Name: TANISHQ

ASSIGNMENT DAY 5 (CLOUDNET WORKSHOP)

THEORY

a) What is the usage of utility computing?

Ans: Utility computing is a plug-in managed by an organization which decides what type of services has to be deployed from the cloud. It facilitates users to pay only for what they use.

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, analysing 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: Five data privacy protection tips to help you tackle the issue of cloud privacy:

1. Avoid storing sensitive information in the cloud.

Many recommendations across the 'Net sound like this: "Don't keep your information on the cloud." Fair enough, but it's the same as if you asked, "How not to get my house burned down?" and the answer would be, "Do not have a house." The logic is solid, but a better way to translate such advice is, "avoid storing sensitive information on the cloud." So if you have a choice you should opt for keeping your crucial information away from virtual world or use appropriate solutions.

2. Read the user agreement to find out how your cloud service storage works.

If you are not sure what cloud storage to choose or if you have any questions as for how that or another cloud service works you can read the user agreement of the service you are planning to sign up for. There is no doubt it's hard and boring but you really need to face those text volumes. The document which traditionally suffers from insufficient attention may contain essential information you are looking for.

3. Be serious about passwords.

You must have heard this warning a hundred times already, but yet most people do not follow it. Did you know that 90 percent of all passwords can be cracked within seconds? Indeed, a great part of all the sad stories about someone's account getting broken is caused by an easy-to-create-and-remember password. Moreover, doubling your email password for other services you use (your Facebook account, your cloud storage account) is a real trap as all your login information and forgotten passwords always arrive to your email.

4. Encrypt.

Encryption is, so far, the best way you can protect your data. Generally encryption works as follows: You have a file you want to move to a cloud, you use certain software with which you create a password for that file, you move that password-protected file to the cloud and no one is ever able to see the content of the file not knowing the password.

5. Use an encrypted cloud service.

There are some cloud services that provide local encryption and decryption of your files in addition to storage and backup. It means that the service takes care of both encrypting your files on your own computer and storing them safely on the cloud. Therefore, there is a bigger chance that this time no one -- including service providers or server administrators -- will have access to your files (the so called "zero-knowledge" privacy). Among such services are Spideroak and Wuala.

d) What do you mean by CaaS?

Ans: Containers as a service (CaaS) is a cloud service that allows software developers and IT departments to upload, organize, run, scale, manage and stop containers by using container-based virtualization. A CaaS provider will commonly provide a framework which allows users to make use of the service. Within the spectrum of cloud computing services, CaaS falls somewhere between Infrastructure as a Service (IaaS) and Platform as a Service (PaaS). However, CaaS is most commonly positioned as a subset of IaaS. The basic resource for CaaS is a container, rather than a virtual machine (VM) or a bare metal hardware host system, which are traditionally used to support IaaS environments.

e) How can a user gain from Utility computing?

Ans: Utility computing allow the user to pay per use means whatever they are using only for that they have to pay. It is a plug in that needs to be managed by the organizations on deciding what type of services has to be deployed from the cloud. Utility computing allows the user to think and implement the services according to them. Most organizations go for hybrid strategy that combines internal delivered services that are hosted or outsourced services.