.
- The most popular material on social media is videos and images, which utilize the entire space available to them. For all of their resource needs, they have the potential to slow down applications and servers.
- Vendors of cloud computing, such as Salesforce and Amazon, currently provide numerous services, including Customer
- Relationship Management (CRM) and Enterprise Resource Planning (ERP). When they deliver these items through cloud storage, without buying standalone software or hardware, consumers can use the simplicity and scalability of the system.
- Social networks, in addition to storing heavy data, use cloud storage for data analytics. So, users can very easily obtain a lot of structured and non-structured knowledge.
- The new and improved analytics that Facebook shows for the benefit of its corporate users is a typical case.
- Backup costs and data recovery costs have been significantly reduced by cloud storage. When data is processed in one location, there is a high probability of losing the data in times of catastrophe. It becomes next to impossible to recover missing data. With cloud computing, however, the data is stored on remote servers and remains available throughout the world. This allows social networking websites to store their users' private information that they cannot afford to misplace under any circumstances.

T) Pint out various components and characteristics of internet of things (IoT).

Ans :-

Ans. : 1. **Interconnectivity** : Everything can be connected to the global information and communication infrastructure.

2. **Heterogeneity** : Devices within IoT have different hardware and use different networks but they can still interact with other devices through different networks.

3. **Things-related services :** Provides things-related services within the constraints of things, such as privacy and semantic consistency between physical and virtual thing.
4. **Dynamic changes :** The state of a device can change dynamically, thus the number of devices can vary.
5. **Integrated into information network :** IoT devices are integrated with information network for communication purpose. It will exchange data with other devices.
6. **Self-adapting :** Self-adaptive is a system that can automatically modify itself in the face of a changing context, to best answer a set of requirements.
7. **Self-configuration** primarily consists of the actions of neighbour and service discovery, network organization and resource provisioning.

U) Describe anyone innovative application of internet of things

Ans :-

1. **Wearables**
   - Wearable technology is the hallmark of IoT applications and one of the earliest industries to deploy IoT. We have fit bits, heart rate monitors and smartwatches these days.
   - Guardian glucose monitoring device has been developed to help people with diabetes. It detects glucose levels in our body, uses a small electrode called the glucose sensor under the skin, and relates it to a radiofrequency monitoring device.
2. **Smart Home Applications**
   - The smart home is probably the first thing when we talk about the IoT application.
   - The example we see the AI home automation is employed by Mark Zuckerberg.
   - Alan Pan's home automation system, where a string of musical notes uses in-house functions.
3. **Health care**
   - IoT applications can transform reactive medical-based systems into active wellness-based systems. Resources that are used in current medical research lack important real-world information. It uses controlled environments, leftover data, and volunteers for clinical trials.

- The Internet of Things improves the device's power, precision and availability. IoT focuses on building systems rather than just tools. Here's how the IoT-enabled care device works.

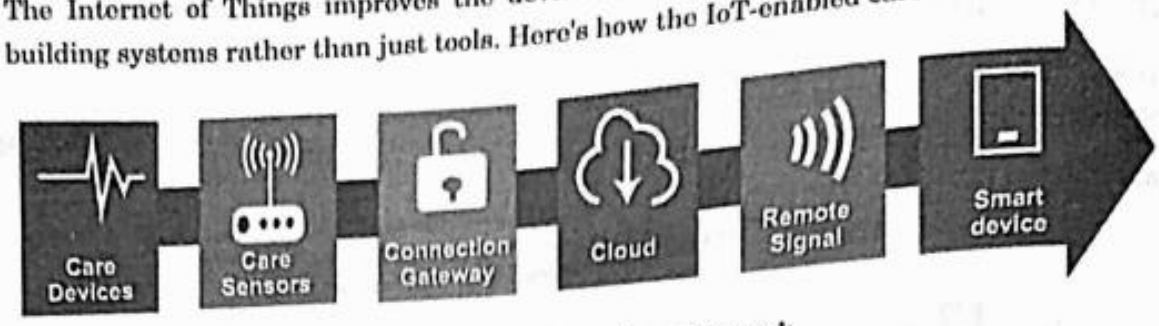


Fig. 6.4.5 : Health Care Sensor Network

4. Smart Cities

- Most of you have heard about the term smart city.
- Smart city uses technology to provide services.
- The smart city includes improving transportation and social services, promoting stability and giving voice to their citizens.
- The problems faced by Mumbai are very different from Delhi. Even global issues, such as clean drinking water, declining air quality, and increasing urban density, occur in varying intensity cities. Therefore, they affect every city.
- Governments and engineers use the Internet of Things to analyze the complex factors of town and each city. IoT applications help in the area of water management, waste control and emergencies.
- Example of a smart city - Palo Alto.

7. Hacked Car

- A connected car is a technology-driven car with Internet access and a WAN network.
- The technology offers the user some benefits such as in-car infotainment, advanced navigation and fuel efficiency.

8. Healthcare

- Healthcare do real-time monitoring with the help of smart devices. It gathers and transfers health data such as blood pressure, blood sugar levels, weight, oxygen, and ECG.
- The patient can contact the doctor by the smart mobile application in case of any emergency.

9. Smart Retail

- IoT applications in retail give shoppers a new experience.
- Customers do not have to stand in long queues as the checkout system can read the tags of the products and deduct the total amount from the customer's payment app with IoT applications' help.

10. Smart Supply Chain

Customers automate the delivery and shipping with a smart supply chain. It also provides details of real-time conditions and supply networks.

11. Smart Farming

- Farmers can minimize waste and increase productivity.
- The system allows the monitoring of fields with the help of sensors.
- Farmers can monitor the status of the area.