CMPE – 272 – Aprill 11th Lab

Team Members:

1. Shreekar Kolanu : 017406493
2. Satwik Upadhyayula : 017423796
3. Vineet Samudrala : 017426253
4. Bala Supriya Vanaparthi : 017464135

When a sender needs to send a 4GB file to a receiver securely over a public network using TCP/IP, there are two common ways to achieve the security goals of Confidentiality, Integrity, Authentication, and Authorization (CIAA):

1. **Secure File Transfer Protocol (SFTP):**
   - **Confidentiality**: SFTP encrypts the data in transit, ensuring that the file content cannot be read by unauthorized parties while it's being transferred.
   - **Integrity**: SFTP uses secure hashing to ensure that the file has not been altered during the transfer.
   - **Authentication**: Both the sender and receiver must authenticate themselves using credentials (such as username and password or public/private key pairs) before the transfer can begin.
   - **Authorization**: Once authenticated, users are granted access based on their permissions, controlling who can access and manipulate the file.
2. **Virtual Private Network (VPN) with File Transfer Protocol (FTP) or other secure transfer methods:**
   - **Confidentiality**: By setting up a VPN, all traffic between the sender and receiver is encrypted, protecting the data in transit.
   - **Integrity**: The encrypted connection ensures that data cannot be modified undetected, providing a level of integrity assurance.
   - **Authentication**: Users authenticate themselves using VPN credentials to establish a secure connection.
   - **Authorization**: Once the VPN connection is established, the sender can use FTP or another secure transfer protocol to transfer the file, ensuring proper access control.

In both cases, ensuring proper configurations and keeping software up to date is crucial to maintain a secure environment.