14 Database Security

14.1 INTRODUCTION

Database security is an important issue in database management because of the sensitivity and importance of data and information of an organisation. The data stored in a DBMS is often vital to the business interests of the organisation and is regarded as a corporate asset. Thus, a database represents an essential resource of an organisation that should be properly secured. The database environment is becoming more and more complex with the growing popularity and use of distributed databases with client/server architectures as compared to the mainframes. The access to the database has become more open through the Internets and corporate intranets. As a result, managing database security effectively has also become more difficult and time consuming. Therefore, it is important for the data base administrator (DBA) to develop overall policies, procedures and appropriate controls to protect the databases.

In this chapter, the potential threats to data security and protection against unauthorised access have been discussed. Various security mechanisms, such as discretionary access control, mandatory access control and statistical database security, have also been discussed.

14.2 GOALS OF DATABASE SECURITY

The goal of database security is the protection of data against threats such as accidental or intentional loss, destruction or misuse. These threats pose problems to the database integrity and access. Threats may be defined as any situation or event, whether intentional or accidental, that may adversely affect a system and consequently the organisation. A threat may be caused by a situation or event involving a person, action or circumstances that are likely to harm the organisation. The harm may be tangible, such as loss of hardware, software, or data. The harm could be intangible, such as loss of credibility or client confidence in the organisation. Database security involves allowing or disallowing users from performing actions on the database and the objects within it, thus protecting the database from abuse or misuse.

The database administrator (DBA) is responsible for the overall security of the database system. Therefore, the DBA of an organisation must identify the most serious threats and enforce security to take appropriate control actions to minimise these threats. Any individual user (a person) or a user group (group of persons) needing to access database system, applies to DBA for a user account. The DBA then creates an account number and password for user to access the database on the basis of legitimate need and policy of the organisation. The user afterwards logs in to the DBMS using the given account number and password whenever database access is needed. The DBMS checks for the validity of the user's entered account number and password. Then the valid user is permitted to use the DBMS and access the database. DBMS maintains these two fields of user account number and password by creating an encrypted table. DBMS keeps on appending this table by inserting a new record whenever a new account is created. When the account is cancelled, the corresponding record is deleted from the encrypted table.

14.3.1 Granting/Revoking Privileges

Granting and revoking privileges to the users is the responsibility of database administrator (DBA) of the DBMS. DBA classifies users and data in accordance with the policy of the organisation. DBA privileged commands include commands for granting and revoking privileges to individual accounts, users or user groups. It performs the following types of actions:

(a) *Account creation:* Account creation action creates a new account and password for a user or a group of users to enable them to access the DBMS.

(b) *Privilege granting:* Privilege granting action permits the DBA to grant certain privileges (access rights) to certain accounts.

(c) *Privilege revocation:* Privilege revoking action permits the DBA to revoke (cancel) certain privileges (access rights) that were previously given to certain accounts.

(d) *Security level assignment:* Security level assignment action consists of assigning user accounts to the appropriate security classification level.

Having an account and a password do not necessarily entitle a user or user groups to access all the functions of the DBMS. Generally, following two levels of privilege assignment is done to access the database system:

(a) ***The account level privilege assignment:*** At the account level privilege assignment, the DBA specifies the particular privileges that each account holds independently of the relations in the database. The account level privileges apply to the capabilities provided to the account itself and can include the following in SQL:

CREATE SCHEMA privilege	: to create a schema
CREATE TABLE privilege	: to create a table
CREATE VIEW privilege	: to apply schema changes such as
ALTER privilege	: adding or removing attributes from relations
DROP privilege	: to delete relation or views
MODIFY privilege	: to delete, insert, or update Tuples
SELECT privilege	: to retrieve information from the database using SELECT query

(b) ***The relation (or table) level privilege assignment:*** At relation or table level of privilege assignment, the DBA controls the privilege to access each individual relation or view in the database. Privileges at the relation level specify for each user the individual relations on which each type of command can be applied. Some privileges also refer to individual attributes (columns) of relations. Granting and revoking of relation privileges is controlled by assigning an owner account for each relation *R* in a database. The owner account is typically the account that was used when the relation was first created. The owner of the relation is given all privileges on the relation. In SQL, the following types of privileges can be granted on each individual relation *R*:

SELECT privilege on *R*	: to read or retrieve tuples from *R*
MODIFY privileges on *R*	: to modify (UPDATE, INSERT and DELETE) tuples of *R*
REFERENCES privilege on *R*	: to reference relationship *R*

14.3.1.1 Examples of GRANT Privileges

In SQL, granting of privileges is accomplished using GRANT command. The syntax for the GRANT command is given as

GRANT {ALL | privilege-list}
ON {table-name [(column-comma-list)] | view-name [(column-comma-list)]}
TO {PUBLIC | user-list}
[WITH GRANT OPTION]

or

GRANT {ALL | privilege-list [(COLUMN-COMMA-LIST)]}
ON {table-name | view-name}
TO {PUBLIC | user-list}
[WITH GRANT OPTION]

Meaning of the various clauses is as follows:

ALL	All the privileges for the object for which the user issuing the GRANT has grant authority, is granted.
privilege-list	Only the listed privileges are granted.
ON	It specifies the object on which the privileges are granted. It can be a table or a view.
column-comma-list	The privileges are restricted to the specified columns. If this is not specified, the grant is given for the entire table/view.
TO	It is used to identify the users to whom the privileges are granted.
PUBLIC	It means that the privileges are granted to all known users of the system who has valid User ID and Password.
user-list	The privileges will be granted to the user(s) specified in the list.
WITH GRANT OPTION	It means that the recipient has the authority to grant the privileges that were granted to him to another user.

Some of the examples of granting privileges are given below.

```
GRANT SELECT
ON EMPLOYEE
TO ABHISHEK, MATHEW
```

This means that the users 'ABHISHEK' and 'MATHEW' are authorised to perform SELECT operations on the table (or relation) EMPLOYEE.

```
GRANT SELECT
ON EMPLOYEE
TO PUBLIC
```

This means that all users are authorised to perform SELECT operations on the table (or relation) EMPLOYEE.

3.1.2 Examples of REVOKE Privileges

In SQL, revoking of privileges is accomplished using REVOKE command. The syntax for the REVOKE mmand is given as

```
REVOKE {ALL | privilege-list}
ON {table-name [(column-comma-list)] | view-name [(column-comma-list)]}
FROM {PUBLIC | user-list}
```

or

```
REVOKE {ALL | privilege-list [(COLUMN-COMMA-LIST)]}
ON {table-name | view-name}
FROM {PUBLIC | user-list}
```

Meaning of the various clauses is as follows:

ALL	All the privileges for the object specified are revoked.
privilege-list	Only the listed privileges are revoked.
ON	It specifies the object from which the privileges are removed. It can be a table or view.
column-comma-list	The privileges are restricted to the specified columns. If this is not specified, the revoke is for the entire table/view.
FROM	It is used to identify the users from whom the privileges are removed.
PUBLIC	It means that the privileges are revoked from all known users of the system.
user-list	The privileges will be granted to the user(s) specified in the list. The user issuing the REVOKE command should be the user who granted the privileges in the first place.

Some of the examples of revoking privileges are given below.

```
REVOKE SELECT
ON EMPLOYEE
FROM MATHEW
```

This means that the user 'MATHEW' is no longer authorised to perform SELECT operations on the PLOYEE table.

```
REVOKE CREATE TABLE
FROM MATHEW
```

This means that the system privilege for creating table is removed from the user 'MATHEW'.

14.6 STATISTICAL DATABASE SECURITY

Statistical database security system is used to control the access to a statistical database, which is used to provide statistical information or summaries of values based on various criteria. A statistical database contains confidential information about individuals or organisations, which is used to answer statistical queries concerning sums, averages, and numbers with certain characteristics. Thus, a statistical database permits queries that derive aggregated (statistical) information, for example, sums, averages, counts, maximums, minimums, standard deviations, means, totals, or a query such as "What is the average salary of Analysts?", etc. They do not permit queries that derive individual information, for example, the query "What is the salary of an Analyst Abhishek?".

In statistical queries, statistical functions are applied to a population of tuples. A population is a set of tuples of relation (or table) that satisfy some selection condition. For example, let us consider a relation EMPLOYEE, as shown in Fig. 14.2. Each selection condition on the EMPLOYEE relation will specify a particular population of EMPLOYEE tuples. For example, the condition EMP-SEX = 'F' specifies the female population. The condition ((EMP-SEX = 'F') AND (EMP-CITY = 'Jamshedpur') specifies the female population who lives in Jamshedpur.

Statistical database security prohibits users not to retrieve individual data, such as the salary of a specific employee. This controlled by prohibiting queries that retrieve attribute values and by allowing only queries that involve statistical aggregate functions such as SUM, STANDARD DEVIATION, MEAN, MAX, MIN, COUNT and AVERAGE.

Fig. 14.2 Relation EMPLOYEE

Relation: *EMPLOYEE*					
EMP-ID	**EMP-NAME**	**EMP-SEX**	**EMP-CITY**	**EMP-PHONE**	**EMP-SALARY**