Mục Lục

[Câu 1: Các mối đe dọa có thể đến với CSDL là gì? Nêu đặc điểm của hệ thống](#_bookmark0) [dựa trên multilevel security 4](#_bookmark0)

[Câu 1.2 Các mối đe dọa, các tấn công có thể đến với CSDL là gì? 5](#_bookmark1)

[Câu 2: Tìm hiểu các cấu hình xử lý CSDL (CSDL tập trung, phân tán, client/server).](#_bookmark2) [Các cấu hình này được áp dụng như thế nào trong thực tế 6](#_bookmark2)

[Câu 3: Các bước thiết kế CSDL. Học và viết chính xác các câu lệnh SQL cơ bản](#_bookmark3) [trong quá trình thiết kế CSDL 8](#_bookmark3)

[Câu 4: Khi cần thiết kế một CSDL an toàn phải đưa ra được các giải pháp an](#_bookmark4) [toàn cho bài toán đó. 9](#_bookmark4)

[Câu 5: Trình bày về SQL. Các câu lệnh SQL cơ bản 11](#_bookmark5)

[Câu 6: Các yêu cầu bảo vệ CSDL 12](#_bookmark6)

[Câu 7: Một số phương pháp đảm bảo tính toàn vẹn dữ liệu (được tích hợp sẵn](#_bookmark7) [trong các DBMS) 13](#_bookmark7)

[Câu 8: Tìm hiểu về transaction. Quá trình thực hiện 1 transaction. 14](#_bookmark8)

[Câu 9.1 Tìm hiểu những vấn đề cần thiết khi mã hóa CSDL (vấn đề mã hóa ở đâu,](#_bookmark9) [bảo vệ khóa, phân phối khóa như thế nào….) 14](#_bookmark9)

[Câu 9.2: Đặc điểm của kiểm soát truy nhập MAC và DAC trong cơ sở dữ liệu. Nêu](#_bookmark10) [sự khác nhau giữa chúng. Ứng dụng 2 chính sách này trong thực tế như nào? 15](#_bookmark10)

[Câu 10: Thế nào là mô hình an toàn? Sự khác nhau giữa mô hình an toàn và](#_bookmark11) [chính sách an toàn? Tìm hiểu mô hình an toàn Bell Lapadula. 17](#_bookmark11)

[Câu 11: Trình bày cơ bản một số phương pháp có thể bảo vệ CSDL trong hệ](#_bookmark12) [quản trị Oracle 18](#_bookmark12)

[Câu 12: Trình bày các lớp người dùng chính trong 1 hệ thống an toàn CSDL và](#_bookmark13) [vai trò của họ 20](#_bookmark13)

[Câu 13: Trình bày việc gán và thu hồi quyền trong MAC, DAC. 20](#_bookmark14)

[Câu 14: Trình bày mô hình RBAC 20](#_bookmark15)

[Câu 15: Trình bày mô hình system – R. Đặc biệt chú ý vấn đề thu hồi quyền đệ](#_bookmark16) [quy và không đệ quy 21](#_bookmark16)

[Câu 16: Nêu ví dụ về đặc quyền hệ thống (system prilvilege) và đặc quyền đối](#_bookmark17) [tượng (object privilega). Viết câu lệnh SQL cho các ví dụ đó. Nêu sự khác nhau](#_bookmark17) [giữa admin option và grant option. Ví dụ các câu lệnh SQL. 22](#_bookmark17)

[CHƯƠNG 3: AN TOÀN TRONG HỆ QUẢN TRỊ CƠ SỞ DỮ LIỆU 24](#_bookmark18)

[**Câu 17: tìm hiểu đặc điểm cơ bản của kiến trúc chủ thể tin cậy (trusted subject)**](#_bookmark19)[**và kiến thức Intergrity Lock. Đặc biệt chú ý kiến trúc Intergrity.** 24](#_bookmark19)

[**CHƯƠNG 4: AN TOÀN ỨNG DỤNG** 25](#_bookmark20)

[**Câu 18: Tìm hiểu kỹ thuật SQL Injection** 25](#_bookmark21)

[**CHƯƠNG 5: CƠ SỞ DỮ LIỆU THỐNG KÊ (SDB)** 26](#_bookmark22)

[**Câu 19: Cơ sở dữ liệu thống kê là gì? Viết các câu lệnh SQL cho các thống kê.**](#_bookmark23) **[Ứng dụng trong thực tế? Các dạng biểu diễn.](#_bookmark23)** [26](#_bookmark23)

[**Câu 20: Tìm hiểu các khái niệm cơ bản trong cơ sở dữ liệu thống kê** 27](#_bookmark24)

[**Câu 21: Thế nào là thống kê nhạy cảm? Cho ví dụ. Working knowledge và**](#_bookmark25)[**sumplementary knowledge?** 27](#_bookmark25)

[**Câu 22: Nêu cách thức tấn công của tấn công dựa vào trình theo dõi, tấn công**](#_bookmark26)[**dựa vào hệ tuyến tính. Cho ví dụ.** 28](#_bookmark26)

[**Câu 23: Các kỹ thuật tấn chống suy diễn trong cơ sở dữ liệu thống kê. Nêu ưu,**](#_bookmark27)[**nhược điểm của từng phương pháp.** 29](#_bookmark27)

[**Câu 24:Tại sao phải bảo vệ CSDL. Những vấn đề cần giải quyết khi mã hóa**](#_bookmark28)[**CSDL. Nhận xét so với các phương pháp bảo vệ khác** 31](#_bookmark28)

[**Câu 25: Địa chỉ rào là gì. Ưu- nhược điểm** 32](#_bookmark29)

[**Câu 26: Tái định vị? Tái định vị động – tĩnh có thể thực hiện trong những thời**](#_bookmark30)[**điểm nào.** 33](#_bookmark30)

[**Câu 27:Tìm hiểu 2 cơ chế phân trang, phân đoạn và so sánh (vẽ hình) . Thế nào**](#_bookmark31)[**là phân mảnh nội vi, phân mảnh ngoại vi. Ví dụ.** 34](#_bookmark31)

[**Câu 28: So sánh hệ thống HIDS(máy trạm) và NIDS(mạng)** 35](#_bookmark32)

[**Câu 29:Trình bày 2 mô hình phát hiện xâm nhập trong IDS. Nêu ưu-nhược điểm**](#_bookmark33)[**từng mô hình. Cho ví dụ.** 36](#_bookmark33)

[GHÉP THÊM 37](#_bookmark34)

[Câu 30: Nêu định nghĩa về ngôn ngữ DDL và ngôn ngữ DML. Cho ví dụ? 37](#_bookmark35)

[Câu 31: Tại sao phải bảo vệ cơ sở dữ liệu? Nêu một số hiểm họa tấn công CSDL 38](#_bookmark36)

[**Câu 32: Phân biệt các khái niệm và thuật ngữ sau : DBMS, SQL, PL/SQL, SQL**](#_bookmark37)[**Server, My SQL** 38](#_bookmark37)

[Câu 33: Cơ sở dữ liệu thống kê là gì? Phân biệt cơ sở dữ liệu thống kê với cơ sở dữ](#_bookmark38) [liệu thường? 39](#_bookmark38)

[**Câu 34: Mô hình an toàn là gì? Thế nào là hệ thống Multi-level Security? Hai**](#_bookmark39)[**chính sách MAC và DAC có dùng cho hệ thống Multi-level không?** 39](#_bookmark39)

[Câu 35: Những vấn đề cần giải quyết khi mã hóa CSDL. 40](#_bookmark40)

[Câu 36 : Hãy mô tả phương pháp kiểm soát dựa vào hạn chế kích cỡ tập truy vấn của](#_bookmark41) [một cơ sở dữ liệu thống kê, cho ví dụ.(q(C), X(C), |X(C)|) 40](#_bookmark41)

[Câu 37: Hãy nêu một số phương pháp có thể áp dụng để bảo mật cơ sở dữ liệu trong](#_bookmark42) [hệ quản trị Oracle 41](#_bookmark42)

[**Câu 38: Nêu ví dụ về đặc quyền hệ thống (system prilvilege) và đặc quyền đối**](#_bookmark43)[**tượng (object privilega). Viết câu lệnh SQL cho các ví dụ đó. Nêu sự khác nhau**](#_bookmark43)[**giữa admin option và grant option. Ví dụ các câu lệnh SQL** 42](#_bookmark43)

[Câu 39: Mô tả chính sách DAC, trong DAC ai là người có thẩm quyền cao nhất để](#_bookmark44) [trao quyền trên một đối tượng cơ sở dữ liệu? 43](#_bookmark44)

[**Câu 40: Thực hiện các thiết kế an toàn. Các bước để thiết kế cơ sở dữ liệu (mô**](#_bookmark45)[**tả)** 43](#_bookmark45)

## Câu 1: Các mối đe dọa có thể đến với CSDL là gì? Nêu đặc điểm của hệ thống dựa trên multilevel security

* Các mối đe dọa có thể đến với CSDL là những hiểm họa có thể được xác định khi đối phương sử dụng các kỹ thuật đặc biệt để tiếp cận nhằm khám phá, sửa đổi trái phép thông tin quan trọng do hệ thống quản lý.
  + Những mối đe dọa có thể xuất phát từ nhiều nguyên nhân: ngẫu nhiên hay có chủ ý.
  + Xâm phạm : đọc, sửa, xóa dữ liệu trái phép
    - Khai thác trái phép thông qua suy diễn thông tin được phép
    - Sửa đổi dữ liệu trái phép
    - Từ chối dịch vụ hợp phép ( DoS)
* Hiểm họa ngẫu nhiên:
  + Các thảm họa trong thiên nhiên.
  + Các lỗi phần cứng hay phần mềm có thể dẫn đến việc áp dụng các chính sách an toàn thông tin không đúng.
  + Các sai phạm vô ý do con người gây ra.
* Hiểm họa có chủ ý:
  + Người dùng hợp pháp: lạm quyền, sử dụng vượt mức quyền hạn cho phép.
  + Người dùng truy nhập thông tin trái phép, có thể là người ngoài tổ chức hoặc bên trong tổ chức: tấn công, phá hoại, leo thang đặc quyền.
* Đặc điểm của hệ thống dựa trên multilevel security- MLS:

+ Định nghĩa: Là hệ thống an toàn nhiều mức, mỗi chủ thể và đối tượng trong đó đều được gán nhãn an toàn thể hiện mức độ nhạy cảm của các chủ thể và các đối tượng đó.

+ Đặc điểm:

* + Mục đích: Phân tách dl theo mức phân loại an toàn của bản thân dl để đảm bảo tính bí mật. Thường áp dụng trong các lĩnh vực quân sự.
  + Trong hệ thống MLS các đối tượng đều được gán một lớp phân loại và mọi chủ thể đều có một mức độ mật. Được quy định bởi nhãn, nhãn bao gồm hai thành phần: mức nhạy cảm của dl và hạng mục.
  + Cơ sở dữ liệu đa mức: là cơ sở dữ liệu mà người dùng và dữ liệu được chia thành các mức an toàn khác nhau (không phân lớp – U, mật là C, tuyệt mật là S, tối mật là TS)
  + Chủ thể khi truy cập bị giới hạn bởi những điều khiển truy nhập bắt buộc là “not read up, not write down” theo mô hình Bell Lapadula.

Vd : Mô hình Bell-Lapadula.

write only read/write read only read only

ư

File A Label: Unclassified

File C Label: Confidential

File B Label: secret

File A Label: Top secret

Process Label: secret

## Câu 1.2 Các mối đe dọa, các tấn công có thể đến với CSDL là gì?

* Các mối đe dọa có thể đến với CSDL là những hiểm họa có thể được xác định khi đối phương sử dụng các kỹ thuật đặc biệt để tiếp cận nhằm khám phá, sửa đổi trái phép thông tin quan trọng do hệ thống quản lý.
  + Những mối đe dọa có thể xuất phát từ nhiều nguyên nhân: ngẫu nhiên hay có chủ ý.
  + Xâm phạm : đọc, sửa, xóa dữ liệu trái phép
    - Khai thác trái phép thông qua suy diễn thông tin được phép
    - Sửa đổi dữ liệu trái phép
    - Từ chối dịch vụ hợp phép ( DoS)
* Hiểm họa ngẫu nhiên:
  + Các thảm họa trong thiên nhiên.
  + Các lỗi phần cứng hay phần mềm có thể dẫn đến việc áp dụng các chính sách an toàn thông tin không đúng.
  + Các sai phạm vô ý do con người gây ra.
* Hiểm họa có chủ ý:
  + Người dùng hợp pháp: lạm quyền, sử dụng vượt mức quyền hạn cho phép.
  + Người dùng truy nhập thông tin trái phép, có thể là người ngoài tổ chức hoặc bên trong tổ chức: tấn công, phá hoại, leo thang đặc quyền.

## + Các tấn công vào cơ sở dữ liệu (database attacks):

* Excessive privileges(đặc quyền quá lớn) : là lỗi gán quyền vượt qua chức năng, nhiệm vụ của người dùng .
* Privilege abuse (lạm dụng quyền): Dùng quyền được cho để sao chép hay bán dữ liệu bất hợp pháp.
* Unauthorized privilege elevation (nâng quyền bất hợp pháp) : attacker chiếm được 1 tài khoản user hợp pháp lợi dụng các stored procedure và weak function để leo thang lên các quyền quản trị cao hơn.
* Platform vulnerabilities : tấn công hệ điều hành để chiếm quyền điều khiển.
* Tấn công SQL Injection: kỹ thuật lợi dụng điểm yếu của nhập input, khi attacker đăng nhập vào tài khoản thì sẽ chèn kí tự đặc biệt nhằm đăng nhập trái phép trong trường hợp xấu nhất có thể vào đúng tài khoản admin từ đó có quyền quản trị website.
* Weak audit (kiểm toán yếu): hệ thống không thể ghi lại đầy đủ những hành động của attacker, dẫn đến việc không thể phát hiện và ngăn chặn kịp thời những hành động tấn công của attacker.
* Denial of service (từ chối dịch vụ): là một loại tấn công trong đó các truy nhập của người dùng hợp pháp vào các ứng dụng mạng hay vào dữ liệu sẽ bị từ chối.
* Database protocol vulnerabilities: lỗ hổng giao thức cơ sở dữ liệu.
* Weak authentication: xác thực yếu, kẻ tấn công tấn công tìm kiếm mật khẩu bằng tấn công từ điển hoặc vét cạn.
* Exposure of backup data (lộ dữ liệu dự phòng)

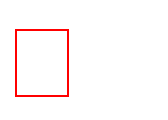
## Câu 2: Tìm hiểu các cấu hình xử lý CSDL (CSDL tập trung, phân tán, client/server). Các cấu hình này được áp dụng như thế nào trong thực tế.

Có 3 thành phần trong mô hình xử lý CSDL: ứng dụng, hệ quản trị CSDL (DBMS), cơ sở dữ liệu.

Có 3 mô hình:

Mô hình CSDL tập trung Mô hình CSDL phân tán

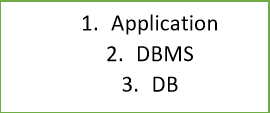
Mô hình CSDL Client/Server

Mô hình CSDL tập trung: cả 3 thành phần là ứng dụng, DBMS, DB cùng nằm chung trên 1 máy.

+ ưu điểm: dễ triển khai, xử lý nhanh, tiết kiệm chi phí.

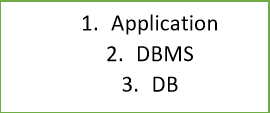
+ nhược: - chỉ áp dụng cho các cá nhân, tổ chức nhỏ, ít dữ liệu

- không lưu trữ nhiều; nếu một máy hỏng thì mất toàn bộ dữ liệu; không lưu trữ khi có nhiều dự án.

+ mô hình:

Mô hình CSDL phân tán: Bao gồm 1 server được kế nối tới nhiều máy tính. Mỗi máy tính chứa DB riêng vsà có một DBMS. Khi máy chủ cần truy xuất dữ liệu, nó sẽ gọi đến các máy tính con, yêu cầu cần quá trình đồng bộ dữ liệu.

* Ưu điểm: lưu trữ nhiều; 1 máy hỏng thì dữ liệu không bị mất; lưu trữ khi đang ở nhiều địa điểm khác nhau.
* Nhược điểm: chi phí cao, khó quản lý, đồng bộ dữ liệu khó khăn.
* Mô hình được áp dụng phù hợp cho các công ty có nhiều chi nhánh khác nhau.
* Mô hình:



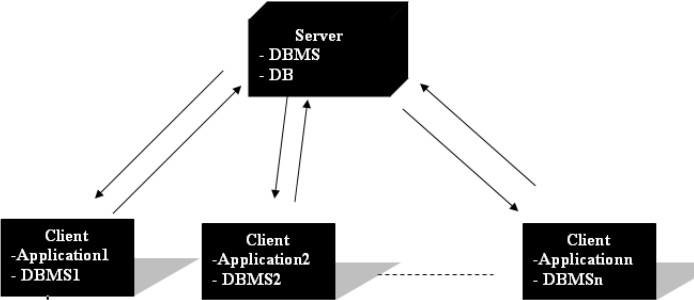
 ………….

Mô hình CSDL client/server: bao gồm một máy chủ server và các máy trạm. Dữ liệu và hệ quản trị cơ sở dữ liệu nằm trên máy chủ, các thành phần ứng dụng làm trên các client.

- Ưu điểm: xử lý nhanh, có thể truy xuất dữ liệu từ xa, phù hợp với các mô hình hệ thống hiện nay.

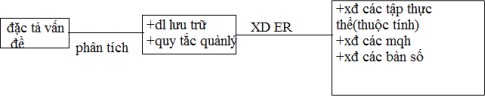
Mô hình:

* Nhược điểm: nếu server sập hay bị tấn công thì toàn bộ dữ liệu sẽ bị mất, dễ bị quá tải vì vậy dễ bị tấn công từ chối dịch vụ.



## Câu 3: Các bước thiết kế CSDL. Học và viết chính xác các câu lệnh SQL cơ bản trong quá trình thiết kế CSDL

* + Các bước thiết kế CSDL:
    - Bước 1: đặc tả vấn đề
      * Phân tích đặc tả để xác định dữ liệu yêu cầu và mối liên quan giữa chúng để xây dựng mô hình thực thể kết hợp.
* Bước 2: Mô hình thực thể kết hợp (ER)
  + Áp dụng quy tắc biến đổi thực thể kết hợp thành CSDL
* Bước 3: Lược đồ CSDL (bảng và mối quan hệ)
  + Các thành phần trong mô hình ER:
* Thực thể, tập thực thể, loại thực thể
* Thuộc tính
* Mối quan hệ, loại mối quan hệ, bản số của mối quan hệ
  + Thực thể: danh từ biểu diễn = hcn
  + Loại thực thể: khái niệm chỉ thực thể giống nhau, có chung 1 số thuộc tính, biểu diễn hình https://lh5.googleusercontent.com/-lMh9tCXyXPwPe3XwbQb_ZSKQZ-mMei-lrN8jLfz3QeVMFQnqQDTh7VR2OlgDsFCkhhO1Vc8K7sqrRizHctywnLtML95szRhVR-bP2j2KLpHfWUQMx_TWYizBkgJmXpVZd4_V6s và được gạch chân
  + Loại thuộc tính: quan trọng nhất là thuộc tính khóa
  + Mối quan hệ: thể hiện sự liên hệ giữa các thực thể, biểu diễn https://lh4.googleusercontent.com/AMBxR84JosquVVi2loNS0IripdL7exbSrDb_-IEDtCN1tPwu57TJQCQ2j79bLPMDkgQZEESzvNTuZbUYs5TUwl65j3QX0CBqFutcn7ApD9XNGI7KYGuEkgVMQjucc229dn1rmMw
  + Bản số của mối quan hệ: 1:1, 1:N, N:N -> biểu thị số thực thể tối thiểu và tối đa xuất hiện ứng với thực thể bên kia .
  + Xây dựng mô hình ER :



* + Biến đổi từ ER sang mô hình quan hệ Mô hình ER

Một tập thực thể một lược đồ quan hệ

Mỗi thuộc tính một thuộc tính

Mỗi thuộc tính nhận diện khóa chính

Mỗi mối kết hợp khóa ngoại hoặc lược đồ quan hệ mới

* + Một số câu lệnh SQL cơ bản trong quá trình thiết kế CSDL:
    - Tạo bảng ( Creat)

Creat table NhanVien( MaNV int notnull, TenNV varchar(100), DiaChi varchar(100),

);

* Lệnh ALTER (thay đổi)

Alter table NhanVien ADD email varchar(30)

* Lệnh DROP (xóa hoàn toàn bảng và dữ liệu) DROP table NhanVien
* Select ( chọn)

Select \* From NhanVien Where MaNV=03;

* Insert ( thêm bản ghi )

Insert into NhanVien Values ( 04, ‘Thanh’, ‘Hung Yen’);

+ Update (Cập nhật)

UPDATE NHANVIEN SET DIACHI = 'Hanoi' WHERE ID = 3;

+ Delete: ( xóa dữ liệu)

Delete From NhanVien Where MaNV =01;

## Câu 4: Khi cần thiết kế một CSDL an toàn phải đưa ra được các giải pháp an toàn cho bài toán đó.

Có 5 bước thiết kế một CSDL an toàn:

Bước 1. Phân tích sơ bộ

         + Đánh giá các rủi ro

         + Ước lượng các chi phí thiết kế

    + Phát triển các ứng dụng cụ thể nào

Bước 2. Các yêu cầu và các chính sách an toàn

* *Phân tích yêu cầu****:***

***+*** Phân tích giá trị : xác định mức nhạy cảm của dữ liệu.

***+*** Nhận dạng đe doạ/phân tích điểm yếu

***+***Phân tích và đánh giá rủi ro: khả năng xảy ra của các biến cố không mong muốn và tác động của chúng.

***+*** Xác định yêu cầu bảo vệ

* *Lựa chọn chính sách:*

+ Chính sách là các quy tắc ở mức cao, bắt buộc phải tuân theo trong các quá trình thiết kế, thực thi và quản lý hệ thống an toàn.

+ Định nghĩa các chế độ truy nhập (đọc, ghi) của chủ thể vào các đối tượng của hệ thống

Bước 3. Thiết kế khái niệm

* Xây dựng mô hình E-R: Vẽ các thực thể và mối quan hệ

giữa các thực thể đó.

Bước 4. Thiết kế lôgíc

* Xây dựng các lược đồ cơ sở dữ liệu ( là các bảng và các

thuộc tính của chúng)

Bước 5. Thiết kế vậy lý

       - Thiết kế thật sự vào hệ thống

## Câu 5: Trình bày về SQL. Các câu lệnh SQL cơ bản

* + SQL (Structured Query Language) là ngôn ngữ truy vấn dữ liệu: là một chuẩn của ANSI (America National Standard Institute) về truy xuất các hệ thống CSDL.
  + SQL cho phép truy cập CSDL và thực hiện các thao tác như : lấy dữ liệu, chèn, xóa, sửa, …
    - Có thể thực thi các câu lệnh SQL trên CSDL như: select, insert, update, delete…
    - SQL hoạt động hầu hết với các chương trình CSDL như MS Acsess,

Oracle, SQL server, My SQL…

* + - SQL có các ngôn ngữ con sau:
      * Ngôn ngữ định nghĩa dữ liệu (DDL): là ngôn ngữ máy tính để định nghĩa lược đồ CSDL. ( creat, alter, drop table ( index- chỉ mục))
      * Ngôn ngữ thao tác dữ liệu (DML): là họ các ngôn ngữ máy tính được người dùng sử dụng để tìm kiếm, chèn, xóa, cập nhật dữ liệu cho 1 CSDL.(select, insert,update, delete)
      * Ngôn ngữ điều khiển dữ liệu (DCL): sử dụng hai từ khóa là GRANT, REVOKE.
      * Ngôn ngữ hỏi (QL): chính là câu lệnh Select trong DML. Các câu lệnh cơ bản trong SQL”
* create database: tạo cơ sở dữ liệu create database hososinhvien
* Create table: tạo bảng create table SinhVien (MaSV int,TenSV varchar(50)
* Alter table : sửa đổi cấu trúc 1 bảng alter table SinhVien add QueQuan int
* Drop table: xóa bảng drop table SinhVien
* Select: chọn dl từ csdl select \* from sinhvien
* Insert: chèn dữ liệu

INSERT INTO sinhvien VALUES(1,’Thanh’);

* Update

UPDATE sinhvien SET ten = ‘Kem’ where masv = 1;

* Delete

delete from sinhvien where masv =1; xóa 1 bản ghi

## Câu 6: Các yêu cầu bảo vệ CSDL

Có 10 yêu cầu bảo vệ CSDL:

* + Bảo vệ chống truy nhập trái phép:
    - Chỉ trao quyền cho những người dùng hợp pháp.
    - Việc kiểm soát truy nhập cần tiến hành trên các đối tượng dữ liệu ở mức thấp hơn file: bản ghi, thuộc tính, giá trị.
  + Bảo vệ chống suy diễn: Suy diễn là khả năng có được các thông tin bí mật từ các thông tin không bí mật (công khai).
  + Bảo vệ toàn vẹn CSDL:
    - Bảo vệ cơ sở dữ liệu khỏ những người dùng không hợp pháp, tránh sửa đổi nội dụng dữ liệu trái phép.
    - Hệ quản trị cơ sở dữ liệu kiểm soát bằng các ràng buộc dữ liệu, thủ tục sao lưu, phục hồi, các thủ tục an toàn đặc biệt, file nhật ký.
    - Một số phương pháp bảo vệ toàn vẹn dữ liệu như: kiểu dữ liệu, không cho phép định nghĩa null, định nghĩa mặc định, các thuộc tính định danh, các ràng buộc, các quy tắc, triggers, các chỉ mục.
  + Toàn vẹn dữ liệu thao tác:
    - Yêu cầu đảm bảo tính tương thích logic của dữ liệu khi có nhiều giao tác thực hiện đồng thời.
    - Một giao dịch (transaction): là một loạt các hoạt động xảy ra được xem như 1 đơn vị công việc nghĩa là hoặc thành công toàn bộ hoặc không làm gì cả.
  + Toàn vẹn ngữ nghĩa của dữ liệu:
    - Yêu cầu này đảm bảo tính tương thích logic của các dữ liệu thay đổi, bằng cách kiểm tra các giá trị dữ liệu có nằm trong khoảng cho phép hay không (đó là các ràng buộc toàn vẹn).
    - Ràng buộc là những thuộc tính mà ta áp đặt lên một bảng hay một cột để tránh việc lưu dữ liệu không chính xác vào CSDL.
    - Các ràng buộc bao gồm: ràng buộc khóa chính, ràng buộc khóa ngoại, ràng buộc kiểm tra.
  + Khả năng lưu vết và kiểm tra:
    - Bao gồm khả năng ghi lại mọi truy nhập tới dữ liệu (các phép toàn read, write).
    - Đảo bảo tính toàn vẹn dữ liệu vật lý, trợ giúp cho việc phân tích dãy truy nhập vào CSDL.
  + Xác thực người dùng:
    - Xác định tính duy nhất của người dùng. Dịnh danh người dùng làm cơ sở cho việc trao quyền. Người dùng được phép truy nhập dữu liệu khi được hệ thống xác thực là hợp pháp.
  + Bảo vệ dữ liệu nhạy cảm:
    - Dữ liệu nhạy cảm là những dữ liệu không nên đưa ra công bố công khai.
    - Kiểm soát truy nhập vào các CSDL bao hàm: bảo vệ tính tin cậy của dữ liệu nhạy cảm, chỉ cho phép người dùng hợp pháp truy nhập. Người dùng được trao quyền trên các dữ liệu này không được phép lan truyền chúng.
  + Bảo vệ nhiều mức:
    - Dữ liệu được phân loại thành nhiều mức nhạy cảm.
    - Mục đích: phân loại các mục thống tin khác nhau, đồng thời phân quyền cho các mức truy nhập khác nhau vào các mục riêng biệt.
  + Sự hạn chế:
    - Tránh chuyển các thông tin không mong muốn giữa các chương trình trong hệ thống.
    - Kênh được cho phép cung cấp thông tin qua các hoạt động được phép: soạn thảo, biên dịch 1 file.

## Câu 7: Một số phương pháp đảm bảo tính toàn vẹn dữ liệu (được tích hợp sẵn trong các DBMS)

* + Một số phương pháp đảm bảo tính toàn vẹn dữ liệu tích hợp trong các DBMS là:
    - Kiểu dữ liệu: ví dụ bạn khai báo kiểu dữ liệu của một cột là Integer thì bạn không thể đưa giá trị thuộc dạng String vào được.
    - Không cho phép định nghĩa NULL: khi được định nghĩa ràng buộc này sẽ không được lưu trữ một giá trị không xác định. Tất cả các trường kháo chính phải thỏa mãn điều kiện này.
    - Định nghĩa mặc định: Nếu một cột được cho một giá trị default thì khi bạn không nhập vào một giá trị cụ thể thì SQL Server sẽ nó dùng giá trị mặc định này. Bạn phải dùng Default đối với đặt Not Null.
    - **Thuộc tính định danh (Identity properties)**: dữ liệu thuộc dạng ID sẽ đảm bảo tính duy nhất của dữ liệu trong bảng dữ liệu.
    - Các ràng buộc: là những quy luật mà ta áp đặt lên một cột để đảm bảo tính chính xác của dữ liệu được nhập vào . có các loại ràng buộc khóa chính, ràng buộc khóa ngoại, ràng buộc kiểm tra.
    - Các quy tắc **(Rules)**: là một đối tượng tương đương với CHECK Constraint nhưng chỉ có thể có một rule cho một cột.
    - Triggers. Một loại *stored procedure* đặc biệt được thực thi một cách tự động khi một bảng được Update, Insert hoặc Delete.
    - Các chỉ mục.(Indexes)

## Câu 8: Tìm hiểu về transaction. Quá trình thực hiện 1 transaction.

* + Transaction:
    - Transaction trong SQL là một đơn vị công việc hoặc 1 dãy công việc được thực hiện theo 1 thứ tự logic và hợp lý, có thể được thao tác bởi người dùng hoặc 1 DB program.
    - Transaction là một nhóm các câu lệnh SQL, xử lý có tuần tự các thao tác trên CSDL nhưng được xem như 1 đơn vị. Vì vậy một transaction sẽ không được coi như thành công nếu như trong quá trình xử lý có 1 thao tác trong nó không hoàn thành => giao dịch thất bại.
    - Transaction có 1 chuẩn gọi là ACID bao gồm 4 thuộc tính chuẩn:
      * Atomicity (tính tự trị): đảm bảo tata cả các thao tác, hành động trong phạm vị một đơn vị giao dịch là thành công hoàn toàn. Ngược lại transaction được coi là thất bại.
      * Consistency (tính nhất quán): đảm bảo tất cả các thao tác trên CSDL được thay đổi sau khi giao dịch thành công và không xảy ra lỗi.
      * Isolation (tính cô lập): đảm bảo transaction này hoạt động độc lập với transaction khác.
      * Durability (tính bền vững): đảm bảo kết quả hoặc tác động của transaction vẫn luôn tồn tại, kể cả khi hệ thống xảy ra lỗi.

Quá trình thực hiện 1 transaction:

* Bắt đầu transaction với câu lệnh: START TRANSACTION; BEGIN;

Lưu ý: nên sử dụng câu lệnh SET autocomit =0 trước khi bắt đầu transaction vì mặc định autocomit =1, transaction sẽ tự động hoàn thành mà không phải sử dụng comit hay rollback.

* Thông báo 1 hay nhiều lênh như SELECT, INSERT, UPDATE, DELETE sau khi bắt đầu transaction.
* Kiểm tra xem có lỗi nào hay không và mọi thứ có theo như yêu cầu của bạn hay không?
* Khi 1 transaction hoàn thành thì cần đưa ra câu lệnh COMIT để mọi hành động tác động đến table được thực sự thay đổi.
* Khi 1 transaction thất bại cần đưa ra câu lệnh ROLLBACK để hủy toàn bộ hành động, phục hồi dữ liệu về trạng thái trước khi bắt đầu transaction.

## Câu 9.1 Tìm hiểu những vấn đề cần thiết khi mã hóa CSDL (vấn đề mã hóa ở đâu, bảo vệ khóa, phân phối khóa như thế nào….)

+ Mã hóa lưu trữ:

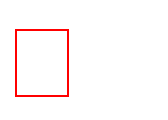
Để mã hóa dữ liệu trong các hệ thống con lưu trữ và do đó bảo vệ dữ liệu đầu cuối. Thích hợp cho mã hóa tệp hoặc toàn bộ thư mục trong hệ điều hành. Dùng các khóa mã hóa cho người dùng riêng biệt để sử dụng cơ sở dữ liệu.

+ Mã hóa cơ sở dữ liệu cho phép bảo mật dl khi nó được chèn vào hoặc được lấy ra từ csdl. Mã hóa có thể là một phần của thiết kế csdl và liên quan đến độ nhạy cảm dữ liệu hoặc đặc quyền của người dùng. Có thể mã hóa bảng, cột hay hàng. Khóa mã hóa phải được truyền hoặc giữ với dl được mã hóa trên phía máy chủ, do đó cung cấp sự bảo vệ hạn chế đối với quản trị viên máy chủ hoặc bất kỳ kẻ xâm nhập nào chiếm đoạt quyền người quản trị.

+ Mã hóa ứng dụng là di chuyển quá trình mã hóa hay giải mã tới tầng ứng dụng khi tạo, xử lý dữ liệu. Mã hóa hóa được thực hiện ở tầng ứng dụng sau đó lưu trữ dl đã mã hóa vào hệ cơ sở dl.

+ Cách bảo vệ khóa là lưu trữ các khóa trong một bảng hoặc tệp csdl bị hạn chế, có khả năng được mã hóa bằng khóa chính. Nhưng có vấn đề là tất cả quản trị có quyền truy cập đặc quyền cũng có thể truy cập các khóa này và giải mã mọi dữ liệu. Để khắc phục vấn đề này, các chipset mã hóa giả mạo chuyên dụng được gọi là module bảo mật phần cứng (HSM- Hardware Security Module), có thể được sử dụng để cung cấp lưu trữ bảo mật an toàn cho các khóa mã hóa. Nói chung, các khóa mã hóa được lưu trứ trên máy chủ được mã hóa bằng khóa chính được lưu trữ trong HSM. Tại thời điểm khi mã hóa hay giải mã, các khóa mã hóa được giải mã một cách tự động bằng HSM (sử dụng khóa chính) và xóa khỏi bộ nhớ máy chủ ngay khi các hoạt động mã hóa được thực hiện.

## Câu 9.2: Đặc điểm của kiểm soát truy nhập MAC và DAC trong cơ sở dữ liệu. Nêu sự khác nhau giữa chúng. Ứng dụng 2 chính sách này trong thực tế như nào?

Kiểm soát truy nhập tùy ý DAC:

* Kiểm soát truy nhập dựa trên định danh của chủ thể hoặc định danh nhóm.
* Chỉ rõ đặc quyền mà mỗi chủ thể có thể có được trên các đối tượng và trên hệ thống.
* Các yêu cầu truy nhập được kiểm tra, thông qua 1 cơ chế kiểm soát tùy ý, truy nhập chỉ được trao cho các chủ thể thỏa mãn các quy tắc cấp quyền của hệ thống.
* Được định nghĩa trên 1 tập :

Các đối tượng an toàn Các chủ thể an toàn

Các đặc quyền truy nhập

* Gán/ thu hồi quyền là tùy ý: chủ thể với 1 số quyền nhất định có thể chuyển quyền của mình cho chủ thể khác (có thể gián tiếp).
* Việc gán và thu hồi quyền là tùy ý do những người dùng này. o Được biểu diễn bởi ma trận truy nhập (ACM).
* Ưu điểm: là kỹ thuật phổ biến, chỉ có một vài vấn đề nghiên cứu mở.

Hầu hết các hệ quản trị thương mại đều hỗ trợ nó như Access, Oracle…

* + dễ thực hiện, hệ thống linh hoạt
* Nhược điểm: Khó quản lí việc gán/thu hồi quyền

Dễ lộ thông tin

Kiểm soát an toàn không tốt Kiểm soát truy nhập bắt buộc MAC:

* Được áp dụng cho các thông tin có yêu cầu bảo vệ nghiêm ngặt.
* Hoạt động trong hệ thống mà dữ liệu hệ thống và ng dung đc phân loại rõ ràng
* Hạn chế truy nhập của các chủ thể vào các đối tượng bằng cách sử dụng các nhãn an toàn (label).
* Cơ chế kiểm soát: dữ liệu được phân loại theo độ mật. Các chủ thể được cấp nhãn truy nhập. Chủ thể chỉ được phép truy nhập đến những dữ liệu có độ mật tương đương với nhãn truy nhập hoặc thấp hơn.
* Lớp an toàn = (Mức nhạy cảm, vùng ứng dụng) Mức nhạy cảm: thành phần phân cáp

Vùng ứng dụng: tp không phân cấp

trong quân sự : có 4 mức nhạy cảm : U,C,S,TS trong thương mại : có 3 mức : U, S, HS

trong Oracle: mỗi lớp an toàn xác định =1 nhãn .

Label = (Level, Compartment, Group)

Level: tp bắt buộc : phân cấp, thể hiện mức nhạy cảm Compartment ( tùy chọn): không phân cấp, dùng phân loại dl Group (tùy chọn) : phân cấp, phân loại ng dùng

* Ưu điểm: độ an toàn cao vì sử dụng các nhãn an toàn, phù hợp với các môi trường đòi hỏi độ an toàn cao như quốc phòng, quân sự. Khác phục được hạn chế của DAC trong vấn đề trao quyền.
* Nhược điểm: phức tạp.

Thiếu kỹ thuật gắn nhãn an toàn tự động.

Không giải quyết được hoàn toàn tấn công trojan horse. Giảm tính linh hoạt hệ thống

Ng dung k đc phép thay đổi quyền

|  |  |
| --- | --- |
| MAC  -Kiểm soát quyền dựa vào các nhãn an toàn gắn với chủ thể và đối tượng  -Việc gán/thu hồi quyền chỉ do 1 nhân viên an toàn  -User không thể thay đổi nhãn hay quyền  -Dùng cho các hệ thống yêu cầu bảo vệ nghiêm ngặt(quân sự),.  -Độ an toàn cao nhưng phức tạp | DAC  -Kiểm soát quyền dựa trên quyền sở hữu đối tượng.  -Việc gán/thu hồi quyền là tùy ý với những chủ thể có đặc quyền.  -User có thể thay đổi quyền tùy vào đặc quyền của người dùng.  -Dùng được cho mọi hệ thống.  -Linh hoạt, độ an toàn không cao |

Ứng dụng 2 chính sách trong thực tế:

MAC: Không phải hệ quản trị nào cũng có, chỉ có Oracle ,DB2, Sybase

DAC: hầu hết các hệ quản trị thương mại đều hỗ trợ : Access, SQL, SQL Server, Oracle,

…

## Câu 10: Thế nào là mô hình an toàn? Sự khác nhau giữa mô hình an toàn và chính sách an toàn? Tìm hiểu mô hình an toàn Bell Lapadula.

* + **Mô hình an toàn**: là một mô hình khái niệm mức cao, độc lập phần mềm và xuất phát từ các đặc tả yêu cầu của tổ chức để mô tả nhu cầu bảo vệ của một hệ thống.
  + **Chính sách an toàn:** là những phát biểu mức tổng quát và an toàn thông tin từ phía nhà quản lí
  + Sự khác nhau giữa mô hình an toàn và chính sách an toàn:

|  |  |
| --- | --- |
| Mô hình an toàn | Chính sách an toàn |
| Là mô hình khái niệm mức cao, độc lập phần mềm, xuất phát từ các đặc tả yêu cầu của tổ chức, mô tả nhu cầu bảo  vệ của một hệ thống. | Là các quy tắc, hướng dẫn ở mức cao, liên quan đến việc thiết kế và quản lý hệ thống trao quyền, là phát biểu mức tổng quát về ATTT của nhà quản lý. |
| Quan tâm đến 2 vấn đề: chủ thể và đối tượng. | Quan tâm đến 3 vấn đề: tính bí mật, tính toàn vẹn, tính sẵn sàng của dữ liệu. |
| Mô hình an toàn được xây dựng đầu tiên trong quá trình thiết kế hệ thống. | Chính sách an toàn được xây dựng từ mô hình an toàn. |

* + Mô hình Bell Paladula:
    - Xuất hiện năm 1975, do quân đội Mỹ.
    - Phù hợp sử dụng trong các hệ thống của quân đội, chính phủ.
    - Mục đích: đảm bảo tính bí mật.
    - Đây là mô hình chính tắc đầu tiên về điều khiển luồng thông tin.
    - Là mô hình tĩnh: mức an toàn (nhãn an toàn) không thay đổi.
    - Người dùng được phân mức độ an toàn, đối tượng được phân mức độ nhạy cảm.
    - Có hai quy tắc:

+ Not Read up: Một chủ thể S được phép truy cập đọc đến đối tượng O khi và chỉ khi Clear(S)>= Class(O).

=> Các chủ thể chỉ được đọc thông tin có mức nhạy cảm ngang hoặc thấp hơn mức an toàn mà nó được gán.

=> Không bị lộ thông tin cho những không được quyền truy xuất đến đối tượng đó.

+ Not write down: Một chủ thể S được phép ghi lên một đối tượng O khi Clear(S)<= Class(O).

=> Các chủ thể chỉ được ghi dữ liệu lên mức nhạy cảm ngang hoặc cao hơn mức an toàn mà nó được gán

=> tránh người dùng vô tình ghi dữ liệu mức cao xuống mức thấp => làm lộ thông tin.

* Ưu điểm: các nhãn an toàn của các chủ thể và các đối tượng không bao giờ được thay đổi trong suốt thời gian hệ thống hoạt động.
* Nhược điểm:
  + mới chỉ quan tâm đến tính bí mật
  + chưa chỉ ra cách thay đổi quyền truy nhập cũng như cách tạo và xóa các chủ thể cũng như đối tượng.

Được áp dụng vào cơ sở dữ liệu : Được áp dụng cho các thông tin có yêu cầu bảo vệ nghiêm ngặt. Mức an toàn quân sự , chính phủ

## Câu 11: Trình bày cơ bản một số phương pháp có thể bảo vệ CSDL trong hệ quản trị Oracle

* + Cơ sở dữ liệu riêng ảo (VPD - Virtual Private Database)
    - Là kiểm soát truy nhập mức mịn hay cơ chế an toàn mức hàng, cung cấp tính năng bảo mật mức hàng cho cơ sở dữ liệu.
    - Cung cấp giải pháp bảo mật tới mức mịn trực tiếp trên các table, view, synonym; gán trực tiếp các chính sách bảo mật lên các đối tượng cơ sở dữ liệu, các chính sách tự động được thực hiện mỗi khi người dùng truy nhập dữ liệu đến đối tượng đó.
    - Ưu điểm: chi phí thấp, trong suốt với người dùng, tăng cao cơ hội kinh doanh
  + An toàn dựa trên nhãn trong Oracle (OLS)
    - Cho phép bảo vệ dữ liệu của các bảng đến mức hàng, mức bản ghi.
    - Cho phép định nghĩa 1 chính sách an toàn được thực thi bằng cách gắn cho các bản ghi trong bảng bởi các nhãn an toàn, thể hiện quyền mà người dùng có thể đọc hay ghi dữ liệu lên các bản ghi.
    - Các tính năng của OLS:
      * Nhãn người dùng cung cấp thông tin về quyền hạn của người dùng.
      * Nhãn dữ liệu cho thấy độ nhạy cảm của thông tin trong hàng đó.
      * Chính sách đặc quyền của người dùng có thể cho phép bỏ qua 1 số khía cạnh của kiểm soát truy nhập dựa vào nhãn.
      * Tùy chọn thực thi chính sách của 1 bảng xác định các khía cạnh khác nhau về cách điều khiển truy nhập thực thi để đọc, ghi lên bảng đó.

Cơ chế kiểm toán mịn

* Cho phép giám sát và ghi lại việc truy nhập dữ liệu dựa trên nội dung của dữ liệu.
* Cho phép định nghĩa một chính sách kiểm toán trên một bảng và các cột tùy chọn.
* Cung cấp cơ chế điều khiển tốt hơn và mức chi tiết nhỏ hơn so với phương pháp kiểm toán thông thường như: kiểm toán câu lệnh, kiểm toán đặc quyền, kiểm toán đối tượng lược đồ.

Oracle Advanced Security

* Là cơ chế an toàn nâng cao trong Oracle, cho phép kiểm soát phòng ngừa, giúp giải quyết nhiều yêu cầu đặt ra, ngăn chặn các hành vi vi phạm dữ liệu, bảo vệ thông tin.
* Cung cấp tính riêng tư, tính toàn vẹn, xác thực, cấp quyền truy nhập với nhiều cách thức khác nhau.

Oracle secure backup (OSB)

* Cho phép bảo vệ dữ liệu đáng tin cậy thông quâ hệ thống tập tin sao lưu.
* Hỗ trợ băng từ, ổ địa, môi trường SAN…
* Là một phần của giải pháp lưu trữ Oracle, giảm tính phức tạp và giảm chi phí cho việc mua phần mềm bổ sung.
* Cung cấp khả năng mở rộng phân phối và khôi phục sao lưu dự phòng.
  + Một số phương pháp đảm bảo tính toàn vẹn dữ liệu tích hợp trong các DBMS là:
    - Kiểu dữ liệu.
    - Không cho phép định nghĩa NULL.
    - Định nghĩa mặc định( default).
    - **Thuộc tính định danh (Identity properties)**:
    - Các ràng buộc:
    - Các quy tắc **(Rules)**
    - Triggers.
    - Các chỉ mục.(Indexes)

## Câu 12: Trình bày các lớp người dùng chính trong 1 hệ thống an toàn CSDL và vai trò của họ

* + Các lớp người dùng chính trong 1 hệ thống an toàn CSDL:
    - Người quản lý ứng dụng: có trách nhiệm đối với việc phát triển và duy trì, hoặc các chương trình thư viện.

+ DBA: quản lý các lược đồ khái niệm và lược đồ bên trong của CSDL.

* Nhân viên an toàn: xác định xác quyền truy nhập, các tiên đề, thông qua các quy tắc trong một ngôn ngữ thích hợp: DDL hoặc DML.
* Kiểm toán viên: chịu trách nhiệm kiểm tra các yêu cầu kết nối và các câu hỏi truy nhập, nhằm phát hiện ra các xâm phạm quyền.

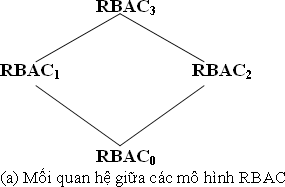
## Câu 13: Trình bày việc gán và thu hồi quyền trong MAC, DAC.

* + DAC
    - Trao truyền: việc trao quyền do người sở hữu đối tượng. Trong DAC có thể lan truyền quyền. Cần các cơ chế trao quyền phức tạp hơn, nhằm tránh mất quyền kiểm soát khi lan truyền quyền từ người trao quyền, hoặc những người có trách nhiệm khác. Ví dụ trong Oracle có grant option, admin option.
    - Thu hồi quyền: người dùng muốn thu hồi quyền phải có đặc quyền để thu hồi quyền. Trong Oracle nếu một người dùng có “grant option” thì người dùng đó có thể thu hồi quyền đã trao cho người khác.
  + MAC
    - Hệ thống được quản lý bởi 1 người quản trị viên trung tâm, gọi là người trao quyền. Người trao quyền sẽ kiểm soát toàn bộ hệ thống trao quyền.
    - Các chủ thể và đối tượng được gán các nhãn an toàn nhất định. Từ đó quy định chủ thể có những quyền gì đối với đối tượng.
    - Người dùng không thể trao hay thu hồi quyền được gán. Mọi sự thay đổi chỉ được phép khi có sự đồng ý của người trao quyền.

## Câu 14: Trình bày mô hình RBAC

* + Hầu hết các hệ quản trị cơ sở dữ liệu đều hỗ trợ RBAC. RBAC có thể dùng kết hợp với mô hình DAC hoặc MAC hoặc dùng độc lập.
  + RBAC được áp dụng vào đầu những năm 1970. Khái niệm chính của RBAC là những quyền hạn được liên kết với những vai trò (role).
  + Mục đích chính của RBAC là giúp cho việc quản trị an toàn một cách dễ dàng hơn.
  + RBAC có thể giới han trước các mối quan hệ vai trò – quyền hạn, làm cho việc gán người dùng đến các vai trò được xác định trước 1 cách dễ dàng hơn.
  + Vai trò (role) là một tập các quyền. RBAC thực hiện gán cho chủ thể một vai trò, khi đó chủ thể đó có mọi quyền thuộc vai trò đó.
  + Mô hình RBAC gồm 4 mô hình con là: RBAC0, RBAC1, RBAC2, RBAC3.
    - Mô hình nền tàng RBAC0 ở dưới cùng, là yêu cầu tối thiểu cho bất kỳ hệ thống nào có hỗ trợ RBAC.
    - Mô hình RBAC1, RBAC2 được phát triển từ mô hình RBAC0 nhữn có thêm các điểm đặc trưng cho từng mô hình. RBAC1 thêm vào khái niệm của hệ thống phân cấp vai trò. RBAC2 thêm vào các ràng buộc. RBAC1 và RBAC2 không liên quan đến nhau.
    - Mô hình RBAC3 là mô hình tổng hợp của 3 mô hình RBAC0, RBAC1, RBAC2.

**(Nếu yêu cầu vẽ thì mới vẽ)**



Mô hình RBAC gồm 4 mô hình: RBAC0 , RBAC1 , RBAC2 , RBAC3.

## Câu 15: Trình bày mô hình system – R. Đặc biệt chú ý vấn đề thu hồi quyền đệ quy và không đệ quy.

* + System R là một hệ quản trị CSDL quan hệ đầu tiên của IBM, dựa trên nguyên tắc cấp quyền quản trị cho người sở hữu.
  + Việc bảo vệ được thực hiện tại mức table:
    - Chủ thể: người dùng.
    - Đối tượng: các bảng và khung nhìn.
  + Các chế độ truy nhập vào một table:
* Read: đọc các bộ của 1 bảng. 1 user truy nhập read có thể định nghĩa các “views” trên table đó
* Insert: thêm các bộ vào bảng
* Delete: xóa các bộ trong bảng
* Update: sửa đổi các bộ có trong bảng
* Drop: xóa toàn bộ bảng
  + System R hỗ trợ quản trị quyền phi tập trung:
    - Người tạo ra bảng có mọi đặc quyền trên bảng đó và có thể trao/thu hồi (grant/revoke) quyền cho các user khác.
    - Điều này có thể không đúng với các khung nhìn.

+ Việc trao và thu hồi quyền của System R được thực hiện bằng các lệnh SQL.

* + Người tạo ra bảng có mọi đặc quyền trên bảng đó và có thể trao/thu hồi quyền cho các user khác, mỗi quyền là 1 bộ gồm:

<s, p, t, ts, g, go>

* s: chủ thể được gán quyền.
* p: đặc quyền được quyền.
* t: tên bảng, trên đó truy nhập được gán.
* ts: thời điểm quyền được gán.
* g: người gán quyền.
* go (yes/no): grant option.
  + Tham số go=yes , s có GRANT OPTION, nên có thể gán đặc quyền p cho các user khác.
  + Tham số : g và ts, để có thể thực hiện các hoạt động revoke quyền sau này 1 cách chính xác , = cách kiểm tra 1 loạt các quyền đã đc gán.
  + Gán quyền: nếu một user được gán quyền trên một table với Grant option, người dùng có thể gán và thu hồi quyền cho các user khác các quyền anh ta có.
  + Thu hồi quyền:
    - Sử dụng cơ chế thu hồi đệ quy.
    - Nếu x thu hồi quyền của y, trong khi đó x không gán quyền gì cho y trước đó, thì việc thu hồi quyền này bị loại bỏ.
    - Người dùng (người trao đặc quyền trên 1 bảng) cũng có thể ghi rõ từ khóa Public, thay cho users. Khi đó, tất cả những người dùng của CSDL đều được trao đặc quyền trên bảng.
  + Thu hồi quyền đệ quy: khi người dùng A thu hồi quyền truy cập của người B thì tất cả các quyền mà B đã gán cho người khác đều được thu hồi.
    - Thu hồi quyền đệ quy trong system R dựa vào nhãn thời gian mỗi lần cấp quyền truy nhập cho người dùng.
  + Thu hồi quyền không đệ quy: khi người A thu hồi quyền truy nhập trên B thì tất cả quyền truy nhập B cấp cho chủ thể khác được thay bằng A đã cấp cho những chủ thể này.
    - Thực tế khi một người dùng A thay đổi công việc hay vị trí thì đôi khi tổ chức chỉ muốn lấy lại quyền truy nhập của A mà không muốn lấy lại các quyền truy nhập mà A đã cấp => áp dụng thu hồi không đệ quy.
    - Vẫn dựa vào nhãn thời gian.

## Câu 16: Nêu ví dụ về đặc quyền hệ thống (system prilvilege) và đặc quyền đối tượng (object privilega). Viết câu lệnh SQL cho các ví dụ đó. Nêu sự khác nhau giữa admin option và grant option. Ví dụ các câu lệnh SQL.

* + Đặc quyền hệ thống: cho phép người dùng tạo những cơ sở dữ liệu mới, tạo các đối tượng mới bên trong cơ sở dữ liệu có sẵn, hay sao lưu cơ sở dữ liệu hoặc nhật ký giao tác.
    - Một số đặc quyền hệ thống: CREATE DATABASE

CREATE database QuanLyNhanVien

CREATE TABLE

CREATE table Nhanvien(

Id int,

Name varchar(25),

Que varchar(30)

);

CREATE PROCEDURE

CREATE PROC Tang\_luong AS

UPDATE NhanVien SET SALARY = SALARY \* 1.1 GO

CREATE DEFAULT

Alter table nhanvien alter name set default ‘Tran Thi Thanh’

CREATE RULE

CREATE rule r\_tuoi as @tuoi > 20

CREATE VIEW

CREATE view v\_ten as select name from nhanvien

BACKUP DATABASE

Backup database QuanLyNhanVien to disk = ‘D:\QLNV.bak’ BACKUP LOG

Backup log QuanLyNhanVien to disk = ‘D:\QLNV.trn’

* + Đặc quyền đối tượng: các quyền dùng đối tượng cho phép người sử dụng, role thực hiện những hành động trên một đối tượng cụ thể trong cơ sở dữ liệu.
    - Một số đặc quyền đối tượng: Select

Insert

Select \* from Nhanvien

Insert into Nhanvien values (1,’Thanh’,’Ha noi’);

Update

Update nhanvien set name = ‘Kem’ where id =1;

Delete

delete from Nhanvien where id =1; Execute

Reference

Alter table Nhanvien add constraint fk\_1 foreign key (id, name) references (id,name);

* + Sự khác nhau giữa Grant option và Admin option:

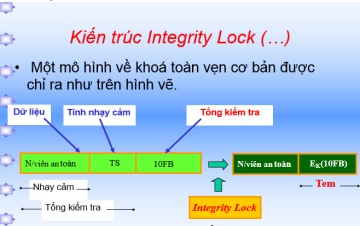
|  |  |
| --- | --- |
| Admin option | Grant option |
| * Tùy chọn trong câu lệnh gán quyền hệ thống. * Cho phép chủ thể lan truyền quyền đó cho chủ thể khác. | * Tùy chọn trong câu lệnh gán quyền đối tượng.   + chỉ người đã cấp đặc quyền mới có thể thu hồi đặc quyền.   * Cho phép chủ thể lan truyền quyền đó sang chủ thể khác. |
| GRANT SELECT ON EMPLOYEE TO user1 WITH ADMIN OPTION | |

GRANT SELECT ON EMPLOYEE TO user1 WITH GRANT OPTION.

# CHƯƠNG 3: AN TOÀN TRONG HỆ QUẢN TRỊ CƠ SỞ DỮ LIỆU

## Câu 17: tìm hiểu đặc điểm cơ bản của kiến trúc chủ thể tin cậy (trusted subject) và kiến thức Intergrity Lock. Đặc biệt chú ý kiến trúc Intergrity.

* + Kiến trúc chủ thể tin cậy Trusted subject
    - Giả sử hệ quản trị cơ sở dữ liệu và một OS tin cậy.
    - DBMS hoạt động như là một chủ thể tin cậy của OS.
    - DBMS có trách nhiệm trong việc bảo vệ đa mức các đối tượng của CSDL.
    - Được sử dụng trong nhiều DBMS thương mại: sybase, informix, oracle…
    - Người dùng kết nới tơi DBMS qua các phần mềm untrusted front end (vì họ kết nối qua Internet).
    - Người dùng được phân loại các mức nhạy cảm khác nhau: high (cao), low (thấp), và một mức DBMS khác với hai mức trên.
    - Các chủ thể và đối tượng được gán một nhãn DBMS không giống với mức high và low.
    - Chỉ có các chủ thể được gán nhãn DBMS mới được phép thực hiện mã lệnh và truy nhập vào dữ liệu.
    - Các chủ thể có nhãn DBMS được coi là chủ thể tin cậy và được miễn kiểm soát bắt buộc của OS.
    - Các đối tượng CSDL được gán nhãn nhạy cảm. Ví dụ: các bộ, các giá trị.
    - Hệ quản trị Sybase tuân theo giải pháp này, với kiến trúc máy khách/máy chủ, sybase thực hiện gán nhãn mức bản ghi (mức hàng).
  + Kiến trúc Intergrity Lock
    - Khóa toàn vẹn được đề xuất lần đầu tiên tại Viện nghiên cứu của lực lương không quân về an toàn cơ sở dữ liệu, được dùng để kiểm soát tính toàn vẹn và sự truy nhập cho cơ sở dữ liệu.



* Kiến trúc Intergrity Lock đã có trong hệ quản trị thương mại TRUDATA.
* TFE (bộ lọc tin cậy) thực thi bảo vệ nhiều mức bằng cách gắn các nhãn an toàn vào các đối tượng CSDL dưới dạng các tem – Stamp.
* Một tem là một trường đặc biệt của một đối tượng, lưu thông tin về nhãn an toàn và các dữ liệu điều khiển liên quan khác.
* Tem là dạng mã hóa của các thông tin trên, sử dụng một kỹ thuật niêm phong mật mã gọi là Intergrity Lock.
* TFE có nhiệm vụ tạo và kiểm tra các tem.
  + TFE sử dụng mật mã khóa bí mật để tạo tem và giải mã các tem. Các tem này có thẻ tạo ra dựa vào tổng kiểm tra (checksum).
  + Khóa bí mật chỉ có TFE biết.
* Insert dữ liệu: khi người dùng muốn insert một mục dữ liệu, TFE sẽ tính:
  + Tổng kiểm tra = mức nhạy cảm dữ liệu + dữ liệu.
  + Mã hóa tổng kiểm tra này bằng một khóa bí mật K, tạo ra tem, và lưu vào trong CSDL cùng với mục dữ liệu đó (gắn với mục dữ liệu).
* Đưa ra dữ liệu: khi đưa ra dữ liệu trả cho người dùng, TFE nhận được dữ liệu từ DBMS không tin cậy, nó sẽ kiểm tra tem gắn với mục dữ liệu xem có chính xác không:
  + Giải mã tem gắn với dữ liệu.
  + So sánh dữ liệu nhận được với dữ liệu sau khi giải mã tem. Nếu không khớp chứng tỏ dữ liệu đã bị sửa đổi.
  + Lưu ý: nếu dùng hàm băm để tạo tem, thì sau khi DBMS nhận được dữ liệu và tem tương ứng, nó sẽ băm dữ liệu này ra và so sánh với tem nhận được xem có trùng nhau không?
* Bộ lọc giao hoán: là quá trình tương tác với cả người sử dụng và hệ quản trị cơ sở dữ liệu.
* Bộ lọc back end: có trách nhiệm trong việc định nghĩa khung nhìn được phép tối đa bằng cách phát hiện tất cả các bản ghi/ thuộc tính không được phép, thay thế các yếu tố không được phép bằng giá trị 0.
* Bộ lọc front end.

# CHƯƠNG 4: AN TOÀN ỨNG DỤNG

## Câu 18: Tìm hiểu kỹ thuật SQL Injection

* + SQL Injection một kỹ thuật tấn công cho phép kẻ tấn công lời dụng lỗ hổng của việc kiểm tra dữ liệu đầu vào trong các ứng dụng web và các thông báo lỗi của hệ quản trị cơ sở dữ liệu trả về để tiêm vào và thi hành các câu lệnh SQL một cách trái phép.
  + SQL Injection có thể cho phép kẻ tấn công thực hiện các thao tác delete, insert, update… trên cơ sở dữ liệu của ứng dụng, thậm chí là máy chủ của ứng dụng đang chạy.
  + Là kỹ thuật được sử dụng dựa trên các lỗi và lỗ hổng bảo mật các lớp ứng dụng để thực hiện một cuộc tấn công vào cơ sở dữ liệu hoặc dữ liệu.
  + Hậu quả để lại rất nghiêm trọng vì nó cho phép kẻ tấn công có thể thực hiện các thao tác xóa, hiệu chỉnh, hoặc có toàn quyền trên cơ sở dữ liệu của ứng dụng.
  + Thường xảy ra trên các ứng dụng web có dữ liệu được quản lý bằng các hệ quản trị cơ sở dữ liệu như SQL server, My SQL, Oracle…
  + Cách phòng tránh SQL Injection:
    - Giới hạn quyền người dùng.
    - Loại bỏ các dấu, ký tự đặc biệt như: ‘:’, ‘- -‘, ‘/’,…
    - Giới hạn những Textox và Input.
    - Mã hóa cơ sở dữ liệu ở các trường hoặc các bản ghi quan trọng.
    - …

# CHƯƠNG 5: CƠ SỞ DỮ LIỆU THỐNG KÊ (SDB)

## Câu 19: Cơ sở dữ liệu thống kê là gì? Viết các câu lệnh SQL cho các thống kê. Ứng dụng trong thực tế? Các dạng biểu diễn.

* + Cơ sở dữ liệu thống kê (SDB):
    - Là một cơ sở dữ liệu được sử dụng cho mục đích phân tích thống kê.
    - Là một cơ sở dữ liệu chứa các bản ghi nhạy cảm mô tả về các cá nhân nhưng chỉ các câu truy vấn thống kê như: COUNT, SUM, AVERAGE, MAX, MIN… mới được trả lời, ngoài các câu truy vấn này thì những truy vấn vào các mục dữ liệu riêng sẽ không được đáp lại.
    - Sự khác biệt chính với CSDL quan hệ thông thường đó là với một SDB những câu truy vấn thống kê mới đc phép truy vấn, những câu truy vấn vào từng trường hợp dl riêng lẻ đều coi không hợp lệ
  + Các câu lệnh SQL thống kê
    - Select Count (\*) from NV.
    - Select SUM(luong) as sum\_luong from NV.
    - Select AVG(luong) as avg\_luong from NV.
    - Select MIN(luong) from NV.
    - Select MAX(luong) from NV.
  + Ứng dụng của SDB trong thực tế:
    - Điều tra dân số.
    - Thống kê số người tử vong.
    - Về kế hoạch kinh tế.
    - Thống kê khám chữa bệnh.
    - Thống kê các vụ tai nạn ô tô.
    - Thống kê về các lĩnh vực kinh tế, giáo dục, tài chính, thương mại…
    - Phân tích và đưa ra chiến lược.
  + Các dạng biểu diễn của SDB:
    - Dạng cơ sở dữ liệu quan hệ: SDB được biểu diễn ở dạng bảng hai chiều bình thường như các cơ sở dữ liệu quan hệ khác.
    - Dạng cơ sở dữ liệu vĩ mô: biểu diễn bằng các bảng chứa các thống kê vĩ mô. Các thống kê thường là count, sum, min, max, avg…

## Câu 20: Tìm hiểu các khái niệm cơ bản trong cơ sở dữ liệu thống kê

* + SDB tĩnh: là SDB không thay đổi trong suốt thời gian tồn tại của chúng. VD: CSDL thống kê dân số.
  + SDB động: thay đổi liên tục theo sự thay đổi của dữ liệu thực, cho phép sửa đổi để phản ánh các thay đổi động của thế giới thực. VD: CSDL nghiên cứu trực tuyến, lớp học trực tuyến khi bổ sung thành viên…
  + SDB trực tuyến (online): người sử dụng nhận được các phản hồi thời gian thực cho các câu truy vấn thống kê của mình.
  + SDB ngoại tuyến (offline): người sử dụng không biết khi nào các thống kê của họ được xử lý, việc SDB bị lộ sẽ khó khăn.
  + Kiến thức làm việc (working knowledge): là tập các mực thông tin (field) và giá trị thuộc tính trong SDB và các kiểu thống kê có sẵn trong SDB mà người dùng có thể biết một cách hợp lệ.
  + Kiến thức bổ sung của người sử dụng (sumplementary knowledge): người sử dụng có thể có kiến thức bên ngoài về các cá nhân được biểu diễn trong SDB. Người dùng hoàn toàn có thể lợi dụng kiến thức này cho các mục đích xấu để suy diễn.
  + Công thức đặc trưng: là một công thức logi, được ký hiệu bởi 1 chữ cái viết hoa, trong đó các giá trị thuộc tính được kết hợp với nhau thông qua các toán tử boolean như or, and, not.
  + Tập truy vấn (query set) của một công thức đặc trưng C là tập tất cả các bản ghi thỏa mãn C. Kí hiệu: X (C).
  + Thống kê trên C: là các câu truy vấn thống kê trên C. Kí hiệu q (C). Ví dụ: count (C).
  + Khái niệm bậc: một thống kê gồm m thuộc tính khác nhau được gọi là thống kê bậc m.
  + Thống kê nhạy cảm: là thống kê được tính toán trên một thuộc tính bí mật trong tập truy vấn có kích cỡ bằng 1.

## Câu 21: Thế nào là thống kê nhạy cảm? Cho ví dụ. Working knowledge và sumplementary knowledge?

* + Thống kê nhạy cảm:
    - Là thống kê có thể được sử dụng để nhận dạng thông tin bí mật về 1 cá nhân được biểu diễn trong SDB.
    - Là thống kê được tính toán trên một thuộc tính bí mật trong tập truy vấn có kích cỡ bằng 1.
  + Ví dụ: COUNT(AGE >50) =1

=>SUM (Salary, AGE >50) là thống kê nhạy cảm.

* + Kiến thức làm việc (working knowledge): là tập các mục thông tin (field) và các giá trị thuộc tính trong SDB và các kiểu thống kê có sẵn trong SDB mà người dùng có thể biết một cách hơp lệ.
  + Kiến thức bổ sung (sumplementary knowledge): người sử dụng có thể có kiến thức bên ngoài về các cá nhân được biểu diễn trong SDB. Người dùng hoàn toàn có thể lợi dụng những kiến thức này cho các mục đích xấu để suy diễn.

## Câu 22: Nêu cách thức tấn công của tấn công dựa vào trình theo dõi, tấn công dựa vào hệ tuyến tính. Cho ví dụ.

* + Tấn công dựa vào trình theo dõi(Tracker)
    - Trình theo dõi là một tập các công thức đặc trưng, có thể được sử dụng để đưa thêm bản ghi vào các tập truy vấn kích cỡ nhỏ, làm cho kích cỡ của chúng nằm trong khoảng [k, N-k].
    - Thông qua các trình theo dõi có thể tính toán được các thống kê bị hạn chế.
    - Giả sử C là công thức đặc trưng người dùng yêu cầu.
    - T là một trình theo dõi. T thỏa mãn điều kiện: K <= |X(T)| <= N-K.
    - Tấn công kiểu 1: K=2 (chỉ thực hiện được khi C = A Λ B)
      * Giả sử:
        + User cần tính count (C), sum (C, luong).
        + Công thức C (A Λ B), count (C) =1. Câu truy vấn này bị cấm.
* Tấn công:
  + Tính T = A Λ (phủ định của B) thỏa mãn k<= |X (T)|<= N-k.
* Tính gián tiếp count (C):

Q (C) = Q (A Λ B) = Q (A) – Q (A Λ (phủ định của B) => Q (C) = Q (A) – Q (T).

* Tấn công kiểu 2:
  + Giả sử: cần tính count (C), count (C) <k. Đây là thống kê bị cấm.
  + Tấn công:
    - Chọn T thỏa mãn: k<=|X (T)|, X |phủ định T|<= N -k.
    - Q (D) = Q(all) = Q(T) + Q (phủ định T) (Q(all) bị cấm)
    - Tính gián tiếp Q (C):

Q(C) = Q(C ν T) + Q (C ν (phủ định T) – Q (D)

* + Tấn công dựa vào hệ tuyến tính (cách thức tấn công đọc giáo trình, nhiều công thức quá)
    - Là loại tấn công bằng cách giải một hệ phương trình có dạng HX = Q với mỗi phương trình tương ứng một câu truy vấn.

## Câu 23: Các kỹ thuật tấn chống suy diễn trong cơ sở dữ liệu thống kê. Nêu ưu, nhược điểm của từng phương pháp.

Các kỹ thuật chống suy diễn bao gồm:

* + Kỹ thuật khái niệm.
  + Kỹ thuật hạn chế.
  + Kỹ thuật gây nhiễu.
  + Kỹ thuật mẫu ngẫu nhiên.
  1. Kỹ thuật khái niệm

Bao gồm 2 kỹ thuật: mô hình lưới và phân hoạch khái niệm.

* + - Mô hình lưới:
      * Ưu điểm: là mô hình an toàn hiệu quả cho nghiên cứu các vấn đề suy diễn và các phương pháp kiểm soát suy diễn. Với nhiều bảng ở các mức gộp khác nhau, ta có thể phân tích:
        + Các kiểu tấn công suy diễn bằng câu truy vấn count, sum, average…
        + Các tấn công kiểu kết hợp các câu truy vấn khác nhau để suy diễn ra dữ liệu nhạy cảm…
        + So sánh các kiểm soát suy diễn: hạn chế tập truy vấn và gây nhiễu dữ liệu.
* Nhược điểm:
  + Không thể cung cấp tính đầy đủ của cơ sở dữ liệu.
  + Không phù hợp với cơ sở dữ liệu động vì khi cập nhật SDB cần phải cập nhập tất cả các bảng trong mô hình lưới => tốn công.

Phân hoạch khái niệm:

* Giải quyết các vấn đề chống suy diễn trong giai đoạn thiết kế khái niệm của SDB.
* Để hỗ trợ việc xác định các yêu cầu an toàn thống kê trong mô hình khái niệm này, người ta đề xuất hệ thống tiện ích quản lý an toàn thống kê (SSMF) gồm có 3 modul: PDC, UKC, CEC
  1. Kỹ thuật hạn chế

1. Kiểm soát kích cỡ tập truy vấn:
   * Một thống kê q(C) chỉ được phép nếu tập truy vấn của nó X(C) thỏa mãn quan hệ sau: K<= |X(C)|<=N-K với 0<=K<=N/2.
   * Trong đó N là tổng số bản ghi trong SDB, k do DBA định nghĩa.
   * Ưu điểm:
     + Đưa ra được kết quả chính xác.
     + Kiểm soát này ngăn chặn các tấn công đơn giản, dựa vào các tập truy vấn rất nhỏ hoặc rất lớn.
   * Nhược điểm:
     + Hạn chế khả năng hữu ích của SDB
     + Chỉ ngăn chặn được các tấn công đơn giản, khó ngăn chặn được các tấn công phức tạp như trình theo dõi, tấn công hệ tuyến tính.
2. Kiểm soát kích cỡ tập truy vấn mở rộng:
   * Ưu điểm: chống được các kiểu tấn công: trình theo dõi, hệ tuyến tính.
   * Nhược điểm:
     + Phải kiểm tra 2^m tập truy vấn ngầm định (hàm mũ tăng rất lớn theo m) nên rất tốn công. => giải pháp này khó thực hiện.
     + Ngoài tập truy vấn ngầm định, kẻ tấn công có thể sử dụng những công thức khác liên quan đến tập truy vấn này để tính ra truy vấn yêu cầu.
3. Kiểm soát chồng lấp tập truy vấn:
   * Ưu điểm: ngăn chặn được các tấn công như trình theo dõi, hệ tuyến tính.
   * Nhược điểm:
     + Vẫn có khả năng bị phá vỡ bởi những tấn công được thiết kế theo dạng chuỗi các câu truy vấn liên tiếp.
     + Hạn chế khả năng hữu ích của SDB.
     + Kém hiệu quả do yêu cầu nhiều so sánh.
     + Tốn thời gian.
4. Kỹ thuật gộp
   * Ưu điểm: tránh được việc để lộ thông tin nhạy cảm.
   * Nhược điểm: kết quả đưa ra không chính xác.
5. Kỹ thuật giấu ô:
   * Được thiết kế cho các SDB vĩ mô (đưa ra các thống kê trong bản 2 chiều, như thống kê dân số).
   * Giấu ô: trong các bảng
     + Giấu đi tất cả các ô tương ứng với các thống kê nhạy cảm.
     + Giấu thêm các ô tương ứng với các thống kê có thể gián tiếp khám phá ra các thống kê nhạy cảm (giấu bổ sung).
   * Tiêu chuẩn giấu ô:
     + Thống kê count: kích cỡ tập truy vấn nhỏ hơn hoặc bằng 1, nghĩa là count (C) =0, count (C) = 1.
     + Thống kê sum: tiêu chuẩn nhạy cảm được sử dụng là quy tắc <<đáp ứng n, trội k%>>.
     + Một thống kê là nhạy cảm nếu n giá trị thuộc tính của n hoặc ít hơn n bản ghi tạo thành k% hoặc lớn hơn k% trong toàn bộ thống kê sum cảu ô đó => ô này bị giấu. Các tham số n, k được giữ bí mật và do DBA xác định (n<N).
     + Ưu điểm: chống được các tấn công kết hợp dựa vào count, sum.
     + Nhược điểm: hạn chế khả năng hữu ích của SDB, vì phải che giấu một số ô trong cơ sở dữ liệu.
   1. Kỹ thuật gây nhiễu
6. Kỹ thuật gây nhiễu dữ liệu:
   * + Gây nhiễu cố định:
       - Ưu điểm: chống được nhiều tấn công, kể cả tấn công tính trung bình (lặp nhiều lần).
       - Nhược điểm: chỉ áp dụng cho thuộc tính số; kết quả trả về không chính xác.

+ Gây nhiễu dựa vào truy vấn:

* Ưu điểm: gây nhiễu dữ liệu nên chống được nhiều tấn công.
* Nhược điểm:
  + - * + Với mỗi thống kê, lại phải áp dụng 1 hàm gây nhiễu f, với giá trị nhiễu => tốn công, giảm hiệu năng hệ thống.
        + Kết quả đưa ra không chính xác.

1. Kỹ thuật gây nhiễu đầu ra:

Ưu điểm: bảo vệ được những tấn công đơn giản.

* + - Nhược điểm:
      * Không chống được những tấn công trung bình, tấn công trình theo dõi.
      * Kết quả đưa ra không chính xác.
  1. Kỹ thuật mẫu ngẫu nhiên.
     + Ưu điểm: chống lại các tấn công trình theo dõi, tấn công lấy trung bình kết quả được lấy mẫu.
     + Nhược điểm: những câu truy vấn tương đương về mặt logic có thể đưa ra kết quả là các tập truy vấn khác nhau.

## Câu 24:Tại sao phải bảo vệ CSDL. Những vấn đề cần giải quyết khi mã hóa CSDL. Nhận xét so với các phương pháp bảo vệ khác

* **Vì sao cần phải bảo vệ:**
* Một CSDL cung cấp những thông tin quan trọng của khách hàng, kế hoạch phát triển của một doanh nghiệp, các dự đoán kinh tế, và nhiều mục đích quan trọng khác…
* Sẽ có lợi cho một tin tặc khi tấn công vào CSDL hơn là nghe lén giao tiếp trên mạng.
* Dữ liệu thường được mã hóa trên đường truyền nhưng lại lưu dưới dạng rõ trong CSDL.
* Sự cố về an ninh xảy ra với CSDL có thể ảnh hưởng nghiêm trọng đến danh tiếng của công ty và quan hệ với khách hàng.

## Phương pháp mã hóa CSDL cần giải quyết:

* + **Mã hóa fie CSDL :**
    - Giải pháp đơn giản nhất bảo vệ dữ liệu trong CSDL ở mức độ tập tin, chống lại sự truy cập trái phép vào các tập tin CSDL là hình thức mã hóa.
    - Tuy nhiên, mã hóa dữ liệu ở mức độ này là giải pháp mang tính “được ăn cả, ngã về không”, giải pháp này không cung cấp mức độ bảo mật truycập đến CSDL ở mức độ bảng (table), cột (column) và dòng (row).
    - Một điểm yếu nữa của giải pháp này là bất cứ ai với quyền truy xuất CSDL đều có thể truy cập vào tất cả dữ liệu trong CSDL. Điều này phát sinh một nguy cơ nghiêm trọng, cho phép các đối tượng với quyền quản trị (admin) truy cập tất cả các dữ liệu nhạy cảm. Thêm vào đó, giải pháp này bị hạn chế vì không cho phép phân quyền khác nhau cho người sử dụng CSDL.

## Mã hóa mức Ứng dụng

* + - Giải pháp thứ hai, đối nghịch với giải pháp mã hóa cấp tập tin nêu trên, giải quyết vấn đề mã hóa ở mức ứng dụng. Giải pháp này xử lý mã hóa dữ liệu trước khi truyền dữ liệu vào CSDL. Những vấn đề về quản lý khóa và quyền truy cập được hỗ trợ bởi ứng dụng. Truy vấn dữ liệu đến CSDL sẽ trả kết quả dữ liệu ở dạng mã hóa và dữ liệu này sẽ được giải mã bởi ứng dụng.
    - Giải pháp này giải quyết được vấn đề phân tách quyền an ninh và hỗ trợ các chính sách an ninh dựa trên vai trò (Role Based Access Control – RBAC). Tuy nhiên, xử lý mã hóa trên tầng ứng dụng đòi hỏi sự thay đổi toàn diện kiến trúc của ứng dụng, thậm chí đòi hỏi ứng

dụng phải được viết lại. Đây là một vấn đề đáng kể cho các công ty có

nhiều ứng dụng chạy trên nhiều nền CSDL khác nhau.

## Rủi ro khi mã hóa:

* Rủi ro lớn nhất có lẽ là mất các khóa :Dẫn đến mất toàn bộ dữ liệu
* Quá trình sinh khóa không đủ ngẫu nhiên:Dẫn đến có thể ‘dễ dàng đoán’ các khóa
* Thực thi mã hóa gặp sự cố:Dẫn đến mã hóa ‘tồi’

## Câu 25: Địa chỉ rào là gì. Ưu- nhược điểm

###  Địa chỉ rào:

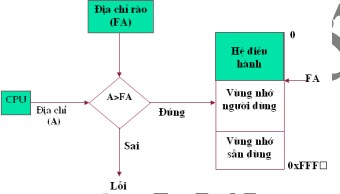
+ Địa chỉ rào đánh dấu ranh giới giữa vùng nhớ dành cho hệ điều hành và vùng nhớ cho tiến trình người dùng.

+ Vùng nhớ dành cho hệ điều hành là vùng nhớ thấp

+ Vùng nhớ dành cho người dùng bắt đầu từ địa chỉ rào

Do vùng nhớ cho Hệ điều hành có thể thay đổi, nên dùng một thanh ghi để lưu địa chỉ rào này.

* Cơ chế bảo vệ bộ nhớ dựa vào địa chỉ rào được mô tả trên hình sau:



Vậy nên phải bảo vệ vùng nhớ dành cho HDH tránh khỏi sự xâm

phạm, tác động của các tiến trình người dùng. Cớ chế dựa vào địa chỉ rào sẽ so sánh địa chỉ mà tiến trình người dùng truy xuất với giá trị của địa chỉ rào, nếu lớn hơn thì đây là một tham tham chiếu chính xác tới vùng nhớ của người dùng, ngược lại không phải là một tham chiếu đúng chương trình bị dùng hoạt động và đưa ra thông báo lỗi với người dùng.

Địa chỉ rào là địa chỉ vật lý, vì vậy khi người dùng truy xuất đến một địa chỉ logic thì CPU sẽ chuyển địa chỉ logic đó thành địa chỉ vật lý A và so sánh với địa chỉ rào FA.

Giá trị địa chỉ rào có thể được lưu trong một thanh ghi rào. Khi đó giá trị rào có thể thay đổi được tùy thuộc vào kích cỡ của OS, đồng thời OS sẽ lưu giá trị mới của địa chỉ rào vào trong thanh ghi. Cá địa chỉ trong chương trình người dùng được so sánh với giá trị lưu trong thanh ghi rào xem có hợp lệ hay không.

***- Ưu điểm:*** bảo vệ được vùng nhớ của hệ điều hành tránh khỏi sự can thiệp của các tiến trình người dùng.

### -Nhược điểm:

* Trong hệ đơn chương: chỉ có 1 tiến trình người dùng, lãng phí CPU.
* Trong hệ đa chương: đ/c rào không bảo vệ được vùng nhớ của người dùng này với người dùng khác.

## Câu 26: Tái định vị? Tái định vị động – tĩnh có thể thực hiện trong những thời điểm nào.

###  Tái định vị:

Tái định vị là quá trình chuyển đổi từ địa chỉ logic trong chương trình sang địa chỉ vật lý.

Địa chỉ vật lý = K + địa chỉ logic, trong đó K là địa chỉ rào của tiến trình người dùng

- Tái định vị có thể thực hiện trong 3 thời điểm :

+ *Thời điểm biên dịch* :biết vị trí chương trình sẽ thường trú trong bộ nhớ(VD:

đc rào là K1) . Trình biên dịch có thể phát sinh ngay mã lệnh thực thi với các địa chỉ tuyệt đối= đ/c tương đối+K1 . Sau đó ctrinh nạp sẽ nạp mã lệnh thực thi này vào vùng nhớ bắt đầu từ K1 . Nếu về sau có sự thay đổi vị trí thường trú lúc đầu của ctrinh cần fai biên dịch lại ctrinh.

*+ Thời điểm nạp:* thời điểm biên dịch k biết K1

Biên dịch-> mã lệnh thực thi tương đối(object code) chứa các địa chỉ tương đối . Thời điểm nạp biêt K1:đ/c tuyệt đối= đ/c tương đối+K1 Đây gọi là **tái định vị tĩnh**. Khi có sự thay đổi lưu trữ tiến trình trong bộ nhớ,chỉ cần nạp lại mà k cần biên dịch lại chương trình

*+ Thời điểm xử lý*

 **Tái định vị động:** các đ/c logic chỉ dc chuyển thành đ/c tuyệt đối tại thời điểm chạy chương trình. Khi đó cần sd cơ chế phần cứng đặc biệt(MMU) bằng cách thay đổi đ/c rào K. Đ/c của chương trình khi đc nạp vào bộ nhớ cha phải là đ/c tuyệt đối, nó có thể đc tái định vị. tái định vị chưa bảo bệ đc vùng nhớ

## Câu 27:Tìm hiểu 2 cơ chế phân trang, phân đoạn và so sánh (vẽ hình) . Thế nào là phân mảnh nội vi, phân mảnh ngoại vi. Ví dụ.

### Cơ chế phân trang:

* Ý tưởng: bộ nhớ vật lý= tổng các page frame(các khối có kích thước cố định và bằng nhau)
* Không gian logic= tổng các page
* 1 page frame= 1page= 2^16 byte=64KB
* Khi cần nạp 1 tiến trình vào bộ nhớ để xử lý,các trang của tiến trình sẽ đc nạp vào những khung trang còn trống.

*-* Ưu điểm:

Loại bỏ hiện tượng phân mảnh ngoại vi

Tạo ra sự phân biệt giữa góc nhìn của ng sd và bộ phận quản lý bộ nhớ vật lý.

Góc nhìn ng sd: 1 tiến trình của ng dùng nhìn thấy bộ nhớ như là 1 không gian liên tục đồng nhất và chỉ chứ duy nhất bản thân tiến trình này

Góc nhìn của bộ nhớ vật lý: 1 tiến trình của ng sd đc lưu trữ phân tán khắp bộ nhớ vât lý, đồng thời cũng chứa những tiến trình khác nhau

Cho phép chia sẻ các trang giữa các tiến trình.

***-*** Nhược điểm:

Vẫn còn hiện tượng phân mảnh nội vi

K phản ánh đúng cách ng dùng cảm nhận về bộ nhớ , họ nhìn bộ nhớ như 1 tập các đối tượng: phân đoạn, thư viện, biến toàn cục,stack, vùng nhơ chia sẻ…

### Cơ chế phân đoạn:

* Ý tưởng: 1 chương trình là 1 tập hợp các đoạn (segment), mỗi segment là 1 đơn vị logic như là: main program,procedure…

Sd bảng phân đoạn(segment table)để ánh xạ địa chỉ logic sang địa chỉ vật lý

* Bảng phân đoạn:mỗi phần trong phân đoạn bao gồm:

+TG cơ sở: lưu trữ đ/c vật lý nơi bắt đầu phân đoạn trong bộ nhớ vật lý

+TG giới hạn: lưu chiều dài của phân đoạn

* Chia sẻ phân đoạn:các tiến trình có thể chia sẻ với nhautừng phần của chương trình , k nhất thiết phải chia sẻ toàn bộ chương trình như trong trg hợp phân trang
* Ưu điểm: thể hiện đc cấu trúc logic của ctrinh như: thủ tục, chương trình, stack,mảng
* Nhược điểm:cũng như trường hợp mô hình phân vùng động, ký thuật phân đoạn phải giải quyết vấn đề cấp phát động.

Hiện tượng phân mảnh ngoại vi lại xuất hiện

### So sánh 2 cơ chế phân trang và phân đoạn:

**\*Phân trang:**

* Bộ nhớ vật lý và logic được chia thành các page có kích thước bằng nhau.
* Cơ chế chuyển đổi địa chỉ dùng bảng trang (page table) do hệ điều hành quản lý.
* Cho phép chia sẻ các trang giữa các tiến trình
* Một tiến trình có thể được nạp vào các trang không liên tục nhau.
* Phân mảnh nội vi.

## \*Phân đoạn:

* Bộ nhớ vật lý và logic được chia thành các segment có kích thước khác nhau.
* Cơ chế chuyển đổi địa chỉ dùng bảng phân đoạn ( segment table) do hệ điều hành quản lý.
* Cho phép chia sẻ các phân đoạn giữa các tiến trình
* Một tiến trình có thể được nạp vào các phân đoạn không liên tục nhau.
* Phân mảnh ngoại vi

### \* Hiện tượng phân mảnh nội vi và ngoại vi

*Hiện tượng phân mảnh nội vi*: Khi bộ nhớ được phân phối lớn hơn không đáng kể so với bộ nhớ được yêu cầu của tiến trình, khi đó phần bộ nhớ dư đó sẽ bị lãng phí.

**Ví dụ**: tiến trình A chỉ yêu cầu 450KB, nhưng lại được cấp 460 KB, do đó là lãng phí mất 10KB.

*Hiện tượng phân mảnh ngoại vi* là hiện tượng khi các khối nhớ tự do (trong bộ nhớ vật lý) đều quá nhỏ, không đủ để chứa một phân đoạn (trong bộ nhớ logic). **Ví dụ:** Các tiến trình (trong không gian logic) có yêu cầu các phân đoạn với dung lượng ít nhất là 25856 KB, nhưng tất cả các phân đoạn trống trong bộ nhớ vật lý đều nhỏ hơn dung lượng này, do đó chúng sẽ bị lãng phí vì không thể dùng cho bất kỳ tiến trình nào.

## Câu 28: So sánh hệ thống HIDS(máy trạm) và NIDS(mạng)

* IDS (Intrusion Detection System:Hệ thống phát hiện xâm nhập) là hệ thống phần mềm hoặc phần cứng chuyên dụng tự động thực hiện quy trình giám sát các sự kiện trong mạng, thực hiện phân tích để phát hiện những vấn đề an ninh cho hệ thống

 **Network based** (Snort, ISS, Juniper IDS, Cisco IPS): IDS/IPS cho toàn mạng

* Giám sát lưu lượng truy cập mạng cho các segment mạng cụ thể hay các thiết bị và phân tích các giao thức mạng, giao thức vận chuyển, giao thức ứng dụng để nhận diện các hoạt động khả nghi.
* Thường dưới dạng Appliance
* Thường được triển khai ở các biên mạng
* Có thể giám sát toàn bộ hệ thống
* Thường dưới dạng thiết bị chuyên dụng
* Quản lý được cả một phân vùng mạng (gồm nhiều host)
* Trong suốt với người sử dụng lẫn kẻ tấn công
* Dễ cài đặt và bảo trì
* Độc lập với OS
* Thường xảy ra cảnh báo giả
* Không phân tích được lưu lượng đã được mã hóa
* Ảnh hưởng tới chất lượng của mạng

 **Host based** (OSSEC, ISS, BroIDS, Tripware, Snort): IDS/IPS cá nhân

* Được triển khai trên từng host, thông thường là một software hay một agent với mục tiêu là giám sát các tính chất cơ bản, các sự kiện liên quan nhằm nhận diện các hoạt động khả nghi.
* Thường được triển khai treencacs host có tính chất quan trọng (public servers, sensitive data servers) hay 1 dịch vụ quan trọng
* Thường dưới dạng phần mềm cài đặt trực tiếp lên host
* Có khả năng xác định người dùng liên quan tới một sự kiện
* Có thể phân tích các dữ liệu mã hoá
* Host IDS hoạt động phụ thuộc vào Host
* Không có khả năng phát hiện tấn công dò quét mạng

## Câu 29:Trình bày 2 mô hình phát hiện xâm nhập trong IDS. Nêu ưu-nhược điểm từng mô hình. Cho ví dụ.

***- Phát hiện sự lạm dụng*** (*Misuse detection models*):

+ Phân tích các hoạt động của hệ thống, tìm kiếm các sự kiện giống với các ***mẫu tấn công*** đã biết trước.

+ ***Ưu điểm:***phát hiện các cuộc tấn công nhanh và chính xác, không đưa ra các cảnh báo sai làm giảm khả nǎng hoạt động của mạng và giúp các người quản trị xác định các lỗ hổng bảo mật trong hệ thống của mình.

+ ***Nhược điểm:*** là không phát hiện được các cuộc tấn công không có trong cơ sở dữ liệu, các kiểu tấn công mới, do vậy hệ thống luôn phải cập nhật các mẫu tấn công mới.

* ***Phát hiện tình trạng bất thường*** (*Anomaly detection models*):

+ Ban đầu, chúng lưu giữ các mô tả sơ lược về các hoạt động bình thường của hệ thống.

+ Các cuộc tấn công xâm nhập gây ra các hoạt động bất bình thường và kỹ thuật này phát hiện ra các hoạt động bất bình thường đó.

* Phát hiện dựa trên mức ngưỡng
* Phát hiện nhờ quá trình tự học
* Phát hiện dựa trên những bất thường về giao thức

***+ Ưu điểm:*** có thể phát hiện ra các kiểu tấn công mới, cung cấp các thông tin hữu ích bổ sung cho phương pháp dò sự lạm dụng

+ ***Nhược điểm:*** thường tạo ra một số lượng các cảnh báo sai làm giảm hiệu suất hoạt động của mạng.

* Ứng dụng: phương pháp dựa trên mẫu được hầu hết các IDS sử dụng còn phương pháp phát hiện tình trạng bất thường chỉ dùng cho các IDS thông minh, và không nhiều các IDS hiện nay được tích hợp phương pháp này.

# GHÉP THÊM

## Câu 30: Nêu định nghĩa về ngôn ngữ DDL và ngôn ngữ DML. Cho ví dụ?

**DDL(**Data Definition Language) là ngôn ngữ định nghĩa lược đồ CSDL. Các lệnh DDL bao gồm:

* + **Lệnh CREATE**: Tạo một bảng, một View của bảng, hoặc đối tượng khác trong Database.
  + **Lệnh ALTER**: Sửa đổi một đối tượng Database đang tồn tại, ví dụ như một bảng.
  + **Lệnh DROP**: Xóa toàn bộ một bảng, một View của bảng hoặc đối tượng khác trong một Database.

Vd :

CREATE TABLE NhanVien( MaNV int NOT NULL,

TenNV varchar(30) NOT NULL, Luong int

)

ALTER TABLE NhanVien ADD email varchar(40) null

DROP TABLE NhanVien

**DML** là ngôn ngữ thao tác với csdl : tìm kiếm , chèn ,xóa, cập nhật…

* **Lệnh SELECT**: Lấy các bản ghi cụ thể từ một hoặc nhiều bảng.
* **Lệnh INSERT:** Tạo một bản ghi.
* **Lệnh UPDATE:** Sửa đổi các bản ghi.
* **Lệnh DELETE:** Xóa các bản ghi. Ví dụ:

Select \* form NhanVien where tenNV = ”nam”

INSERT INTO NhanVien VALUES (101, ‘Lan', [1000, ’lan@yahoo.com’](mailto:lan@yahoo.com)) UPDATE NhanVien SET tenNV = ‘Minh' WHERE MaNV = 101

DELETE FROM NhanVien WHERE MaNV = 101

## Câu 31: Tại sao phải bảo vệ cơ sở dữ liệu? Nêu một số hiểm họa tấn công CSDL

* CSDL chứa nhiều thông tin quan trọng và nhạy cảm đó có thể là thông tin cá nhân, thông tin tổ chức, hoạt động giao dịch,….
* Sẽ có lợi cho một tin tặc khi tấn công vào CSDL hơn là nghe lén giao tiếp trên mạng.
* Dữ liệu thường được mã hóa trên đường truyền nhưng lại lưu dưới dạng rõ trong CSDL.
* Sự cố về an ninh xảy ra với CSDL có thể ảnh hưởng nghiêm trọng đến danh tiếng của công ty và quan hệ với khách hàng.
  + Một số hiểm họa tấn công CSDL
    - Các mối đe dọa có thể đến với CSDL là những hiểm họa có thể được xác định khi đối phương sử dụng các kỹ thuật đặc biệt để tiếp cận nhằm khám phá, sửa đổi trái phép thông tin quan trọng do hệ thống quản lý.
      * Những mối đe dọa có thể xuất phát từ nhiều nguyên nhân: ngẫu nhiên hay có chủ ý.
      * Xâm phạm : đọc, sửa, xóa dữ liệu trái phép
        + Khai thác trái phép thông qua suy diễn thông tin được phép
        + Sửa đổi dữ liệu trái phép
        + Từ chối dịch vụ hợp phép ( DoS)
      * Hiểm họa ngẫu nhiên:
        + Các thảm họa trong thiên nhiên.
        + Các lỗi phần cứng hay phần mềm có thể dẫn đến việc áp dụng các chính sách an toàn thông tin không đúng.
        + Các sai phạm vô ý do con người gây ra.
      * Hiểm họa có chủ ý:
        + Người dùng hợp pháp: lạm quyền, sử dụng vượt mức quyền hạn cho phép.
        + Người dùng truy nhập thông tin trái phép, có thể là người ngoài tổ chức hoặc bên trong tổ chức: tấn công, phá hoại, leo thang đặc quyền.

## Câu 32: Phân biệt các khái niệm và thuật ngữ sau : DBMS, SQL, PL/SQL, SQL Server, My SQL

* DBMS: Hệ quản trị cơ sở dữ liệu ( Database Management System – DBMS), là phần mềm hay hệ thống được thiết kế để quản trị một cơ sở dữ liệu.
* Ưu điểm của DBMS:
* Quản lý được dữ liệu dư thừa.
* Đảm báo tính nhất quán cho dữ liệu.
* Tạo khả năng chia sẻ dữ liệu nhiều hơn.
* Cải tiến tính toàn vẹn cho dữ liệu.
* Nhược điểm Hệ quản trị cơ sở dữ liệu:
* HQTCSDL tốt thì khá phức tạp.
* HQTCSDL tốt thường rất lớn chiếm nhiều dung lượng bộ nhớ.
* Giá cả khác nhau tùy theo môi trường và chức năng.
* HQTCSDL được viết tổng quát cho nhiều người dùng thì thường chậm.

**SQL:**

* SQL là viết tắt của Structured Query Language, là ngôn ngữ truy vấn cấu trúc.

Tất cả DBMS như MySQL, Oracle, MS Access, Sybase, Informix, Postgres và SQL Server sử dụng SQL như là ngôn ngữ cơ sở dữ liệu chuẩn.

**PL/SQL:**

* PL/SQL (PL : Procedural Language – Ngôn ngữ Thủ tục) là một mở rộng của SQL, kết hợp vào trong đó rất nhiều đặc tính của các ngôn ngữ lập trình gần đây. Nó cho phép các thao tác dữ liệu và các câu lệnh query SQL bao gồm các đoạn mã có cấu trúc khối và tính thủ tục (block-structure and procedural unit of code), làm cho PL/SQL thành một ngôn ngữ xử lý giao dịch mạnh mẽ.
* PL/SQL hỗ trợ tốt cho đa số các lệnh DML và các lệnh điều khiển giao dịch trong SQL.

**SQL Server:** là một hệ quản trị cơ sở dữ liệu quan hệ (Relational Database Management System (RDBMS) ) sử dụng câu lệnh SQL (Transact-SQL) để trao đổi dữ liệu giữa máy Client và máy cài SQL Server.

**MY SQL**: là hệ quản trị cơ sở dữ liệu mã nguồn mở phổ biến nhất thế giới và được các nhà phát triển rất ưa chuộng trong quá trình phát triển ứng dụng.

## Câu 33: Cơ sở dữ liệu thống kê là gì? Phân biệt cơ sở dữ liệu thống kê với cơ sở dữ liệu thường?

Cơ sở dữ liệu thống kê (SDB):

* + Là một cơ sở dữ liệu được sử dụng cho mục đích phân tích thống kê.
  + Là một cơ sở dữ liệu chứa các bản ghi nhạy cảm mô tả về các cá nhân nhưng chỉ các câu truy vấn thống kê như: COUNT, SUM, AVERAGE, MAX, MIN… mới được trả lời, ngoài các câu truy vấn này thì những truy vấn vào các mục dữ liệu riêng sẽ không được đáp lại.

Sự khác biệt chính với CSDL quan hệ thông thường đó là

* + Khả năng truy vấn bị giới hạn (với một SDB những câu truy vấn thống kê mới đc phép truy vấn, những câu truy vấn vào từng trường hợp dữ liệu riêng lẻ đều coi không hợp lệ.)
  + Việc truy vấn chỉ được giới hạn ở một vài phép toán thống kê: đếm, tính tổng, tính giá trị trung bình và một vài phép khác

## Câu 34: Mô hình an toàn là gì? Thế nào là hệ thống Multi-level Security?

**Hai chính sách MAC và DAC có dùng cho hệ thống Multi-level không?**

**Mô hình an toàn:** là một mô hình khái niệm mức cao, độc lập phần mềm và xuất phát từ các đặc tả yêu cầu của tổ chức để mô tả nhu cầu bảo vệ của một hệ thống.

**Hệ thống multilevel security:** Là hệ thống an toàn nhiều mức, mỗi chủ thể và đối tượng trong đó đều được gán nhãn an toàn thể hiện mức độ nhạy cảm của các chủ thể và các đối tượng đó

Trong 2 chính sách MAC và DAC thì chỉ có chính sách MAC có dùng hệ thống Multi-level

,theo mô hình của bell-Lapadula: những điều khiển truy nhập bắt buộc là :’not read up , not write down’

## Câu 35: Những vấn đề cần giải quyết khi mã hóa CSDL.

* **Phương pháp mã hóa CSDL cần giải quyết:**
  + **Mã hóa fie CSDL :**
    - Giải pháp đơn giản nhất bảo vệ dữ liệu trong CSDL ở mức độ tập tin, chống lại sự truy cập trái phép vào các tập tin CSDL là hình thức mã hóa.
    - Tuy nhiên, mã hóa dữ liệu ở mức độ này là giải pháp mang tính “được ăn cả, ngã về không”, giải pháp này không cung cấp mức độ bảo mật truycập đến CSDL ở mức độ bảng (table), cột (column) và dòng (row).
    - Một điểm yếu nữa của giải pháp này là bất cứ ai với quyền truy xuất CSDL đều có thể truy cập vào tất cả dữ liệu trong CSDL. Điều này phát sinh một nguy cơ nghiêm trọng, cho phép các đối tượng với quyền quản trị (admin) truy cập tất cả các dữ liệu nhạy cảm. Thêm vào đó, giải pháp này bị hạn chế vì không cho phép phân quyền khác nhau cho người sử dụng CSDL.
* **Mã hóa mức Ứng dụng**
  + Giải pháp thứ hai, đối nghịch với giải pháp mã hóa cấp tập tin nêu trên, giải quyết vấn đề mã hóa ở mức ứng dụng. Giải pháp này xử lý mã hóa dữ liệu trước khi truyền dữ liệu vào CSDL. Những vấn đề về quản lý khóa và quyền truy cập được hỗ trợ bởi ứng dụng. Truy vấn dữ liệu đến CSDL sẽ trả kết quả dữ liệu ở dạng mã hóa và dữ liệu này sẽ được giải mã bởi ứng dụng.
  + Giải pháp này giải quyết được vấn đề phân tách quyền an ninh và hỗ trợ các chính sách an ninh dựa trên vai trò (Role Based Access Control – RBAC). Tuy nhiên, xử lý mã hóa trên tầng ứng dụng đòi hỏi sự thay đổi toàn diện kiến trúc của ứng dụng, thậm chí đòi hỏi ứng

dụng phải được viết lại. Đây là một vấn đề đáng kể cho các công ty có nhiều ứng dụng chạy trên nhiều nền CSDL khác nhau.

**Rủi ro khi mã hóa:**

* Rủi ro lớn nhất có lẽ là mất các khóa :Dẫn đến mất toàn bộ dữ liệu
* Quá trình sinh khóa không đủ ngẫu nhiên:Dẫn đến có thể ‘dễ dàng đoán’ các khóa
* Thực thi mã hóa gặp sự cố:Dẫn đến mã hóa ‘tồi’

## Câu 36 : Hãy mô tả phương pháp kiểm soát dựa vào hạn chế kích cỡ tập truy vấn của một cơ sở dữ liệu thống kê, cho ví dụ.(q(C), X(C), |X(C)|)

* + Q(C) là các truy vấn thống kê trên C ví dụ: count(C), sum(C,Aj),min(C,Aj),max(C,Aj),avg(C, Aj)
  + X(C) là tập truy vấn của công thức đặc trưng C, là tập tất cả các bản ghi trong thỏa mãn C
  + |X(C)| là lực lượng của X(C): số lượng bản ghi thỏa mãn C , chính là giá trị của truy vấn count(C)
  + **Ví dụ :**



* + **Nhớ thêm trường lương giá trị tự điền**
  + C= {(ten=’Huệ’}

+ câu truy vấn thống kê trên C như: sum(C, lương)

+ tập truy vấn X(C):

**NHỚ VIẾT THÊM TRƯỜNG LƯƠNG NHA**

+ |X(C)| = 1

## Câu 37: Hãy nêu một số phương pháp có thể áp dụng để bảo mật cơ sở dữ liệu trong hệ quản trị Oracle

**Cơ sở dữ liệu riêng ảo (VPD - Virtual Private Database)**

+ Là kiểm soát truy nhập mức mịn hay cơ chế an toàn mức hàng, cung cấp tính năng bảo mật mức hàng cho cơ sở dữ liệu.

+ Cung cấp giải pháp bảo mật tới mức mịn trực tiếp trên các table, view, synonym; gán trực tiếp các chính sách bảo mật lên các đối tượng cơ sở dữ liệu, các chính sách tự động được thực hiện mỗi khi người dùng truy nhập dữ liệu đến đối tượng đó.

+ Ưu điểm: chi phí thấp, trong suốt với người dùng, tăng cao cơ hội kinh doanh

**An toàn dựa trên nhãn trong Oracle (OLS)**

+ Cho phép bảo vệ dữ liệu của các bảng đến mức hàng, mức bản ghi.

+ Cho phép định nghĩa 1 chính sách an toàn được thực thi bằng cách gắn cho các bản ghi trong bảng bởi các nhãn an toàn, thể hiện quyền mà người dùng có thể đọc hay ghi dữ liệu lên các bản ghi.

+ Các tính năng của OLS:

* Nhãn người dùng cung cấp thông tin về quyền hạn của người dùng.
* Nhãn dữ liệu cho thấy độ nhạy cảm của thông tin trong hàng đó.
* Chính sách đặc quyền của người dùng có thể cho phép bỏ qua 1 số khía cạnh của kiểm soát truy nhập dựa vào nhãn.
* Tùy chọn thực thi chính sách của 1 bảng xác định các khía cạnh khác nhau về cách điều khiển truy nhập thực thi để đọc, ghi lên bảng đó.

**Cơ chế kiểm toán mịn**

* Cho phép giám sát và ghi lại việc truy nhập dữ liệu dựa trên nội dung của dữ liệu.
* Cho phép định nghĩa một chính sách kiểm toán trên một bảng và các cột tùy chọn.
* Cung cấp cơ chế điều khiển tốt hơn và mức chi tiết nhỏ hơn so với phương pháp kiểm toán thông thường như: kiểm toán câu lệnh, kiểm toán đặc quyền, kiểm toán đối tượng lược đồ.

**Oracle Advanced Security**

+ Là cơ chế an toàn nâng cao trong Oracle, cho phép kiểm soát phòng ngừa, giúp giải quyết nhiều yêu cầu đặt ra, ngăn chặn các hành vi vi phạm dữ liệu, bảo vệ thông tin.

+ Cung cấp tính riêng tư, tính toàn vẹn, xác thực, cấp quyền truy nhập với nhiều cách thức khác nhau.

**Oracle secure backup (OSB)**

* Cho phép bảo vệ dữ liệu đáng tin cậy thông quâ hệ thống tập tin sao lưu.
* Hỗ trợ băng từ, ổ địa, môi trường SAN…
* Là một phần của giải pháp lưu trữ Oracle, giảm tính phức tạp và giảm chi phí cho việc mua phần mềm bổ sung.
* Cung cấp khả năng mở rộng phân phối và khôi phục sao lưu dự phòng.

## Câu 38: Nêu ví dụ về đặc quyền hệ thống (system prilvilege) và đặc quyền đối tượng (object privilega). Viết câu lệnh SQL cho các ví dụ đó. Nêu sự khác nhau giữa admin option và grant option. Ví dụ các câu lệnh SQL

**Đặc quyền hệ thống**: cho phép người dùng tạo những cơ sở dữ liệu mới, tạo các đối tượng mới bên trong cơ sở dữ liệu có sẵn, hay sao lưu cơ sở dữ liệu hoặc nhật ký giao tác.

Một số đặc quyền hệ thống: CREATE DATABASE CREATE TABLE CREATE PROCEDURE CREATE VIEW

Ví dụ: Create table SinhVien (MaSV varchar(10) not null primary key, Hoten varchar(30) not null)

**Đặc quyền đối tượng:** các quyền dùng đối tượng cho phép người sử dụng, role thực hiện những hành động trên một đối tượng cụ thể trong cơ sở dữ liệu.

Một số đặc quyền đối tượng: Select, Insert, Update, Delete, Execute

Ví dụ: Select \* from SinhVien where MaLop = ‘ML01’

Update SinhVien Set Hoten = ‘Nguyen Thi Minh’ where MaSV = ‘MS17’

Sự khác nhau giữa Grant option và Admin option:

|  |  |
| --- | --- |
| Admin option | Grant option |
| * Tùy chọn trong câu lệnh gán quyền hệ thống. * Cho phép chủ thể lan truyền quyền đó cho chủ thể khác. | * Tùy chọn trong câu lệnh gán quyền đối tượng. * Cho phép chủ thể lan truyền quyền đó sang chủ thể khác. |

## Câu 39: Mô tả chính sách DAC, trong DAC ai là người có thẩm quyền cao nhất để trao quyền trên một đối tượng cơ sở dữ liệu?

* + Kiểm soát truy nhập tùy ý DAC:
    - Là nền tảng cho các hệ điều hành và các DBMS.
    - Kiểm soát truy nhập dựa trên định danh của chủ thể hoặc định danh nhóm.
    - Chỉ rõ đặc quyền mà mỗi chủ thể có thể có được trên các đối tượng và trên hệ thống.
    - Các yêu cầu truy nhập được kiểm tra, thông qua 1 cơ chế kiểm soát tùy ý, truy nhập chỉ được trao cho các chủ thể thỏa mãn các quy tắc cấp quyền của hệ thống.
    - Người chủ sở hữu (owner) có thể gán quyền truy nhập(read,write,execute,..) tới các user khác.
    - Việc gán và thu hồi quyền là tùy ý do những người dùng này.
    - Trao quyền: việc trao quyền do người sở hữu đối tượng. tuy nhiên trong DAC có thể lan truyền các quyền, ví dụ: trong Oracle có grant option, admin option.
    - Thu hồi quyền: người dùng muốn thu hồi quyền ( người đã được trao quyền đó) phải có đặc quyền để thu hồi quyền
    - Các chếc độ kiểm soát truy nhập : có thể được áp dụng ở các mức độ chi tiết khác nhau trong hệ thống
    - Ví dụ về mô hình DAC điển hình: mô hình ma trận truy nhập, mô hình take-grant
* Trong DAC, **người có thẩm quyền cao nhất** để trao quyền trên một đối tượng cơ sở dữ liệu là người sở hữu đối tượng CSDL ấy

## Câu 40: Thực hiện các thiết kế an toàn. Các bước để thiết kế cơ sở dữ liệu (mô tả)

* Xem xét các yêu cầu an toàn bảo đảm tính sẵn sàng, bí mật và toàn vẹn cho hệ thống
* Xem xét xem cần bảo vệ bảng dữ liệu nào, những bảng nào có chứa dữ liệu nhạy cảm. Ví dụ như bảng điểm có trường điểm thi
* Lựa chọn hệ quản trị csdl phù hợp có tính bảo mật cao như Oracle hay SQL
* Lựa chọn dùng các phương pháp để đảm bảo an toàn như:

o +Dùng chính sách cấp quyền DAC, MAC

o +Dùng cơ chế sao lưu phục hồi dữ liệu

o +Dùng cơ chế mã hoá dữ liệu

Có 5 bước thiết kế một CSDL an toàn: Bước 1. Phân tích sơ bộ

+ Đánh giá các rủi ro

+ Ước lượng các chi phí thiết kế

+ Phát triển các ứng dụng cụ thể nào Bước 2. Các yêu cầu và các chính sách an toàn

* + *Phân tích yêu cầu:*

*+* Phân tích giá trị : xác định mức nhạy cảm của dữ liệu.

*+* Nhận dạng đe doạ/phân tích điểm yếu

*+*Phân tích và đánh giá rủi ro: khả năng xảy ra của các biến cố không mong muốn và tác động của chúng.

*+* Xác định yêu cầu bảo vệ

* + *Lựa chọn chính sách:*

+ Chính sách là các quy tắc ở mức cao, bắt buộc phải tuân theo trong các quá trình thiết kế, thực thi và quản lý hệ thống an toàn.

+ Định nghĩa các chế độ truy nhập (đọc, ghi) của chủ thể vào các đối tượng của hệ thống Bước 3. Thiết kế khái niệm

* Xây dựng mô hình E-R: Vẽ các thực thể và mối quan hệ giữa các thực thể đó.

Bước 4. Thiết kế lôgíc

* Xây dựng các lược đồ cơ sở dữ liệu ( là các bảng và các thuộc tính của chúng)

Bước 5. Thiết kế vậy lý

* Thiết kế thật sự vào hệ thống