1. **What are the main essential characteristics of the cloud computing?**

The main essentials of cloud computing in cloud computing is :

Resource pooling (the most fundamendal characterstic) , Consumers provision , broad network , rapid elasticity and Measured service (explain them to show your skills on the exam)

**Resource pooling** is when the provider gathers the resources and collects them into a pool, which can be assign to different consumers

**The Consumers** assignment is to provide resources from pool using on demand self service and manage the resources themselves. They don’t have to talk to the human administrator to take this action.

**Broad Networking Access** means that all resources is available on the network and there’s no need for physical access. The network itself isn’t a part of the service.

**Rapid elasticity** allows the consumer to expand or compress resources for pool to get scalable provision. This allows the consumer to match resource consumption with demand (ex. Add virtual services as demand increases and shutting them down after dropping.

**Measured service** is to ensure that consumers only use the resources they are allocated for and if not , they should be charged for it, the client only pays for what they use.

**2. Name three service models of the cloud and explain their differences, including the level of**

**responsibility fo cybersecurity between cloud user and cloud provider.**

The three service models are : Sofware as a service , Platform as a service , infrastructure as a service

**SAAS software as a service :** is a full application that is managed and hosted by its provider ( the provider has the responsible for the application , physical server databases , os , virtualization , Network and storage , data center ) , but the consumer can access the SAAS application with a webbrowser (ex: BigCommerce, Google Apps, Salesforce, Dropbox, MailChimp, ZenDesk, DocuSign, Slack, Hubspot)

The SAAS – is when the consumer gets a finished ready to use application (mostly saas applications are built on IAAS and PAAS platforms.

In SAAS the provider hosts and manages the application , the user or consumer has not so much responsibility. The only thing the user is responsible for is to secure their data on the application and control the access yourself. The users are responsible for securing the login credentials so it doesn’t get stolen in phishing or social engineering attacks.

The provider is almost responsible for securing every perspective of the underlying infrastructure to the application

**Platform as A service :PAAS** is gives and provides developed or application plattforms platforms (often built on top of an IAAS platform for reducing the need of system administrator) like databases, apps that supports Python,Java , Js , etc coding) . it also provides file storaging and collaboration applications and application processing apps and apps where the api has full access to SAAS apps) :

The difference here is that the consumer only manage the data and apps

and app can’t manage the resources in the undelying server like with any infrastructure or even manage the network. While the provider has the responsibily of the physical server databases , os , virtualization , Network and storage , data center

Ex: AWS Elastic Beanstalk, Heroku, Windows Azure (mostly used as PaaS), Force.com, OpenShift, Apache Stratos, Magento Commerce Cloud , IntelliJ

In PAAS unlike the IAAS you have fewer security responsibilities , but instead you are responsible for control the access to the service and configure it. The provider is responsible for the application and the OS and it is also responsible for the security on the server like for example it ensures the users subscription and login creds is secure. The user is responsible for securing the data or any content on the platform.

**IAAS (Infrastructure As A Service)**

IAAS is when the consumer gets the opportunity to access a resource pool of fundamental computing infrastructure like compute, network or storage. In IAAS services like virtual machine, the consumer has more security responsibilities like patching the os system of your vm and securing their data. The provider is responsible for things like the storage and the services , disk , network

Responsibilities and accountibility:

****

**3. What the deployment models of the cloud that you know? What kind of deployment model will**

**you recommend for the following cases keeping in mind data privacy and cybersecurity:**

**(i) public air quality monitoring website, (ii) criminal police cases, (iii) county registry of the education projects in regional schools**

There are four types of deployment models: Public cloud, private cloud , community cloud and hybrid cloud.

1. **public air quality monitoring website**

For this case I would personally recommend using a public cloud. The reason why is because this is a public website which means it should be access by people in public. In public cloud the resource on the site is available for usage, such as storage and apps and so on is also available. The security on the website depends on which cloud provider the site use, for example Google and Azure provides different security mechanisms on their clouds. The website can use third part cloud services to secure the data on the website to secure private data (admin data etc) even though its public. Small organizations don’t have the resources for implementing a strong security on their servers. The security level on public cloud is great because every time a server is attacked the security gets better and in public cloud the consumer doesn’t need to patch their server it is done by the provider itself which helps to improve the security on the website

1. **criminal police cases**

in criminal police cases the data should be kept in private. This means that they should use a cloud that fulfill this requirement. The private cloud would be the best option for the police in this case. The reason why is that is in private cloud, the police is able to control their own cloud, like giving them access to resources. They have control of the underlying infrastructure which means that they can manage things on the cloud, and this helps them to keep their data private and access them through the firewall. It can also be hosted by a third part on prem or off prem. In private cloud the organization is responsible like the police for pathing the OS, upgrade etc to secure the cloud from malware attacks or unauthorized access. The private cloud helps the police to gain better control over the server, network, app security and data on the network. The network on the private cloud is limited which helps police to decide who can access their server which is helpful for improving the security on the server and minimize the risk of malware attacks on the server.

**(iii) county registry of the education projects in regional schools**

This is a special case, because we’re dealing with data that can be both private and public. It depends on the government, they can decide whether this registry should be publicly access or privately or both. If so, I would recommend using hybrid cloud. A hybrid cloud consists of a private and a public cloud (combination of two cloud environments). With this type of deployment model, the organization can decide if the data should be access in public or have private access. Like the when the project is set to begin can be access publicly, but sensitive data about the project like info about the study should be managed in the private cloud and can be only access by the organization users. This helps the government to easily handle their data and helps them to secure the sensitive data from being stolen or modified in transit. The security level in hybrid clouds is also great because of the private and the public cloud. The resources and data can be shared between the clouds, like if someone tries to attack their webserver, the data can be secured by transferring the data from public cloud to private (the data is encrypted).

**A public cloud is made to be available publicly or to industries , it’s operated by organizations who sell cloud services**

Public cloud:

Private cloud

Community cloud

Hybrid cloud

**gjør dette på søndag**

**Et bilde som inneholder tekst

Automatisk generert beskrivelse**

**4. Name main differences between virtual machines and containers.**

**A virtual machine (Vm)** is a collection of physical hardware that turns one servere into many servers. The machine uses the hypervisors which allows the computer to run multiple VMs. The disadvantages of VMs is that they include a full copy of the os which require the computer to have a lot of storage or space to run them (they can take up to tens of MBs each and even GBs). The other thing is that they are slow when booting them.

**Containers :** is a unit of software in the app layer that packeges code and its dependencies to help the application to run quickly and reliably from one computer. They can run on the same machine and share the OS kernel with other containers where is running as isolated processes in user space. Unlike the VMs the Containers take less space and take less MBs. The containers handle more apps and require fewer VMs and OS’s..

**The key** difference between Vms and containers is that the Vms vitualize an entire os (this includes the hardware as weel) which require a lot of space and this allows the computer to run multiple vms

While the containers only virtualize the software layers in the Os , this allows the computer to run multiple tasks or containers to run on a single OS , containers require less space than Vm to run.

The containers are similar to Vm unlike the vm which virtualize the entire machine, the container only virtualize above the operating system level which is the software.