Assignment No 2

Course: Cloud Computing

Submitted By:

Hamza Riaz (12282)

BS (SE) Section: A

Submitted To:

Sir Omer Rauf

Dated: 06/6/2020

Cloud Computing

Sessional Assignment

- Explain in detail Service Oriented Architecture (SOA) in cloud computing.
- Explain in detail prominent security threats to the cloud computing.
- Explain in detail Cloud Infrastructure Mechanisms

Answer no 1: Service Oriented Architecture: It is an architectural approach in which application components makes use of a collection of services available in a network which communicates with each other. In SOA services communicate with each other to pass the data. It is also used to integrate widely divergent components by providing them an interface and set of protocols to communicate with the service bus.

Roles in SOA: The major three roles in service oriented architecture are:

- Service provider
- Service broker
- Service consumer

1) Service Provider: is the maintainer of the service and works in conjunction with the service registry, debating the whys and how's of the services being offered, such as security, availability, what to charge, and more.

2) Service Brokers: Service brokers are those who makes and stores information regarding services.

3) Service Consumers: Service consumers are those who locate entries in broker registry and binds it to service provider.

Elements of SOA: Elements of SOA are:

- Application frontend
- Contracts
- Service
- Interface
- Business logic
- Data
- Service repository
- Service bus

Advantages of SOA:

Service reusability: In Service oriented Architecture, applications are produced from existing services. From that services that are reused we can make many applications.

Easy maintenance: As services are independent so it can be updated and modified easily without affecting other services.

Platform independent: SOA allows to create a complex application by merging the services picked from different sources.

Availability: The facilities of SOA are easily available to anyone on request.

Reliability: The applications of SOA are more reliable because it is easy to debug small services rather than huge codes.

Scalability: The services can run on different servers within an environment, this increases scalability.

Disadvantages of SOA:

High overhead: The affirmation of input parameters of services is done whenever services interact this decreases performance as it increases load and response time.

High investment: A huge initial investment is required for Service Oriented Architecture.

Complex service management: When services interact with each other will exchange messages to tasks. The number of messages may go in millions. It becomes a huge task to handle a large number of messages.

Answer No 2:

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 Breach: The threats of data breach exist 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 as an 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. Unauthorized Access
Unauthorized access could be due to human error. For example, system administrator forget to remove user access of an employee setting an easy 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.

6. 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.

7. 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.

Answer no 3:

Cloud Infrastructure Mechanism: It can be defined as the isolation of a network environment from the rest of a communications network, the logical network perimeter establishes a virtual network boundary that can encompass and also isolate group of related based IT resources that may be physically distributed.

The cloud infrastructure mechanisms are:

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

1) Logical Network Perimeter: Logical network perimeter are typically established via network devices that supply and control the connectivity of a data center.

2) Virtual Server: It is a form of virtualization software that emulates a physical server. It can be used by cloud providers to share the same physical server with multiple cloud consumers by providing cloud consumers with individual virtual server.

3) Cloud Usage Monitor: Cloud monitor mechanism is lightweight software program responsible for collecting and processing IT resource usage data.

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

5) 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 installed resources of IT ready to be used and customized by a cloud consumer.