**CS435: Cloud Computing**

**Assignment No. 02**

**Spring 2022**

**Question No. 1:**

Collaboration is a process in which two or more people, entities, and organizations work together to complete a task. There are many traditional collaborations shifted to the internet to make things convenient for users. You are required to write down the name of cloud collaborations corresponding to the following examples

|  |  |
| --- | --- |
| **Example** | **Cloud collaborations** |
| Voice over Internet Protocol (VoIP) Tools | Communication collaboration |
| Web-based free access to a word processor, spreadsheet and presentation programs to create, Google Docs share, edit, print and download the documents stored on Cloud. | Coordination collaboration |
| Virtual Face-to-face meetings. | Cooperation collaboration |
| Users can compose, send, receive and read the emails by using the web browser. | Communication collaboration |
| Free cloud storage for video contents worldwide. | YouTube collaboration |

**Question No. 2:**

Assume you work for a private company and are required to travel out of the city for a few days due to the company's operations. Due to some technical issues, your internet is not working, and you have to send an urgent mail to admin department. You went to the internet cafe to send the email. The web-browser in your PC was already opened, but you used it for sending the email and left.

**You are required to answer the following in the context of the above scenario:**

**What type of risks and issues you can face? Give at least one valid reason.**

1. The main issue is Security Risk because the internet use public network which is not secure as compared to private network.
2. If we use the browser which is already open and someone already use it and we leave after using and don’t delete the sent mail then our mail is being seen by someone else and they leak our important information.

**Write down three solutions recommended by NIST for SaaS users.**

1. Consumer ensures that device should be protected to control the attacks.
2. Use strong encryption algorithm for each web session as well as for data.
3. The consumer should ensure that data is completely deleted after use the browser.