Cloud Computing **ID# 12939**
Sessional Assignment **section 'B'**

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

Answer:

SOA (Service Oriented Architecture) is built on computer engineering approaches that offer an architectural advancement towards enterprise system.

It describes a standard method for requesting services from distributed components and after that the results or outcome is managed. The primary focus of this service oriented approach is on the characteristics of service interface and predictable service behavior. Web Services means a set or combination of industry standards collectively labeled as one. SOA provides a translation and management layer within the cloud architecture that removes the barrier for cloud clients obtaining desired services. Multiple networking and messaging protocols can be written using SOA's client and components and can be used to communicate with each other. SOA provides access to reusable Web services over a TCP/IP network, which makes this an important topic to cloud computing going forward.

Benefits of SOA

With high-tech engineering and enterprise point of view, various offers are provided by SOA which proved to be beneficial. These are:

Language Neutral Integration:

Regardless of the developing language used, the system offers and invoke services through a common mechanism. Programming language neutralization
is one of the key benefits of SOA's integration approach.

Component Reuse:

Once an organization built an application component, and offered it as a service,
the rest of the organization can utilize that service.

Organizational Agility:

SOA defines building blocks of capabilities provided by software and it offers some service(s) that meet some organizational requirement; which can be recombined and integrated rapidly

Leveraging Existing System: This is one of the major use of SOA which is to classify elements or functions of existing applications and make them available to the organizations or enterprise.

Key Benefits Along With Risks of SOA

Dependence on the network
Provider cost
Enterprise standards
Agility

SOA Architecture

SOA architecture is viewed as five horizontal layers. These are described below:

Consumer Interface Layer:

These are GUI based apps for end users accessing the applications.

Business Process Layer:

These are business-use cases in terms of application.
Services Layer:
These are whole-enterprise, in service inventory.
Service Component Layer:
are used to build the services, such as functional and technical libraries.
Operational Systems Layer: It contains the data model.

Explain in detail prominent security threats to the cloud computing.
Answer:
Enterprises are no longer sitting on their hands, wondering if they should risk migrating applications and data to the cloud. They're doing it but security remains a serious concern.
The first step in minimizing risk in the cloud is to identify the prominent security Threats.
Threat No. 1: Data breaches
Cloud environments face many of the same threats as traditional corporate networks, but due to the vast amount of data stored on cloud servers, providers
become an attractive target. The severity of potential damage tends to depend on the sensitivity of the data exposed. Exposed personal financial information tends to get the headlines, but breaches involving health information, trade secrets, and intellectual property can be more devastating.When a data breach
occurs, companies may incur fines, or they may face lawsuits or criminal charges. Breach investigations and customer notifications can rack up significant
costs. Indirect effects, such as brand damage and loss of business, can impact organizations for years.
Threat No. 2: Compromised credentials and broken authentication
Data breaches and other attacks frequently result from lax authentication, weak
passwords, and poor key or certificate management. Organizations often struggle with identity management as they try to allocate permissions appropriate to the user’s job role. More important, they sometimes forget to remove user access when a job function changes or a user leaves the organization.Multifactor authentication systems such as one-time passwords, phone-based authentication, and smartcards protect cloud services because they make it harder for attackers to log in with stolen passwords. The Anthem breach, which exposed more than 80 million customer records, was the result of
stolen user credentials. Anthem had failed to deploy multifactor authentication, so once the attackers obtained the credentials, it was game over.
Threat No. 3: Hacked interfaces and APIs
Practically every cloud service and application now offers APIs. IT teams use interfaces and APIs to manage and interact with cloud services, including those
that offer cloud provisioning, management, orchestration, and monitoring.
The security and availability of cloud services -- from authentication and access

control to encryption and activity monitoring -- depend on the security of the API.

Risk increases with third parties that rely on APIs and build on these interfaces,
as organizations may need to expose more services and credentials, the CSA warned. Weak interfaces and APIs expose organizations to security issues related to confidentiality, integrity, availability, and accountability.

Threat No. 4: Exploited system vulnerabilities

System vulnerabilities, or exploitable bugs in programs, are not new, but they've
become a bigger problem with the advent of multitenancy in cloud computing. Organizations share memory, databases, and other resources in close proximity
to one another, creating new attack surfaces.

Fortunately, attacks on system vulnerabilities can be mitigated with “basic IT processes,” says the CSA. Best practices include regular vulnerability scanning,
prompt patch management, and quick follow-up on reported system threats.

Threat No. 5: Account hijacking

Phishing, fraud, and software exploits are still successful, and cloud services add a new dimension to the threat because attackers can eavesdrop on activities,
manipulate transactions, and modify data. Attackers may also be able to use the
cloud application to launch other attacks.

Common defense-in-depth protection strategies can contain the damage incurred by a breach. Organizations should prohibit the sharing of account credentials between users and services, as well as enable multifactor authentication schemes where available. Accounts, even service accounts, should be monitored so that every transaction can be traced to a human owner.

The key is to protect account credentials from being stolen, the CSA says

Threat No. 6: Malicious insiders

The insider threat has many faces: a current or former employee, a system administrator, a contractor, or a business partner. The malicious agenda ranges
from data theft to revenge. In a cloud scenario, a hellbent insider can destroy whole infrastructures or manipulate data. Systems that depend solely on the cloud service provider for security, such as encryption, are at greatest risk.

The CSA recommends that organizations control the encryption process and keys, segregating duties and minimizing access given to users. Effective logging,
monitoring, and auditing administrator activities are also critical.

Threat No. 7: The APT parasite

The CSA aptly calls advanced persistent threats (APTs) “parasitical” forms of attack. APTs infiltrate systems to establish a foothold, then stealthily exfiltrate data and intellectual property over an extended period of time.

APTs typically move laterally through the network and blend in with normal traffic,
so they're difficult to detect. The major cloud providers apply advanced

techniques to prevent APTs from infiltrating their infrastructure, but customers need to be as diligent in detecting APT compromises in cloud accounts as they would in on-premises systems.

Common points of entry include spear phishing, direct attacks, USB drives preloaded with malware, and compromised third-party networks. In particular, the CSA recommends training users to recognize phishing techniques.

Threat No. 8: Permanent data loss

As the cloud has matured, reports of permanent data loss due to provider error have become extremely rare. But malicious hackers have been known to permanently delete cloud data to harm businesses, and cloud data centers are as vulnerable to natural disasters as any facility.Cloud providers recommend distributing data and applications across multiple zones for added protection. Adequate data backup measures are essential, as well as adhering to best practices in business continuity and disaster recovery. Daily data backup and off-site storage remain important with cloud environments.

The burden of preventing data loss is not all on the cloud service provider. If a customer encrypts data before uploading it to the cloud, then that customer must be careful to protect the encryption key. Once the key is lost, so is the data.

Threat No. 9: Inadequate diligence

Organizations that embrace the cloud without fully understanding the environment and its associated risks may encounter a “myriad of commercial, financial, technical, legal, and compliance risks,” the CSA warned. Due diligence applies whether the organization is trying to migrate to the cloud or merging (or working) with another company in the cloud. For example, organizations that fail to scrutinize a contract may not be aware of the provider’s liability in case of data loss or breach.

Threat No. 10: Cloud service abuses

Cloud services can be commandeered to support nefarious activities, such as using cloud computing resources to break an encryption key in order to launch an attack. Other examples including launching DDoS attacks, sending spam and phishing emails, and hosting malicious content.

Providers need to recognize types of abuse -- such as scrutinizing traffic to recognize DDoS attacks -- and offer tools for customers to monitor the health of their cloud environments. Customers should make sure providers offer a mechanism for reporting abuse. Although customers may not be direct prey for malicious actions, cloud service abuse can still result in service availability issues and data loss.

Explain in detail Cloud Infrastructure Mechanisms.

Answe: CloudInfrastructure Mechanisms

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

The following cloud infrastructure mechanisms are described :Logical Network Perimeter
Virtual Server
Cloud Storage Device
Cloud Usage Monitor
Resource Replication
Read-Made Environment

Logical Network Perimeter

An isolation of network environment establishing a virtual network boundary.
Purposes?
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, and
control the bandwidth that is available to isolated IT resources.
Typically established via network devices that supply and control the connectivity of a data center (commonly deployed as virtualized IT environment), which includes
Virtual Firewall – actively filter incoming and outgoing traffic.
Virtual Network – isolates the network environment within the data center.

Virtual Servers

A form of virtualization software that emulates a physical server.
Used by a cloud provider for resources sharing.
Virtual server = virtual machine

Cloud Storage Devices Mechanism

Storage devices designed specifically for cloud-based environment.
Instances of these storage could be virtualized.
Able to provide fix-increment capacity allocation in support of pay-per-use mechanism.

Cloud Storage Levels

Files – Collections of data are grouped into files that are located in folders.
Blocks – The lowest level of storage and the closest to the hardware, a block is the smallest unit of data that is still individually accessible.
Datasets – Sets of data are organized into a table-based, delimited, or record format.
Objects – Data and its associated metadata are organized as Web-based resources.

Cloud Usage Monitor Mechanism

A lightweight and autonomous software program responsible for collecting and processing IT resource usage data.
Metrics – amount of data, number of transactions, usage time, etc.
Three common agent-based implementation formats:
Monitoring agent
Resource agent
Polling agent

Monitoring Agent

A service agent existing along communication paths, monitoring and analyzing data flows.
Measure network traffic and message metrics.

Resource Agent

Even-driven agent monitoring resource usage based on pre-defined, observable at the resource software level such as initiating, suspending, resuming and vertical scaling.

Polling Agent

A processing module that collects cloud service usage data by polling IT resources.

Commonly used to periodically monitor IT resource status, such as uptime and downtime.

Resource Replication

The creation of multiple instances of the same IT resource.

Replication is typically performed when an IT resource’s availability and performance need to be enhanced.

Ready-Made Environment

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.

Typically equipped with Software Development Kit (SDK)