SHOUZAB KHAN.

SKHAN6.

ASSIGNMENT 3.

1. Spock wants to store his files remotely on Kirk's server. Spock is concerned about the integrity of his files. He is considering several solutions. Please discuss the pros and cons of each of the solutions listed below. (4x2.5=10)

a. Spock keeps a copy of his files locally. He periodically downloads his files from Kirk's server and compares them with the local copies of the files.

**ANSWER:**

**PROS:**

1. In this scenario where Spock keeps the copy of files locally, he has pros in that he can check the integrity of the files very easily if the Kirk cloud provider has tampered with the data or not.
2. If the Kirk server gets compromised and all the data gets breached, Spock will have files on his local machine.

**CONS:**

1. These scenarios can just be used for the small size of files.
2. Managing the files locally can consume a lot of space in your local machine, which cannot be cost-efficient. Also, it will take a lot of bandwidth and time.
3. Spocks also make mistakes while comparing the files and blames the Kirks server after that for not keeping the integrity of the file, but that can be a human fault.

b. Spock keeps a hash of his files locally but deletes the files from local storage after uploading to Kirk's server. He periodically downloads the files from Kirk's servers and, hashes them and compares the hashes with his local hashes.

**ANSWER:**

**PROS:**

1. Keeping the hash and deleting the files locally can give much free space, which can be used for other purposes.
2. The cloud provider like Kirk cannot cheat while giving the hashes.

**CONS:**

1. If the hashes that were kept locally got compromised or lost, Spock won’t be able to verify the integrity of the files because he has deleted the files locally.
2. This scenario is computationally extensive because we have to look for the hash, download the hash, and then verify its integrity.

c. Spock keeps a hash of his files locally but deletes the files from local storage after uploading to Kirk's server. He periodically asks Kirk for a hash of the files and compares the hashes with his local hashes.

**ANSWER:**

**PROS:**

1. It will be easier for spocks to directly ask for the hashes of the files from kirks and check the integrity of files.
2. It will be most time-efficient to have the hash directly from Kirks.
3. It will also be more cost-efficient for spocks, and they won’t spend their resources on downloading the file for getting hash.

**CONS:**

1. Spock won’t have access to the files if he checks the integrity of the files.
2. Kirks’s server can also send the compromised hash to the Spock, which can alter the integrity result of the files.
3. The kirks can also cheat, and we also don’t know if the cloud has the files or not.

d. Spock keeps a hash of individual file blocks locally but deletes the files from local storage after uploading to Kirk's server. For each file, Spock randomly chooses a set of blocks and asks Kirk to send the hash of those file blocks. Spock then compares them with his local hashes.

**ANSWER:**

**PROS:**

1. It can be very easy to identify which block of the file integrity is compromised specifically.
2. Spocks won’t need to download the whole file; he can download and ask for a specific block of the file, which can also save a lot of memory.
3. It is also faster than other ways.

**CONS:**

1. Verifying each specific hash of the blocks can be very complex and may require a lot of techniques and automation.
2. The provider can cheat in this. As he knows the pattern of the client, he asks for the block's hash so he can just keep that specific hash and delete the remaining data.

2. Riker calls Data over the phone and asks him to calculate the fifth root of 100 large integers. After a few seconds, Data tells him the results. Riker is suspicious, and he wants to verify Data's results.

Name four methods for doing this and explain how each of them would work and the pros and cons of them. (4x2.5=10)

ANSWER:

1. **Re Computation:**

The re-computation is when Riker does all his computation by himself again.

**PROS:**

The result of Riker for re-computation will be 100% correct if there are any mistakes that will be noticed.

**CONS:**

Riker will have to re-compute all the calculations again from the start, which will take a long time and resources on both sides, which is not good for outsourcing computation.

1. **Sampling:**

The input values that lead to what we already know are fed into the sampling process. In order to find the answer, Riker can provide the value before sending the actual calculation.

**PROS:**

This method is effective. Once we get the test results, we can depend on the computation of the Data to give him the actual data.

**CONS:**

Before computing the actual values, the attacker may be able to find the test values. The attacker can seem to be real at first but then change their actual values.

1. **Replication:**

The same task is replicated over numerous nodes to make the replication function. The majority vote of the nodes is then used to verify the correctness.

**PROS:**

This computation can be faster because these tasks run in parallel.

**CONS:**

All the tasks of the same computations have to run multiple copies, so for that reason, the cost of this solution will be high. But still, we have to trust the majority result if the attacker compromises all of our testing servers.

1. **Auditing:**

Ask every node to note what process it did for the results during the computations.

**PROS:**

Nodes won't be able to change what they did. The signing process provides non-repudiation.

Also, this will help with forensics investigation. If something goes wrong, we may look back and see where a wrong computation happened.

**CONS:**

This solution is expensive.

Cryptography is the reason for being expensive because it takes all the resources and reduces performance.