IQRA National University, Peshawar

Sessional Assignment
Subject: Cloud Computing
Submitted By: Aamir Saleem (12290)
Class/Section: Software Engineering - 8th Semester (Section-A)
Submitted To: Sir Omer Rauf
Date: 12th-june-2020

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

Answer: Introduction:

SOA (Service Oriented Architecture) is built on computer engineering approaches that offer an architectural advancement towards enterprise system. It describes a standard method for requesting services from distributed components and after that the results or outcome is managed. The primary focus of this service-oriented approach is on the characteristics of service interface and predictable service behavior. Web Services means a set or combination of industry standards collectively labeled as one. SOA provides a translation and management layer within the cloud architecture that removes the barrier for cloud clients obtaining desired services. Multiple networking and messaging protocols can be written using SOA's client and components and can be used to communicate with each other. SOA provides access to reusable Web services over a TCP/IP network, which makes this an important topic to cloud computing going forward.

Benefits:

Language Neutral Integration: Regardless of the developing language used, the system offers and invoke services through a common mechanism. Programming language neutralization is one of the key benefits of SOA's integration approach.

Component Reuse: Once an organization built an application component, and offered it as a service, the rest of the organization can utilize that service.

Organizational Agility: SOA defines building blocks of capabilities provided by software and it offers some service(s) that meet some organizational requirement; which can be recombined and integrated rapidly.

Leveraging Existing System: This is one of the major uses of SOA which is to classify elements or functions of existing applications and make them available to the organizations or enterprise.

Layers Of SOA: SOA architecture is viewed as five horizontal layers. These are described below:

Consumer Interface Layer: These are GUI based apps for end users accessing the applications.

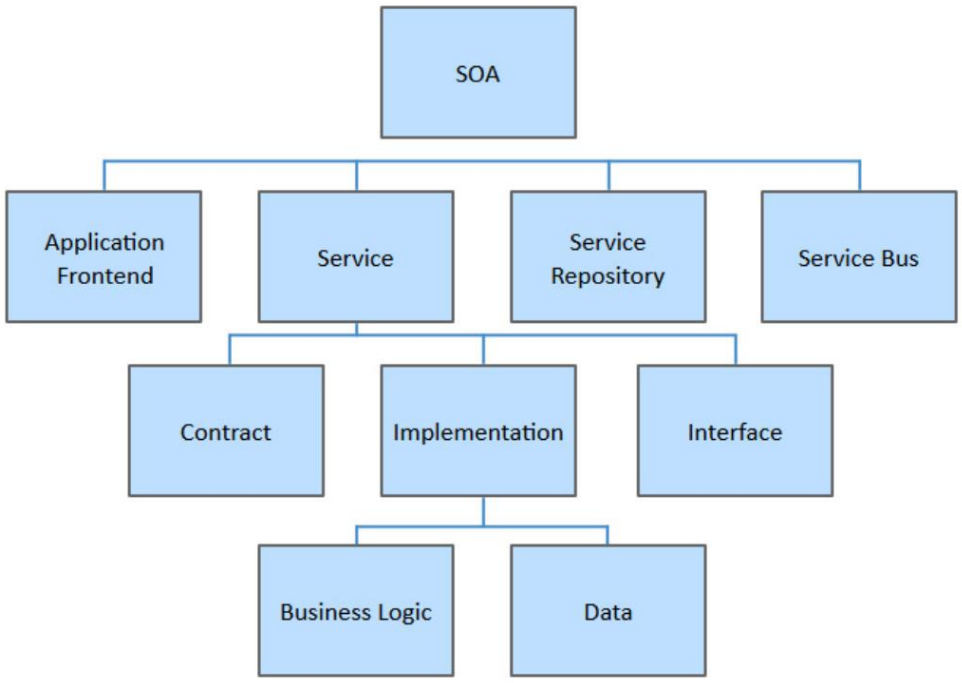
Business Process Layer: These are business-use cases in terms of application.

Services Layer: These are whole-enterprise, in service inventory.

Service Component Layer: are used to build the services, such as functional and technical libraries.

Operational Systems Layer: It contains the data model.

Elements of SOA:



Question 2: Explain in detail prominent security threats to the cloud computing.
Answer: Below are stated the biggest security threats to cloud computing;

1. Data Ownership & Control

The move to cloud will inevitably lead to some loss of control of your organization's data as it is stored on the cloud provider's servers. Issues such as the geographic location of your data, specific backup processes and the steps taken to ensure your data is private and secure are no longer in your control. Moving to the cloud also means that the service provider could have some degree of access to your data. In addition to privacy concerns relating to sensitive data, this may also impact your compliance controls and requirements.

2. Data Loss

Regardless of where and how your data is stored, the permanent loss of data is likely a major concern. Data loss can have a huge impact financially, operationally and even legally as data loss may result in the failure to meet compliance policies or data protection requirements.

In addition to the threat of malicious attacks; natural disaster, technical failure and accidental erasure of data can all affect cloud-based services in the same manner as an internal infrastructure.

Preventing against data loss is not solely the responsibility of the cloud provider. If the relevant encryption key is lost by your organization the data is rendered useless.

3. Data Breaches

Data breach threats exists regardless of whether data is stored internally or on cloud. Some cloud services may be more vulnerable to potential attacks and the hijacking of data due to new methods of attack such as

"Man-in-the-Cloud". This takes advantage of synchronization services to access and extract data, compromise files or attack end-users.

While a cloud provider will implement security measures to reduce the risk of data breaches, it is important to keep in mind that you are ultimately responsible for the security of your organization's data and a breach can have serious legal and financial consequences.

4. Malicious Attacks & Abuse

Hackers or even authorized users may potentially attack and abuse cloud storage for illegal activities. This can include the storing and spread of copyrighted materials, pirated software, malware or viruses. This can occur when individuals directly attack the service or take over the cloud service's resources.

Cloud resources can also be attacked directly through attacks such as malware injection which have become a major threat in recent years. This involves hackers gaining access to the cloud and then running scripts containing hidden malicious code.

5. Insider Threat

While attacks and misuse of data by your own employees may seem low-risk, the insider threat is very real. This can lead to the misuse of important data such as customer or financial information. For organizations who handle sensitive information such as finance or the healthcare industry this can be a major concern.

Assigning incorrect access levels or neglecting to remove user access for ex-employees can also lead to users having access to information they should not have. Apart from users with malicious intent, the threat of accidental deletion or release of data also exists if they are not adequately trained in the use of the software.

6. Unauthorized Access

Unauthorized access could be due to human error. For example, a system administrator forgetting to remove user access or an employee setting an easy to guess password or using the same login credentials across several services.

Other potential risks include lax authentication or poor certificate management on the part of the cloud service provider. This can leave the service exposed to the usual risks of password guessing and theft which could expose your organization's data.

7. Regulatory Compliance

Using a cloud service may impact on privacy or data protection laws and the specific regulations, such as HIPAA, the Sarbanes-Oxley or the EU Data Protection Directive, your business must comply with.

Regulations may state how data is processed and for how long it must be retained. The cloud service must also be capable of providing you with all the necessary data, such as audit trails and logs, in the event of an audit or investigation.

Storing data on a cloud service may mean your organization must comply with other regulations as your data may be physically stored in another country or even several different ones.

The forthcoming General Data Protection Regulation (GDPR) which is law from May 2018 will further enforce Data Protection legislation and have widespread consequences for businesses found to be in breach of Data Protection.

8. 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 large DDoS attacks, only very large cloud providers will be capable of withstanding at attack. If you use a smaller provider, your service is likely to slow to a crawl or your data may become totally inaccessible.

Question 3: Explain in detail Cloud Infrastructure Mechanisms.
Answer: Cloud infrastructure mechanisms are foundational building blocks of cloud environments that establish primary artifacts to form the basis of fundamental cloud technology architecture.

The following cloud infrastructure mechanisms are described below:

1 Logical Network Perimeter:

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. It is defined as the isolation of a network environment from the rest of a communications network.

Logical network perimeters are typically established via network devices that supply and control the connectivity of a data center and are commonly deployed as virtualized IT environments that include:

- Virtual Firewall – An IT resource that actively filters network traffic to and from the isolated network while controlling its interactions with the Internet.
- Virtual Network – Usually acquired through VLANs, this IT resource isolates the network environment within the data center infrastructure.

2 Virtual/Cloud Servers:

A cloud server is a virtual server (rather than a physical server) running in a cloud computing environment. It is built, hosted and delivered via a cloud computing platform via the internet, and can be accessed remotely. They are also known as virtual servers. Cloud servers have all the software they require to run and can function as independent units.

As a commodity mechanism, the virtual server represents the most foundational building block of cloud environments. Each virtual server can host numerous IT resources, cloud-based solutions, and various other cloud computing mechanisms. The instantiation of virtual servers from image files is a resource allocation process that can be completed rapidly and on-demand.

Cloud consumers that install or lease virtual servers can customize their environments independently from other cloud consumers that may be using virtual servers hosted by the same underlying physical server. Figure 2 depicts a virtual server that hosts a cloud service being accessed by Cloud Service Consumer B, while Cloud Service Consumer A accesses the virtual server directly to perform an administration task.

3 Cloud Storage Device:

The cloud storage device mechanism represents storage devices that are designed specifically for cloud-based provisioning. Instances of these devices can be virtualized, similar to how physical servers can spawn virtual server images. They 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 devices.

A primary concern related to cloud storage is the security, integrity, and confidentiality of data, which becomes more prone to being compromised when entrusted to external cloud providers and other third parties. There can also be legal and regulatory implications that result from relocating data across geographical or national boundaries. Another issue applies specifically to the performance of large databases. LANs provide locally stored data with network reliability and latency levels that are superior to those of WANs.

Cloud Storage Device Levels:

Cloud storage device mechanisms provide common logical units of data storage, such as:

Files – Collections of data are grouped into files that are located in folders.

Blocks – The lowest level of storage and the closest to the hardware, a block is the smallest unit of data that is still individually accessible.

Datasets – Sets of data are organized into a table-based, delimited, or record format.

Objects – Data and its associated metadata are organizing as Web-based resources.

Each of these storage levels is commonly associated with a certain type of technical interface which corresponds to a particular type of cloud storage device and cloud storage service used to expose its API.

4 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 designated to forward collected usage data to a log database for post-processing and reporting purposes.

Monitoring Agent

A monitoring agent is an intermediary, event-driven program that exists as a service agent and resides along existing communication paths to transparently monitor and analyze dataflows (Figure 1). This type of cloud usage monitor is commonly used to measure network traffic and message metrics.

Resource Agent

A resource agent is a processing module that collects usage data by having event-driven interactions with specialized resource software (Figure 1). This module is used to monitor usage metrics based on pre-defined, observable events at the resource software level, such as initiating, suspending, resuming, and vertical scaling.

5 Resource Replication:

Resource replication is defined as the creation of multiple instances of the same IT resource, and is typically performed when an IT resource's availability and performance need to be enhanced. Virtualization technology is used to implement the resource replication mechanism to replicate cloud-based IT resources

The resource replication mechanism is commonly implemented as a hypervisor. For example, the virtualization platform's hypervisor can access a virtual server image to create several instances, or to deploy and replicate ready-made environments and entire applications.

6 Ready-Made Environment:

The ready-made environment mechanism (Figure 1) 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 a 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.

A ready-made environment is generally equipped with a complete software development kit that provides cloud consumers with programmatic access to the development technologies that comprise their preferred programming stacks.

Middleware is available for multitenant platforms to support the development and deployment of Web applications. Some cloud providers offer runtime performance and billing parameters. For example, a frontend instance of a cloud service can be configured to respond to time-sensitive requests more effectively than a backend instance. The former variation will be billed at a different rate than the latter.