Cloud Computing

Sessional Assignment

Name: Nouman Zafar **ID #6824**

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

Answer:

SOA (service oriented Architecture :

A service-oriented architecture (SOA) is an architectural pattern in computer software design in which application components provide services to other components via a communications protocol, typically over a network. The principles of service-orientation are independent of any product, vendor or technology.

SOA is based on some key principles which are mentioned below

1. **Standardized Service Contract** - Services adhere to a service description. A service must have some sort of description which describes what the service is about. This makes it easier for client applications to understand what the service does.
3. **Loose Coupling** – Less dependency on each other. This is one of the main characteristics of web services which just states that there should be as less dependency as possible between the web services and the client invoking the web service.
4. **Service Abstraction** - Services hide the logic they encapsulate from the outside world. The service should not expose how it executes its functionality; it should just tell the client application on what it does and not on how it does it.
4. **Service Reusability** - Logic is divided into services with the intent of maximizing reuse. In any development company re-usability is a big topic because obviously one wouldn't want to spend time and effort building the same code again and again across multiple applications which require them.
5. **Service Autonomy** - Services should have control over the logic they encapsulate. The service knows everything on what functionality it offers and hence should also have complete control over the code it contains.
6. **Service Statelessness** - Ideally, services should be stateless. This means that services should not withhold information from one state to the other. This would need to be done from either the client application.
7. **Service Discoverability** - Services can be discovered (usually in a service registry). We have already seen this in the concept of the UDDI, which performs a registry which can hold information about the web service.

8. **Service Composability** - Services break big problems into little problems. One should never embed all functionality of an application into one single service but instead, break the service down into modules each with separate business functionality.

9. **Service Interoperability** - Services should use standards that allow diverse subscribers to use the service. In web services, standards as XML and communication over HTTP are used to ensure it conforms to this principle.

- Explain in detail prominent security threats to the cloud computing.

  Answer:
  Security threats in cloud computing:

  1) Consumers Have Reduced Visibility and Control. When transitioning assets/operations to the cloud, organizations lose some visibility and control over those assets/operations. When using external cloud services, the responsibility for some of the policies and infrastructure moves to the CSP.

  2) **On-Demand Self Service Simplifies Unauthorized Use**. CSPs make it very easy to provision new services. The on-demand self-service provisioning features of the cloud enable an organization's personnel to provision additional services from the agency's CSP without IT consent. The practice of using software in an organization that is not supported by the organization's IT department is commonly referred to as shadow IT.

  3) **Internet-Accessible Management APIs can be Compromised**. CSPs expose a set of application programming interfaces (APIs) that customers use to manage and interact with cloud services (also known as the management plane). Organizations use these APIs to provision, manage, orchestrate, and monitor their assets and users. These APIs can contain the same software vulnerabilities as an API for an operating system, library, etc. Unlike management APIs for on-premises computing, CSP APIs are accessible via the Internet exposing them more broadly to potential exploitation.

  4) **Separation Among Multiple Tenants Fails**. Exploitation of system and software vulnerabilities within a CSP's infrastructure, platforms, or applications that support multi-tenancy can lead to a failure to maintain separation among tenants.

  5) **Data Deletion is Incomplete.** Threats associated with data deletion exist because the consumer has reduced visibility into where their data is physically stored in the cloud and a reduced ability to verify the secure deletion of their data.

  6) **Vendor Lock-In Complicates Moving to Other CSPs**. Vendor lock-in becomes an issue when an organization considers moving its assets/operations from one CSP to another. The organization discovers the cost/effort/schedule time necessary for the move is much higher than initially considered due to factors such as non-standard data formats, non-standard APIs, and reliance on one CSP's proprietary tools and unique APIs.

  7) **Credentials are Stolen**. If the attacker can have access to the CSP's services to provision additional resources (if credentials allowed access to provisioning), as well as target the organization's assets.

  8) **Insiders Abuse Authorized Access**. Insiders, such as staff and administrators for both organizations and CSPs, who abuse their authorized access to the organization's or CSP's networks, systems, and data are uniquely positioned to cause damage or infiltrate information.

- Explain in detail Cloud Infrastructure Mechanisms.

  Answer:
  Technology mechanisms foundational to cloud platforms are covered,

  1) Logical Network Perimeter
     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.
  2) Virtual Server
     The virtual server represents the mode fundamental building block of cloud environment. The instantiation of virtual servers from image files is a resource allocation process that can be completed rapidly and on-demand.
  3) Cloud Storage Device
     The cloud storage device mechanism represents storage devices that are designed specifically for cloud-based provisioning.
  4) Cloud Usage Monitor
     The cloud usage monitor mechanism is a lightweight and autonomous software program responsible for collecting and processing IT resource usage.
  5) Resource Replication
     Replication is usually performed when resource's availability and performance need to be enhanced.
  6) Ready-Made Environment
     The ready-made environment mechanism is a defining component of the PaaS cloud delivery model that represents a platform comprised of a set of already installed IT resources, ready to be used and customized by a cloud consumer.