Sessional Assignment

Course Name: Cloud Computing

Submitted By:

Musab Awais (13028)

BS (SE-8) Section: A

Submitted To:

Sir M Omer Rauf

Dated: 08 June 2020

Department of Computer Science,
IQRA National University, Peshawar Pakistan

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

Answer:

Service Oriented Architecture (SOA):

Definition: Service oriented architecture (SOA) is made on computer engineering approaches that provide architectural advancement towards enterprise system. It describes a typical methodology for requesting services from distributed elements and afterward the results or outcome is managed. The first focus of this service oriented approach is on the characteristics of service interface and certain service behavior. SOA provides a translation and management layer inside the cloud architecture that removes the barrier for cloud clients getting desired services. Multiple networking and electronic communication protocols can be written using SOA's client and elements and may be used to communicate with one another. SOA provides access to reusable web services over a TCP/IP network that makes this a very important topic to cloud computing.

SOA Architecture: SOA architecture is viewed as 5 horizontal layers that are defined below:

- **Consumer Interface Layer:** These are user interface based apps for end users accessing the applications.

- **Business process Layer:** The layer provides facilities to compose existing business processes, services, and service components into new business processes. It also provides services-oriented collaboration control between business processes, services, and service components.

- **Services Layer:** These are full enterprise, which is present in service inventory.

- **Service component Layer:** These are cast-off to build the services, like functional and technical libraries.

- **Operational Systems Layer:** It contains the information model.

Elements of SOA: Following are the elements of SOA:

- Application Frontend
- Service
    - Contract
    - Implementation
        - Business Logic
        - Data
    - Interface
- Service Repository
- Service Bus

SOA Protocols:

- **Business Processes:** Business Process Execution Language for Web Service (WS-BPEL)
- **Quality of Service (QoS):** Reliability, Transactions, Management
- **Description:** Web Services Description Language (WSDL)
- **Messaging:** SOAP, Extensible Markup Language (XML)

Security in SOA: With the immense use of cloud technology and its on-demand applications, there's a necessity for well-outlined security policies and access management. With the betterment of these problems, the success of SOA design can increase. Actions may be taken to confirm security and reduce the risks once managing SOE (Service oriented Environment). We can build policies which will influence the patterns of development and therefore the approach services are used. Moreover, the system should be set-up so as to take advantage of the benefits of public cloud with resilience. Users should embody safety practices and thoroughly measure the clauses in these respects.

Benefits of SOA: With sophisticated engineering and enterprise point of view, numerous offers are provided by SOA that are proven to be helpful. These are:

- **Language Neutral Integration:** No matter the developing language used, the system offers and invoke services through a typical mechanism. Programming language neutralization is one among the key advantages of SOA's integration approach.
- **Component Reuse:** Once an organization engineer an application element, and offered it as a service, the remainder of the organization will utilize that service.
- **Organizational Agility:** SOA defines building blocks of capabilities provided by software package and it offers some service(s) that meet some organizational requirement; which may be recombined and integrated quickly.
- **Leveraging Existing System:** This is one among the key use of SOA that is to classify components or functions of existing applications and build them obtainable to the organizations or enterprise.

Key Benefits:

- Dependence on the network
- Provider cost
- Enterprise standards
- Agility

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

Answer:

Security threats in cloud computing:

- **Data Breaches:** Due to the large quantity of information stored on cloud servers, suppliers become an attractive target. The severity of potential damage tends to rely upon the sensitivity of the information exposed. Exposed personal financial info tends to induce the headlines, however breaches involving health info, trade secrets, and belongings may be additional devastating. Once a data breach happens, corporations could incur fines, or they will face lawsuits or criminal charges. Breach investigations and client notifications will rack up vital costs. Indirect effects, like brand damage and loss of business, will impact organizations for years.

- **Compromised credentials:** Many developers make the error of embedding credentials and crypto graphical keys in source code and leaving them in public-facing repositories. Keys got to be fittingly protected, and a well-secured public key infrastructure is important. Multifactor authentication systems like one-time passwords, phone-based authentication, and smartcards shield cloud services because they make it tougher for attackers to log in with taken passwords.

- **Hacked interfaces and APIs:** The security and handiness of cloud services -- from authentication and access management to encryption and activity observation -- depend upon the protection of the API. Risk will increase with third parties that rely on API and repose on these interfaces, as organizations might have to show a lot of services and credentials. Weak interfaces and APIs result in organizations security problems like secret information disappearance, personal data loss, availability issues, and responsibility. APIs and interfaces tend to be the foremost exposed part of a system because they are typically accessible from the open web.

- **Account hijacking:** Phishing, fraud, and software package exploits are still fortunate, and cloud services add a new dimension to the threat because attackers will snoop on activities, manipulate transactions, and modify knowledge. Attackers can also be able to use the cloud application to launch different attacks. This might happen because of sharing of account credentials between users and services.

- **Malicious insiders:** The insider threat has several faces: a current or former worker, a supervisor, a contractor, or a business partner. The malicious agenda ranges from information theft to revenge. During a cloud state of affairs, a hell bent insider will destroy whole infrastructures or manipulate information. Systems that rely exclusively on the cloud service supplier for security, like encryption, are at greatest risk.

- **The APT parasite:** The advanced persistent threats (APTs) are additionally known as "parasitical" types of attack. APTs infiltrate systems to ascertain a grip, and then stealthily infiltrate information belongings over an extended amount of time. APTs usually move laterally through the network and mix in with traditional traffic, thus they are tough to find. Common points of entry embody spear phishing; direct attacks, USB drives preloaded with malware, and compromised third-party networks.

- **Permanent data loss:** Malicious hackers are noted to permanently delete cloud information to hurt businesses, and cloud information centers are as vulnerable to natural disasters as any facility. The burden of preventing information loss isn't all on the cloud service provider. If a client encrypts information before uploading it to the cloud, then that client should use caution to protect the encryption key. Once the key is lost, information might be lost too. Compliance policies usually stipulate however long organizations should retain audit records and different documents. Losing such information might have serious restrictive consequences.

- **Inadequate diligence:** Organizations that embrace the cloud while not totally understanding the environment and its associated risks could encounter a "myriad of economic, financial, technical, legal, and compliance risks". This applies when an organization is attempting to migrate to the cloud or merging (or working) with another company within the cloud. For instance, organizations that fail to scrutinize a contract might not be aware of the provider's liability in case of information loss or breach. Operational and architectural problems arise if a company's development team lacks familiarity with cloud technologies as apps are deployed to a specific cloud.

- **Cloud service abuses:** Cloud services are often commandeered to support villainous activities, like using cloud computing resources to break encryption key so as to launch attack. Alternative examples including launching DoS attacks, causing spam and phishing emails, and hosting malicious content. Though customers might not be directly responsible for malicious actions, cloud service abuse will still end in service accessibility problems and information loss.

- **Shared technology:** Exposure in shared technology cause a major threat to cloud computing. Cloud service suppliers share platforms, applications, and infrastructure, and if a vulnerability arises in any of those layers, it affects everybody. A wrong configuration will result in vulnerability of a complete provider's cloud. If integral element gets compromised -- say a hypervisor, a shared platform element, or application it exposes the whole cloud to potential compromise and breach.

Question 3: Explain in detail Cloud Infrastructure Mechanisms.

Answer:

Cloud Infrastructure Mechanisms: Cloud infrastructure mechanisms are foundational building blocks of cloud environments that establish primary artifacts to form the premise of elementary cloud technology style. It includes of following mechanism:

- Logical Network Perimeter
- Virtual Server
- Cloud storage device
- Cloud Usage Monitor
- Resource Replication
- Read-Made environment

- **Logical Network Perimeter:** Isolation of network setting establishing a virtual network boundary. Its functions are 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's accessible to isolated IT resources.

  Typically established via network devices that offer and manage the connectivity of a knowledge center (commonly deployed as virtualized IT environment), which incorporates
    - Virtual Firewall – actively filter incoming and outgoing traffic.
    - Virtual Network – isolates the network setting inside the information center.

- **Virtual Servers:** A type of virtualization software system that emulates a physical server. Utilized by cloud supplier for resources sharing. Virtual server = virtual machine.

  Template Virtual Servers (may embrace pre-installed software/applications) examples:

- Small Virtual Server Instance – one virtual processor core, four GB of virtual RAM, twenty GB of storage space within the root file system.

- Medium Virtual Server Instance – two virtual processor cores, eight GB of virtual RAM, twenty GB of storage space within the root file system.

- Large Virtual Server Instance – eight virtual processor cores, sixteen GB of virtual RAM, twenty GB of storage space within the root file system.

- Memory massive Virtual Server Instance – eight virtual processor cores, sixty four GB of virtual RAM, twenty GB of storage space within the root file system.

- Processor massive Virtual Server Instance – thirty two virtual processor cores, sixteen GB of virtual RAM, twenty GB of storage space within the root file system.

- Ultra-Large Virtual Server Instance – 128 virtual processor cores, 512 GB of virtual RAM, forty GB of storage space within the root file system.

- **Cloud Storage Devices:** Storage devices designed specifically for cloud-based setting. Instances of this storage may well be virtualized. It's able to give fix-increment capability allocation in support of pay-per-use mechanism.

    - Cloud Storage Levels:

    - Files – Collections of knowledge are classified into files that are situated in folders.

    - Blocks – the lowest level of storage and therefore the nearest to the hardware, a block is that the smallest unit of knowledge that's still separately accessible.

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

    - Objects – knowledge and its associated data are organized as Web-based resources.

Technical Interfaces to Storage:

- Network Storage Interfaces – Most inheritance network storage falls below this class, e.g., port for storage blocks, NFS for network storage.

- Storage process levels and thresholds for file allocation are typically determined by the file system itself (tend to be suboptimal).

- Object Storage Interfaces - numerous kinds of knowledge is documented and hold on as internet resources. This is often cited as object storage. REST protocol, internet service-based cloud services as examples.

- Database Storage Interfaces – support a query language additionally to basic storage operations.

- Relational data Storage – depends on table to arrange similar knowledge into rows and columns. Use of the business standard structured query language (SQL). Examples are IBM DB2, Oracle database, Microsoft SQL and MySQL.

- Complex relational database styles will imposes higher process overhead and latency.

- Non-relational data Storage – aims at reducing process overhead of relative databases.

Drawback – tend to not support computer database functions like transactions or joins.

- **Cloud Usage Monitor:** A light-weight and autonomous software system program liable for aggregation and process IT resource usage knowledge.

  Metrics – quantity of knowledge, range of transactions, usage time, etc.

  Three common agent-based implementation formats: monitoring agent, Resource agent and Polling agent.

  - **Monitoring Agent:** A service agent existing on communication methods, watching and analyzing knowledge flows. Live network traffic and message metrics.

  - **Resource Agent:** Even-driven agent watching resource usage supported pre-defined, noticeable at the resource software system level like initiating, suspending, resuming and vertical scaling.

- **Polling Agent:** It is a process module that collects cloud service usage knowledge by polling IT resources. Normally accustomed sporadically monitor IT resource standing, like period of time and time period.

- **Resource Replication:** The creation of multiple instances of identical IT resource. Replication is often performed once IT resource's availableness and performance got to be increased.
  A set of high-availability virtual servers which will be mechanically resettled to physical servers running in numerous knowledge centers in response to severe failure conditions.

- **Ready-Made Environment:** A process part of the PaaS cloud delivery model that represents a pre-defined, cloud-based platform comprised of a group of already put in IT resources, able to be used and customized by a cloud client. Usually equipped with software system Development Kit (SDK).