
**Assignment Title:** Sessional Assignment

**Course Name:** Cloud Computing

**Submitted By:**

Abdul Musawir (12991)

BS (SE) Section: A

**Submitted To:**

Sir Omer Rauf

**Dated: 4th june 2020**

**Department of Computer Science,**
**IQRA National University, Peshawar Pakistan**

**Cloud Computing**

**Sessional Assignment**

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

Answer:

SOA (Service Oriented Architecture) is made on computer engineering approaches that provide an architectural advancement towards enterprise system. It describes a typical method for requesting services from distributed components and then the results or outcome is managed. the first focus of this service oriented approach is on the characteristics of service interface and predictable service behavior. Web Services means a group or combination of industry standards collectively labeled together. It provided a translation and management layer with in the cloud architecture that vanish the barrier for cloud clients getting choice services. Multiple networking and messaging protocols are often written using SOA's client and components and may be wont to communicate with one another. It provided approach to recycable Web services above a TCP/IP network, which made this a crucial topic to cloud computing going forward.

**Benifit of SOA**

These are:

**Language Neutral Integration**: No matter the developing language used, the system offers and invoke services through a standard mechanism. Programming language neutralization is one among the key benefits of SOA's integration approach.

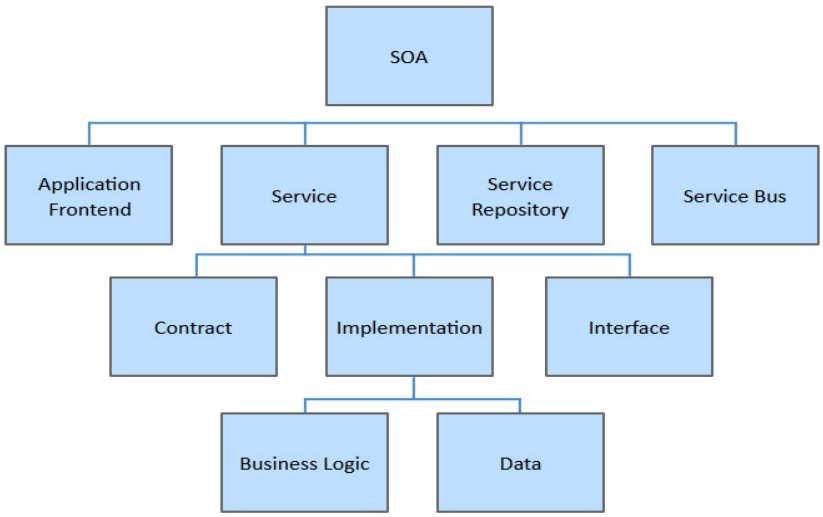
**Component Reuse:** Once a corporation built an application component, and offered it as a service, the remainder of the organization can utilize that service.

**Organizational Agility:** it explain building blocks of ablitiy provide by software and it requests some service that connect some organizational requirement; which can be recombined and integrated quickly.

**Leveraging Existing System**: this is often one among the main use of SOA which is to classify elements or functions of existing applications and make them available to the organizations or enterprise.

**Elements of SOA**

In the diagram figure showing the various elements of SOA:



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

Answer:

Below are a number of the foremost prominent security threats to the cloud computing:

**1. Data Ownership & Control**

The move to cloud will inevitably cause some loss of control of your organization's data because it is stored on the cloud provider's servers. Issues like the geographic location of your data, specific backup processes and therefore the steps taken to make sure your data is private and secure are not any longer in your control. Moving to the cloud also means the service provider could have a point of access to your data. additionally to privacy concerns concerning sensitive data, this might also impact your compliance controls and requirements.

**2. Data Loss**

Regardless of where and the way your data is stored, the permanent loss of knowledge is probably going a serious concern. Data loss can have an enormous impact financially, operationally and even legally as data loss may end in the failure to satisfy compliance policies or data protection requirements. In addition to the threat of malicious attacks; natural disaster, technical failure and accidental erasure of knowledge can all affect cloud-based services within the same manner as an indoor infrastructure. Preventing against data loss isn't solely the responsibility of the cloud provider. If the relevant encryption key's lost by your organisation the info is rendered useless.

**3. Data Breaches**

Data breach threats exists no matter whether data is stored internally or on cloud. Some cloud services could also be more vulnerable to potential attacks and therefore the hijacking of knowledge thanks to new methods of attack like "Man-in-the-Cloud". While a cloud provider will implement security measures to scale back the danger of knowledge breaches, it's important to stay in mind that you simply are ultimately liable for the safety of your organization's data and a breach can have serious legal and financial consequences.

**4. Malicious Attacks & Abuse**

Hackers or maybe authorized users may potentially attack and abuse cloud storage for illegal activities. this will include the storing and spread of copyrighted materials, pirated software, malware or viruses. this will occur when individuals directly attack the service or take over the cloud service's resources. Cloud resources also can be attacked directly through attacks like malware injection which became a serious threat in recent years. This involves hackers gaining access to the cloud then running scripts containing hidden malicious code.

**5. Insider Threat**

While attacks and misuse of knowledge by your own employees could seem low-risk, the insider threat is extremely real. this will cause the misuse of important data like customer or financial information. For organizations who handle sensitive information like finance or the healthcare industry this will be a serious concern. Assigning incorrect access levels or neglecting to get rid of user access for ex-employees also can cause users having access to information they ought to not have. aside from users with malicious intent, the threat of accidental deletion or release of knowledge also exists if they're not adequately trained within the use of the software.

**6. Unauthorized Access**

Unauthorized access might be thanks to human error. for instance, a supervisor forgetting to get rid of user access or an employee setting a simple to guess password or using an equivalent login credentials across several services. this will leave the service exposed to the standard 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 therefore the specific regulations, like HIPAA, the Sarbanes-Oxley or the EU Data Protection Directive, your business

must suits. Regulations may state how data is processed and for a way long it must be retained. The cloud service must even be capable of providing you with all the required data, like audit trails and logs, within the event of an audit or investigation. Storing data on a cloud service may mean your organization must suits other regulations as your data could also be physically stored in another country or maybe several different ones.

**8. Denial of Service Attacks Distributed Denial of Service (DDoS)**

attacks became more frequent, more sophisticated and bigger in recent years. As you share resources with all other users on the cloud, an attack on another tenant may result in your service being affected. With the quantity of bandwidth consumed by large DDoS attacks, only very large cloud providers are going to be capable of withstanding at attack. If you employ a smaller provider, your service is probably going to slow to a crawl or your data may become totally inaccessible.

- Explain in detail Cloud Infrastructure Mechanisms.

Answer:

Cloud infrastructure mechanisms are foundational building blocks of cloud environments that establish primary artifacts to make the idea of fundamental cloud technology architecture. The following cloud infrastructure mechanisms are described in the following:

**Logical Network Perimeter**

Cloud Infrastructure Mechanisms explained because the isolation of a network sorrounding from the remnant of a communications network, the logical network perimeter settled a virtual network boundary which will enclose and seperated a crowd of related cloud-based IT resources which will be physically divided

**Virtual Server**

A virtual server may be a sort of virtualization software that emulates a physical server. Virtual servers are employed by cloud providers to share an equivalent physical server with multiple cloud consumers by providing cloud consumers with individual virtual server instances. The virtual server represents the foremost foundational building block of cloud environments. All virtual server may host various IT resources, cloud-based solutions, and numerous other cloud computing mechanisms.

**Cloud Storage device**

The cloud memory device mechanism express storage devices that is made specifically for cloud-based provision. Instances of those devices are often virtualized, almost like how physical servers can spawn virtual server images. Cloud storage devices are frequently set to provide fixed-increased size grant in help of the pay-per-use mechanism. Cloud storage devices are often exposed for remote access via cloud storage services

**Cloud Usage Monitor**

The cloud usage monitor mechanism may be a lightweight and autonomous software program liable for collecting and processing IT resource usage data. Cloud usage monitors can exist in several formats. The impending sections define three common agent-based peformance formats. all are often made to progress collect use data to a log database for post-processing and reporting missions.

**Resource Replication**

Defined because the creation of multiple instances of an equivalent IT resource, replication is usually performed when an IT resource's availability and performance got to be enhanced. Virtualization technology is employed to implement the resource replication mechanism to duplicate cloud-based IT resources.

**Ready-Made Environment**

The ready-made environment mechanism may be a defining component of the PaaS cloud delivery model that represents a pre-defined, cloud-based platform comprised of a group of already installed IT resources, able to be used and customized by a cloud consumer. These surroundings are used by

cloud customers to rarely develop and locate their own services and applications within a cloud. Classically ready-made surroundings include pre-installed IT resources, like databases, middleware, development tools, and governance tools