Cloud Computing

Sessional Assignment

Name: Wisal Zafar

Id: 13156

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

Answer:
SOA is construct o computer engineering approaches which offer an architectural development towards enterprise system.
Service-Oriented Architecture:
It is a style of software design where services are presuming to the other components by application components, through a communication protocol over a network.It's important to note that SOA can work with or without cloud computing,more line of work are moving files to the cloud cloud so it makes sense to use cloud computing and SOA together.
There are some core values which are as follow:
1. Flexibility
2. Business value
3. Strategic goals
4. Intrinsic inter-operability
5. Evolutionary refinement
As we have talked about what SOA is and how it can be used to promote your business, which can be used for the advancement of business.

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

Answer:

1. Permanent Data Loss: as the clouds have get matured the reports of permanent loss of data provider error has become very rare but the malicious hackers has known to permanent delete the the cloud data to harm business,cloud data centers are as vulnerable to natural disaster as any facility.the burden of preventing the loss of data is not only on the cloud service provider if the customer encrypts the data before uploading it then that customer must protect the encryption key if the key is lost so is the data.
2. Dos Attacks: Dos attacks have been for years and they have gain dpominence again due to the cloud computing they often affect the availability. Systems may get slower or simply time out.Experiencing the Dos (Denial of service) attack is just like being caught in rush hour traffic gridlock; and the reports says that there is only way to get your

destination is just you have to wait for it.It consumes a large amount of processing power bill that customer may ultimately have to pay.

3. Share technology Shared danger: Indebtedness in shared technology pose a significant threat to loud computing.The providers share infrastructure platforms and applications and if a vulnerability arise in any of this layer it affects all the layers.a single vulnerabilities or misconfiguration can lead to a compromise across the entire provider's cloud.
4. The APT parasite: The CSA advanced persistent threats(APTs) parasitical forms of attack APTs infiltrate the systems to Establish a foothold then stealthily exfiltarte the data and intellectual property over an extended to period of tme.It typically move latterly through the network and blendd in with normal traffic so they are

difficult to detect.The major providers apply the advance technique to prevent APTs.
5. Malicious Attacks & Abuse: Hackers or even authorized users may potentially attack and abuse cloud storage for illegal activities. This can include the storing and spread of copyrighted materials, pirated software, malware or viruses.This can occur when individuals directly attack the service or take over the cloud service's resources. Cloud resources can also be attacked directly through attacks such as malware injection which have become a major threat in recent years.
6. Insider Threat: While attacks and misuse of data by the employees may seem low-risk, the threat is very real. It can lead to the misuse of important data such as customer or money information. For organizations who handle sensitive information such as finance or the health care industry this can be a major concern.
7. Unauthorized Access: Assigning the incorrect access levels or mistreat to remove user access for ex-employees can also lead to users having access to information. Apart from users with malicious intent, the threat of accidental deletion or release of data also exists if they are not adequately trained in the use of the software.
8. Regulatory Compliance: Regulations may state how data is processed and for how long it must be retained. The cloud service must also be capable of providing you with all the necessary data, such as audit trails and logs, in the event of an audit or investigation. Storing data on a cloud service may mean your organization must comply with other regulations as your data may be physically stored in another country or even several different ones.

- ## Explain in detail Cloud Infrastructure Mechanisms.

Answer:

Cloud infrastructure mechanisms are foundation 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 in this chapter:
• Logical Network Perimeter: It is defined as the isolation of network environment from the rest of communication networks the LNP establishes a virtual network boundary that encompasses and isolates the group of related cloud based IT resources.They are typically established via network devices that supply and control the connectivity of a data centre.
• Virtual Server: It is a form of virtualization software that emulates a physical server.They are used by the cloud providers to the same physical server with the multiple cloud customers by providing it with the individual virtual server instanesIt represents the most foundation building block of cloud Environment.each virtual server can host numerous IT resources.
• Cloud Storage Device: The cloud storage mechanism represents the storage devices that are designed specially for cloud based provisioning. These devices can be virtualized similar to how physically servers can spawn virtual server images. A primary concern related to cloud storage is the security integrity and confidentiality of the data.
• Resource Replication:It is defined as the creation of multiple instances of the same IT resources its replication is typically performed when an IT resources availability and performance need to be enhanced.
• Ready-Made Environment: IT is a defining component of the Paas cloud delivery model that shows the pre defined cloud based platform compromise of a set of already installed IT resources ready to be used and customize by a cloud consumer.