**Security and Authorization**

A DBMS system always has a separate system for security which is responsible for protecting database against accidental or intentional loss, destruction or misuse.

Security Levels:

Database level: - DBMS system should ensure that the authorization restriction needs to be there on users.

Operating system Level: - Operating system should not allow unauthorized users to enter in system.

Network Level: - Database is at some remote place and it is accessed by users through the network so security is required.

Security Mechanisms:

Access Control (Authorization)

Which identifies valid users who may have any access to the valid data in the Database and which may restrict the operations that the user may perform?

For Example, the movie database might designate two roles:” users” (query the data only) and “designers” (add new data) user must be assigned to a role to have the access privileges given to that role.

Each application is associated with a specified role. Each role has a list of authorized users who may execute/Design/administers the application.

Authenticate the User:

Which identify valid users who may have any access to the data in the Database?

Restrict each user’s view of the data in the database

This may be done with help of concept of views in Relational databases.

Cryptographic control/Data Encryption:

Encode data in a cryptic form (Coded)so that although data is captured by unintentional user still, he/she can’t be able to decode the data.

Used for sensitive data, usually when transmitted over communications links but also may be used to prevent by passing the system to gain access to the data.

Inference control:

Ensure that confidential information can’t be retrieved even by deduction.

Prevent disclosure of data through statistical summaries of confidential data.

Flow control or Physical Protection:

Prevents the copying of information by unauthorized person.

Computer systems must be physically secured against any unauthorized entry.

Virus control:

At user level authorization should be done to avoid intruder attacks through humans.

There should be mechanism for providing protection against data virus.

User defined control:

Define additional constraints or limitations on the use of database.

These allow developers or programmers to incorporate their own security procedures in addition to above security mechanism.

Authorization

Authorization is finding out if the person, once identified, is permitted to have the resource.

Authorization explains that what you can do and is handled through the DBMS unless external security procedures are available.

Database management system allows DBA to give different access rights to the users as per their requirements.

Basic Authorization we can use any one form or combination of the following basic forms of authorizations

Resource authorization: -Authorization to access any system resource. e.g. sharing of database, printer etc.

Alternation Authorization: - Authorization to add attributes or delete attributes from relations

Drop Authorization: -Authorization to drop a relation.

Granting of privileges:

A system privilege is the right to perform a particular action, or to perform an action on any schema objects of a particular type.

An authorized user may pass on this authorization to other users. This process is called as granting of privileges.

Syntax:

GRANT <privilege list>

ON<relation name or view name>

TO<user/role list>

Example:

The following grant statement grants user U1,U2 and U3 the select privilege on Emp\_Salary relation:

GRANT select

ON Emp\_Salary

TO U1,U2 and U3.

Revoking of privileges:

We can reject the privileges given to particular user with help of revoke statement.

To revoke an authorization, we use the revoke statement.

Syntax:

REVOKE <privilege list>

ON<relation name or view name>

FROM <user/role list>[restrict/cascade]

Example:

The revocation of privileges from user or role may cause other user or roles also have to lose that privileges. This behavior is called cascading of the revoke.

Revoke select

ON Emp\_Salary

FROM U1,U2,U3.

Some other types of Privileges:

Reference privileges:

SQL permits a user to declare foreign keys while creating relations. Example: Allow user U1 to create relation that references key ‘Eid’ of Emp\_Salary relation.

GRANT REFERENCES (Eid)

ON Emp\_Salary

TO U1.

Execute privileges:

This privilege authorizes a user to execute a function or procedure. Thus, only user who has execute privilege on a function Create\_Acc() can call function.

GRANT EXECUTE

ON Create\_Acc

TO U1.