CHANDIGARH ENGINEERING COLLEGE

B.TECH.(CSE 5th Sem.)

Notes Subject: Database Management System

Subject Code: ((BTCS 501-18))

Unit 5

Authentication in DBMS

Authentication is a process in which the identity of any user is verified before they can access anything in your database. It is the process of securing data from unauthorized access. It is important to implement user authentication in DBMS to prevent data theft, data loss, or network attacks.

There are various methods of data authentication in DBMS such as multi-factor authentication, password authentication certificate authentication, biometrics token authentication, device authentication API authentication, etc.

There are various benefits of user authentication in DBMS:

- Preventing unauthorized or malicious access: Proper authentication in DBMS will allow you to prevent unauthorized access which can lead to harm such as stealing, modifying, or deleting your important data.
- Preventing Data Loss & corruption: User authentication in DBMS allows you to prevent data loss and corruption by verifying only experts are allowed to access the database. An unauthorized person may not have proper understanding about the structure of the DBMS which may lead to accidental deletion of important data.
- Providing Access Control: It means that only some specific user roles (such as Administrators) are allowed to access the data which helps prevent data abuse and accidental information loss.
- Securing Networks and Network Chains: User authentication in a fairly large database will help prevent ransomware attacks on a large network of any organization by preventing unauthorized access to the interface.
- Preventing Data theft: User authentication will help prevent data theft by not allowing hackers or people with malicious intent to access and leak the data on the dark web.

Database security authentication practices:

- Access control

Use granular access control policies, such as the principle of least privilege, to limit what each user can do.

- Authorization

Use authorization processes to ensure users only have access to the data and resources they are authorized to access.

- Monitor database activity

Continuously monitor and audit database activity to detect and respond to suspicious activities.

- Network security

Use firewalls to restrict network traffic and enforce your organization's data security policy.

- Regular database audit

Use auditing capabilities to track who did what on the service and on specific databases.

- Regular data backup and encryption

Regularly back up and encrypt data to preserve its integrity and confidentiality.

Other database security practices include:

- Remote Authentication Dial-In User Service (RADIUS), a standard lightweight protocol for user authentication, authorization, and accounting.
- Attribute-based access control (ABAC), which allows you to determine if someone has authorization for a resource in real-time.

Database Security

- Security of databases refers to the array of controls, tools, and procedures designed to ensure and safeguard confidentiality, integrity, and accessibility. This tutorial will concentrate on confidentiality because it's a component that is most at risk in data security breaches.
- Security for databases must cover and safeguard the following aspects:
- The database containing data.
- Database management systems (DBMS)
- Any applications that are associated with it.
- Physical database servers or the database server virtual, and the hardware that runs it.
- The infrastructure for computing or network that is used to connect to the database.
- Security of databases is a complicated and challenging task that requires all aspects of security practices and technologies. This is inherently at odds with the accessibility of databases. The more usable and accessible the database is, the more susceptible we are to threats from security. The more vulnerable it is to attacks and threats, the more difficult it is to access and utilize.

What is DAC?

DAC is identity-based access control. DAC mechanisms will be controlled by user identification such as username and password. DAC is discretionary because the owners can transfer objects or any authenticated information to other users. In simple words, the owner can determine the access privileges.

Examples: Permitting the Linux file operating system is an example of DAC.

What is MAC?

The operating system in MAC will provide access to the user based on their identities and data. To gain access, the user has to submit their personal information. It is very secure because the rules and restrictions are imposed by the admin and will be strictly followed. MAC settings and policy management will be established in a secure network and are limited to system administrators.

Examples: Access level of Windows for ordinary users, admins, and guests are some of the examples of MAC.

Role-based Access Control

One technique for limiting network access based on the responsibilities of certain users within an organization is called role-based access control, or RBAC. RBAC, also known as role-based security, is a tool used by organizations to categorize access levels according to the roles and responsibilities of individual employees.

Restricting network access is crucial for companies with a large workforce, contractors, or third parties that have access to the network, such suppliers and customers. This is because it may be difficult to adequately monitor network access. Businesses that use RBAC are better equipped to protect their sensitive information and vital apps. RBAC keeps users from accessing information that is irrelevant to them and makes sure they only access the data they need to do their duties.

Intrusion Detection System (IDS)

An Intrusion Detection System (IDS) is a security tool that monitors a computer network or systems for malicious activities or policy violations. It helps detect unauthorized access, potential threats, and abnormal activities by analyzing traffic and alerting administrators to take action. An IDS is crucial for maintaining network security and protecting sensitive data from cyber-attacks.

A system called an intrusion detection system (IDS) observes network traffic for malicious transactions and sends immediate alerts when it is observed. It is software that checks a network or system for malicious activities or policy violations. Each illegal activity or violation is often recorded either centrally using an SIEM system or notified to an administration. IDS monitors a network or system for malicious activity and protects a computer network from unauthorized access from users, including perhaps insiders. The intrusion detector learning task is to build a predictive model (i.e. a classifier) capable of distinguishing between ‘bad connections’ (intrusion/attacks) and ‘good (normal) connections’.

Working of Intrusion Detection System (IDS)

- An IDS (Intrusion Detection System) monitors the traffic on a computer network to detect any suspicious activity.
- It analyzes the data flowing through the network to look for patterns and signs of abnormal behavior.
- The IDS compares the network activity to a set of predefined rules and patterns to identify any activity that might indicate an attack or intrusion.
- If the IDS detects something that matches one of these rules or patterns, it sends an alert to the system administrator.
- The system administrator can then investigate the alert and take action to prevent any damage or further intrusion.

SQL Injection

SQL injection is a code injection technique that might destroy your database.

SQL injection is one of the most common web hacking techniques.

SQL injection is the placement of malicious code in SQL statements, via web page input.

What is SQL Injection?

- SQLi or SQL Injection is a web page vulnerability that lets an attacker make queries with the database.
- Attackers take advantage of web application vulnerability and inject an SQL command via the input from users to the application.
- Attackers can SQL queries like SELECT to retrieve confidential information which otherwise wouldn't be visible.
- SQL injection also lets the attacker to perform a denial-of-service (DoS) attacks by overloading the server requests.