Cloud Computing
Sessional Assignment
Name: Syed M. Hassan Shah   ID: 6853
BS(SE)   section: B
Semester: 8th

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

Answer: Service-oriented architecture (SOA) is a style of software design where services are provided to the other components by application components, through a communication protocol over a network.
SOA (Service Oriented Architecture) is built on computer engineering approaches that offer an architectural advancement towards enterprise system
SOA provides a translation and management layer within the cloud architecture that removes the barrier for cloud clients obtaining desired services.
Service-oriented architecture (SOA) is a software development model that allows services to communicate across different platforms and languages to form applications. In SOA, a service is a self-contained unit of software designed to complete a specific task.
Benefits:
➢ The primary goal of Service Oriented Architecture is to align business users with information technologies (IT). Service-oriented architecture (SOA) enables increased business agility, improved business workflows, extensible architecture, enhanced reuse, and a longer life span of applications.
➢ **SOA** allows users to combine a large number of facilities from existing services to form applications. SOA encompasses a set of design principles that structure system development and provide means for integrating components into a coherent and decentralized system.
Importance:
➢ **SOA** can support you to align your business goals with your IT architecture.
SOA architecture can also give the business real time access to the data they need – business activity monitoring (BAM). With BAM information business users can make their process decisions based on real time data.

……………………………………………………………………………………………
Question:2 Explain in detail prominent security threats to the cloud computing.
Answer: The main security risks of cloud computing are: Compliance violations. Identity theft, Malware infections and data breaches.
Some of the most traditional cloud computer cyber threats include:
• Data breach or loss.
• Abuse of cloud services.
• Insecure interface and APIs.
• Malicious insiders.
• Illegal access to cloud systems.
• Privilege escalation.
• Natural disasters.
• Hardware failure.
Loss or theft of intellectual property, Compliance violations and regulatory actions. Loss of control over end user actions, Malware infections that unleash a targeted attack.

………

Question:3 Explain in detail Cloud Infrastructure Mechanisms.

Answer: Cloud infrastructure mechanisms are foundational building blocks of cloud environments that establish primary artifact to form the basis of fundamental cloud technology architecture.

The audit monitor is a specialized variation of the cloud usage monitor dedicated to collecting audit tracking data for networks and IT resources. The cloud usage monitor mechanism is a lightweight and autonomous software program responsible for collecting and processing IT resource usage data.

Virtual Server: The virtual server, also known as virtual machine (VM), is a form of virtualization software that emulates a physical server and is used by cloud providers to share the same physical server with multiple cloud consumers by providing cloud consumers with individual virtual server instances.