(**Cloud Computing**)

Mid Paper
Submitted To:

M Omer Rauf

Dept.: BSSE

Submitted by:

Muhammad Hilal

Registration No.13064 Semester – 8th

QNO: 01

(A)

(Explain essential characteristics of cloud computing)

Characteristics of cloud computing:

- **On Demand Self Service:**
  In On-demand Self-service Cloud service providers provide on demand computer services like email, applications, network or server service are often utilized with none human interaction with each service provider. Some example of to such services that provides are Amazon Web Services (AWS), Microsoft, Google, IBM and Salesforce.com.

- **Broad Network Service**:
  Cloud Capabilities are available over the network refers to resources hosted in a private cloud network that are available for access from a wide range of devices, such as mobile phones, laptops and PDAs.

- **Resource Pooling**:
  Resource pooling is an IT term employed in cloud computing environments to elucidate a situation during which providers serve multiple clients, customers or "tenants" with provisional and scalable services. These services are often adjusted to suit each client's needs with none changes being apparent to the client or user.

- **Rapid Elasticity**:
  Cloud services may be rapidly and elastically provisioned, in some cases automatically, to quickly scale out and rapidly released to quickly scale in. To the patron, the capabilities available for provisioning often appear to be unlimited and may be purchased in any quantity at any time.

- **Measured Service**:
  While using the services the customer are charged about their amounts too. They follow the metering concept for measuring the amount of usage , controlled that resources and provide a report regarding the services also give transparency for both the provider and consumer of the utilized service .

(B)

(Explain in detail the key properties of cloud computing)

Properties of Cloud Computing:

- **Cloud Computing Is User Centric:**
  When a user is connected to the cloud, can access all the data which is stored in the cloud it can be the user documents, images and application etc and the user can also share or edit the data. The devices that are connected to the cloud become the user devices.

- **Cloud Computing Is Task-Centric:**
  Instead of that specialize in the appliance and what it can do, the main focus is on what one need done how the appliance can pair for us. Traditional applications—word processing, spreadsheets, email, then on—are becoming shorter than the documents they create.

- **Cloud Computing Is Powerful:**
  Cloud computing is much powerful you can connect hundreds or thousands of devices at a time to the cloud for managing and controlling your data on the cloud which can be impossible on a single device.

- **Cloud Computing Is Accessible:**
  Because data is stored within the cloud, users can instantly retrieve more information from multiple repositories. We don't seem to be limited to one source of information, as we do with a desktop PC.

- **Cloud Computing Is Intelligent:**
  With all the various data stored on the computers in an exceedingly cloud, processing and analysis are necessary to access that information.

- **Cloud Computing Is Programmable:**
  Information stored on one computer within the cloud must be replicated on other computers within the cloud. If that one computer goes offline, the cloud's programming automatically redistributes that computer's data to a replacement computer within the cloud.

  Some of the tasks that are necessary for processing with cloud computing must be automated.

QNO: 02

(A)

(Explain in detail different service models of cloud computing)

Different service models of cloud computing:

- **Software as a Service(SaaS):**
  SaaS, or software as a service, could be a cloud service that revolves around, you guessed it, software. Easily the most important and most cloud-based service, SaaS uses the cloud to deliver software to users, which is then usually accessed via your applications programme. Unlike physical software that you simply install on your computer, SaaS solutions are hosted on a provider's services. This means that the provider is to blame for software maintenance and updates, which translates to the very fact that users will all be using the identical version of software and find updates at the identical time.

- **Platform as a Service (PaaS):**

  PaaS is a cloud-based service that provides users with computing platforms. Most companies who utilize PaaS do so to either host or develop their own software solutions, or to provide support for software used by employees.

  The main reason many companies integrate PaaS is because it reduces the costs and complexity often associated with buying, developing, configuring, installing, and managing the hardware and software solutions that are necessary for the custom-built applications that many businesses rely on.

  While PaaS is gaining in popularity with many small businesses, most won't have a lot of first-hand interaction with this type of cloud, especially those who work with IT providers like us. Essentially, most providers will utilize PaaS in order to deliver custom applications and solutions to the end-user.

❖ ***3. IaaS***

a. IaaS, or infrastructure as a service, is essentially cloud-based computers and resources. The most popular and well known type of IaaS is the virtual machine which is a digital version of a computer or server that is accessed over an Internet connection. The infrastructure is physically kept off site, and usually managed by a provider, but you access and interact with it as if it is located on your computer or in your office.

b. In other words, if you are looking to virtualize your systems via the cloud, IaaS could be a good place to start as it allows you to move existing support systems into the cloud. Other solutions can then be migrated or introduced as needed.

c. While the cloud can offer a wide variety of benefits and solutions to companies, it can be a chore to choose the service which is best for your company's needs. We highly recommend that if you are considering a cloud solution, you get in contact with us. We can help find the best solution for the needs of your business and to also manage it, thereby ensuring proper migration and implementation, leaving you to focus on running your business.

d. Explain in detail different deployment models of cloud computing.
Cloud computing is composed of four deployment models which are Private Cloud, Community Cloud, Public Cloud, and Hybrid Cloud.

Public cloud provides the opportunity for general public to access infrastructure and computational resources through the Internet. It is controlled and operated by a cloud provider and the services are usually accessible free or on a pay-per-use model. "*The* security risks and lack of negotiability of the terms of public cloud services typically will foreclose the possibility of subscribing to an off-the-shelf public cloud provider". On the other hand, a private cloud is a deployment model that provides core technologies such as virtualization and multitenant application exclusively for a single organization. It is clear that this deployment model is less threatening than a public cloud. Most companies adopt cloud computing through a hybrid process which is a mixture of both public and private cloud services. Decision makers should understand the characteristics of public and private clouds and evaluate carefully security and privacy requirements.

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.

The cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community, or public).

QNO: 03

(A)

(Explain in detail roles and boundaries in cloud)

This section would cover the following topics:

1. **Cloud Provider:**
The organization that provides cloud-based IT resources is the *cloud provider*. When assuming the role of cloud provider, an organization is responsible for making cloud services available to cloud consumers, as per agreed upon SLA guarantees. The cloud provider is further tasked with any required management and administrative duties to ensure the on-going operation of the overall cloud infrastructure.

2. **Cloud Consumer:**
Wider to use IT resources made available by the cloud provider. Specifically, the cloud consumer uses a cloud service consumer to access a cloud service

3. **Cloud Service Owner:**
The person or organization that legally owns a cloud service is called a *cloud service owner*. The cloud service owner can be the cloud consumer, or the cloud provider that owns the cloud within which the cloud service resides.

4. **Cloud Resource Administrator**
A cloud resource administrator is the person or organization responsible for administering a cloud-based IT resource (including cloud services). The cloud resource administrator can be (or belong to) the cloud consumer or cloud provider of the cloud within which the cloud service resides. Alternatively, it can be (or belong to) a third-party organization contracted to administer the cloud-based IT resource.

5. **Organizational Boundaries**
An *organizational boundary* represents the physical perimeter that surrounds a set of IT resources that are owned and governed by an organization. The organizational boundary does not represent the boundary of an actual organization, only an organizational set of IT assets and IT resources. Similarly, clouds have an organizational boundary.

6. **Trust Boundaries**
When an organization assumes the role of cloud consumer to access cloud based IT resources, it needs to extend its trust beyond the physical boundary of the organization to include parts of the cloud environment.

(B)

(Explain in detail cloud risk and challenges)

Risk and Challenges:

- **A Lack Of Visibility/Control:**

  One of the biggest benefits of using cloud-based technologies is that the customer doesn't have to manage the resources needed to keep it working (such as servers). However, handing off the responsibility for managing the day-to-day maintenance of a software, platform , or computing asset can result in having less visibility and control over that asset.

- **Some Cloud Platforms May Not Comply With Industry Regulations:**

  Organizations often have to meet special regulatory compliance requirements, such as HIPAA, PCI DSS, GDPR, or FISMA. Failure to meet these standards can result in censures, fines, and other penalties that negatively impact the business. Unfortunately, not all cloud service providers have security measures that comply with every industry regulation.

- **Data Privacy Issues:**
  If a cloud service doesn't have strong cyber security, moving sensitive data to it could expose that data to theft. Even with strong cyber security measures, moving data to the cloud could be a violation of data privacy agreements between the company and its customers. This could lead to fines and business restrictions

- **Notifying Customers Affected by Data Breaches:**

  One of the problems with not having absolute control and visibility of a network is that if the network is compromised, then it can be difficult to establish what resources and data have been affected. With a cloud service, if it doesn't offer strong visibility features and access to event logs, then it can be nearly impossible to identify which customers have been affected by a data breach and what data was compromised.

- **User Access Control:**

  As one of the components that is almost always the user's responsibility, user access control is a crucial challenge for cloud security no matter what type of cloud service is used. However, as with on-premises security solutions, user access control in the cloud can be difficult—especially if the cloud service doesn't have very robust control settings.

- **Vendor Lock-In for Security Features:**

  One major potential challenge is the risk of "vendor lock" when it comes to security features. Being restricted to a single compatible security solution choice for a cloud service is extremely limiting—and it can lead to poor return on investment for security.

- **Lack of Personnel Experienced in Cloud Security Measures:**

  There's a consistent challenge to find qualified security experts for any kind of production environment. This problem can be exacerbated with the cloud, as not everyone will be familiar with the security measures that the solution will use right off the bat.