Assumptions:
The database system supports role-based access control (RBAC).
The teams have separate database user accounts with the corresponding roles assigned.
The database schema is designed according to the provided SQL schema in Section2.
This access control strategy ensures that each team can perform their specific tasks, while preventing unauthorized access or modifications to the data. It follows the principle of least privilege, granting only the minimum required permissions to each team. Additionally, it enforces data security and integrity.
-- Scalability: As company expands and more teams are formed, more roles can be created in the database
-- Create roles for each team
CREATE ROLE logistics;
CREATE ROLE analytics;
CREATE ROLE sales;
-- Grant privileges to Logistics
GRANT SELECT ON tbl_Transactions TO logistics;
GRANT UPDATE ON tbl_Transactions TO logistics;
-- Grant privileges to Analytics
GRANT SELECT ON tbl_Transactions TO analytics;
GRANT SELECT ON tbl_Members TO analytics;
GRANT SELECT ON tbl_Items TO analytics;
-- Grant privileges to Sales
GRANT INSERT, DELETE ON tbl_Items TO sales;
-- Assign users to roles
ALTER USER logistics_user SET ROLE logistics;
ALTER USER analytics_user SET ROLE analytics;
ALTER USER sales_user SET ROLE sales;
-- Create an admin role (superuser)
CREATE ROLE admin WITH SUPERUSER;