DXC Technologies- Google Cloud Platform

Assignment-2

Name: Mansi Venkitachal Sarma

Question1: Explain why Cloud Computing is needed? explain IaaS , Paas, SaaS with example each?

Answer 1:

Cloud computing is basically the availability of on demand computer system resources such as data storage without needing to be directly managed by the user. It is used to refer to the data stored in large data centres to multiple users over the internet.

There are mainly 3 types of clouds:

1. Private cloud
2. Public cloud
3. Hybrid cloud

A cloud is needed for the following reasons:

- Efficiency / cost reduction:
  Investment in hardware, facilities, utilities, or building out a large data centre to grow your business is not required. It also reduces costs related to downtime.
- Data security:
  Cloud offers many advanced security features that guarantee that data is securely stored and handled.
- Scalability
  Cloud based solutions are ideal for businesses with growing or fluctuating bandwidth demands. Scalability is probably the greatest advantage of the cloud.
- Mobility
  Cloud computing allows mobile access to corporate data via smartphones and devices. Resources in the cloud can be easily stored, retrieved, recovered, or processed.
- Disaster recovery
  Cloud infrastructure can also help you with loss prevention. The data stored in the cloud remains accessible for any computer with an internet connection, even if something happens to your work computer.

IaaS, SaaS and PaaS are Services provided by a cloud provider.

1. IaaS (Infrastructure as Service):
   This is the most common service model of cloud computing as it offers the fundamental infrastructure of virtual servers, network, operating systems and data storage drives. It allows for the flexibility, reliability and scalability that many businesses seek with the cloud, and removes the need for hardware in the office. This makes it ideal for small and medium sized organisations looking for a cost-effective IT solution to support business growth. IaaS is

a fully outsourced pay-for-use service and is available as a public, private or hybrid infrastructure.

2. PaaS (Platform-as-a-Service):
   This is where cloud computing providers deploy the infrastructure and software framework, but businesses can develop and run their own applications. Web applications can be created quickly and easily via PaaS, and the service is flexible and robust enough to support them. PaaS solutions are scalable and ideal for business environments where multiple developers are working on a single project. It is also handy for situations where an existing data source (such as CRM tool) needs to be leveraged.

3. SaaS (Software as a Service):
   This cloud computing solution involves the deployment of software over the internet to various businesses who pay via subscription or a pay-per-use model. It is a valuable tool for CRM and for applications that need a lot of web or mobile access – such as mobile sales management software. SaaS is managed from a central location so businesses don't have to worry about maintaining it themselves, and is ideal for short-term projects.

Question 2: Explain the many forms of Cloud & traits of cloud computing ?

Answer 2:

There are three forms of cloud: public, private and hybrid.

1. Public Cloud:
   Public cloud solutions are readily available from Google, Amazon, Microsoft, and others. Public cloud services provide infrastructure and services to the public, and you, or your organization, secure a piece of that infrastructure and network. Resources are shared by hundreds or thousands of people. Gmail and U of I Box are examples of public cloud services.

2. Private Cloud:
   Private cloud solutions are dedicated to one organization or business, and often have much more specific security controls than a public cloud. Many medical offices, banking institutions, and other organizations who are required to meet federal and state guidelines for data controls use a private cloud. Using private cloud storage allows them to control highly sensitive data by meeting regulations and industry-based criteria, whether that be medical records, trade secrets, or other classified information.

3. Hybrid Cloud:
   Hybrid cloud solutions are a blend of public and private clouds. This is a more complex cloud solution in that the organization must manage multiple platforms and determine where data is stored. An example of a hybrid cloud solution is an organization that wants to keep

confidential information secured on their private cloud, but make more general, customer-facing content on a public cloud.

The main traits of cloud computing are:

- Resilience and Elasticity:
  The information and applications hosted in the cloud are evenly distributed across all the servers, which are connected to work as one. Therefore, if one server fails, no data is lost and downtime is avoided. The cloud also offers more storage space and server resources, including better computing power. This means your software and applications will perform faster.
- Flexibility and Scalability:
  Cloud hosting offers an enhanced level of flexibility and scalability in comparison to traditional data centres. The on-demand virtual space of cloud computing has unlimited storage space and more server resources. Cloud servers can scale up or down depending on the level of traffic your website receives, and you will have full control to install any software as and when you need to. This provides more flexibility for your business to grow.
- Automation:
  A key difference between cloud computing and traditional IT infrastructure is how they are managed. Cloud hosting is managed by the storage provider who takes care of all the necessary hardware, ensures security measures are in place, and keeps it running smoothly.

- Running Costs:
  Cloud computing is more cost effective than traditional IT infrastructure due to methods of payment for the data storage services. With cloud-based services, you only pay for what is used – similarly to how you pay for utilities such as electricity. Furthermore, the decreased likelihood of downtime means improved workplace performance and increased profits in the long run.

Question 3: Explain the benefits of cloud computing & risks related with it ?

Answer 3:

There are many benefits to cloud technology. They are:

- Efficiency / cost reduction:
  Investment in hardware, facilities, utilities, or building out a large data centre to grow your business is not required. It also reduces costs related to downtime.
- Data security:
  Cloud offers many advanced security features that guarantee that data is securely stored and handled.
- Scalability
  Cloud based solutions are ideal for businesses with growing or fluctuating bandwidth demands. Scalability is probably the greatest advantage of the cloud.
- Mobility
  Cloud computing allows mobile access to corporate data via smartphones and devices. Resources in the cloud can be easily stored, retrieved, recovered, or processed.

- Disaster recovery
  Cloud infrastructure can also help you with loss prevention. The data stored in the cloud remains accessible for any computer with an internet connection, even if something happens to your work computer.

Along with benefits, there are also risks related to cloud technology. These Risks include:

- Consumers Have Reduced Visibility and Control:
  When transitioning assets/operations to the cloud, organizations lose some visibility and control over those assets/operations. When using external cloud services, the responsibility for some of the policies and infrastructure moves to the CSP.
- On-Demand Self Service Simplifies Unauthorized Use:
  CSPs make it very easy to provision new services. The on-demand self-service provisioning features of the cloud enable an organization's personnel to provision additional services from the agency's CSP without IT consent. The practice of using software in an organization that is not supported by the organization's IT department is commonly referred to as shadow IT.
- Internet-Accessible Management APIs can be Compromised:
  CSPs expose a set of application programming interfaces (APIs) that customers use to manage and interact with cloud services (also known as the management plane). Organizations use these APIs to provision, manage, orchestrate, and monitor their assets and users. These APIs can contain the same software vulnerabilities as an API for an operating system, library, etc.
- Separation Among Multiple Tenants Fails:
  Exploitation of system and software vulnerabilities within a CSP's infrastructure, platforms, or applications that support multi-tenancy can lead to a failure to maintain separation among tenants. This failure can be used by an attacker to gain access from one organization's resource to another user's or organization's assets or data. Multi-tenancy increases the attack surface, leading to an increased chance of data leakage if the separation controls fail.
- Data Deletion is Incomplete:
  Threats associated with data deletion exist because the consumer has reduced visibility into where their data is physically stored in the cloud and a reduced ability to verify the secure deletion of their data.

Question 4: What is virtualization & why its needed?

Answer 4:

Virtualization is a process whereby software is used to create an abstraction layer over computer hardware that allows the hardware elements of a single computer to be divided into multiple virtual computers.

Virtualization can help you shift your IT focus from managing boxes to improving the services you provide to the organization. If you are managing multiple servers and desktops, virtualization can help you to:

- Save money:
  Companies often run just one application per server because they don’t want to risk the possibility that one application will crash and bring down another on the same machine. Estimates indicate that most x86 servers are running at an average of only 10 to 15 percent

of total capacity. With virtualization, you can turn a single purpose server into a multi-tasking one, and turn multiple servers into a computing pool that can adapt more flexibly to changing workloads.

- Save energy:
  Businesses spend a lot of money powering unused server capacity. Virtualization reduces the number of physical servers, reducing the energy required to power and cool them.
- Save time:
  With fewer servers, you can spend less time on the manual tasks required for server maintenance. On the flip side, pooling many storage devices into a single virtual storage device, you can perform tasks such as backup, archiving and recovery more easily and more quickly. It's also much faster to deploy a virtual machine than it is to deploy a new physical server.
- Reduce desktop management headaches:
  Managing, securing and upgrading desktops and notebooks can be a hassle. Desktop virtualization solutions let you manage user desktops centrally, making it easier to keep desktops updated and secure.

Question 5: What is Virtual machine & how it works in Cloud ?

Answer 5:

A virtual machine (VM) is a software-based computer that exists within another computer's operating system, often used for the purposes of testing, backing up data, or running SaaS applications.

Some of the most popular reasons people run virtual machines include:

- Testing - Oftentimes software developers want to be able to test their applications in different environments. They can use virtual machines to run their applications in various OSes on one computer. This is simpler and more cost-effective than having to test on several different physical machines.
- Running software designed for other OSes - Although certain software applications are only available for a single platform, a VM can run software designed for a different OS. For example, a Mac user who wants to run software designed for Windows can run a Windows VM on their Mac host.
- Running outdated software - Some pieces of older software can't be run in modern OSes. Users who want to run these applications can run an old OS on a virtual machine.

Question 6: What is a Container & difference between Virtualization & Private cloud ?

Answer 6:

Containers are a lighter-weight, more agile way of handling virtualization. Rather than spinning up an entire virtual machine, a container packages together everything needed to run a small piece of software.

Virtualization is a process whereby software is used to create an abstraction layer over computer hardware that allows the hardware elements of a single computer to be divided into multiple virtual computers.

Private Cloud layers on top of virtualization and, as such, server virtualization is a required component of a private cloud.

Most modern private clouds offer:

- On-Demand Service Provisioning / Self-Service:
  Self-service is a primary feature of a private cloud environment. Users should be able to deploy new services on their own, or at least with minimal guidance from IT infrastructure administrators. As a part of this capability, private cloud environments require a certain level of automation and orchestration capabilities.
- Simple Resource Scaling:
  As your environment grows you will have to add more resources such as compute, RAM, and storage. Today, servers and storage are usually bought and managed separately. When these resources are combined into individual nodes that create an infrastructure that seamlessly snaps together, this is known as hyperconverged infrastructure, an essential building block in a private cloud. To scale your environment, you'll need a solution that can simply and effectively scale resources.
- Multi-Tenancy:
  With multi-tenancy your private cloud can securely support different computing environments (your "tenants"). Public cloud providers require multi-tenancy, as every customer is a different tenant in their public cloud. Enterprises use multi-tenancy in a very similar way in their private clouds. For example, development, test, and production environments can each be securely managed as different tenants.

Question 7: Explain Service level agreement (SLA)?

Answer 7:

A service-level agreement (SLA) defines the level of service expected by a customer from a supplier, laying out the metrics by which that service is measured, and the remedies or penalties, if any, should the agreed-on service levels not be achieved. Usually, SLAs are between companies and external suppliers, but they may also be between two departments within a company.

An SLA pulls together information on all of the contracted services and their agreed-upon expected reliability into a single document. They clearly state metrics, responsibilities and expectations so that, in the event of issues with the service, neither party can plead ignorance. It ensures both sides have the same understanding of requirements.

Question 8: Explain IaaS pricing model ? - also explain Migration to Cloud ?

Answer 8:

IaaS (infrastructure as a service) pricing refers to the billing model(s) used by vendors who deliver IT infrastructure services via the cloud. As with any business, a cloud IaaS vendor has to meet several requirements in order to successfully price its services.

Cloud migration is the process of moving digital business operations into the cloud.

Every business has different needs and will therefore follow a slightly different process for cloud migrations. Cloud providers can help businesses set up their migration process. Most cloud migrations will include these basic steps:

1. Establish goals:
   What performance gains does a business hope to see? On what date will legacy infrastructure be deprecated? Establishing goals to measure against helps a business determine if the migration was successful or not.
2. Create a security strategy:
   Cloud cybersecurity requires a different approach compared to on-premises security. In the cloud, corporate assets are no longer behind a firewall, and the network perimeter essentially does not exist. Deploying a cloud firewall or a web application firewall may be necessary.
3. Copy over data:
   Select a cloud provider, and replicate existing databases. This should be done continually throughout the migration process so that the cloud database remains up-to-date.
4. Move business intelligence:
   This could involve refactoring or rewriting code (see below). It can be done piecemeal or all at once.
5. Switch production from on-premises to cloud:
   The cloud goes live. The migration is complete.

Question 9: Explain various Cloud Security Concerns?

Answer 9:

There are many cloud security concerns that should be thought of before migrating to the cloud. They are:

1. Data Breaches
2. Hijacking of Accounts
3. Insider Threat
4. Malware Injection
5. Abuse of Cloud Services
6. Insecure APIs
7. Denial of Service Attacks
8. Insufficient Due Diligence
9. Shared Vulnerabilities
10. Data Loss

Question 10: Encryption & Compliance in cloud?

Answer 10:

Cloud Data Encryption Best Practices:

- Identify every piece of sensitive data you're sending to your cloud applications and develop policies to apply appropriate levels of encryption to them. You'll need to work with all lines

of business using the cloud to determine their exact uses for it and their cloud encryption needs.

- Encrypt or otherwise protect all sensitive data you handle before it leaves your premises. Encrypt and do not store the most sensitive cardholder and authentication data: full track data, card verification codes, and PINs and PIN blocks.

- Integrate your cloud encryption solution with DLP tools that can detect and generate alerts on activity around sensitive data to prevent the unauthorized access or sharing of data and documents that contain protected information.