Sessional Assignment

Course Name: Cloud Computing

Submitted By:

Muhammad Safeer (13033)

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:

Definition: Cloud computing is a model used for enabling convenient and usage-based network access to configurable computing resources (e.g. networks, servers etc.) that can be provided and used rapidly.

- It provides a chance to business users to implement services with usage-based billing that is changed according to their requirements without need of consulting with IT department.
- It provides an abstraction layer between computing resources and its technical implementation details and sequentially enables computational resources to be used while avoiding efforts in infrastructure management.

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

- **Infrastructure-as-a-Service (IaaS)**: It provides a hardware platform as a service.
- **Platform-as-a-Service (PaaS)**: It provides end-users an application development environment delivered over the internet.
- **Software-as-a-Service (SaaS)**: It provides end-users standardized, network-delivered IT applications.

The distinctions are made according to availability and the location of installation in the deployment models. Private clouds are internal company services whereas public clouds are the services that are available to the public on internet.
In the large companies where IT plays an important role, internal company cloud solutions are often built in their own data centers. Small and medium companies often use public cloud services. Cloud Computing provides a very flexible and scalable platform through processing external services and also has the ability to connect with customers, suppliers etc.

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

Answer:

- **Data Breach:** A data breach (or leak) is possibly the most widespread cloud security concern. It usually happens as a result of cloud computing security attacks, when unauthorized users or programs gain access to confidential data and can view, copy, or transmit it.

- **Data Loss:** Unlike data breaches, data loss often happens due to natural or man-induced disasters, as a result of the physical destruction of the servers or human error. However, it can also be a result of a targeted attack. Regardless of the cause, the result will be the same: you lose all of the data you've been collecting for years.

- **Denial of Service (DoS):** Another popular type of cloud computing security attack, a Denial of Service (DoS) attack can shut down your cloud services, making them temporarily (or indefinitely) unavailable to your users. This can be done by either

flooding the system with extensive traffic, which the servers simply can't buffer, or crash it by taking advantage of the bugs and vulnerabilities.

- **Crypto jacking:** A relatively new cloud security threat, crypto jacking was widely adopted last year, largely due to the growing crypto currency frenzy. In this type of cloud computing security attack, hackers use your computing resources to process crypto currency transactions by installing a crypto mining script on your servers without your consent. This leads to an increased CPU load and, as a result, can significantly slow down your system.

- **Account Hijacking:** Even if your employees aren't using default, insecure passwords, hackers still can "guess" the credentials, gain access to your cloud using your staffs' accounts, and, as a result, steal or manipulate your data or sabotage your business processes in general. This is called, "account hijacking."

- **Insecure APIs:** Even if your own systems are safe, there are often third-party services that can introduce additional cloud security risks. Namely, IoT solutions are typically considered a threat to data privacy: devices, such as connected cars, health monitors, and home appliances, collect and transmit tons of sensitive data in real time. As a result, intruders can hijack your data by hacking your APIs, not the cloud itself.

- **Insider Threats:** Apart from external security threats in cloud computing, there are enough internal risks. For example, your own employees can cause privacy violations or major data leaks. This can be due to targeted malicious behavior or simply a result of human error. Moreover, they can serve as an entry point for malware, e.g. by using their devices for work-related tasks as a part 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 form the basis of fundamental cloud technology architecture

- **Logical Network Perimeter:** Defined as the isolation of a network environment from the rest of communications network, 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
  This mechanism can be implemented 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 consumers
  • control the bandwidth that is available to isolate IT resources

- **Virtual Server:** A virtual server is a form of virtualization software that emulates a physical server. Virtual servers are used by cloud providers to share the same physical server with multiple cloud consumers by providing cloud consumers with individual virtual server instances**.** The number of instances a given physical server can share is limited by its capacity.

- **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. Cloud storage devices 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 services.

- **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 designed to forward collect usage data to a log database for post-processing and reporting purposes.

- **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 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**.**