1. Assume a file system with 3 users: Alice, Bob, and Charlie. There are four files: file1, file2, file3, and file4, with the following access rights:

Alice can access file1 (read, write), file2 (read), file3(read, write), and file4 (write)

Bob can access file1 (read), file2 (read, write), and file3 (write)

Charlie can access file3 (write) and file4(read, write).

(a) Write the **access control matrix** for the system given the above subjects and objects and access rights. (Must use a table) (**22.5 points**)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| SUBJECT | FILE 1 | FILE 2 | FILE 3 | FILE 4 |
| ALICE | read, write | read | read, write | write |
| BOB | read | read, write | write | none |
| CHARLIE | none | none | write | read, write |

(b) Write the **access control lists**for the files given the above subjects and objects and access rights. You must use the following format:

x: a (write), b (read, write), if for file x, a has write permissions, and b has both read and write permissions. (**22.5 points**)

FILE 1: ALICE (read, write), BOB (read)

FILE 2: ALICE (read), BOB (read, write)

FILE 3: ALICE (read, write), BOB (write), CHARLIE (write),

FILE 4: ALICE (write), CHARLIE (read, write)

2. In Module 8, we discussed cloud security. Examine the following scenarios and discuss/explain whether there are any security issues for using a cloud for that scenario. (2.5x2=5 points)

**a. NASA's space telescope data.**

A main instrument for studying our solar system is the telescope. This is the result of years of scientific investigation and has allowed scientists to understand the creation of the universe, which was previously unknown. This shows that the data is sensitive and that storing it in the cloud can cause many kinds of security issues.

Safety Concerns:

When NASA uploads data to the cloud, several kinds of problems could occur. The first issue to address will be co-tenancy. NASA is unsure about the reliability of the equipment operating next to them. Also, cloud service providers have trust among them. NASA will check the accuracy of the data continuously and effectively by transferring the data to the cloud. For example, the cloud provider can keep the hash and delete the data if NASA continues to verify the data hash.

The cloud provider owns the services, and competitors can access sensitive information. Next, there will be concerns about the high availability. The cloud providers handle the majority of security; in the event of an attack or service problems, NASA's data will be unavailable, and a new approach will need to be developed.

**b. A hospital with sensitive medical records**

Every patient needs to be examined by the hospital. For the hospital, knowing that each patient's data is secure and undamaged will be difficult. It will be difficult for the hospital to find the patient's back record and treat her if the cloud provider was fake and they made some changes in the data.

An attacker could interrupt the service if the cloud has been hacked, which would prevent the hospital from accessing its data when it's needed.

Moreover, the attacker may be a co-tenant. The person living next to you might represent a significant risk to your security.

The data may leak if the cloud provider is compromised or malicious in and of itself. Data that contains private information about patients that they don't want made public can be published. The patient's address, phone number, and date of birth are among the other details in the data that may be used for further spamming purposes.