**Final Term Paper (Spring - 2020)**
**Cloud Computing**

**Name: Siyad Ali** **ID# 6839**

**Semester: 8th** **Date: 25, June, 2020**
**Time: 6 hours** **Total Marks: 50**
**Instructor: M Omer Rauf**

**Note: Attempt all Questions. Answers should be in your own words. Plagiarism will not be tolerated, if detected, it will lead to failure.**

## Question No. 1: (20)

## a. Explain in detail network and cloud-based storage.

**ANS: Network:**
A network could be a collection of computers, servers, mainframes, network devices, peripherals, or other devices connected to 1 another to permit the sharing of knowledge.

**Example:**
A network is that the Internet, which connects ample people everywhere the globe.

**Network topologies and kinds of networks:**
The term constellation describes the connection of connected devices in terms of a geometrical graph. Devices are represented as vertices, and their connections are represented as edges on the graph. It describes what percentage connections each device has, in what order, and it what style of hierarchy.

Typical network configurations include the topology, mesh, ring topology, network topology, tree topology and hybrid topology.

**Examples of network topologies**

Most home networks are configured in an exceedingly tree topology that connects to the net. Corporate networks often use tree topologies, but they also often incorporate star topologies, and an Intranet.

**Public and Private networks:**

**Public:**
Public Wi-Fi networks require a password before a connection is created. If the network displays a lock icon in your list of obtainable Wi-Fi networks, it requires a password.
Some networks don't require a password to attach, but require you to log in using your application program before you'll access the net.

**Private:**
Private networks have security measures in situ to stop unwanted or unauthorized connections. Private networks are often used for home, business, or school Wi-Fi networks, or mobile hotspots for security and to preserve bandwidth.

## Cloud storage :

Cloud storage may be a remote platform that uses a highly virtualized, multi-tenant infrastructure to supply enterprises with scalable storage resources that may be provisioned dynamically as needed by the organization. This service is obtainable by a large array of cloud storage providers.

**Clouds Provide:**

- Elasticity
- Scalability
- Multi-tenancy
- Metered resources

Cloud based storage has several unique attributes that make it attractive for enterprises attempting to compete in today's data-intensive business environment.

**Example:**

The resources are distributed to enable dynamic elasticity and availability
The resources are replicated for disaster recovery and fault tolerance
Data replication is eventually consistent to make sure availability

**How Cloud Storage Work:**

Cloud storage involves a minimum of one data server that a user connects to via the web. The user sends files manually or in an automatic fashion over the net to the information server which forwards the knowledge to multiple servers. The stored data is then accessible through a web-based interface.

**Their infrastructure and services include:**

- Servers
- Storage
- Networking
- Data center operations

**Types of Cloud Storage:**

There are four general styles of cloud storage: personal cloud storage, private cloud storage, public cloud storage, and hybrid cloud storage.

**Personal cloud storage:**

Personal cloud storage is enabled by a network-attached device that permits users to store differing kinds of private data. samples of cloud storage include text, graphics, photos, video, and music. The user owns and controls the device, and might access it from anywhere via the net. The device is de facto a private cloud drive.

**Private cloud storage:**

Private cloud storage uses on-premises storage servers that are under the control of the corporate that owns them. Like public cloud storage and data centers, private cloud storage takes advantage of virtual machines.

**Public cloud storage:**
Public cloud storage is offered from a third-party as a service. Amazon AWS Cloud Storage, Microsoft Azure Cloud Storage, and Google Cloud Storage tend to be popular among enterprises. These public cloud storage options are available as a service.

**Hybrid cloud storage:**
Hybrid cloud storage is a few combination of public cloud, private cloud and data center as a corporation prefers. It typically combines resources that are owned and managed by the enterprise with public cloud storage services that are managed by a 3rd party.

## Question No. 2: (20)

## a. Explain in detail web application and multitenant technology.

### ANS:Web Application:

A Web application is an application that's stored on a foreign server and delivered over the web through a browser interface. Web services are Web apps by definition and plenty of, although not all, websites contain Web apps.

**How Web applications work:**
Web applications don't have to be downloaded since they're accessed through a network. Users can access an internet application through an internet browser like Google Chrome, Mozilla Firefox or Safari.

**Benefits:**
Web applications have many alternative uses, and with those uses, comes many potential benefits. Some common benefits of Web apps include:

- Allowing multiple users access to the identical version of an application.
- Web apps don't must be installed.
- Web apps are often accessed through various platforms like a desktop, laptop, or mobile.
- Can be accessed through multiple browsers.

**Web Application vs. other application types:**
Within the mobile computing sector, Web apps are sometimes contrasted with native apps, which are applications that are developed specifically for a specific platform or device and installed thereon device.

### Multitenant Technology

The multitenant application design was created to enable multiple users (tenants) to access the identical application logic simultaneously. Each tenant has its own view of the applying that it uses, administers, and customizes as an avid instance of the software while remaining unaware of other tenants that are using the identical application.

**Common characteristics of multitenant applications include:**

**Usage Isolation :**
The usage behavior of 1 tenant doesn't affect the applying availability and performance of other tenants.

**Data Security:**
Tenants cannot access data that belongs to other tenants.

**Recovery:**
Backup and restore procedures are separately executed for the information of every tenant.

**Application Upgrade**:
Tenants aren't negatively littered with the synchronous upgrading of shared software artifacts.

**Scalability :**
the appliance can scale to accommodate increases in usage by existing tenants and/or increases within the number of tenants.

**Metered Usage:**
Tenants are charged just for the appliance processing and features that are literally consumed.

**Data Tier Isolation:**
Tenants can have individual databases, tables, and/or schemas isolated from other tenants. Alternatively, databases, tables, and/or schemas will be designed to be intentionally shared by tenants.

## b. Explain in detail cloud security threats?

**ANS:Threats to cloud computing:**
**It is n**ecessary for the organizations to remember of cyber threats. in line with the Cloud Security Alliance report, here are the highest threats to cloud computing:

**1. Data breaches:**
Data breach may be the most goal of an attack through which sensitive information like health, financial, identity, intellectual and other related information is viewed, stolen or employed by an unauthorised user.

**2. Insufficient identity, credential and access management:**
Security threats may occur thanks to inadequate protection of the credentials. An unauthorised user might read, modify and delete data or release a malicious software.

**3. Insecure interfaces and APIs:**
Cloud service providers expose a collection of software user interfaces or application programming interfaces (APIs) that organizations use to manage and interact with the cloud services. Moreover, customers and third-party users often offer services to their customers through these interfaces.

An unauthorized user may access and re-use these APIs or passwords. they'll transmit content, get authorizations and logging capabilities.

**4. System vulnerability:**
Security breaches may occur because of exploitable bugs in programs that stay within a system. this permits a foul actor to infiltrate and obtain access to sensitive information or crash the service operations.

**5. Account or service hijacking – using stolen passwords:**
Account or service hijacking will be done to achieve access and abuse highly privileged accounts. Attack methods like fraud, phishing, and exploitation of software vulnerability are disbursed mostly using the stolen passwords.

**6. Malicious insider:**
A malicious insider can access sensitive data of the supervisor or may even get control over the cloud services at greater levels with little or no risk of detection. A malicious insider may affect a corporation through brand damage, financial impact and productivity loss.

**7. Data loss:**
The data loss threat occurs in cloud because of interaction with risks within the cloud or architectural characteristics of the cloud application. Unauthorized parties may access data to delete or alter records of a company.

**8. Lack of due diligence:**
Most cloud providers develop a decent strategy for due diligence when evaluating cloud technologies. Enterprises that choose providers without analysing the technologies and also the due diligence expose of it, expose themselves to risks.

**9. Abuse and nefarious use of cloud services:**
This threat refers to attackers leveraging the resources of cloud computing to focus on users, enterprises, and other cloud providers. Examples include launching DDoS attacks, phishing, email spams, get access to credential databases, and more.

**10. Shared technology vulnerabilities:**
Cloud providers deliver their services by sharing applications, or infrastructure. Sometimes, the components that structure the infrastructure for cloud technology as-a-service offering don't seem to be designed to supply strong isolation properties for a multi-tenant cloud service.

## Question No. 3: (10)

## a. Briefly describe following.

## a. Advantages and disadvantages of cloud computing.

**ANS:Advantages:**

**Cost Reduction:**
It’s a basic financial principle that profit comes from making extra money than you spend.
Good servers will run you thousands of dollars only for the hardware. Then there’s the continued software and hardware maintenance.

**Security:**
In spite of some high-profile cloud data breaches, there are numerous arguments for why cloud computing is safer than in-house computing.

**Reliability:**
Let’s say you have got a server. What happens if there’s a tough drive failure? Unless you invested in an exceedingly redundant array of independent discs (RAID), all of your data and server-based applications become immediately unavailable.

**Disadvantage :**

**Downtime:**
Downtime is maybe the only greatest disadvantage of cloud computing. We’re not talking about server downtime, but your Internet access happening.
As long as your Internet access is out, you can’t do anything with the cloud.

**Security:**
Security, at one level, is a plus of cloud computing for the explanations discussed above. Security is additionally an obstacle at a unique level.

**Cloud Service Closes Shop**
In a mature industry, you always cope with one in every of a couple of known players that supply time-tested, reliable services. Cloud computing may be a young industry with many companies vying for business. there's a break that your cloud provider will run out of cash and shut their doors forever.

## b. Collaborative meeting in cloud?

**ANS:Collaborative Meeting:**

A good thing when people at a meeting were said to have their heads in the clouds. Today, however, cloud-based meetings and cloud-based collaboration tools are some of the information technology industry's hottest items. What began as web-based e-mail has exploded to include cloud-based conference meetings, face-to-face voice over Internet protocol phone calls on virtually any device, document sharing, and streaming media content.