7. Database Security

Authorization in SQL:

Database needs a security inorder to safeguard information stored in its tables from unauthorized users.

There are 3 main objectives when designing a secure database application:

① Secrecy: Information should be disclosed to unauthorized users.

② Integrity: only authorized users should be allowed to modify data.

③ Availability:- Authorized users should not be denied access.

To achieve these objectives, a clear and consistent security policy should be developed to describe what security measures must be enforced.

Access control:-

DBMS offers two main approaches to access control

1: Discretionary access control OR previleges.

2: Mandatory access control

① Discretionary access control:-

SQL supports discretionary access control through through the GRANT, REVOKE Commands.

GRANT gives users previleges to base tables and views.

syntax: GRANT previleges ON objects TO users [with GRANT option]

Object : Basetable, view.

privileges: SELECT, INSERT(columnname), DELETE, REFERENCES(columnname)

If a user has a privilege with grant option, he she can pass it to another user with or without the grant option by using grant command.

only owner of a schema can execute the DDL statements CREATE, ALTER, DROP on that schema. the right to execute these statements cannot be granted or revoked.

privileges are assigned in SQL to authorization IDs, which can denote a single user or a group of users. A user must specify an authorization ID, in many systems, a corresponding password before DBMS Accepts any commands from him or her.

Eg: User Joe has created the table employee dept

① GRANT insert, DELETE ON employee TO yuppy with GRANT option

② GRANT SELECT ON dept TO Kohls

③ GRANT SELECT ON employee to paul with GRANT OPTION.

④ GRANT UPDATE(ename) ON employee TO nagabhushanam

REVOKE : complementary command to GRANT. this allows the withdrawal of privileges.

Syntax:

REVOKE [GRANT OPTION FOR] privileges
ON object FROM Users {RESTRICT / CASCADE}

This command also used to revoke just grant option on privileges.

Eg① GRANT SELECT ON employee TO Korth WITH GRANT OPTION (executed by Joe)

② GRANT SELECT ON employee TO paul WITH GRANT OPTION (executed by Korth)

③ REVOKE SELECT ON employee FROM Korth CASCADE (executed by Joe).

Korth loses the SELECT privilege on employee.
- then paul who received privilege from Korth & only Korth loses this privilege.
- paul's privilege is said to abandoned when the privilege from which it was derived.

Authorization graph

① GRANT SELECT ON employee TO Korth with GRANT OPTION. (executed by joe)

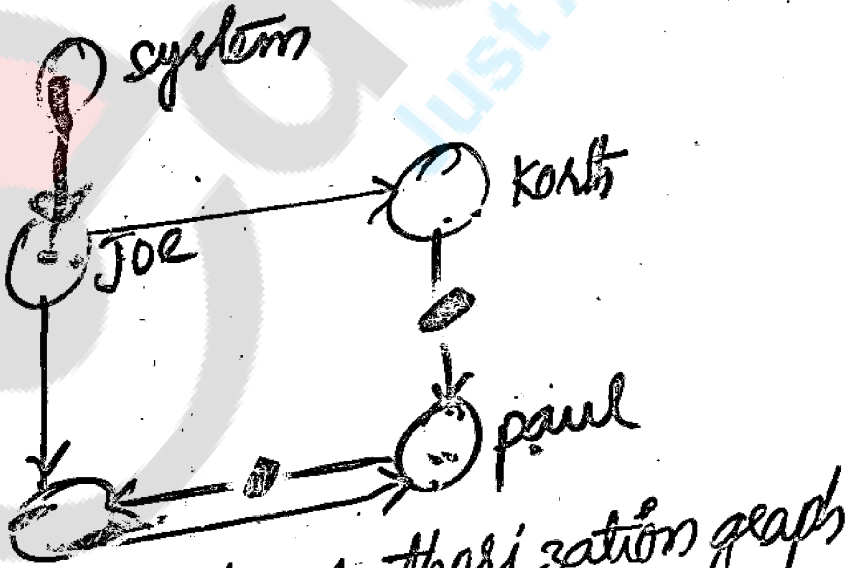
② GRANT SELECT ON employee TO paul WITH GRANT OPTION. (executed by Korth)

③ GRANT SELECT ON employee TO Rob WITH GRANT OPTION (executed by paul)

④ GRANT SELECT ON employee TO Rob with GRANT OPTION (executed by joe)

⑤ GRANT SELECT ON employee TO paul WITH GRANT OPTION (executed by Rob)

⑥ REVOKE SELECT ON employee FROM Korth CASCADE.



example Authorization graph

MANDATORY ACCESS CONTROL

The popular Model for mandatory access control called Bell-Lapadula Model; is described in terms of objects.

Eg: tables, rows, views, columns

Subjects: users, programs.

security classes & clearance.

each database object is assigned a security class.

each subject is assigned clearance for a security class

the class of an object or subject A as class(A)

→ the security class in a system are organised according to a partial order.

with most secure class

least secure class.

Eg. assume there are 4 classes

Top secret (TS), Secret (S), confidential (C)

and Unclassified (U).

$$TS > S > C > U$$

Bell-Lapadula model imposes 2 restrictions on all reads & writes of database objects.

① Simple security property :- (read)

② * - property :- (write)

① Simple Security property:

subject s is allowed to read object o only if class (S) ≥ class (O).

Eg: A user with TS clearance can read a table with C clearance, but user with C clearance is not allowed to read a table with TS classification.

② *- property:

Subject s is allowed to write object o only if class (S) ≤ class (O).

Eg: A user with 'S' clearance can write only objects with S or TS classification.

Covert channel can be used to defeat the Bell-Lapadula model:

Eg: if a malicious subject wants to find the salary of new employee.-

→ They can issue query to find the average salary in department & The total number of current employees.

- Then malicious subject can calculate the new employees salary based on the increase in average salary & number of employees.

Multilevel Relations and polyinstantiation :-

To apply mandatory access control policies in relational DBMS, a security class must be assigned to each database object. The objects can be at the granularity of table, rows, or even individual column values.

– each row is assigned a security class. This leads to the concept of a multilevel table.

polyinstantiation.

Relation R.

Eg

Cid	Carname	Security class
1	Honda	U
1	Ford	C
2	Toyota	C
3	Mazda	C
3	Ferrari	TS

Then subject with security class U will see R as:

Cid	Carname	Security class
1	Honda	U

Subjects with security class C will see R as:

cid	carname	securityclass
1	Honda	U
1	Ford	C
2	Toyoto	C
3	Mazda	C

Subject with security class TS will see R as:

cid	carname	Security class
1	Honda	U
1	Ford	C
2	Toyota	C
3	Mazda	C
3	Ferrari	TS

if cid is primary key

The two rows with cid = 1 can be interpreted in one of 2 ways.

- only the row with the higher classification actually exists (or) both exist and their presence is revealed to users according to their clearance level

⇒ The choice of interpretation is upto application developers and users.

Polyinstantiation: multiple rows with same PK distinguished by S.level

The presence of data objects that appear to have different values to users with different clearances is called polyinstantiation.

→ drawback of Mandatory access control scheme is their
- rigidity.
- classifications are not flexible.

covert channels, DOD Security Levels.

even if DBMS enforces the mandatory access control scheme, information can flow from a higher classification level to a lower classification level through indirect means, called covert channels.

DBMS vendors recently started implementing MAC Mechanisms because of DOD (Department of Defense) requires for its systems.

DOD — requirements described in terms of security levels A, B, C, D. A - Highest D - lowest.

level 'C' requires discretionary access control.

C — C1, C2, C3 requires some degree of accountability

B — B1, B2, B3, This level requires support for MAC.