Database Security

What Does Database Security Entail?

Database security refers to the measures taken to protect a database from unauthorized access, misuse, or corruption. It involves a combination of physical, technical, and administrative controls to ensure data confidentiality, integrity, and availability. Security measures include authentication, authorization, encryption, backup strategies, and access control policies.

What is a Security Policy?

A security policy is a set of rules and guidelines that define how data should be protected and who has access to it. It specifies user roles, data access levels, and security protocols. A well-defined security policy helps prevent unauthorized access, data breaches, and insider threats.

Access Control Mechanisms in DBMS

A Database Management System (DBMS) provides access control mechanisms to enforce security policies. Two complementary types of access control mechanisms include:

1. Discretionary Access Control (DAC)

DAC allows the owner of an object (such as a table or view) to grant or revoke access permissions to other users. It is implemented using SQL commands like GRANT and REVOKE.

Example:

GRANT SELECT, INSERT ON employees TO user1;
REVOKE INSERT ON employees FROM user1;

Advantages:

- Flexible and easy to implement.
- Allows users to control their own data.

Disadvantages:

- Prone to insider threats.
- Difficult to manage in large systems.

2. Mandatory Access Control (MAC)

MAC enforces strict security policies based on predefined classifications. Users are assigned security levels, and data is classified accordingly.

Example:
A government database may classify data as Public, Confidential, Secret, or Top Secret. Users can only access data for which they have the required clearance level.

Advantages:
- Provides high security.
- Prevents unauthorized access more effectively than DAC.

Disadvantages:
- Less flexible and harder to implement.
- Requires strict security administration.

Understanding Views and Security Enforcement
A view in a database is a virtual table that provides a specific representation of data. It is based on a SELECT query and does not store data itself.

How Views Enforce Security:
- Restrict access to sensitive columns by only exposing required fields.
- Provide role-based access by allowing different users to see different data subsets.
- Prevent direct modifications by limiting operations on underlying tables.

Example:
```
CREATE VIEW employee_view AS
SELECT name, department FROM employees WHERE role = 'Manager';
```

Encryption in Database Security
Encryption is the process of converting data into an unreadable format to prevent unauthorized access. It ensures data confidentiality both at rest and in transit.

Example of Encryption Use:
Storing user passwords as hashed and encrypted values prevents unauthorized access in case of a data breach.

Example SQL:
```
UPDATE users SET password = AES_ENCRYPT('mypassword', 'secret_key');
```

Security Through Access Control
Access control is a critical aspect of database security. It defines who can access data and what operations they can perform.

Types of Access Control:
- Role-Based Access Control (RBAC):Assigns permissions based on user roles.

- Attribute-Based Access Control (ABAC): Uses attributes (e.g., department, location) to define access.
- Time-Based Access Control: Restricts access based on time constraints.

Example RBAC Implementation:

```
GRANT SELECT ON employees TO hr_manager;
REVOKE DELETE ON employees FROM hr_manager;
```