Mumbai Education Trust's

INSTITUTE OF ENGINEERING, BKC, NASHIK.

T.E. (Computer Engineering)

CLOUD COMPUTING (Elective II)(2019 Pattern)

END-SEM EXAMINATION

Time : 3 Hour *[Max. Marks :70]*

Instructions to the candidates:

1) *Answer Q.1 or Q.2, Q.3 or Q.4, Q.5 or Q.6, Q7 or Q.8*
2) *Neat diagrams must be drawn wherever necessary.*
3) *Assume suitable data if necessary.*
4) *Figures to the right indicate full marks.*

Date : 09/07/2022

MODEL ANSWERSHEET-2022

Q. 1 a) Define Virtualization? Explain different types of Virtualization. 8-M

→ **Definition :** "Virtualization is the "creation of a virtual (rather than actual) version of something, such as a server, a desktop, a storage device, an operating system or network resources". 1-Mark

Types of Virtualizations :(Explain any 3 types) 1-Mark

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

1. Hardware Virtualization : 2-Mark

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

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

2. Operating System Virtualization: 2-Mark

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

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

3. Server Virtualization: 2-Mark

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

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

4. Storage Virtualization:

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

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

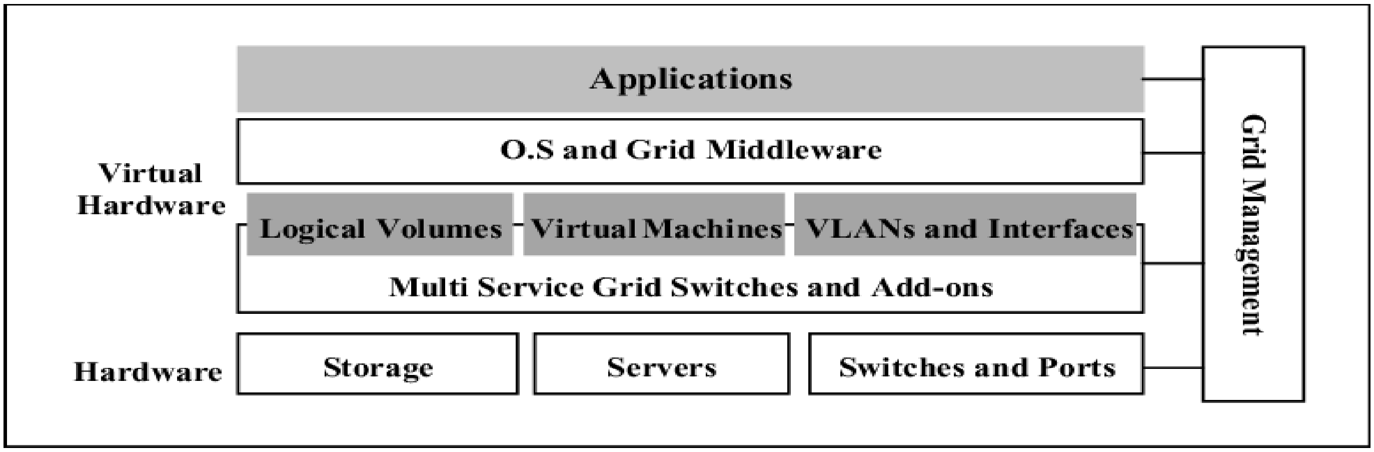
b) Discuss Virtualization in Grid and Virtualization in Cloud. 9-M

→ Virtualization in Grid : 2-Mark

- The primary focus in Grid Computing lies in secure resource sharing in terms of access to computers, software and data in a dynamic environment. Sharing of those resources has to be fine grained and highly controlled. Moreover, Foster proposed a three point checklist which characterizes a Grid more in detail:

- **Delivery of nontrivial qualities of service;**
- Usage of standard, open, general-purpose protocols and interfaces e.g. for inter-communication;

- Coordination of resources that are not subject to centralized control
- Operating System virtualizations are just a use of software which allows the hardware of a system to run multiple operating systems concurrently. This further provides the benefit to run multiple applications requiring a different operating system on a single computer.
- **Examples of virtualization in the IT world include**: Running multiple Windows VM servers on an Intel box, or running different IBM i, Linux, and AIX partitions on an IBM POWER machine are well known implementations of server virtualization. 2-Mark



- **Virtualization in Cloud :** 2-Mark

  Virtualization in Cloud Computing is a technology that enables the sharing of the physical instance of a single server or resources among multiple users or multiple organizations; in other words, it is basically making a virtual platform of the server OS (Operating System), storage devices, a desktop or network resources. When we talk about virtualization in the cloud, virtualization occurs with the help of resources that are available in the cloud, which are then shared across users to make cloud virtualization possible.

Following are the couple of ways that allows us to enable virtualization in the cloud those are: 3-Mark

1. **OS Level Virtualization:** In this virtualization of cloud computing, multiple instances of an application can run in a single OS.
2. **Hypervisor-based Virtualization:** In this process, the OS shares the hardware of the host computer, and hence it allows multiple OS (Operating Systems) to run on a single host.
3. **Grid Approach:** Here, a given workload is distributed to many physical servers, and once the result is calculated, it is delivered back. This type of service is mainly used for scientific purposes.

OR

Q.2 a) Differentiate between full and para Virtualization? 8-M

→ Note : atleast 8 points Each points 1-Mark

S.No.	Full Virtualization	Paravirtualization
1.	In Full virtualization, virtual machines permit the execution of the instructions with the running of unmodified OS in an entirely isolated way.	In paravirtualization, a virtual machine does not implement full isolation of OS but rather provides a different API which is utilized when OS is subjected to alteration.
2.	Full Virtualization is less secure.	While the Paravirtualization is more secure than the Full Virtualization.
3.	Full Virtualization uses binary translation and a direct approach as a technique for operations.	While Paravirtualization uses hypercalls at compile time for operations.
4.	Full Virtualization is slow than paravirtualization in operation.	Paravirtualization is faster in operation as compared to full virtualization.
5.	Full Virtualization is more portable and compatible.	Paravirtualization is less portable and compatible.

S.No.	Full Virtualization	Paravirtualization
6.	Examples of full virtualization are Microsoft and Parallels systems.	Examples of paravirtualization are Microsoft Hyper-V, Citrix Xen, etc.
7.	It supports all guest operating systems without modification.	The guest operating system has to be modified and only a few operating systems support it.
8.	The guest operating system will issue hardware calls.	Using the drivers, the guest operating system will directly communicate with the hypervisor.
9.	It is less streamlined compared to para-virtualization.	It is more streamlined.
10.	It provides the best isolation.	It provides less isolation compared to full virtualization.

b) Explain the functionality of Hypervisor?What is type-1 and type-2 hypervisor?9-M

→ **Functionality of Hypervisor :** 2-Mark

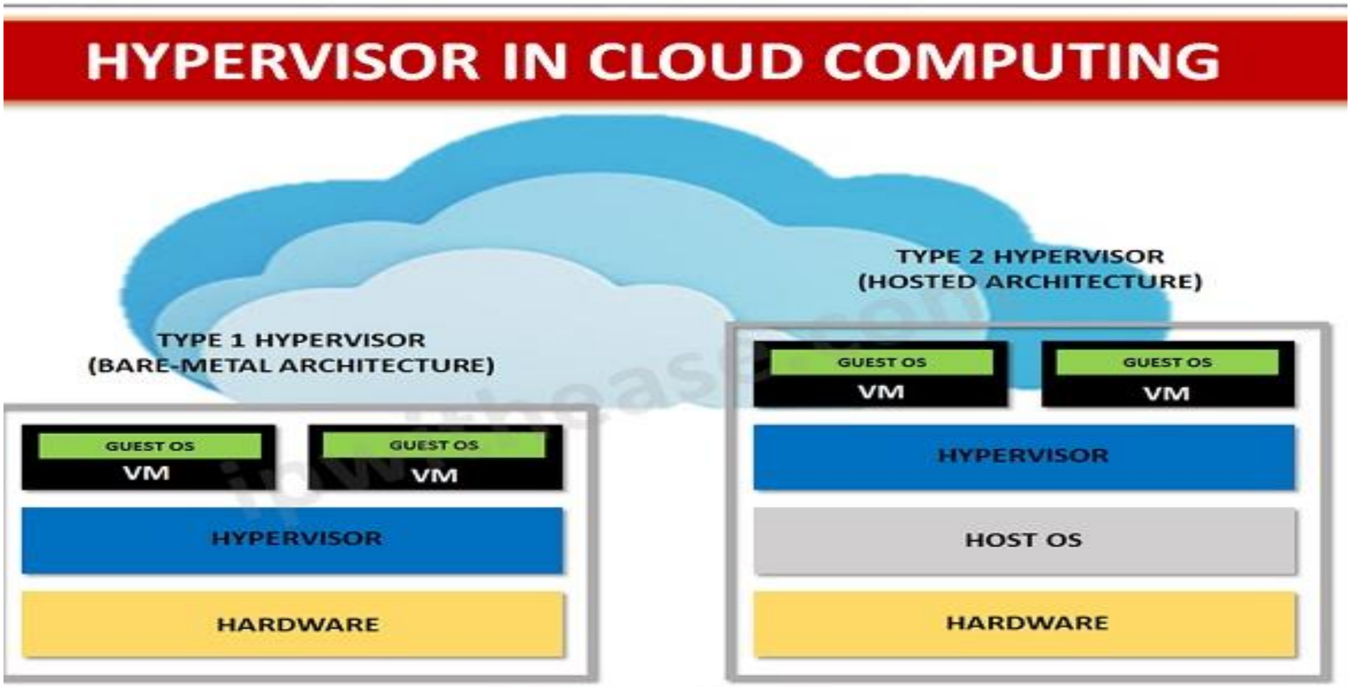
1. A hypervisor is a form of virtualization software used in Cloud hosting to divide and allocate the resources on various pieces of hardware.
2. The program which provides partitioning, isolation, or abstraction is called a virtualization hypervisor.
3. The hypervisor is a hardware virtualization technique that allows multiple guest operating systems (OS) to run on a single host system at the same time. A hypervisor is sometimes also called a virtual machine manager(VMM).

Use of a hypervisor : 1-Mark

- Hypervisors allow the use of more of a system's available resources and provide greater IT versatility because the guest VMs are independent of the host hardware which is one of the major benefits of the Hypervisor.

- In other words, this implies that they can be quickly switched between servers. Since a hypervisor with the help of its special feature, it allows several virtual machines to operate on a single physical server. So, it helps us to reduce:
    - The Space efficiency
    - The Energy uses
    - The Maintenance requirements of the server.

Diagram - 2-Mark



- **Type-1 hypervisor :** 2-Mark

1. The native or bare metal hypervisor, the Type 1 hypervisor is known by both names.
2. It replaces the host operating system, and the hypervisor schedules VM services directly to the hardware.
3. The type 1 hypervisor is very much commonly used in the enterprise data center or other server-based environments.
4. It includes KVM, Microsoft Hyper-V, and VMware vSphere. If we are running the updated version of the hypervisor then we must have already got the KVM integrated into the Linux kernel in 2007.

- **Type-2 hypervisor :** 2-Mark

1. It is also known as a hosted hypervisor, The type 2 hypervisor is a software layer or framework that runs on a traditional operating system.

2. It operates by separating the guest and host operating systems. The host operating system schedules VM services, which are then executed on the hardware.
3. Individual users who wish to operate multiple operating systems on a personal computer should use a form 2 hypervisor.
4. This type of hypervisor also includes the virtual machines with it.
5. Hardware acceleration technology improves the processing speed of both bare-metal and hosted hypervisors, allowing them to build and handle virtual resources more quickly.

Q. 3 **a) Enlist the different services offered by Amazon web Service? Explain it? 8-M**

→ **Services offered by Amazon web Services :** 2-Mark

1. Amazon Elastic Cloud Compute(EC2)
2. Amazon S3(Simple Storage Service)
3. Amazon Virtual Private Cloud(VPC)
4. Amazon Cloudfront
5. Amazon RDS(Relational Database Service)

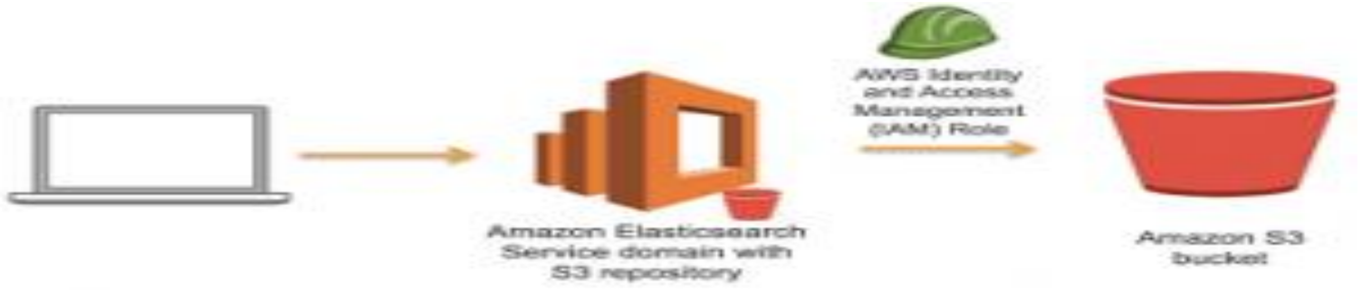
1. Amazon Elastic Cloud Compute(EC2) : 2-Mark

→ The Amazon EC2 service comes under the compute domain and it provides services that help to compute workloads. Amazon EC2 web interface is used to reduce the expensive physical servers by creating virtual machines. Also, they help in managing different features of the virtual servers such as security, ports, and storage. Amazon EC2 is highly preferable while creating a virtual server within a few minutes with just a few clicks according to the user’s operating system conveniently. It offers resizable compute capacity in the cloud. This helps a lot to focus more on the project rather than the server maintenance.

Amazon EC2
Amazon EC2
Instance
Instances
AMI
DB on Instance
Instance with CloudWatch
Elastic IP

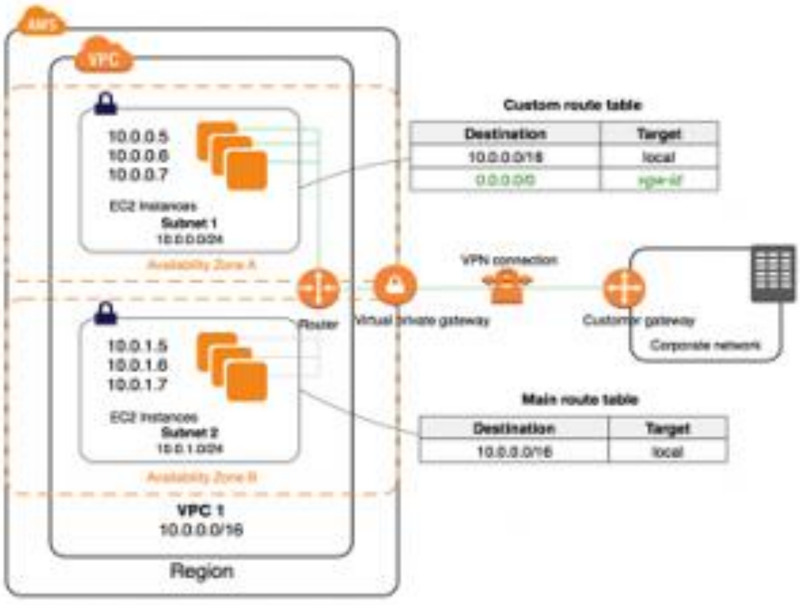
2. Amazon S3(Simple Storage Service) : 2-Mark

→ Amazon S3 is categorized under storage domain that provides data storage over the Internet services. Primarily, S3 stores data over the cloud in the form of objects. Amazon S3 stores the data with high security because of its improved infrastructure. The information is distributed over different physical regions and has a high-quality integration. This prevents the data from getting lost and helps to retrieve stored data irrespective of time and space via the Internet. Amazon S3 is highly available so that users can access their data just by one click with minimum or zero retrieving time.


AWS Identity and Access Management (IAM) Role
Amazon Elasticsearch Service domain with S3 repository
Amazon S3 bucket

3. Amazon Virtual Private Cloud(VPC) : 2-Mark

→ Amazon VPC falls under the Networking domain of AWS which is used to isolate the network infrastructure of user's computer. Every Amazon account holds a unique virtual network that protects the information from being accessed by others. These networks are logically isolated from other virtual networks in AWS clouds. This makes the user information risk-free in the AWS cloud.



b) Discuss Amazon Dynamo Database Service in detail? 9-M

→ Databases play a crucial role in the functioning of an application. Also, performance of an application is directly dependent on how the underlying database performs for the application. AWS Database Services is a set of databases offered by AWS on the cloud.

Amazon DynamoDB is a fast, fully managed, and flexible NoSQL database. It also supports document-based data. AWS affirms that DynamoDB delivers single-digit millisecond performance at any scale. DynamoDB comes with built-in Security, Backup, and Restore features. 2-Mark

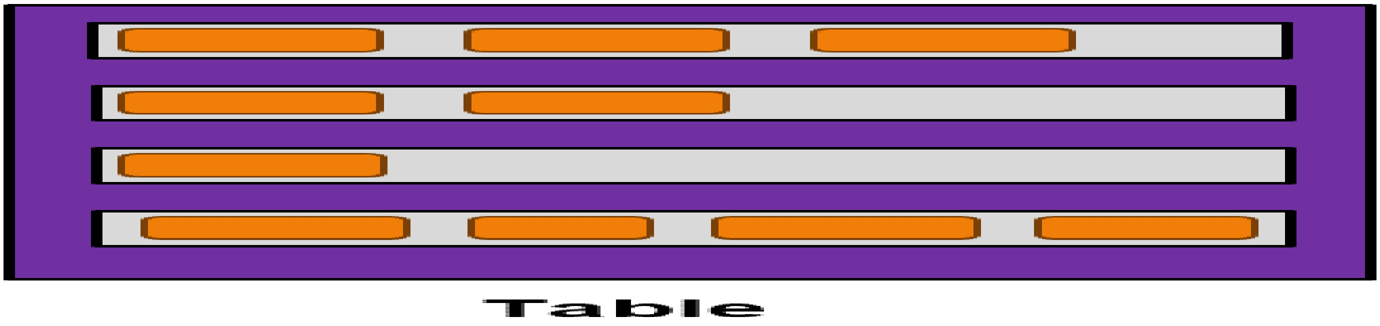
Since DynamoDB is a NoSQL database, it doesn't require any schema. In DynamoDB, there are basically three core components:

Features of DynamoDB : 3-Mark

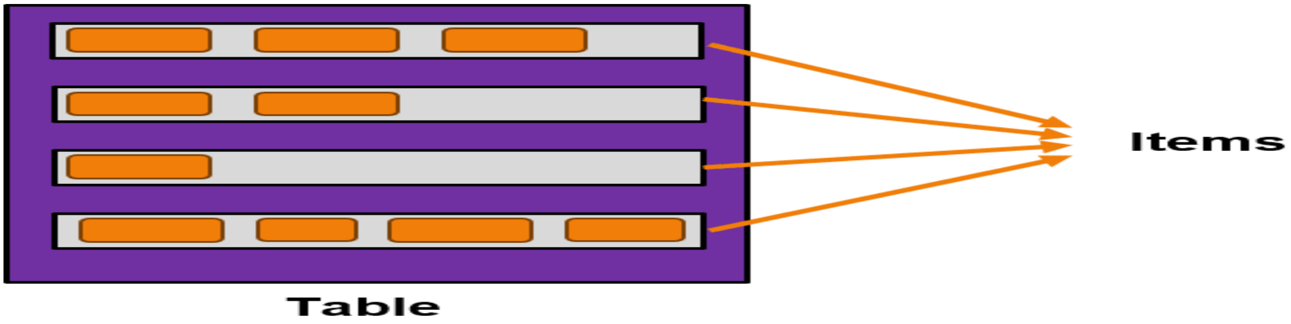
1. **On-demand capacity mode:** The applications using the on-demand service, DynamoDB automatically scales up/down to accommodate the traffic.
2. **Built-in support for ACID transactions:** DynamoDB provides native/ server-side support for transactions.
3. **On-demand backup:** This feature allows you to create a complete backup of your work at any given point of time.
4. **Point-in-time recovery:** This feature helps you with the protection of your data in case of accidental read/ write operations.
5. **Encryption at rest:** It keeps the data encrypted even when the table is not in use. This enhances security with the help of encryption keys.

Components of DynamoDB : 4-Mark

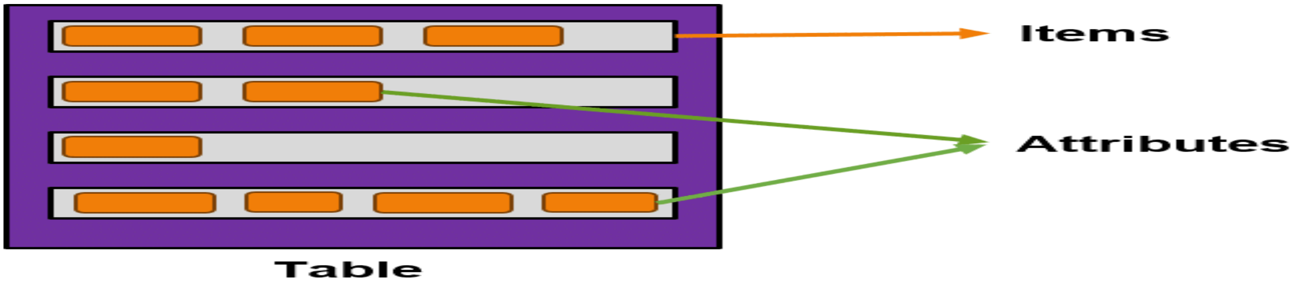
1. Tables: The collection of data is called a table in DynamoDB. It's not a structured table with a fixed number of rows and columns.



2. Items: Tables in DynamoDB contain one or more items. Items are made up of a group of uniquely identifiable attributes.



3. Attributes: Attributes are the data elements or values that reside in each item. They are equivalent to data values in a relational database that reside in a particular cell of a table.



Following are some of the benefits of using Amazon DynamoDB:

- Easy to set up and manage
- Data is automatically replicated across multiple Availability Zones
- Supports both key–value and document-based data models

OR

Q. 4 a) Explain Microsoft Windows Azure Platform? 8-M

→ Definition : 2-Mark

"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."

Services of Miccrosoft Azure Platform : 4-Mark

1. **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.

2. **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**.**
3. **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.
4. **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.

Microsoft Azure is used in a broad spectrum of applications like: 2-Mark

1. Infrastructure Services
2. Mobile Apps
3. Web Applications
4. Cloud Services
5. Storage, Backup, and Recovery
6. Data Management
7. Media Services

b) Elaborate the unique features Google App Engine with suitable example? 9-M

→ Each points 1-Mark

1. **Popular language:** Users can build the application using language runtimes such as Java, Python, C#, Ruby, PHP or build their own runtimes.
2. **Open and flexible:** Custom runtimes allow users to bring any library and framework to App Engine by supplying a Docker container.
3. **Fully managed:** It allows users to add your web application code to the platform while it manages the infrastructure. The engine ensures that web apps are secure and running and enables the firewall to save them from malware and threats.

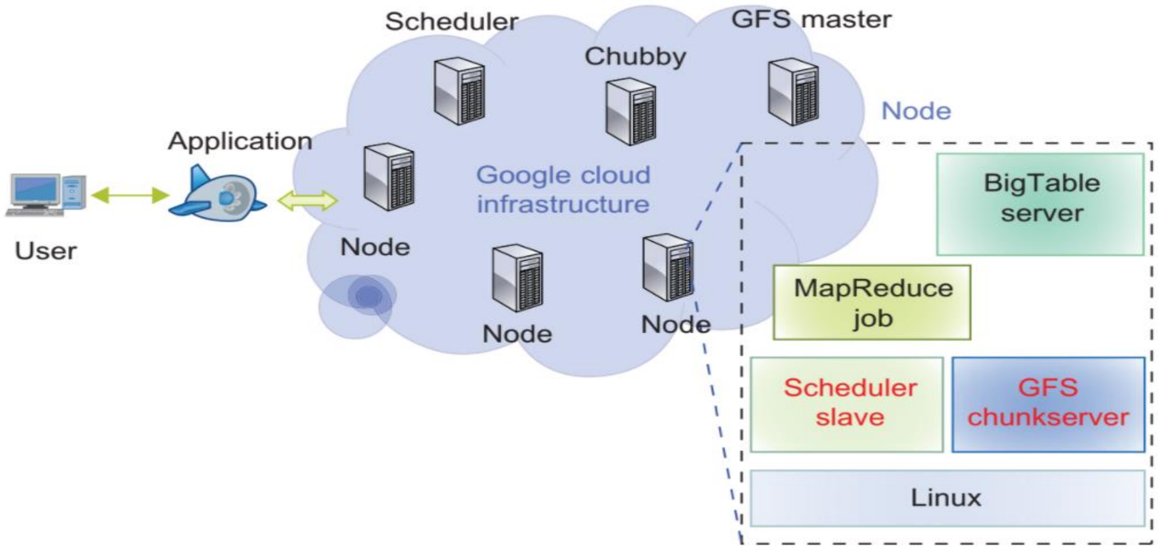
4. **Powerful application diagnostics:** Google App engine uses cloud monitoring and cloud logging to monitor the health and performance of the app and to diagnose and fix bugs quickly it uses cloud debugger and error reporting.
5. **Application versioning:** It easily hosts different versions of the app, and create development, test, staging, and production environments.
6. **Application security:** Google App Engine helps safeguard the application by defining access rules with an App Engine firewall and leverage managed SSL/TLS certificates by default on the custom domain without incurring any additional cost.
7. **Increased Scalability :**

   Scalability is synonymous with growth — an essential factor that assures success and competitive advantage. The good news is that the Google App Engine cloud development platform is automatically scalable. Whenever the traffic to the web application increases, GAE automatically scales up the resources, and vice-versa.

8. Cost Saving :

With Google App Engine, you do not have to spend extra on server management of the app. The Google Cloud service is good at handling the backend process.

Also, Google App Engine pricing is flexible as the resources can scale up/down based on the app's usage. The resources automatically scale up/down based on how the app performs in the market, thus ensuring honest pricing in the end.



Q. 5 a) Discuss the various Cloud Security Services with its necessity? 9-M

→ Atleast 5 services Each points 2-Mark

1. **Identity and Access Management** should provide controls for assured identities and access management. Identity and access management includes people, processes and systems that are used to manage access to enterprise resources by assuring the identity of an entity is verified and is granted the correct level of access based on this assured identity. Audit logs of activity such as successful and failed authentication and access attempts should be kept by the application/solution.
2. **Data Loss Prevention** is the monitoring, protecting and verifying the security of data at rest, in motion and in use in the cloud and on-premises. Data loss prevention services offer protection of data usually by running as some sort of client on desktops/servers and running rules around what can be done. Within the cloud, data loss prevention services could be offered as something that is provided as part of the build, such that all servers built for that client get the data loss prevention software installed with an agreed set of rules deployed.
3. **Web Security** is real-time protection offered either on-premise through software/appliance installation or via the cloud by proxying or redirecting web traffic to the cloud provider. This provides an added layer of protection on top of things like AV to prevent malware from entering the enterprise via activities such as web browsing. Policy rules around the types of web access and the times this is acceptable also can be enforced via these web security technologies.
4. **E-mail Security** should provide control over inbound and outbound e-mail, thereby protecting the organization from phishing and malicious attachments, enforcing corporate policies such as acceptable use and spam and providing business continuity options. The solution should allow for policy-based encryption of e-mails as well as integrating with various e-mail server offerings. Digital signatures enabling identification and non-repudiation are features of many cloud e-mail security solutions.
5. **Encryption systems** typically consist of algorithms that are computationally difficult or infeasible to break, along with the processes and procedures to manage

encryption and decryption, hashing, digital signatures, certificate generation and renewal and key exchange.

6. **Network Security** consists of security services that allocate access, distribute, monitor and protect the underlying resource services. Architecturally, network security provides services that address security controls at the network in aggregate or specifically addressed at the individual network of each underlying resource. In a cloud/virtual environment, network security is likely to be provided by virtual devices alongside traditional physical devices.

b) What are different Risks in Cloud computing and how to manage them? 9-M

→ Atleast 5 risks Each points 2-Mark

1. **Data Loss**

Data loss is the most common cloud security risks of cloud computing. It is also known as data leakage. Data loss is the process in which data is being deleted, corrupted, and unreadable by a user, software, or application. In a cloud computing environment, data loss occurs when our sensitive data is somebody else's hands, one or more data elements can not be utilized by the data owner, hard disk is not working properly, and software is not updated.

2. **Data Breach**

Data Breach is the process in which the confidential data is viewed, accessed, or stolen by the third party without any authorization, so organization's data is hacked by the hackers.

3. **Vendor lock-in**

Vendor lock-in is the of the biggest security risks in cloud computing. Organizations may face problems when transferring their services from one vendor to another. As different vendors provide different platforms, that can cause difficulty moving one cloud to another.

4. **Increased complexity strains IT staff**

Migrating, integrating, and operating the cloud services is complex for the IT staff. IT staff must require the extra capability and skills to manage, integrate, and maintain the data to the cloud.

5. Denial of Service (DoS) attacks

Denial of service (DoS) attacks occur when the system receives too much traffic to buffer the server. Mostly, DoS attackers target web servers of large organizations such as banking sectors, media companies, and government organizations. To recover the lost data, DoS attackers charge a great deal of time and money to handle the data.

6. Account hijacking

Account hijacking is a serious security risk in cloud computing. It is the process in which individual user's or organization's cloud account (bank account, e-mail account, and social media account) is stolen by hackers. The hackers use the stolen account to perform unauthorized activities.

OR

Q. 6 a) Explain security authorization challenges in cloud computing? 9-M

→ Atleast 5 services Each points 2-Mark

1. Data Breaches

Consequences of a data breach may include:

- Impact to reputation and trust of customers or partners
- Loss of intellectual property (IP) to competitors, which may impact products release
- Regulatory implications that may result in monetary loss
- Brand impact which may cause a market value decrease due to previously listed reasons
- Legal and contractual liabilities
- Financial expenses incurred due to incident response and forensics

2. Misconfiguration and Inadequate Change Control

This is one of the most common challenges of the cloud. In 2017, a misconfigured AWS Simple Storage Service (S3) cloud storage bucket exposed detailed and private data of 123 million American households. The data set belonged to Experian, a credit bureau, which sold the data to an online marketing and data analytics company called Alteryx. It was Alteryx that exposed the file. Such instances can be disastrous.

3. Lack of Cloud Security Architecture and Strategy

Worldwide, organizations are migrating portions of their IT infrastructure to public clouds. One of the biggest challenges during this transition is the implementation of appropriate security architecture to withstand cyberattacks. Unfortunately, this process is still a mystery for many organizations. Data are exposed to different threats when organizations assume that cloud migration is a “lift-and-shift” endeavor of simply porting their existing IT stack and security controls to a cloud environment. A lack of understanding of the shared security responsibility model is also another contributing factor.

4. Insufficient Identity, Credential, Access and Key Management

Cloud computing introduces multiple changes to traditional internal system management practices related to identity and access management (IAM). It isn’t that these are necessarily new issues. Rather, they are more significant issues when dealing with the cloud because cloud computing profoundly impacts identity, credential and access management. In both public and private cloud settings, CSPs and cloud consumers are required to manage IAM without compromising security.

5. Account Hijacking

Account hijacking is a threat in which malicious attackers gain access to and abuse accounts that are highly privileged or sensitive. In cloud environments, the accounts with the highest risks are cloud service accounts or subscriptions. Phishing attacks, exploitation of cloud-based systems, or stolen credentials can compromise these accounts.

6. Insider Threat

The Netwrix 2018 Cloud Security Report indicates that 58 percent of companies attribute security breaches to insiders. Insider negligence is the cause of most security incidents. Employee or contractor negligence was the root cause of 64 percent of the reported insider incidents, whereas 23 percent were related to criminal insiders and 13 percent to credential theft, according to the Ponemon Institute’s 2018 Cost of Insider Threats study. Some common scenarios cited include: misconfigured cloud servers, employees storing sensitive company data on their own insecure personal devices and systems, and employees or other insiders falling prey to phishing emails that led to malicious attacks on company assets.

B) Discuss how we need to perform secure cloud software testing. 9-M

→ **Cloud Testing** is one type of software testing in which the software applications are tested by using cloud computing services. Cloud testing intends to test the software based on functional and non-functional requirements using cloud computing services that ensure faster availability, scalability, and flexibility that saves time and cost for software testing.

Forms of Cloud Testing. 2-Mark

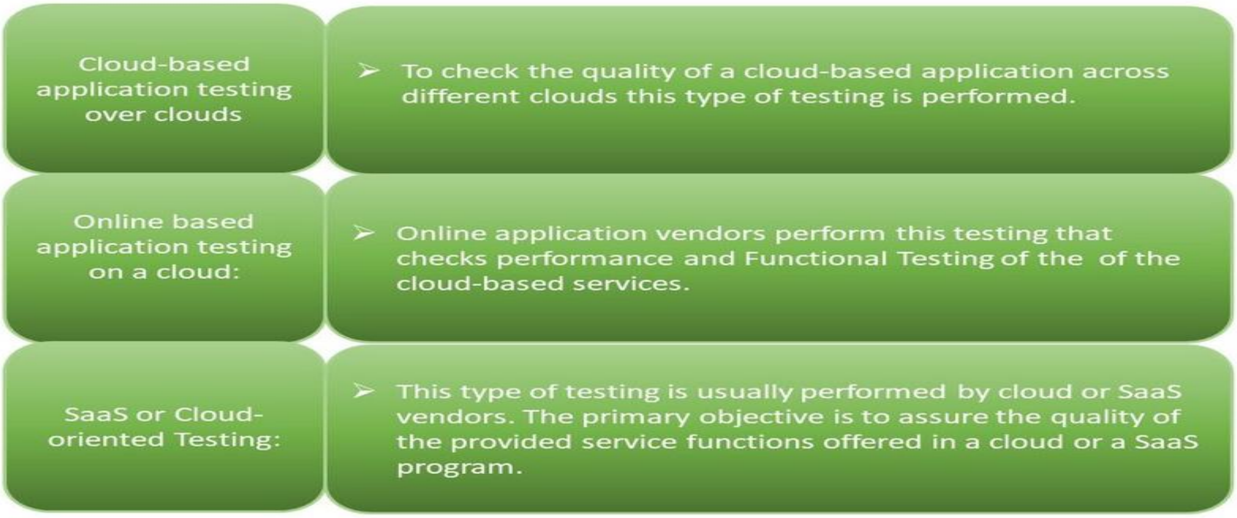
There are four forms of Cloud Testing performed: 2-Mark

1. **Testing of the whole cloud:** In this, the cloud is taken as a whole entity, and based on its features, testing is carried out.
2. **Testing within a cloud:** This is the testing that is carried out internally inside the cloud by testing each of its internal features.
3. **Testing across the clouds:** In this, the testing is carried out based on the specifications on the different types of clouds-like public, private and hybrid clouds.
4. **SaaS testing in the cloud:** In this, functional and non-functional testing takes place based on requirements.

Types of Cloud Testing 5-Mark

There are three types of cloud testing:

1. **Cloud-Based Application Tests over Cloud:** These types of tests help determine the quality of cloud-based applications concerning different types of clouds.
2. **Online-Based Application Tests on a Cloud:** Online application supervisors/vendors perform these tests to check the functions and performance of their cloud-based services. This testing takes place with the help of Functional Testing. Online applications are connected with a legacy system and the connection quality between the application and the legacy system is tested.
3. **SaaS or Cloud Oriented Testing:** These tests are performed by SaaS or Cloud vendors. The objective of these tests is to evaluate the quality of individual service functions that are offered in SaaS or cloud programs.



Cloud-based application testing over clouds

➢ To check the quality of a cloud-based application across different clouds this type of testing is performed.

Online based application testing on a cloud:

➢ Online application vendors perform this testing that checks performance and Functional Testing of the of the cloud-based services.

SaaS or Cloud-oriented Testing:

➢ This type of testing is usually performed by cloud or SaaS vendors. The primary objective is to assure the quality of the provided service functions offered in a cloud or a SaaS program.

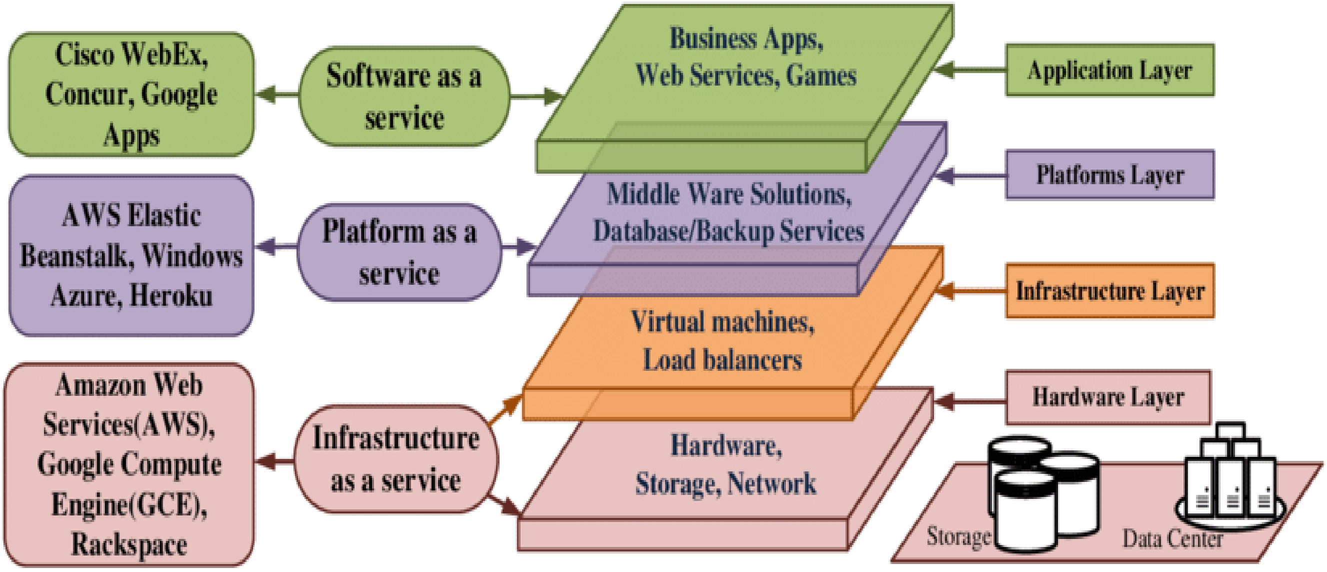
Q. 7 a) Discuss Energy Aware Cloud Computing with suitable example? 9-M

→ **Atleast 7 points.** Each points 1-Mark

1. Cloud computing as a trending model for the information technology, provides unique features and opportunities including scalability, broad accessibility and dynamic provision of the computing resources with limited capital investments.
2. It represents criteria, assets, and models for energy-aware cloud computing practices and the envisioned market structure for cloud computing services that exclusively addresses the impact of the quality and price of the energy supply on the quality and cost of cloud computing services.
3. The cloud computing market is driven by a limited number of vendors while a global market is emerging over the horizon.
4. The considerable energy consumption for cloud providers highlights the interdependence among the energy and cloud computing markets.
5. The energy management practices for cloud providers at the macro- and micro-levels to improve the cost and reliability measures of the cloud services are presented.
6. Cloud computing as an emerging computing model provides computing resources as general utilities for the end users through the internet.
7. Cloud computing is a model that enables on-demand access to the shared pool of customizable computing resources (e.g. servers, storage, networks, and applications) and services.

8. These resources could be rapidly deployed with minimal management efforts and marginal interactions with the service providers.
9. Providing dynamic computing resources in the cloud computing paradigm, enables the corporates to scale up/down the provided services, considering the clients' demand and the cost of the leveraged resources that contribute to the operation cost of the information technology (IT) facilities.
10. The scalability of the cloud services enables the smaller businesses to benefit from different categories of expensive computing-intensive services that were once exclusively available to large enterprises.
11. Cloud computing remedies the IT barriers especially for small and medium-sized enterprises and provides efficient and economical IT solutions as the cloud providers develop tools and skills to exclusively focus on handling the computational and IT challenges.

Diagram – 2 Marks

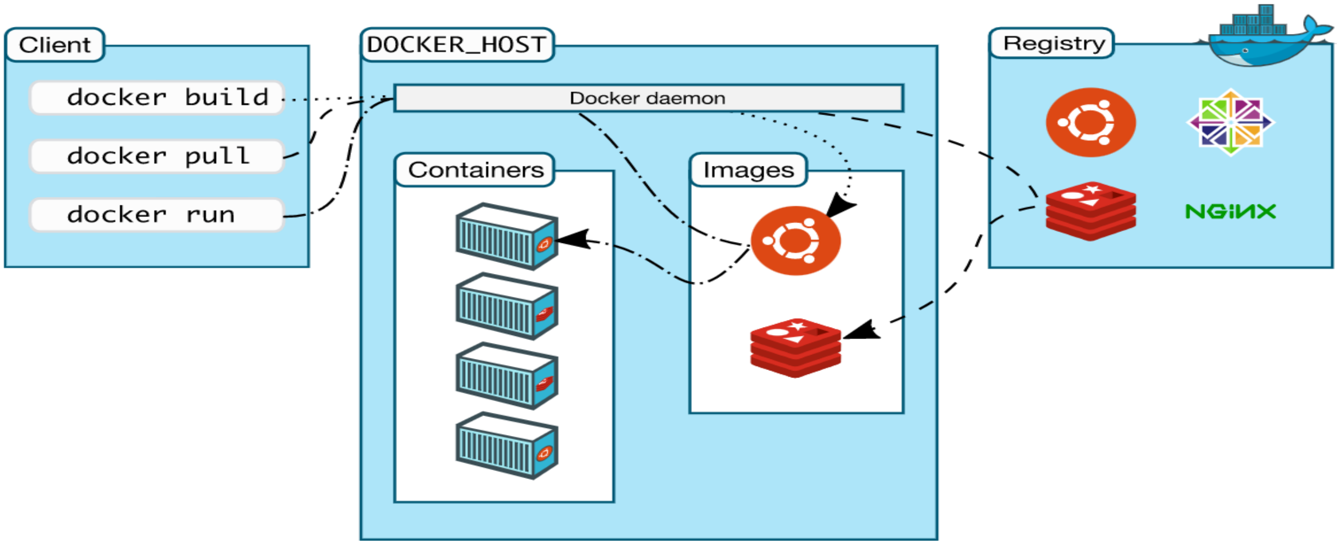

Cisco WebEx, Concur, Google Apps
Software as a service
Business Apps, Web Services, Games
Application Layer
AWS Elastic Beanstalk, Windows Azure, Heroku
Platform as a service
Middle Ware Solutions, Database/Backup Services
Platforms Layer
Virtual machines, Load balancers
Infrastructure Layer
Amazon Web Services(AWS), Google Compute Engine(GCE), Rackspace
Infrastructure as a service
Hardware, Storage, Network
Hardware Layer
Storage
Data Center

b) Explain with example, working of Docker? 9-M

→ Docker is an open platform for developing, shipping, and running applications. Docker enables you to separate your applications from your infrastructure so you can deliver software quickly. With Docker, you can manage your infrastructure in the same ways you manage your applications. By taking advantage of Docker's methodologies for shipping, testing, and deploying code quickly, you can significantly reduce the delay between writing code and running it in production. 2-Mark

Docker Architecture : 2-Mark

Docker uses a client-server architecture. The Docker client talks to the Docker daemon, which does the heavy lifting of building, running, and distributing your Docker containers. The Docker client and daemon can run on the same system, or you can connect a Docker client to a remote Docker daemon. The Docker client and daemon communicate using a REST API, over UNIX sockets or a network interface. Another Docker client is Docker Compose, that lets you work with applications consisting of a set of containers. 2-Mark



1. The Docker daemon : 3-Mark

The Docker daemon (dockerd) listens for Docker API requests and manages Docker objects such as images, containers, networks, and volumes. A daemon can also communicate with other daemons to manage Docker services.

2. The Docker client :

The Docker client (docker) is the primary way that many Docker users interact with Docker. When you use commands such as docker run, the client sends these commands to dockerd, which carries them out. The docker command uses the Docker API. The Docker client can communicate with more than one daemon.

3. Docker Desktop :

Docker Desktop is an easy-to-install application for your Mac or Windows environment that enables you to build and share containerized applications and microservices. Docker Desktop includes the Docker daemon (dockerd), the Docker client (docker), Docker Compose, Docker Content Trust, Kubernetes, and Credential Helper. For more information, see Docker Desktop.

4. Docker registries

A Docker registry stores Docker images. Docker Hub is a public registry that anyone can use, and Docker is configured to look for images on Docker Hub by default. You can even run your own private registry.

When you use the docker pull or docker run commands, the required images are pulled from your configured registry. When you use the docker push command, your image is pushed to your configured registry**.**

5. Docker objects

When you use Docker, you are creating and using images, containers, networks, volumes, plugins, and other objects. This section is a brief overview of some of those objects.

OR

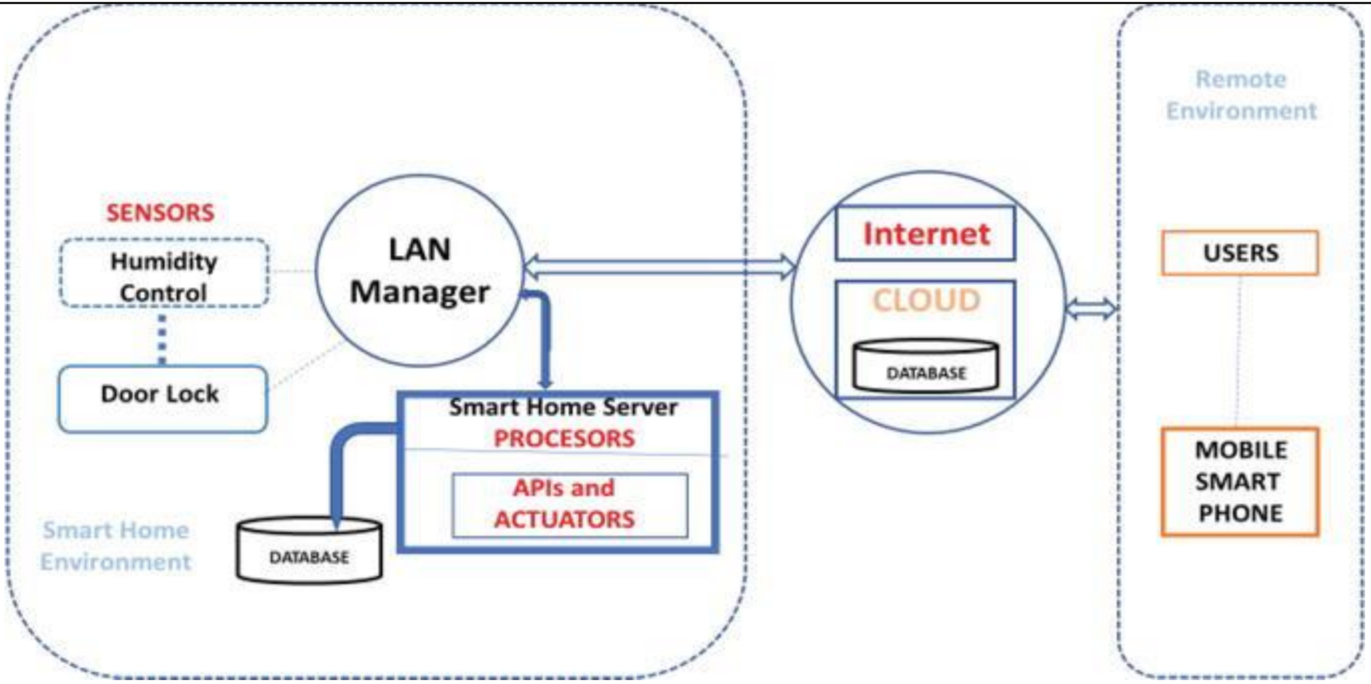
Q.8 a) How the Cloud and IoT together works for Home Automation? 9-M

→

1. Smart Devices: The Sensory Organs of Your Home : 3-Mark

The IoT based home automation consist of several smart devices for different applications of lighting, security, home entertainment etc. All these devices are integrated over a common network established by gateway and connected in a mesh network. This means that it gives users the flexibility to operate one sensor based followed by the action of the other. For e.g. you can schedule to trigger the living room lights as soon as the door/windows sensor of your main door triggers after 7pm in the evening.

Thus all the sensors within a common network can perform cross-talk via the main controller unit. As shown in the figure, some of the smart sensors in home automation acts as sensor hubs. These are basically the signal repeaters of signal bouncers which that are located in the midway between the hub installation location and the sensors that are at a distant location. For such long distances, these sensor hubs play an important role to allow easy transmission of signals to sensors that are far away from the main controller but in closer proximity to the sensor hub. The commonly used sensor hubs in IoT based Home Automation system are Smart Plugs.



Examples : atleast 3 points **Each of** 2-Mark

1. Smart Lighting –

Smart lighting for home helps in saving energy by adapting the life to the ambient condition and switching on/off or dimming the light when needed.

Smart lighting solutions for homes achieve energy saving by sensing the human movements and their environments and controlling the lights accordingly.

2. Smart Appliances –

Smart appliances with the management are here and also provide status information to the users remotely.

Smart washer/dryer can be controlled remotely and notify when the washing and drying are complete.

Smart refrigerators can keep track of the item store and send updates to the users when an item is low on stock.

3. Intrusion Detection –

- Home intrusion detection systems use security cameras and sensors to detect intrusion and raise alerts.
- Alert can we inform of an SMS or an email sent to the user.
- Advanced systems can even send detailed alerts such as an image shoot or short video clips.

4. Smoke/gas detectors –

- Smoke detectors are installed in homes and buildings to detect smoke that is typically an early sign of Fire.
- It uses optical detection, ionization for Air sampling techniques to detect smoke.
- Gas detectors can detect the presence of harmful gases such as CO, LPG, etc.
- It can raise alerts in the human voice describing where the problem is.

b) Differentiate Distributed Cloud Computing Vs Edge Computing? 9-M

→ **Atleast 9 points Each of 1-Marks**

Sr. No	Edge Computing	Distributed Cloud Computing
1	Edge computing is used to process time-sensitive data	cloud computing is used to process data that is not time-driven
2	Edge computing refers to processing that happens only at the system's edge.	A distributed cloud includes computation, processing, and transmission in a micro-cloud located beyond the centralized information cloud.
3	Edge computing is a modern version of cloud computing that's also focused on a distributed computing paradigm that offers data storage.	Distributed computing model of distributed systems, that are comprised of multiple processing devices communicating with others.
4	It incorporates specialized edge server farms to give extra security measures.	The system is safe since its elements are dispersed among numerous computers.
5	Reduced operating and maintenance expenses because the instruments and computing are handled nearby.	When contrast to standard cloud computing infrastructure, operating and maintenance costs are marginally greater but still relatively affordable
6	Towards greater scalability, edge technologies employ the concept of	A distributed computing infrastructure is laterally scalable, which means that the

	dispersed information collection and analysis.	performance of the units could be enhanced.
7	It provides addition security measures by incorporating specialized edge center.	System components are distributed across multiple computers making the system secure.
8	Less operational and maintenance costs as the devices and computing is done locally.	Operational and maintenance cost is little bit higher but relatively cost-effective compared to traditional cloud computing architecture.
9	Example include autonomous cars, streaming services, smart homes, industrial manufacturing etc	Example include internet, world wide web, intranet, email, cellular network etc.

************************** THE END****************************