**Cloud Computing**

**Sessional Assignment**

**ID: 12943**

**Name: M Arsalan Khan**

**BSSE 8th Semester**

**Section: B**

* Explain in detail Service Oriented Architecture (SOA) in cloud computing.
* Ans: 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 is also intended to be independent of vendors, products and technologies.
* Service-Oriented Architecture (SOA) is an architectural approach in which applications make use of services available in the network. In this architecture, services are provided to form applications, through a communication call over the internet.
* Characteristics of Service Oriented Architecture Services. Reusable: depending on their granularity, services can be used by multiple processes and other coarse-grained services. Autonomous units of business functionality, each service provides a business function that is independent of other services.
* When it comes to implementing service-oriented architecture (SOA), there is a wide range of technologies that can be used, depending on what your end goal is and what you’re trying to accomplish.
* Typically, Service-Oriented Architecture is implemented with web services, which makes the “functional building blocks accessible over standard internet protocols.”
* An example of a web service standard is [SOAP](https://en.wikipedia.org/wiki/SOAP), which stands for Simple Object Access Protocol. In a nutshell, SOAP “is a messaging protocol specification for exchanging structured information in the implementation of web services in computer networks. Although SOAP wasn’t well-received at first, since 2003 it has gained more popularity and is becoming more widely used and accepted. Other options for implementing Service-Oriented Architecture include Jini, COBRA, or REST.

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

### Ans: 1. Distributed-Denial-of-Service Attacks

When cloud computing first became popular, Distributed Denial-of-Service (DDoS) attacks against cloud platforms were largely unthinkable; the sheer amount of resources cloud computing services had made DDoS attacks extremely difficult to initiate. But with as many Internet of Things devices, smartphones, and other computing systems as there are available now, DDoS attacks have greatly increased in viability. If enough traffic is initiated to a cloud computing system, it can either go down entirely or experience difficulties.

2. Shared Cloud Computing Services

Not all cloud hosting solutions and cloud computing services are made equal. Many cloud solutions do not provide the necessary security *between clients*, leading to shared resources, applications, and systems. In this situation, threats can originate from *other clients* with the cloud computing service, and threats targeting one client could also have an impact on other clients.

3. Employee Negligence

Employee negligence and employee mistakes remain one of the biggest security issues for *all* systems, but the threat is particularly dangerous with cloud solutions. Modern employees may log into cloud solutions from their mobile phones, home tablets, and home desktop PCs, potentially leaving the system vulnerable to many outside threats.

4. Data Loss and Inadequate Data Backups

Inadequate data backups and improper data syncing is what has made many businesses vulnerable to [*ransomware*](https://www.cwps.com/blog/the-ransomware-trend-are-you-vulnerable), a specific type of cloud security threat. Ransomware "locks" away a company's data in encrypted files, only allowing them to access the data once a ransom has been paid. With appropriate data backup solutions, companies need no longer fall prey to these threats.

5. Phishing and Social Engineering Attacks

Due to the openness of a cloud computing system, phishing and social engineering attacks have become particularly common. Once login information or other confidential information is acquired, a malicious user can potentially break into a system with ease -- as the system itself is available from anywhere. Employees must be knowledgeable about phishing and social engineering enough to avoid these types of attacks.

6. System Vulnerabilities

Cloud computing systems can still contain system vulnerabilities, especially in networks that have complex infrastructures and multiple third-party platforms. Once a vulnerability becomes known with a popular third-party system, this vulnerability can be easily used against organizations. Proper patching and upgrade protocols -- in addition to network monitoring solutions -- are critical for fighting this threat.

Cloud computing security issues are not insurmountable; in fact, many of the risks above can be protected against through the use of a dedicated data protection service. [Cloud data protection solutions](https://www.cwps.com/cloud-data-protection) will both protect data from loss and against cyber security threats, allowing businesses to leverage the power of the cloud without the associated risk.

* Explain in detail Cloud Infrastructure Mechanisms.
* Ans: