Sessional Assignment

Course Name: Cloud Computing

Submitted By:

Yahya Riaz (12280)

BS (SE) Section: A

Submitted To:

Sir Omer Rauf

Dated: 6th June 2020

Department of Computer Science,
IQRA National University, Peshawar Pakistan

Question #1: Explain in detail Service-Oriented Architecture (SOA) in cloud computing.

What is service-oriented architecture?

Service-oriented architecture (SOA) is a software design where services are provided to one component by other application components over a network through a communication protocol. Its principles are independent of vendors and other technologies. In SOA, 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.

Characteristics of Service-Oriented Architecture:

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

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

Horizontal scaling basis in cloud computing different models:

Infrastructure-as-a-Service (IaaS):

It provides a hardware platform as a service.

Platform-as-a-Service (PaaS):

It provides application development environment delivered over the internet.

Software-as-a-Service (SaaS):

It provides end-users standardized, network-delivered IT applications.

The differences are made according to availability and the location of installation in the deployment models. Private clouds are used within the company services where public clouds are available on the public internet.

In large companies where IT plays a very important role, internal company cloud solutions are usually built-in in their data centers. Small and medium companies mostly use public cloud services. Cloud

computing delivers a very flexible and scalable platform through processing external services and also has the ability to connect with customers and suppliers etc.

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 the end goal is and what is to be accomplish.

Service-Oriented Architecture is implemented with web services, which makes the building blocks accessible over standard internet protocols.

Importance of Service-Oriented Architecture:

There are many benefits to service-oriented architecture, especially in a web service band business:

Use service-Oriented Architecture to create reusable code:

Not only does this cut down on time spent on the development process, theirs is no need to reinvent the coding process every time a company needs to create a new service or process. Service-Oriented Architecture allows for using multiple coding languages because it has central interface.

Use Service-Oriented Architecture to promote interaction:

With Service-Oriented Architecture, a standard and platforms to function independent of each other. In this interaction, Service-Oriented Architecture is also able to work with firewalls, allowing companies to share services that are vital to operations.

Use Service-Oriented Architecture for scalability:

It’s important to be able to scale a business to meet the needs of the client, however certain dependencies can back on the client-service interaction which allows for greater scalability.

Use Service-Oriented Architecture to reduce cost:

It is possible to reduce cost with Service-Oriented Architecture while still maintaining a desired level of output. Using Service-Oriented Architecture allows business to limit the amount of analysis required when developing custom solutions.

Question #2: Explain in detail prominent security threats to the cloud computing.

Security threats to the cloud computing:

Data loss:

Data loss usually happens due to natural or man-induced faults or disasters, as a result of the physical destruction of the servers or human fault. However, it can also be caused by a targeted attack. Regardless of the cause, the result will be the same: all the data is lost that you have been compiling for years.

Data Breach:

Data breach or leak mostly occurs due the widespread cloud security. It usually happens when cloud computing security lacks when someone unauthorized user intrudes to get access to confidential data and can copy, view or transmit it.

Cloud service abuses:

Cloud services can be used to support despicable activities, such as using cloud computing resources to break an encryption key for launching as attack. For example: Dos attacks, sending spam emails and hosting malicious content.

Shared technology, shared threats:

The cloud vulnerabilities in shared technology puts the data in danger. Cloud service providers share infrastructure, platform and applications and if any issue arises in these layers, it affects everyone who are sharing the same resources.

Denial of Service Attacks:

Distributed Denial of Service (DDOS) attacks have become more frequent, more sophisticated and larger in recent years. Operating on a cloud-based service can increase your risk of being affected. As you share resources with all other users on the cloud, an attack on another tenant can result in your service being affected. With the amount of bandwidth consumed by larger DDOS attacks. If you use a smaller provider, your service is likely to get slow or your data may become totally inaccessible.

Crypto jacking:

A relatively new cloud security threat, crypto jacking was widely adopted in past few years due to an immense growth of crypto currency frenzy. In this type of cloud computing attacks, hackers use your computing resources to process crypto currency transactions by installing a crypto mining script on your server without your consent. This leads to an increased CPU load and as a result can significantly slow down your system.

Insecure API's:

Even if your own systems are safe, often there are third-party services that can introduce additional cloud security risks. IoT solutions are typically considered a threat to data privacy: devices such as

connected cars, health monitors and home appliances, collect and transmits tons of sensitive data in real time. As a result, intruder can takeover your data by hijacking your API's not the cloud itself.

Account Hijacking:

Even if your employees are not using default, insecure passwords, hackers can still hijack by guessing the credentials, can gain access to your cloud using your team's accounts and as a result they can steal and manipulate your data or can sabotage your business processes.

Insider Threats:

External threats are there in cloud computing but keeping that aside, there are also enough internal risks. For example, your own employee can cause privacy violations or major data leaks. This can be due to targeted malicious behavior or simply can be a result of human error. However, they can serve as an entry point for malware, e.g. by using their devices for work-related tasks as a part of the BYOD policy.

Question #3: Explain in detail Cloud Infrastructure Mechanism.

Cloud infrastructure mechanisms are foundational building blocks of cloud environments that establish primary artifacts to form the basis of fundamental cloud technology architecture.

Virtual Server:

A virtual server is a form of virtualization software that emulates a physical serve. Virtual servers are used by cloud providers to share the same physical server with multiple cloud consumers by providing cloud consumers with individual virtual server instances. The number of instances a given physical server can share limited by its capacity.

Cloud Storage Device:

The cloud storage device mechanism represents storage devices that are designed specifically for cloud-based provisioning instances of these devices can storage devices are commonly able to provide fixed-increment capacity allocation in support of the pay-per-use mechanism. Cloud storage devices can be exposed for remote access via cloud storage services.

Resource Replication:

It is defined as the creation of multiple instances of the same IT resource. Replication typically is performed when an IT resource availability and performance need to be enhanced.

Logical Network Perimeter:

It is defined as 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. This mechanism can be implemented to:

- Isolate IT resources in a cloud from non-authorized users.
- Isolate IT resources in a cloud from non-users.
- Isolate IT resources in a cloud from cloud customers.
- Control the bandwidth that is available to isolate IT resources.

Cloud Usage Monitor:

The cloud usage monitor mechanism is a lightweight and autonomous software program responsible for collecting and processing IT resource usage data. Depending on the type of usage metrics they are designed to collect and the manner in which usage data needs to be collected, cloud usage monitors can exist in different formats. The upcoming sections describe three common agent-based implementation formats. Each can be designed to forward collect usage data to a log database for post-processing and reporting purposes.

Cloud Storage Device:

The cloud storage device mechanism represents storage devices that are designed specifically for cloud-based provision instances of these devices can be virtualized, similar to how physical servers can spawn virtual server images. Cloud storage devices are commonly able to provide fixed-increment capacity allocation in support of the pay-per-use mechanism. Cloud storage devices can be exposed for remote access through cloud storage services.

Ready-Made environment:

The Ready-Made environment mechanism is a defining component of the PaaS cloud delivery model that represents a pre-defined cloud-based platform comprised of a set of already installed IT resources, ready to be used and customized by the cloud consumer. These environments are utilized by cloud consumers to remotely develop and deploy their own services and applications within a cloud. Typical ready-made environments include pre-installed IT resources, such as databases, middleware, development tools and governance tools.