Parul®
University

Database Management System

Mr. Parth R Singh, Assistant Professor
Computer Science & Engineering

CHAPTER-5

Database Security

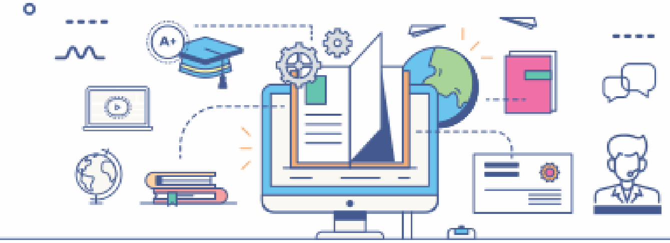
Data Security

- It is protecting data from unauthorized access or allowing only authorized access.
- Only DBA is allowed to access any data or update any data while other users are permitted to access any record or update any data according to their relevance or authority level.

Authentication

- Process of using credentials for validating user
- Its main objective is to provide security and integrity control to data

  - Integrity : It is all about validity of data either to make sure data is not corrupt and incorrect
  - Security : It is to protect data and making sure data access is to only those who are allowed to access that data.



Authorization

- Process of validation the access of the user for any data.
- It checks what data a particular user can access for example accessing a file from hard disk
- It ensures data privacy as well as access control of data.

Access Control

- Access control is a strategy for ensuring that clients are who they state they are and that they have the fitting access to data.

- There are mainly three access control model
- That is DAC,MAC, RBAC

DAC : Discretionary access control

- Here the data access control is availed by the user who has created that data either the owner of particular data.

- Here single user can have multiple permission and multiple users can have same permission all according to the owner of the data often referred as object.

- Discretionary access control is supported by SQL with help of following two command:

  1) Grant :- It is used to assign specific access to any user. Syntax:- GRANT privilege ON object TO user [WITH GRANT OPTION]

  2) Revoke :- It is used to remove any permission from the user. Syntax:- REVOKE privilege ON object FROM user {RESTRICT/CASCADE}

MAC: Mandatory Access Control

- Here individual access is not assigned.

- The access permission are bifurcated into particular levels according to sensitivity or importance of data for the respective organization.

- The users are also divided into several groups which has different clearance by which they can access the data of different levels

- Higher the clearance level more levels of data can be accesed.

MAC: Mandatory Access Control

- Four Components for implement multilevel Mandatory access control.

1. Subjects

1. Objects

1. Clearance Level

1. Security Level

MAC: Mandatory Access Control

- Database management system determines which user can read or do write operation based on some object rule.

- These rule make sure that sensitive data are protected and are not received by unwanted entities

- User Can Access data by following two rules :-
  1) Security Property
  2) Star Security Property

RBAC:- Role Based Access Control

- In this model role of user in an organization plays an important role to define the access to the data.
- Roles in this model defines access level of a employee have to the network.
- User is allowed to access only those data which is needed to perform his duties effectively.
- Factors on which access may be based: Authority, Responsibility, Job Competency

Intrusion Detection System

- An Intrusion Detection System (IDS) is a system or programming application that screens network traffic or system for dubious action or strategy infringement and issues alarms at the point when such action is found.

- It is a software application that scans a network or a system for hurtful movement or strategy breaking.

- Any malicious endeavor or infringement is typically revealed either to a head or gathered centrally utilizing a security information and event management (SIEM) system.

SQL Injection

- Also known as SQLI
- Its an common attack done on any database using SQL CODE which manipulates the background code of any database and reveals sensitive or un intended data.
- This Reveal data can be any costly or private data like user profiles, customers detail etc.
- A successfully implemented attack may result in alteration of data or deletion of entire tables or acquiring administrative rights to database etc. which all are highly hazardous to any organization.

Data Encryption

- Its an way to achieve data security by encoding the data so that even if unintended access is done data remains useless for the unauthorized user.
- Here some encryption algorithm is used to encode the data and this encoded data is known as cipher text.
- Basically its an process that only authorized user are only able to read it and its unreadable for unauthorized user.

Data Decryption

- It’s a process to decrypt the cipher text rather saying converting unreadable text to readable or original data.

- As for encryption algorithm is used similarly the same algorithm is designed to decrypt the cipher text in to original data

Types of encryption

- Mainly two types of encryption :

  1) Symmetric key encryption / Private key encryption

  2) Asymmetric key encryption / Public key encryption

Types of encryption

- Symmetric Key Encryption:-
  - Encryption and decryption key are same.
  - Sender an receiver need to share the key securely.

- Asymmetric Key Encryption:-
  - Encryption and decryption key are different.
  - Encryption is done by the public key of the receiver by the sender.
  - While decryption is done by the receiver by its own private key.

DIGITAL LEARNING CONTENT

Parul® University