DBMS QB – UNIT – 6

[4-marks]

1. Define Database Security

- **Database security** refers to the protection of a database from unauthorized access, misuse, damage, or disclosure. It ensures that only authorized users can view or modify the data stored in the database.
- The main aim of database security is to protect the **confidentiality, integrity, and availability** of data. Confidentiality ensures data is not leaked, integrity ensures data remains correct, and availability ensures data is accessible when needed.
- Database security involves multiple layers such as **user authentication, access control, encryption, and auditing**. These mechanisms work together to keep sensitive data safe from internal and external threats.

2. List any four database security issues

- **Legal and Ethical Issues** arise because some data is protected by laws and moral rules. Personal, medical, and financial data must not be accessed without proper authorization.
- **Policy Issues** involve rules set by organizations or governments about what data should remain confidential. These policies decide which information can be shared and which must remain secret.
- **System-Related Issues** occur because security can be applied at different levels like hardware, operating system, or DBMS. A weak layer can compromise the entire database system.
- **Multi-Level Security Issues** arise when data and users are classified into levels such as confidential or secret. The DBMS must strictly enforce access based on these classifications.

3. What is Discretionary Access Control (DAC)?

- **Discretionary Access Control (DAC)** is a database security mechanism where access permissions are granted or revoked by the **database administrator or data owner**. The decision depends on the discretion of the owner of the database object.
- In DAC, users are given specific privileges like **SELECT, INSERT, UPDATE, and DELETE** on tables or views. These privileges define exactly what actions a user can perform on the data.
- DAC is flexible and widely used in commercial DBMSs. However, it does not strictly control how information flows once a user has access.

4. Define Grant and Revoke privileges in DAC

- **GRANT** is a command used to give specific database privileges to users. These privileges allow users to perform actions such as reading data, modifying data, or creating database objects.
- The GRANT command can also include a **GRANT OPTION**, which allows a user to pass the privilege to other users. This helps in delegating responsibilities but must be controlled carefully.
- **REVOKE** is a command used to remove previously granted privileges from a user. It is important when a user's role changes or when access is no longer required.
- When a privilege is revoked, any privileges passed to others through that user may also be removed automatically. This prevents unauthorized access.

5. What is Mandatory Access Control (MAC)?

- **Mandatory Access Control (MAC)** is a strict database security mechanism where access decisions are made by the **system security policy**, not by individual users. Users cannot change or share permissions on their own.
- In MAC, both users (subjects) and data (objects) are assigned **security classifications** such as Top Secret, Secret, Confidential, or Unclassified. Access is allowed only if the user's clearance level is sufficient.
- MAC follows rules like **"No Read Up" and "No Write Down"**, which prevent data leakage across security levels. It is commonly used in military and government systems

6. Define Role-Based Access Control (RBAC)

- **Role-Based Access Control (RBAC)** is a security mechanism where access permissions are assigned based on a user's **job role** rather than to individual users. Each role represents a set of responsibilities within an organization.
- In RBAC, users are assigned roles such as admin, manager, or employee, and each role has predefined privileges. This makes permission management easier because changes are applied to roles instead of individual users.
- RBAC is commonly used with **mandatory access control systems** to support multilevel security. It reduces errors, improves consistency, and ensures users access only what is required for their role.

7. What is the purpose of access control in a database?

- The main purpose of **access control** is to prevent unauthorized users from accessing the database system. It ensures that only valid users can log in using proper authentication like usernames and passwords.
- Access control restricts what actions a user can perform on the database. This includes controlling who can read, insert, update, or delete data.
- It helps protect sensitive information such as salaries, medical records, and financial data. By limiting access, access control maintains data confidentiality and integrity in multi-user environments.

8. Differentiate between DAC and MAC

- **Discretionary Access Control (DAC)** allows data owners or DBAs to decide who gets access to data. Permissions are granted or revoked using commands like GRANT and REVOKE.
- **Mandatory Access Control (MAC)** is controlled by system-enforced security policies. Users cannot change permissions, and access depends on security classifications.
- DAC is flexible and easy to use, making it popular in commercial systems. However, it does not control information flow strictly.
- MAC provides strong security by enforcing rules like “no read up” and “no write down”. It is used in military and government systems where data leakage must be prevented.

9. What is a security policy in DBMS?

- A **security policy** in DBMS is a set of rules that defines how data should be protected and who can access it. These rules are set by organizations or governments based on legal and operational needs.
- The policy specifies what data is confidential and what data can be shared publicly. It also defines acceptable and unacceptable actions by users.
- Security policies guide the implementation of access control, encryption, and auditing. They ensure consistent protection of data across the entire database system.

10. What is multilevel security in databases?

- **Multilevel security** is a database security approach where data and users are classified into different security levels. Common levels include Top Secret, Secret, Confidential, and Unclassified.
- Each user is assigned a clearance level, and data objects are assigned classification levels. A user can access data only if their clearance level is equal to or higher than the data classification.
- The DBMS enforces these rules automatically to prevent unauthorized access. Multilevel security is mainly used in high-security environments like defense and intelligence systems

11. Name any two threats to database security

- **Loss of Integrity** is a major threat to database security. It occurs when data is modified incorrectly or changed by unauthorized users, either intentionally or by mistake. Such incorrect data can lead to wrong decisions, fraud, or inaccurate reports in organizations.
- **Loss of Confidentiality** is another serious threat where sensitive data is exposed to unauthorized users. This can result in privacy violations, legal problems, and loss of public trust. Examples include leaking credit card details or confidential government information.

12. What is a user privilege in DBMS?

- A **user privilege** in DBMS is a permission given to a user that defines what actions they are allowed to perform. These actions may include reading data, inserting new records, updating existing data, or deleting records.
- Privileges help control access to database objects such as tables, views, or schemas. By assigning proper privileges, the DBA ensures users can only perform tasks necessary for their role.
- User privileges improve database security by preventing misuse or accidental damage to data. They are managed using commands like GRANT and REVOKE.

13. Define Subject and Object in access control

- A **Subject** is an active entity that requests access to the database. It can be a user, an account, or a program that performs operations such as reading or updating data.
- Subjects are assigned security clearances or privileges that determine what data they can access. These clearances are checked before allowing any operation.
- An **Object** is a passive entity that contains data, such as a table, record, attribute, or view. Objects are assigned security classifications to control access.
- Access is granted only when the subject's authorization level matches the object's security requirements.

14. Give an example of discretionary access control

- An example of **Discretionary Access Control (DAC)** is when a table owner grants SELECT permission on a table to another user. This decision is made by the owner, not enforced by a system-wide policy.
- For instance, the owner of an EMPLOYEE table may allow a user to read employee names and salaries. The owner can also restrict access by creating a view with limited columns.
- If the access is no longer required, the owner can revoke the permission at any time. This flexibility is a key feature of DAC.

15. Define Authorization in database security

- **Authorization** in database security is the process of determining what actions a user is allowed to perform after they log in. It controls access to database resources based on assigned privileges.
- Authorization ensures that authenticated users can access only permitted data and operations. For example, some users may only read data, while others can modify it.
- It is enforced using access control mechanisms like discretionary or mandatory security. Proper authorization prevents unauthorized data access and maintains confidentiality and integrity.

[5-marks]

1. Explain Discretionary Access Control (DAC) with an example of Grant and Revoke privileges

- **Discretionary Access Control (DAC)** is a database security mechanism where the database administrator or the owner of a database object decides who can access the data. The word "discretionary" means the control lies with the data owner, not with a fixed system policy.
- In DAC, users are given specific privileges such as SELECT, INSERT, UPDATE, or DELETE. These privileges define exactly what operations a user can perform on a table or view.
- The **GRANT** command is used to give privileges to users. For example, a table owner can grant SELECT permission on an EMPLOYEE table to another user so they can read data.
- The **REVOKE** command is used to remove privileges when access is no longer required. This helps maintain security when user roles change or when misuse is suspected.

2. Explain Mandatory Access Control (MAC) and its working in multilevel security

- **Mandatory Access Control (MAC)** is a strict security mechanism where access decisions are controlled by system-defined security policies. Users cannot change permissions or share access at their own discretion.
- In MAC, both users (subjects) and data objects are assigned **security classifications** such as Top Secret, Secret, Confidential, and Unclassified. These classifications decide who can access which data.
- MAC works using rules like **"No Read Up"**, which means a user cannot read data above their clearance level. This prevents users from viewing more sensitive information.
- Another rule is **"No Write Down"**, which prevents users from writing sensitive data to lower security levels. This avoids data leakage in multilevel security systems.

3. Describe Role-Based Access Control (RBAC) with an example

- **Role-Based Access Control (RBAC)** is a security mechanism where access permissions are assigned based on a user's job role. Instead of assigning privileges to individual users, roles are created with predefined permissions.
- Each role represents a specific responsibility in an organization, such as admin, manager, or employee. Users are assigned roles based on their work requirements.
- For example, an HR role may have permission to read and update employee records. A regular employee role may only have permission to view limited information.
- RBAC simplifies security management because permissions are managed at the role level. It also reduces errors and ensures consistency in access control.

4. Explain the difference between DAC, MAC, and RBAC

- **DAC** gives control to the data owner or DBA to grant or revoke privileges. It is flexible and easy to use but does not strictly control information flow.
- **MAC** is controlled by system-enforced security policies and uses security classifications. It provides strong protection but is rigid and difficult to manage.
- **RBAC** assigns permissions based on roles rather than individual users. It simplifies administration and is suitable for organizations with structured job roles.
- DAC is commonly used in commercial systems, MAC in military or government systems, and RBAC in organizations where role-based responsibilities are clear.

5. List and explain common database security issues

- **Legal and Ethical Issues** arise because certain data is protected by laws and moral rules. Unauthorized access to personal or medical data can lead to legal penalties.
- **Policy Issues** occur when organizations define rules about what information must remain confidential. These policies guide access decisions and data sharing.
- **System-Related Issues** happen when security is weak at the hardware, operating system, or DBMS level. A weakness at any level can compromise the entire database.
- **Multi-Level Security Issues** involve handling data with different sensitivity levels. The DBMS must ensure users access only data appropriate to their clearance.

6. Explain multilevel security in databases and its importance

- **Multilevel security** is a database security approach in which both users and data are classified into different security levels. Common levels include Top Secret, Secret, Confidential, and Unclassified, arranged from highest to lowest.
- Each user is given a clearance level, and each database object is assigned a classification level. A user can access data only if their clearance level is equal to or higher than the data's classification.
- The DBMS automatically enforces these rules using mandatory access control policies. This prevents unauthorized users from accessing sensitive data.
- The importance of multilevel security lies in preventing data leakage across levels. It is especially crucial in military, government, and intelligence systems where data sensitivity varies greatly.

7. Explain the concept of privileges and permissions in DBMS

- **Privileges and permissions** in DBMS define what actions a user is allowed to perform on database objects. They control operations such as reading data, inserting records, updating values, or deleting data.
- Privileges can be granted at different levels, such as account level or table level. This allows fine-grained control over who can access which part of the database.
- By assigning correct privileges, the DBA ensures users can only perform tasks related to their role. This reduces the risk of accidental data damage or misuse.
- Privileges are managed using commands like GRANT and REVOKE. These commands help maintain security throughout the database lifecycle.

8. Write a short note on user authentication and authorization in DBMS

- **User authentication** is the process of verifying the identity of a user before allowing access to the database. It is usually done using a user account and password created by the DBA.
- The DBMS stores account information securely, often in encrypted form. Only users with valid login credentials are allowed to enter the system.
- **Authorization** determines what actions an authenticated user can perform. It controls access to tables, views, and operations based on assigned privileges.
- Together, authentication and authorization ensure that only legitimate users access the database and only in permitted ways. This helps protect data confidentiality and integrity.

9. Explain how Grant and Revoke commands are used to control user access

- The **GRANT** command is used to give specific privileges to users in a database. These privileges allow users to perform actions such as SELECT, INSERT, UPDATE, or DELETE.
- GRANT can be applied to tables, views, or schemas, and may include the GRANT OPTION. This option allows a user to pass privileges to other users.
- The **REVOKE** command is used to remove previously granted privileges. It is important when users change roles or leave an organization.
- When a privilege is revoked, any privileges passed on by that user may also be removed. This helps prevent unauthorized access and privilege misuse.

10. Describe the role of roles and permissions in RBAC

- In **Role-Based Access Control (RBAC)**, roles represent job functions within an organization. Each role is assigned a set of permissions required to perform specific tasks.
- Users are assigned roles instead of being given permissions directly. This makes access control easier to manage and more consistent.
- Permissions define what operations a role can perform, such as reading or updating certain data. All users with the same role share the same permissions.
- RBAC reduces administrative effort and security errors. It ensures users access only what is necessary for their role and nothing more

11. Explain how DAC can be implemented in SQL

- **Discretionary Access Control (DAC)** is implemented in SQL using the **GRANT** and **REVOKE** commands. These commands allow the database owner or DBA to control which users can access specific database objects.
- Using the **GRANT** command, privileges such as SELECT, INSERT, UPDATE, and DELETE can be given to users on tables or views. This clearly defines what operations a user is allowed to perform.
- SQL also supports granting privileges with the **GRANT OPTION**, which allows a user to pass the same privilege to other users. This helps in delegating responsibilities when needed.
- The **REVOKE** command is used to remove privileges when access is no longer required. This ensures that outdated or unnecessary access rights are properly controlled.

12. Discuss the threats posed by unauthorized access to databases

- **Unauthorized access** can lead to a **loss of confidentiality**, where sensitive data such as personal or financial information is exposed. This can result in privacy violations and legal consequences.
- It can also cause a **loss of integrity**, where unauthorized users modify or delete important data. Such incorrect data can lead to wrong decisions and operational failures.
- Unauthorized access may also result in a **loss of availability**. Attackers can disrupt services, making the database unavailable to legitimate users.
- These threats reduce trust in the system and can damage an organization's reputation. Hence, controlling unauthorized access is critical for database security.

13. Explain the concept of security labels in MAC

- In **Mandatory Access Control (MAC)**, **security labels** are used to classify both users and data. These labels indicate the sensitivity level of users and database objects.
- Common security labels include Top Secret, Secret, Confidential, and Unclassified. These labels are assigned according to organizational or government security policies.
- A user can access data only if their clearance level is equal to or higher than the data's security label. This rule is enforced automatically by the DBMS.
- Security labels help prevent information leakage across different levels. They are essential for maintaining strict security in multilevel database systems.

14. Explain how RBAC simplifies security administration

- **Role-Based Access Control (RBAC)** simplifies security administration by assigning permissions to roles instead of individual users. This reduces the complexity of managing access rights.
- When a new user joins, the DBA only needs to assign an appropriate role. The user automatically receives all permissions associated with that role.
- If job responsibilities change, the user's role can be changed easily without modifying individual permissions. This saves time and reduces errors.
- RBAC improves consistency and security across the system. It ensures users have access only to what is required for their role.

15. Explain the importance of access control in multi-user database systems

- In **multi-user database systems**, many users access the same database simultaneously. Access control ensures that users do not interfere with each other's data.
- It restricts users to only the data and operations they are authorized to perform. This helps protect sensitive information from misuse.
- Access control also helps maintain data integrity by preventing unauthorized updates or deletions. Only trusted users can modify critical data.
- Without proper access control, databases become vulnerable to errors, misuse, and security breaches. Therefore, access control is essential for safe and reliable database operations.

[10-marks]

1. Explain in detail the database security issues and challenges faced by organizations

- **Legal and Ethical Issues** are a major challenge for organizations because many types of data are protected by laws and ethical rules. Personal data, medical records, and financial information must not be accessed or disclosed without proper authorization, otherwise legal action can be taken.
- **Policy Issues** arise when organizations define rules about which data must remain confidential. These policies decide what information can be shared publicly and what must be restricted to specific users only.
- **System-Related Security Issues** occur because database security can be implemented at different levels such as hardware, operating system, or DBMS. If security is weak at any one level, attackers may exploit it to access the database.
- **Multi-Level Security Challenges** exist in organizations that use security classifications like Top Secret, Secret, Confidential, and Unclassified. The DBMS must strictly enforce access rules based on these classifications to prevent data leakage.
- **Loss of Integrity** is a serious security issue where data is modified incorrectly or by unauthorized users. This can result in wrong decisions, fraud, and inaccurate reports.
- **Loss of Availability** happens when authorized users cannot access the database due to crashes, network failures, or attacks. This can disrupt business operations and critical services.
- **Loss of Confidentiality** occurs when sensitive data is exposed to unauthorized users. Such breaches can lead to loss of trust, legal penalties, and damage to an organization's reputation.
- **Security as a System-Wide Challenge** is important because a database does not work alone. Weaknesses in applications, servers, or networks can still compromise database security even if the DBMS itself is strong.

2. Describe Discretionary Access Control (DAC). Explain how Grant and Revoke privileges work with examples

- **Discretionary Access Control (DAC)** is a database security mechanism where the database administrator or the owner of a database object controls access to data. The term “discretionary” means the data owner has the freedom to decide who gets access.
- In DAC, users are given specific **privileges** such as SELECT, INSERT, UPDATE, and DELETE. These privileges define exactly what operations a user can perform on tables or views.
- DAC allows access control at different levels such as table level, record level, or attribute level. This makes it flexible and suitable for most commercial database systems.
- The **GRANT** command is used to give privileges to users. For example, a table owner can grant SELECT privilege on an EMPLOYEE table so another user can read employee data.
- GRANT can also be given with the **GRANT OPTION**, which allows a user to pass the same privilege to other users. This helps in delegating tasks but must be managed carefully.
- The **REVOKE** command is used to remove privileges that were previously granted. This is important when a user changes roles or no longer needs access.
- When a privilege is revoked, any privileges that were passed to others through that user may also be removed. This prevents unauthorized access from spreading.
- DAC is easy to use and widely implemented, but it does not strictly control information flow. Once a user has access, DAC cannot prevent misuse through malicious programs.

3. Explain Mandatory Access Control (MAC) and how multilevel security is implemented in a DBMS

- **Mandatory Access Control (MAC)** is a strict database security mechanism where access to data is controlled by system-defined security policies. In this model, users cannot decide or change permissions on their own, unlike discretionary systems.
- In MAC, every **subject** (user, program, or account) and every **object** (table, record, attribute, or view) is assigned a **security classification**. These classifications usually include Top Secret, Secret, Confidential, and Unclassified.
- Multilevel security is implemented by comparing the clearance level of a user with the classification level of the data. A user can access data only if their clearance level is equal to or higher than the data's classification.
- MAC follows two important rules from the **Bell–LaPadula model**. The first rule is *"No Read Up"*, which prevents a user from reading data at a higher security level.
- The second rule is *"No Write Down"*, which prevents a user from writing sensitive data to a lower security level. This rule avoids accidental or intentional leakage of confidential information.
- The DBMS enforces these rules automatically, without relying on user decisions. This ensures strong protection against information leakage and unauthorized access.
- Multilevel security also uses techniques like **filtering**, where users at lower levels see restricted or NULL values instead of sensitive data. This allows the same table to appear differently for users with different clearances.
- MAC is mainly used in military, government, and intelligence systems. These environments require very high security and strict control over information flow.

4. Describe Role-Based Access Control (RBAC) in detail. Explain its advantages over DAC and MAC

- **Role-Based Access Control (RBAC)** is a database security mechanism where permissions are assigned to roles instead of individual users. A role represents a job function or responsibility within an organization.
- In RBAC, users are assigned one or more roles such as admin, manager, or employee. Each role has a predefined set of permissions required to perform specific tasks.
- Permissions in RBAC define what operations a role can perform, such as reading, inserting, updating, or deleting data. All users with the same role automatically get the same permissions.
- RBAC simplifies security management because administrators manage permissions at the role level. This avoids the need to assign or revoke privileges for every individual user.
- Compared to **DAC**, RBAC is more organized and less error-prone. DAC requires managing privileges for each user separately, which becomes difficult in large organizations.
- Compared to **MAC**, RBAC is more flexible and easier to administer. MAC requires strict classification of all users and data, which increases administrative overhead.
- RBAC reduces security risks by ensuring users only access what is required for their job. When a user's role changes, permissions can be updated simply by changing their role.
- Because of its balance between security and usability, RBAC is widely used in modern organizations and enterprise database systems

5. Compare and contrast DAC, MAC, and RBAC in terms of security, flexibility, and usability

- **Discretionary Access Control (DAC)** provides security by allowing the database owner or DBA to grant and revoke privileges. However, once a user gets access, DAC does not strictly control how the data is later used or shared, which can reduce overall security.
- In terms of **flexibility**, DAC is very flexible because permissions can be easily granted or revoked using SQL commands. This makes DAC suitable for commercial and academic database systems where requirements change frequently.
- Regarding **usability**, DAC is easy to understand and manage. Users and administrators find it simple because access is controlled through familiar privileges like SELECT and UPDATE.
- **Mandatory Access Control (MAC)** offers very strong security because access decisions are enforced by system policies. Users cannot override rules, and information flow is strictly controlled using classification levels.
- MAC is **not flexible**, as every user and data item must be labeled with a security level. Any change requires updating classifications, which increases administrative effort.
- In terms of **usability**, MAC is difficult to use in dynamic environments. It is mainly suitable for military or government systems where strict control is more important than convenience.
- **Role-Based Access Control (RBAC)** provides balanced security by assigning permissions to roles instead of individuals. This reduces mistakes and prevents users from having unnecessary access.
- RBAC is more **flexible than MAC** and more structured than DAC. Administrators can easily manage permissions by modifying roles rather than individual users.
- From a **usability** perspective, RBAC is efficient and scalable. It is widely used in organizations because it combines good security with easy administration.

6. Explain multilevel security with examples of classification levels, subjects, and objects

- **Multilevel security** is a database security approach where data and users are classified into different security levels. These levels help control access based on the sensitivity of the data.
- Common **classification levels** include Top Secret, Secret, Confidential, and Unclassified. These levels are arranged from highest sensitivity to lowest sensitivity.
- A **subject** refers to an active entity that requests access to the database. Subjects include users, programs, or accounts that perform operations like reading or updating data.
- Each subject is assigned a **clearance level**. This clearance defines the highest level of data the subject is allowed to access.
- An **object** is a passive entity that stores data, such as a table, tuple, attribute, or view. Each object is assigned a security classification level.
- Multilevel security works by comparing the subject's clearance with the object's classification. Access is allowed only if the subject's clearance is equal to or higher than the object's classification.
- For example, a user with Secret clearance can access Confidential and Unclassified data but cannot access Top Secret data. This rule prevents unauthorized data exposure.
- The DBMS enforces these rules automatically using mandatory access control policies. This prevents data leakage and ensures strict security in high-risk environments.
- Multilevel security is essential in military, government, and intelligence systems. These systems handle highly sensitive data and require strict control over information access.

7. Explain the process of user authentication, authorization, and privilege management in a DBMS

- **User authentication** is the first step in database security and is used to verify the identity of a user. Anyone who wants to access the database must apply for a user account, which is created by the Database Administrator (DBA).
- During authentication, the user logs in using an account number and password. The DBMS checks this information against a securely stored, encrypted table of user accounts to confirm the user is valid.
- Authentication ensures that only legitimate users and authorized application programs can enter the database system. Without proper authentication, unauthorized users could gain access to sensitive data.
- **Authorization** comes into effect after successful authentication. It determines what actions an authenticated user is allowed to perform on the database.
- Authorization controls access to database objects such as tables, views, and records. For example, a user may be allowed to read data but not modify or delete it.
- **Privilege management** is the process of assigning and controlling permissions given to users. Privileges define specific operations like SELECT, INSERT, UPDATE, and DELETE.
- The DBA manages privileges to ensure users receive only the access necessary for their role. This helps reduce misuse and accidental damage to data.
- The DBMS also tracks user activities through logs. These logs help in auditing and identifying which user performed which operation, strengthening overall security.

8. Discuss SQL commands related to database security, including Grant, Revoke, and Role Management

- SQL provides several commands to enforce **database security** by controlling user access. The most important security-related commands are GRANT, REVOKE, and role-based permission management.
- The **GRANT** command is used to give specific privileges to users or roles. These privileges allow users to perform operations such as reading data, inserting new records, or updating existing data.
- GRANT can be applied at different levels, such as table level or view level. It may also include the **GRANT OPTION**, which allows a user to pass the granted privilege to other users.
- The **REVOKE** command is used to remove previously granted privileges. This is important when users change roles, leave the organization, or no longer require access.
- When a privilege is revoked, any privileges passed to other users through that user may also be removed automatically. This prevents unauthorized privilege propagation.
- **Role management** groups multiple privileges into a single role. Instead of assigning privileges to users individually, the DBA assigns a role to a user.
- Role management simplifies administration and reduces errors. When permissions need to change, the DBA only updates the role rather than each individual user.
- Together, GRANT, REVOKE, and role management help maintain confidentiality, integrity, and controlled access in a multi-user database environment.

9. Explain the importance of access control and auditing in database security with real-world examples

- **Access control is very important in database security** because it ensures that only authorized users can access the database system. In a multi-user environment, many users work on the same database, but not all users should have the same level of access. Sensitive data must be protected from users who do not need it for their work.

- **Access control protects data confidentiality** by restricting access to private and sensitive information. Data such as employee salaries, medical records, and bank account balances should only be visible to specific authorized users. For example, in a bank database, normal clerks should not be allowed to view or modify customer account balances.

- **Access control also helps maintain data integrity** by allowing only trusted users to update or delete data. When unauthorized users are prevented from modifying data, the chances of accidental mistakes or intentional corruption are reduced. This ensures that the data stored in the database remains accurate and reliable.

- **Auditing plays an equally important role in database security** because it keeps a record of all user activities. The DBMS tracks information such as which user logged in, what operations were performed, and from which computer or device the access was made.

- **Auditing helps in detecting misuse and security breaches** by providing a detailed activity log. If incorrect or suspicious data is found, administrators can check audit logs to identify who made the changes. For example, in a hospital database, audit logs can reveal which staff member modified a patient's record.

- **In banking systems, auditing is especially critical** because databases are accessed by many users frequently. If fraud or unauthorized access occurs, audit trails help trace responsibility and support investigations.

- **Access control prevents security problems**, while **auditing helps detect and investigate them**. Together, they strengthen overall database security and build trust in the system.

10. Case Study – Database Security in a Hospital System

a) Identifying security issues in a hospital database

- A hospital database stores **highly sensitive data** such as patient records, medical history, and billing details. Unauthorized access to this data can violate privacy laws and ethical rules.
- If access control is weak, staff members may see information they are not supposed to view. For example, a receptionist should not access detailed medical reports.
- Without proper auditing, it becomes difficult to identify who modified or accessed patient records. This can lead to misuse without accountability.

b) Proposed security model – Role-Based Access Control (RBAC)

- **RBAC** is suitable for a hospital because users have clearly defined job roles. Doctors, nurses, receptionists, and administrators all require different levels of access.
- RBAC simplifies security by assigning permissions to roles instead of individual users. This reduces errors and makes management easier.

c) Assigning and revoking privileges

- **Doctor role**: Granted SELECT and UPDATE privileges on patient medical records. This allows doctors to view and update treatment details.
- **Nurse role**: Granted SELECT privilege on patient records but restricted UPDATE access. Nurses can view information but cannot modify diagnoses.
- **Receptionist role**: Granted limited SELECT privilege on appointment and billing information only. Medical data remains inaccessible.
- **Administrator role**: Granted full privileges to manage users and roles.
- If an employee changes roles or leaves the hospital, privileges are **revoked** immediately. This prevents unauthorized future access.
- Auditing logs are used to track all actions performed by users. This ensures accountability and supports investigation in case of misuse.