CLOUDNET ASSIGNMENT DAY-5

Name: - Tounov Datta

Registered Email ID: - td8013@srmist.edu.in

Email ID (in gcr): - tounov.datta@gmail.com

THEORY

a) What is the usage of utility computing?

Ans) Utility computing is a model in which computing resources are provided to the customer based on specific demand. The service provider charges exactly for the services provided, instead of a flat rate.

The foundational concept is that users or businesses pay the providers of utility computing for the amenities used – such as computing capabilities, storage space and applications services. The customer is thus, absolved from the responsibility of maintenance and management of the hardware. Consequently, the financial layout is minimal for the organization.

Utility computing helps eliminate data redundancy, as huge volumes of data are distributed across multiple servers or backend systems. The client however, can access the data anytime and from anywhere.

Utility computing plays a significant role in business models and gives a unique service provider to the customer IT services according to pay per use methods. The few IT services are provided to customer storage, software applications, and computing power. So for any questions and advice required for deployment in the business model, the service providers provide the unit divisions to the company. As the term “Utility” refers to

basic amenities like electricity, water, gas, the basic software requirements for a business model are provided by utility computing. The working, components, properties, and use cases are explained in this article.

b) Explain security management regarding cloud computing?

Ans) Security management in the cloud is a set of strategies designed to allow a business to use cloud applications and networks to their greatest potential while limiting potential threats and vulnerabilities. This is often done with several independent tactics:

- **Identifying and assessing cloud services.** First, you need to spend time identifying which cloud products and services are being used in your organization, and which ones might be considered in the future. Then, you'll need to assess and audit those items, analyzing their security and potential vulnerabilities.
- **Auditing and adjusting native security settings.** Within each application, you'll have full control of your own privacy and security settings. It's on your cloud security team to understand which settings are available, and take full advantage of them to grant your organization the highest possible level of security.
- **Encrypting data.** In many cases, you'll need to take extra efforts to prevent data loss and preserve data integrity by encrypting your data and securing your

connections. It’s your responsibility to allow legitimate network traffic and block suspicious traffic.

- **Managing devices.** Cloud applications allow you to reduce the amount of physical infrastructure you maintain, but you and your employees will still be accessing data and services with specific devices. You’ll need some way to manage and monitor those devices to ensure only authorized devices can access your data.
- **Managing users.** Similarly, you’ll need to consider user-level controls. Establish varying levels of user permissions, to restrict access to your most valuable or sensitive information, and change user permissions as necessary to allow secure access.
- **Reporting.** It’s also important to monitor cloud activity from a high level, and report on that activity so you can better understand your risks and ongoing operations.

c) How would you secure your data for transport in the cloud?

Ans) When transporting data in a cloud computing environment, keep two things in mind: Make sure that no one can intercept your data as it moves from point A to point B in the cloud, and make sure that no data leaks (malicious or otherwise) from any storage in the cloud.

In the cloud, the journey from point A to point B might be within a cloud environment, over the public Internet between an enterprise and a cloud provider, or between clouds.

The security process may include segregating your data from other companies' data and then encrypting it by using an approved method. In addition, you may want to ensure the security of older data that remains with a cloud vendor after you no longer need it.

A *virtual private network (VPN)* is one way to manage the security of data during its transport in a cloud environment. A VPN essentially makes the public network your own private network instead of using dedicated connectivity. A well-designed VPN needs to incorporate two things:

- A *firewall* to act as a barrier to between the public Internet and any private network (like at your enterprise).
- *Encryption* to protect your sensitive data from hackers; only the computer that you send it to should have the key to decode the data.

d) What do you mean by CaaS?

Ans) Containers as a service (CaaS) is a cloud service model that allows users to upload, organize, start, stop, scale and otherwise manage containers, applications and clusters. It enables these processes by using either a container-based virtualization, an application programming interface (API) or a web portal interface. CaaS helps users construct security-rich, scalable containerized applications through on-premises data centers or the cloud. Containers and clusters are used as a

service with this model and are deployed in the cloud or in onsite data centers.

e) How can a user gain from Utility computing?

Ans) Utility computing allows the user to pay only for what they are using. It is a plug-in managed by an organization which decides what type of services has to be deployed from the cloud.

Most organizations prefer hybrid strategy.