IQRA NATIONAL UNIVERSITY

Final Paper Summer 2020

Course Title: Cloud computing

Instructor: Madam Rimsha Khan

Name : CHANGAIZ KHAN

ID:13206

Total Marks: 50

Question 1:

When each of the following deployment models should be used?

- Public Cloud
- Private Cloud
- Community Cloud
- Hybrid Cloud

ANSWER:

- **Public Cloud ;**

The public cloud deployment model is the most widely understood out of the four. Chances are you use some sort of public cloud product already. Some of the most common examples of public cloud offerings are:

- SaaS – Gmail, Microsoft 365, Dropbox, etc.
- PaaS – Google App Engine, Heroku.
- IaaS – Microsoft Azure, Amazon Web Service.

Basically, public clouds

- Are open to the public
- Can be owned, managed, and operated by pretty much anyone

- Are located on the provider‘s premises

- **Private Cloud ;**

Private cloud is a popular cloud deployment that addresses some of the main issues with using public cloud. As you can probably guess, the private cloud deployment model has a key difference to public cloud .It is privately used by a single organization, and not open to the public. It is also sometimes called internal cloud or corporate cloud.

The cloud infrastructure is provisioned exclusive use by a single organization comprising multiple consumers (e.g., business units). It may be owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on or off premises. The only key difference is that is used exclusively by one organization.

The main advantages are

- Control over how a cloud is setup and run
- Control over privacy and security practices
- Control over the geographical location of data

- **Community Cloud ;**

The cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be owned, managed, and operated by one or more of the organizations in the community, a third party, or some combination of them, and it may exist on or off premises .A community cloud could be built by one organization in an industry, and then rented out to others in the same industry with similar computing and security requirements. Or, a community of businesses with similar needs could group together to share the cost of each building their own public clouds. If your business has very similar cloud computing needs to many others, community cloud might be a good fit. This will be highly dependent on what‘s available in your industry.

Community cloud has many of the advantages of both public and private clouds. Those are

- Cloud configuration and security that meet the needs of your industry
- More scalable than private cloud.

- Cheaper than private cloud

- **Hybrid Cloud;**

The cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds)

Basically, any cloud configuration that combines multiple deployment models is a hybrid cloud. As long as they are ’bound together somehow to form a coherent unit.

Just like community cloud, the hybrid cloud deployment model aims to get benefits from multiple deployment models. By having both a private (or community) cloud that works seamlessly with a public cloud means you can

- Keep sensitive data safe
- Still, get some of the scalability and cost-effectiveness of public cloud
- Ultimate flexibility

Question 2:

Which layer of Cloud Computing Architecture is responsible for? Answer in one word?

ANSWER:

Resource Scheduling: ***PAAS***

Connection with the cloud: ***SAAS***

Hardware Resources: ***IAAS***

Load Balancing: ***SAAS***

Question 3;

How Cloud Architectures can be made secured?

ANSWER:

There are a lot of best practices when it comes to securing cloud architecture. Some of them are as follows;

Perform due diligence;

As a cloud consumer, it is essential to understand the applications, network, and security of the system. Due diligence is required throughout the lifecycle of the system. This includes during the planning, development, operations and decommissioning stage.

Managing Access;

There are three capabilities that come under access management. This includes the following:

• ***Identifying and authenticating users***:

Here a multifactor authentication system should be used to minimize the risk of a credential leak or breach. Remember, if a hacker gets access to user credentials, they can access and control your cloud data. Using multiple factors ensures this doesn't happen.

• Assigning user access rights:

Never give one person enough access to affect the entire data center negatively. Instead, plan roles in such a way that they are shared by the different individuals. This reduces the power of any one entity. Limited access further mitigates the effect of a credential compromise

Data protection;

Access control isn’t the only way of building secure cloud architectures. Instead, data protection is also required. There are three significant challenges to deal with here. Firstly, you must protect your data from authorized access. Secondly, you must ensure continued access to essential data even in case of failure of the system, and thirdly you must prevent accidental disclosure of information that was deleted.

Data protection from unauthorized access;

The best way to protect data from unauthorized access is by encrypting it. Cloud services deliver encryption features. For it to be effective, it is crucial that you manage the encryption keys properly. CPPs offer consumers a choice between consumer managed and CSP managed keys. The latter takes away the control from you regarding how and where the keys are stored. However, it reduces the responsibility on your end. On the other hand, consumer-managed keys give enhanced control to you. But, the burden of responsibility is with the owner in this case.

Question 4;

Present DC Function Rooms diagrammatically with explanation?

ANSWER:

DC cinch meters chip away at the rule of the Lobby Impact. Lobby impact sensors sense the attractive field brought about by current stream which causes a little voltage over the Corridor impact sensor. That voltage, which is relative to current is then enhanced and estimated.

A Lobby impact sensor is a gadget to quantify the size of an attractive field. Its yield voltage is straightforwardly corresponding to the attractive field quality through it. A wheel containing two magnets passing by a Corridor impact sensor.

The attractive cylinder in this pneumatic chamber will cause the Corridor impact sensors mounted on its external divider to initiate when it is completely withdrawn or expanded.

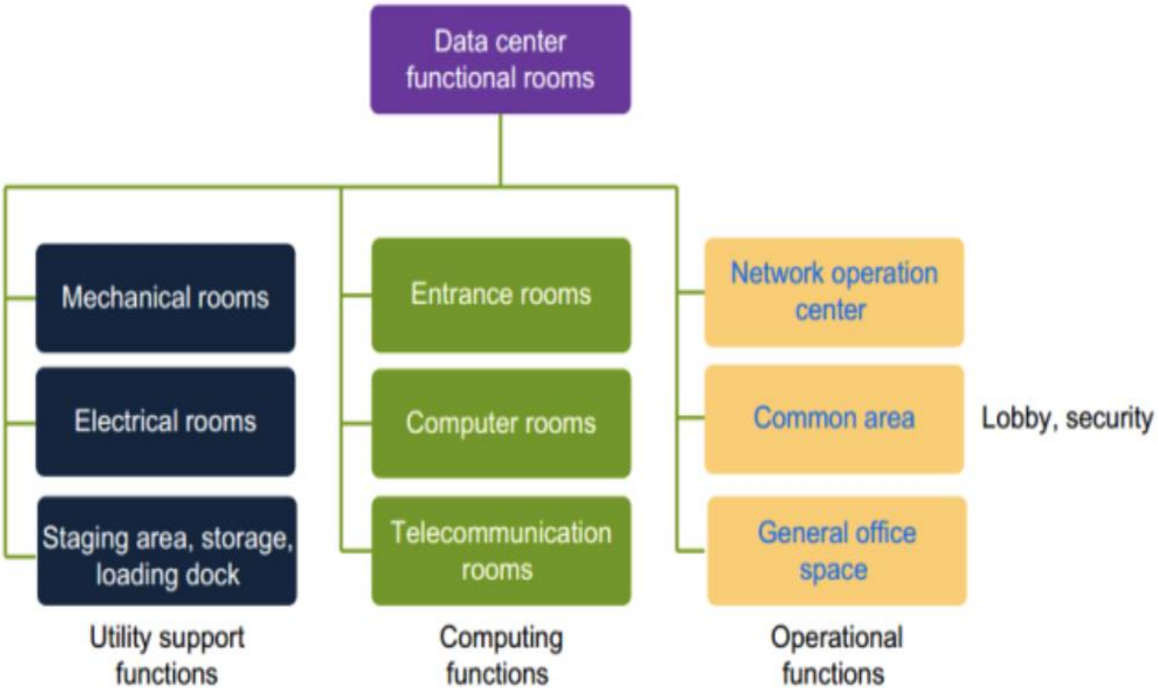
Motor fan with Lobby impact sensor,

Generally utilized circuit image ,

Lobby impact sensors are utilized for closeness detecting, situating, speed location, and current detecting applications.

Much of the time, a Corridor sensor is joined with edge recognition, so it goes about as and is known as a switch. Ordinarily observed in modern applications, for example, the envisioned pneumatic chamber, they are additionally utilized in purchaser gear; for instance, some PC printers use them to distinguish missing paper and open spreads. They can likewise be utilized in PC consoles, an application that requires super high dependability. Another utilization of a Corridor sensor is in the production of MIDI organ pedal-sheets, where the development of a "key" on the pedal-board is deciphered as an on/off switch by Lobby sensors.

Corridor sensors are normally used to time the speed of haggles, for example, for inside burning motor start timing, tachometers and non-freezing stopping mechanisms. They are utilized in brushless DC electric engines to identify the situation of the perpetual magnet. In the imagined wheel with two similarly divided magnets, the voltage from the sensor tops twice for every upheaval. This plan is ordinarily used to direct the speed of circle drives.



<u>Question 5;</u>

Why do we need Infrastructure as a Service (IaaS)?

<u>ANSWER:</u>

IAAS means Infrastructure as a Service. It is one of the components of cloud computing that provides us with "virtualized" computing infrastructures such as storage space, servers, virtual machines, and network connections. Below are the main reasons as to why we need IaaS.

Helps us to save cost;

IaaS helps us to save on costs since one is not required to buy hardware. All the hardware requirements are provided by the cloud service provider.

Helps us in having a Virtual Data Center;

IaaS helps us to have access to a centralized virtual data center. This enables every member of the organization to have access to the organization's computing resources without the need to relocate.

Provides a back plan;

The cloud service providers provide their customers with data back up plans

Better security;

With the appropriate service agreement, a cloud service provider can provide security for your applications and data that may be better than what you can attain in-house.

Gets new apps to users faster;

Because you don’t need to first set up the infrastructure before you can develop and deliver apps, you can get them to users faster with IaaS.

Focus on your core business;

IaaS frees up your team to focus on your organization’s core business rather than on IT infrastructure.

Innovate rapidly;

As soon as you’ve decided to launch a new product or initiative, the necessary computing infrastructure can be ready in minutes or hours, rather than the days or weeksand sometimes months. it could take to set up internally.