Sessional Assignment

Course Name: Cloud Computing

Submitted By:

Abdul Razzaq (12938)

BS (SE-8) Section: A

Submitted To:

Sir M Omer Rauf

Dated: 05 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: Cloud computing could be a model used for sanctionative convenient and usage-based network access to configurable computing resources (e.g. networks, servers etc.) that may be provided and used quickly.

- It provides an opportunity to business users to implement services with usage-based charge that's modified in line with their needs while not want of consulting with IT department.

- It provides abstraction layer between computing resources and its technical implementation details and consecutive allows process resources to be used whereas avoiding efforts in infrastructure management.

Models of SOA: Below are the models that are differentiated on the horizontal scaling basis in cloud computing

- Infrastructure-as-a-Service (IaaS): hardware platform is provided as a service.

- Platform-as-a-Service (PaaS): It provides end-users application development setting delivered over the net.

- Software-as-a-Service (SaaS): It provides end-users standardized, network-delivered IT applications.

The distinctions are created in line with convenience and therefore the location of installation within the readying models. Personal clouds are internal company services whereas public clouds are the services that are offered to the general public on web.
In the massive corporations wherever IT plays a very important role, internal company cloud solutions are typically in-built their own information centers. Tiny and medium corporations typically use public cloud services. Cloud Computing provides a really versatile and ascendible platform through process external services and conjointly has the flexibility to attach with customers, suppliers etc.

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

Answer:

- **Data Breach:** A knowledge breach (or leak) is probably the foremost widespread cloud security concern. It always happens as a result of cloud computing security attacks, once unauthorized users or programs gain access to confidential information and may read, copy, or transmit it.

- **Data Loss:** In contrast to information breaches, information loss usually happens thanks to natural or man-induced disasters, as a result of the physical destruction of the servers or human error. However, it may be a result of a targeted attack. in spite of the cause, the result are going to be the same: you lose all of the info you've been grouping for years.

- **Denial of Service (DoS):** Another common kind of cloud computing security attack, a Denial of Service (DoS) attack will close up your cloud services, creating them quickly (or indefinitely) untouchable to your users. this may be done by either flooding the system with in depth traffic, that the servers merely can't buffer, or crash it by taking advantage of the bugs and vulnerabilities.

- **Crypto jacking:** A comparatively new cloud security threat, crypto jacking was wide adopted last year, mostly thanks to the growing crypto currency craze. during this kind of cloud computing security attack, hackers use your computing resources to method crypto currency transactions by putting in a crypto mining script on your servers while not your consent. This ends up in associate hyperbolic central processing unit load and, as a result, will considerably weigh down your system.

- **Account Hijacking:** Even if your staffs aren't exploitation default, insecure passwords, hackers still will "guess" the credentials, gain access to your cloud exploitation your staffs' accounts, and, as a result, steal or manipulate your information or sabotage your business processes normally. This is often referred to as, "account hijacking."

- **Insecure APIs:** Even if your own systems area unit safe, there area unit usually third-party services that may introduce further cloud security risks. Namely, IoT solutions area unit usually thought of a threat to information privacy: devices, like connected cars, health monitors, and residential appliances, collect and transmit plenty of sensitive information in real time. As a result, intruders will hijack your information by hacking your APIs, not the cloud itself.

- **Insider Threats:** Excluding external security threats in cloud computing, there area unit enough internal risks. As an example, your own staff will cause privacy violations or major information leaks. This may flow from to targeted malicious behavior or just a result of human error. Moreover, they will function associate entry purpose for malware, e.g. by exploitation their devices for work-related tasks as a neighborhood of the BYOD policy.

Question 3: Explain in detail Cloud Infrastructure Mechanisms.

Answer:

Cloud infrastructure mechanisms are foundational building blocks of cloud environments that establish primary artifacts to make the premise of elementary cloud technology design.

- **Logical Network Perimeter:** Outlined because the isolation of a network surroundings from the remainder of communications network, the logical network perimeter

establishes a virtual network boundary which will comprehend and isolate a bunch of connected cloud-based IT resources which will be physically distributed.
This mechanism is enforced to:

- isolate IT resources during a cloud from non-authorized users
- isolate IT resources during a cloud from non-users
- isolate IT resources during a cloud from cloud shoppers
- management the information measure that's accessible to isolate IT resources

- **Virtual Server:** A virtual server may be a kind of virtualization software package that emulates a physical server. Virtual servers are employed by cloud suppliers to share an equivalent physical server with multiple cloud shoppers by providing cloud shoppers with individual virtual server instances. The quantity of instances a given physical server will share is proscribed by its capability.

- **Cloud Storage Device:** The cloud device mechanism represents storage devices that are designed specifically for cloud-based provisioning Instances of those devices is virtualized, almost like however physical servers will spawn virtual server pictures. Cloud storage devices are normally able to offer fixed-increment capability allocation in support of the pay-per-use mechanism. Cloud storage devices are exposed for remote access via cloud storage services.

- **Cloud Usage Monitor:** The cloud usage monitor mechanism may be a light-weight and autonomous software package program answerable for collection and process IT resource usage knowledge. Counting on the sort of usage metrics they're designed to gather and also the manner during which usage knowledge must be collected, cloud usage monitors will exist in several formats. The future sections describe 3 common agent-based implementation formats. Every designed to forward collect usage knowledge to a log info for post-processing and coverage functions.

- **Ready-Made Environment:** The ready-made surroundings mechanism may be a shaping part of the PaaS cloud delivery model that represents a pre-defined, cloud-based platform comprised of a collection of already put in IT resources, able to be used and customized by a cloud shopper. These environments are utilized by cloud shoppers to remotely develop and deploy their own services and applications inside a cloud. Typical ready-made environments embrace pre-installed IT resources, like databases, middleware, development tools, and governance tools.