File permission in Linux is essential to securing files and directories on the system. Linux provides a powerful permission system that allows administrators to control who can access files and directories and what actions they can perform on them. In this essay, we will explore the basics of file permissions in Linux, how they work, and how to use them to secure files and directories. File permissions in Linux are based on a three-part system: user ownership, group ownership, and permissions. When a file or directory is created, it is assigned a unique owner, who has full control over the file or directory. The owner can also assign the file or directory to a group, allowing other group members to access the file or directory. The permissions on a file or directory are set using a three-digit code. The first digit represents the owner's permissions, the second digit represents the group's permissions, and the third digit represents the other users' permissions. Each digit comprises three numbers, representing the read, write, and execute permissions. The read permission allows a user to view the contents of a file but not modify it. The write permission allows a user to modify the contents of a file but not execute it. The execute permission allows a user to execute a file but not view its contents. To set permissions on a file or directory, users can use the chmod command. The chmod command allows users to change the permissions of a file or directory, add or remove permissions, and set permissions for the owner, group, or other users.