In Linux, file systems use a variety of advanced permissions and attributes that offer granular control over who can access, modify, or execute files.

Access Control Lists (ACLs):

- ACLs allow for more fine-grained control over file permissions than the standard owner/group/others model in Linux.
- With ACLs, you can specify permissions for multiple users and groups on individual files and directories.
- ACLs allow you to set specific permissions for individual users and groups on a file or directory.

Commands:

- getfacl -> to view the ACL of a file.
- setfacl -> to modify the ACL of a file.

Assign rwx permission to 'username' on 'filename'.

-> setfacl -m u:username:rwx filename

->setfacl -m u:username:permissions filename

->setfacl -m g:groupname:permissions filename

View ACL entries for a file.

-> getfacl filename

File Attributes:

- File attributes provide extra control over how files can be modified.
- File attributes in Linux are metadata that provide additional information about a file or directory beyond the basic permissions (read, write, execute).
- They help in managing and controlling file behavior and access
- They are managed using the chattr (change attributes) and lsattr (list attributes) commands.
- Common file attributes include:

    i: Immutable (prevents deletion, modification, or renaming).
    a: Append-only (can only be appended, not modified or deleted).
    d: Excluded from backups.

Make a file immutable
Set: chattr +i filename
Unset: chattr -i filename

View file attributes.
lsattr filename

Special Permissions (SUID, SGID, Sticky Bit):

These are special permission bits that enhance the behavior of executable files and directories

a) SUID (Set User ID):

- When the SUID bit is set on an executable file, it allows the file to be executed with the privileges of the file owner rather than the user executing the file.
- **Example**: The passwd command uses SUID to allow users to change their password (which requires root privileges) without having root access.

  Set SUID using:
  Enable SUID on a file.
  ->chmod u+s filename

SGID (Set Group ID):

- When applied to files, SGID ensures that the file is executed with the group privileges of the file owner.
- When applied to directories, SGID ensures that files created within the directory inherit the directory's group ownership, not the user's default group.
- Set SGID using:

  Enable SGID on a directory.
  chmod g+s directoryname

Sticky Bit:

- The sticky bit is used mainly for directories. When the sticky bit is set on a directory, only the file owner (or root) can delete or rename files within that directory.
- It is commonly used in shared directories like /tmp.
- Set the sticky bit using:

  chmod +t directoryname # Set the sticky bit on a directory.