Assignment 1

Cloud Computing

Submitted to

Ma,am Sana Jehan

Submitted by :

Muhammad islam

ID : 6844

BS (Software Engineering)

1. Cloud management Issues :

Managing a cloud is not an easy task. It consist a lot of technical challenges.

A lot of dramatic predictions are famous about the impact of cloud computing. People think that traditional IT department will be outdated and research supports the conclusions that cloud impacts are likely to be more gradual and less linear. Cloud services can easily change and update by the business users. It does not involve any direct involvement of IT department. It is a service provider's responsibility to manage the information and spread it across the organisation. So it is difficult to manage all the complex functionality of cloud computing

2. Security Issues :

Security is the greatest challenge or issue of cloud computing according to International Data Corporation.
When we save our data or run our software into others hard disk using others CPU appears loss, phishing, botnet etc. Some security concerns are given below:

- **Security concern 1;** Control on physical security is lost in cloud computing because resources are shared with other companies and no one knows where the resources are run.
- **Security Concern 2;** Laws are violated by the company which increase the risk of data seizure by the foreign government.
- **Security Concern 3;** There is storage incompatibility between different cloud services vendors when the user wants to shift from one cloud to

another type of cloud (Google cloud is incompatible with Microsoft cloud).

- **Security concern 4;** There is no common standard to ensure the data integrity till now.

3. Vendor lock-In:

Because cloud computing is still relatively new, standards are still being developed, Many cloud platforms and services are proprietary, meaning that they are built on the specific standards, tools and protocols developed by a particular vendor for its particular cloud offering. This can make migrating off a proprietary cloud platform prohibitively complicated and expensive.

Three types of vendor lock-in can occur with cloud computing:

- **Platform lock-in:** cloud services tend to be built on one of several possible virtualization platforms, for example VMware or Xen. Migrating from a cloud provider using one platform to a cloud provider using a different platform could be very complicated.
- **Data lock-in:** since the cloud is still new, standards of ownership, i.e. who actually owns the data once it lives on a cloud platform, are not yet developed, which could make it complicated if cloud computing users ever decide to move data off of a cloud vendor's platform.
- **Tools lock-in:** if tools built to manage a cloud environment are not compatible with different kinds of both virtual and physical infrastructure, those tools will only be able to manage data or apps that live in the vendor's particular cloud environment.

4. Software bug:

A software bug is a problem causing a program to crash or produce invalid output. The problem is caused by insufficient or erroneous logic. A bug can be an error, mistake, defect or fault, which may cause failure or deviation from expected results.

Most bugs are due to human errors in source code or its design. A program is said to be buggy when it contains a large number of bugs, which affect program functionality and cause incorrect results.

Some bugs might not have serious effects on the functionality of the program and may remain undetected for a long time. A program might crash when serious bugs are left unidentified. Another category of bugs called security bugs may allow a malicious user bypass access controls and obtain unauthorized privileges.

5. Abuse :

While providing cloud services, it should be ascertained that the client is not purchasing the services of cloud computing for nefarious purpose. In 2009, a banking Trojan illegally used the popular Amazon service as a command and control channel that issued software updates and malicious instruction to PCs that were infected by the malware.