Cloud Computing

Sessional Assignment

Name: Siyad Ali **ID# 6839**

Section : B [BS(SE)] **Semester :8th**

- Explain in detail Service Oriented Architecture (SOA) in cloud computing.

Ans: **Service-Oriented Architecture (SOA):**

Service-Oriented Architecture (SOA) is a style of software design where services are provided to the other components by application components, through a communication protocol over a network. Its principles are independent of vendors and other technologies. A number of services communicate with each other, in one of two ways: through passing data or through two or more services coordinating an activity. This is just one definition of Service-Oriented Architecture.

Characteristics Of Service-Oriented Architecture:

While the defining concepts of Service-Oriented Architecture vary from company to company, there are six key t that overarch the broad concept of Service-Oriented Architecture. These core values include:

- Business value
- Strategic goals
- Intrinsic inter-operability
- Shared services
- Flexibility
- Evolutionary refinement

Service-Oriented Architecture Patterns:

There are three roles in each of the Service-Oriented Architecture building blocks: service provider; service broker, service registry, service repository; and service requester/consumer.

The service provider works in conjunction with the service registry, debating the whys and hows of the services being offered, such as security, availability, what to charge, and more. This role also determines the service category and if there need to be any trading agreements.

The service broker makes information regarding the service available to those requesting it. The scope of the broker is determined by whoever implements it.The service requester locates entries in the broker registry and then binds them to the service provider. They may or may not be able to access multiple services; that depends on the capability of the service requester.

Implementing Service-Oriented Architecture

When it comes to implementing service-oriented architecture (SOA), there is a wide range of technologies that can be used, depending on what your end goal is and what you're trying to accomplish.Typically, Service-Oriented Architecture is implemented with web services, which makes the "functional building blocks accessible over standard internet protocols."

- Explain in detail prominent security: threats to the cloud computing.

Ans: **Prominent Security:**

The main security risks of cloud computing are:

- Loss of data
- Malware infections and data breaches
- Compliance violations
- Identity theft
- Diminished customer trust and potential revenue loss

1. **Loss of data:**

By its very nature, cloud computing involves some ceding of control from the customer to the service provider. While this leaves users more time and financial resources to focus on other facets of the business, there is always the risk that sensitive data is in somebody else's hands. If the security of a cloud service is breached, hackers could potentially gain access to intellectual property or other personal files.

2. **Malware infections**

Due to the high volume of data stored on the cloud, which requires an internet connection to store this data, anybody using cloud services is potentially at risk of cyberattacks. An increasingly common threat is Distributed Denial of Service (DDoS) attacks, whereby hackers send unprecedented volumes of traffic to a web-based application, thereby crashing the servers.

3. Legal/compliance issues

With increasing legislation on data protection, from GDPR in Europe to HIPAA for healthcare, staying compliant is becoming more difficult. Companies must have steadfast rules governing who can access what data and what they can do with it. With cloud computing's easy access to data on a large scale, it can be difficult to keep track of who can access this information.

- Explain in detail Cloud Infrastructure Mechanisms.

Ans: **Cloud Infrastructure Mechanisms:**

Technology mechanisms foundational to cloud platforms are covered, including:

- Logical Network Perimeter
- Virtual Server
- Cloud Storage Device
- Cloud Usage Monitor
- Resource Replication
- Ready-Made Environment

Logical Network Perimeter

The isolation of a network environment from the rest of communications network, the logical network perimeter establishes a virtual network boundary that can encompass and isolate a group of related cloud-based IT resources that may be physically distributed. Logical network perimeter can be implement to isolate IT resources in a cloud from cloud users and control the bandwidth via network devices by deploying virtual firewall and virtual network.

Virtual Server:

A virtual server is a form of virtualization software that emulates a physical service. The virtual server represents the mode fundamental building block of cloud environment. The instantiation of virtual servers from image files is a resource allocation process that can be completed rapidly and on-demand. Cloud customers that install or lease virtual servers can customize their environments independently from other customers.

Cloud Storage:

The cloud storage device mechanism represents storage devices that are designed specifically for cloud-based provisioning. Cloud storage devices are commonly able to provide fixed-increment capacity allocation in support of the pay-per-use mechanism. υThe primary concern related to cloud storage is the security, integrity, and confidentiality.

There are several levels in providing common logical units of data storage: files located in a folder Blocks lowest level of storage closest to the HW Datasets table-based, delimited, or record collection Objects web-based resources

According to different storage levels, there are three kinds of interfaces implemented:

Network storage interfaces files or blocks Object storage interfaces web resources Databasre storage interfaces relational or non-relational

Monitor Agent:

Each monitor agent can be designed to forward collected usage data to a log database for postprocessing and reporting purposes. Monitoring agent is usually an event-driven program to network traffic and message metrics. Resource agent monitors usage metrics based on pre-defined, observable events at the resource software level, such as initiating, suspending, resuming, and vertical scaling. ט polling agent polls IT resources to periodically monitor IT resource status, eg. up or down time.

Replication:

Replication is usually performed when resource's availability and performance need to be enhanced. Resource replication mechanism usually uses virtualization technology to replicate cloud-based IT resources

Ready-made Environment:

The ready-made environment mechanism is a defining component of the PaaS cloud delivery model that represents a platform comprised of a set of already installed IT resources, ready to be used and customized by a cloud consumer.