Experiment – 1.5 : Enroll system users

Enrolling system users is a crucial task for a database administrator (DBA) when managing a database system. This process involves adding new users to the system, assigning them appropriate roles and privileges, and ensuring that they can access the system securely. Below is an experiment solution outlining the steps to enroll system users in a database:

Enrolling System Users

Objective: The objective of this experiment is to enroll system users into a database system. These users may include administrators, employees, customers, or any other relevant roles.

Experiment Steps:

1. Database Connection:

- Ensure that you are connected to the database system with administrative privileges (e.g., as a DBA or a user with appropriate administrative roles).

2. User Role and Privilege Planning:

- Determine the roles and privileges that each type of user will need within the database. Roles may include administrators, regular users, and others, each with their own set of permissions.

3. User Account Creation:

- Create user accounts in the database using SQL commands or a database management tool. For example, to create a new user named "john_doe," you can execute SQL like this:

```
CREATE USER john_doe IDENTIFIED BY password;
```

4. Role Assignment:

- Assign roles to the users to define their access privileges. For example, to grant the "employee" role to "john_doe," you can execute SQL like this:

```
GRANT employee TO john_doe;
```

5. Default Schema Assignment (Optional):

- If required, specify the default schema for each user. This determines the namespace in which objects are created when the user issues CREATE statements. For example:

```
ALTER USER john_doe DEFAULT TABLESPACE users;
```

6. Password Management:

- Enforce strong password policies and require users to change their passwords periodically. For example:

```
ALTER USER john_doe PASSWORD EXPIRE;
```

7. User Authentication:

- Ensure that the authentication method for each user is secure. You may use password-based authentication, multi-factor authentication (MFA), or other secure methods.

8. Data Access:

- Grant specific object-level privileges to users to control their access to database tables, views, and procedures. For example:

```
GRANT SELECT, INSERT, UPDATE, DELETE ON employees TO john_doe;
```