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

**NAME:Muhammad Hilal** **ID#13064**
**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 program that is stored on a remote server and delivered over the Internet through a browser interface. Web services are Web apps by definition and many, although not all, websites contain Web apps.

How Web applications work:
Web applications do not need to be downloaded since they are accessed through a network. Users can access a Web application through a web browser such as Google Chrome, Mozilla Firefox or Safari.

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

Allowing multiple users access to the same version of an application.
Web apps don’t need to be installed.
Web apps can be accessed through various platforms such as 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 particular platform or device and installed on that device.

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

Common characteristics of multitenant applications include:
Usage Isolation :
The usage behavior of one tenant does not affect the application 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 data of each tenant.
Application Upgrade – Tenants are not negatively affected by the synchronous upgrading of shared software artifacts.
Scalability :
The application can scale to accommodate increases in usage by existing tenants and/or increases in the number of tenants.

Metered Usage:
Tenants are charged only for the application processing and features that are actually consumed.
Data Tier Isolation:
Tenants can have individual databases, tables, and/or schemas isolated from other tenants. Alternatively, databases, tables, and/or schemas can be designed to be intentionally shared by tenants.

**b. Explain in detail cloud security threats.**

ANS:threats to cloud computing:
It is necessary for the organizations to be aware of cyber threats. According to the Cloud Security Alliance report, here are the top threats to cloud computing:

1. Data breaches
Analyse data protection during design and run time.
Organizations must restrict access to data and maintain adherence to industry standards and compliance.
Implementation of strong API access control.
The environment and infrastructure should be designed to restrict access and monitor traffic.
Organizations must encrypt and protect data in transit.
Implement backup and retention strategies.
2. Insufficient identity, credential and access management
Security awareness should be provided to contractors, third-party users and employees.
Use of two-factor authentication should be implemented to secure accounts.
Organizations must identity and access rights to detect violations.
Segregate accounts based on business needs.
The data owner should restrict the internal corporate or customer (tenant) user-account credentials.
3. Insecure interfaces and APIs
Use a good security model of software interfaces.
Practise strong authentication methods and limit access with encrypted transmission.
Use standard API frameworks.
4. System vulnerability
Customer access grants must be implemented using a need-to-know, need-to-access protocol.
Organizations must regularly detect data assessments and system disclosure alteration, or destruction.
Privileges should be separated between business-as-usual systems-level access, and escrowed credential access for sensitive root or system accounts.
Frequent check of quality and integrity of system as well as services.
5. Account or service hijacking – using stolen passwords

Use strong two-factor authentication techniques where possible.
The organization needs to take proper steps to verify identity, restrict access and maintain adherence to industry standards and compliance.
6. Malicious insider
Organizations must understand the practices performed by cloud providers, how to grant access to employees, and set compliance policies.
There should be security and privacy awareness programs to understand, recognize and report any suspicious activity.
Organizations should automate their processes and use technologies that scan frequently for misconfigured resources and remediate unknown activity in real time.
7. Data loss:
Cloud service providers should provide adequate security controls to customers as well as specify backup and retention strategies to them.

Use strong API access control.
Encrypt security of data in transit.
8. Lack of due diligence
Organizations must know what certifications the cloud provider itself has in place.
Clear protocols must be defined related to accountability and responsibility of management support and involvement.
Use strong passwords with Multi-Factor Authentication (MFA) tokens.

9. Abuse and nefarious use of cloud services
Organizations must use strong IDS/IPS.
Organizations must use firewalls that can inspect incoming and outgoing traffic.
The integration of cloud services must not be left up to individuals, groups for implementation.
An organization must choose their storage vendors wisely. The process must be corporate IT or security team only.
10. Shared technology vulnerabilities
Cloud providers deliver their services by sharing applications, or infrastructure. Sometimes, the components that make up the infrastructure for cloud technology as-a-service offering are not designed to offer strong isolation properties for a multi-tenant cloud service. This may lead to vulnerabilities in shared technology that can be attacked in almost all delivery models.

**Question No. 3:**
**(10)**
**a. Briefly describe following.**
**a. Advantages and disadvantages of cloud computing**
ANS3:
Cloud Computing Advantages and Disadvantages
Since cloud computing does offer some serious advantages, let's start with those:

Advantage – Cost Reduction
It's a basic financial principle that profit comes from making more money than you spend. Do you know what doesn't come cheap? Just about everything related to computers. So when it comes to cloud computing advantages and disadvantages, this is at the top of the whole list for most businesses.

Good servers will run you thousands of dollars just for the hardware. Then there's the ongoing software and hardware maintenance.

You also need a secure room to set them up. If you don't have one already, you'll need to get one built on-site. Servers also need constant cooling to work properly, so brace yourself for some brutal air conditioning costs.

A company can go broke buying software licenses for high-end programs.

Cloud computing solves all of these problems for a business. The cloud provider takes on all of the hassles associated with infrastructure, maintenance and utility management for the servers.

Cloud-based applications are usually a fraction of the cost of locally installed software.

You also get the advantage of only paying for the server time or space that you use.

Advantage – Security
In spite of some high-profile cloud data breaches, there are numerous arguments for why cloud computing

is more secure than in-house computing.

your data and any potentially disgruntled employees.

The most obvious argument is that cloud providers will make a point to keep security protocols and software up to date because their business depends on it. Odds are good that most cloud providers have full-time staff members who specialize in digital/network security. How many small to medium-sized businesses can say the same?

Advantage – Reliability

Let's say you have a server. What happens if there's a hard drive failure? Unless you invested in a redundant array of independent discs (RAID), all of your data and server-based applications become immediately unavailable.

It is, in short, the nightmare scenario.

Cloud providers survive on redundancy. Your data isn't just stored on a server. It's stored across multiple servers.

Depending on the provider, it might even be stored on servers in multiple locations. Just in case there's a catastrophic failure at a given server farm.

This means that no single hardware failure will hamstring your business. It also means that you can expect superb reliability in terms of accessing your data or services. Most providers even guarantee 99.99% uptime.

Disadvantage – Downtime

Downtime is perhaps the single greatest disadvantage of cloud computing. We're not talking about server downtime, but your Internet access going down.

As long as your Internet access is out, you can't do anything with the cloud.

Robust mobile data plans can help to offset that problem temporarily. Cellular service often remains viable when internet access and even power goes out. Of course, data plans are capped and mobile devices have limited battery life.

Then again, if the power is out, you've probably got bigger concerns than accessing your cloud services.

Disadvantage – Security

"Hold on for a second," you might be thinking. "Didn't you just say security was an advantage of cloud computing?"

The user is the weak link in almost all security systems. If you don't use basic digital security methods, cloud computing is about as secure as leaving your laptop open at a coffee shop.

Security is one area where determining cloud computing advantage and disadvantages depends on the angle from which you look at the issue.

Disadvantage – Cloud Service Closes Shop

In a mature industry, you usually deal with one of a handful of known players that offer time-tested, reliable services. Cloud computing is a young industry with lots of companies vying for business. There is a possibility that your cloud provider will run out of money and close their doors forever.

**b. Collaborative meeting in cloud.**
Therefore, a collaborative meeting is a real-time discussion between people working together towards a common goal.

Collaborative meetings require people to do some work in advance of the meeting, so they can understand the goal and how they'll contribute. Then, these meetings help groups coordinate how they'll work together afterwards to accomplish that goal.

**EXAMPLES OF COLLABORATIVE MEETINGS:**

1. Project kick-offs, status meetings, sign-offs, and post-mortems
2. Discovery / requirements gathering meetings
3. Working committee meetings
4. Board meetings
5. Brainstorming sessions
6. Emergency response coordination
7. Strategy sessions
8. Negotiation and mediation sessions

Ideally when their time as a team concludes, those who hold collaborative meetings have jointly created something they can show, such as a completed project, a list of new ideas, an action plan, or a new legal agreement.