MỤC LỤC

[Câu 1 : Thế nào là mô hình an toàn? Có mấy loại? Cho ví dụ. Sự khác nhau giữa mô hình an toàn](#_bookmark0) [và](#_bookmark0) [chính sách an toàn](#_bookmark0) [2](#_bookmark0)

[Câu 2: Nêu đặc điểm của mô hình Bell-Lapadula. Mô hình này thường áp dụng cho những loại dữ](#_bookmark1) [liệu nào?](#_bookmark1) [3](#_bookmark1)

[Câu 3: Nêu định nghĩa về ngôn ngữ DDL và ngôn ngữ DML. Cho ví dụ?](#_bookmark2) [3](#_bookmark2)

[Câu 4: Thế nào là thống kê nhạy cảm với một cơ sở dữ liệu thống kê? Cho ví dụ. Working](#_bookmark3) [knowledge và sumplementary knowledge?](#_bookmark3) [4](#_bookmark3)

[Câu 5: Tại sao phải bảo vệ cơ sở dữ liệu? Nêu một số hiểm họa tấn công CSDL](#_bookmark4) [4](#_bookmark4)

[Câu 6: Phân biệt các khái niệm và thuật ngữ sau : DBMS, SQL, PL/SQL, SQL Server, My SQL](#_bookmark5) [5](#_bookmark5)

[Câu 7: Trình bày mô hình system – R. Đặc biệt chú ý vấn đề thu hồi quyền đệ quy và không đệ quy.](#_bookmark6)

[. 6](#_bookmark6)

[Câu 8: Cơ sở dữ liệu thống kê là gì? Phân biệt cơ sở dữ liệu thống kê với cơ sở dữ liệu thường?](#_bookmark7) [7](#_bookmark7)

[Câu 9: Vẽ sơ đồ mối quan hệ giữa các mô hình RBAC? Giải thích](#_bookmark8) [8](#_bookmark8)

[Câu 10: Một số phương pháp đảm bảo tính toàn vẹn dữ liệu (được tích hợp sẵn trong các DBMS)](#_bookmark9) [9](#_bookmark9)

[Câu 11: Mô hình an toàn là gì? Thế nào là hệ thống Multi-level Security? Hai chính sách MAC và](#_bookmark10) [DAC có dùng cho hệ thống Multi-level không?](#_bookmark10) [9](#_bookmark10)

[Câu 12: Những vấn đề cần giải quyết khi mã hóa CSDL](#_bookmark11) [10](#_bookmark11)

[Câu 13 : Hãy mô tả phương pháp kiểm soát dựa vào hạn chế kích cỡ tập truy vấn của một cơ sở dữ](#_bookmark12) [liệu thống kê, cho ví dụ.(q(C), X(C), |X(C)|)](#_bookmark12) [10](#_bookmark12)

[Câu 14 : Có mấy giao đoạn để hoàn tất một giao dịch? Giả sử có một giao dịch (transaction) như](#_bookmark13) [sau](#_bookmark13) [11](#_bookmark13)

[Câu 15: Trình bày những lớp người dùng chính của một hệ thống ATCSDL, và vai trò của họ ?](#_bookmark14) [12](#_bookmark14)

[Câu 16: Mô tả kiến trúc Integrity Lock, nó được dùng cho DBMS nào? Tại sao gọi kiến trúc này là](#_bookmark15) [khóa toàn vẹn?](#_bookmark15) [12](#_bookmark15)

[Câu 17: Hãy nêu một số phương pháp có thể áp dụng để bảo mật cơ sở dữ liệu trong hệ quản trị](#_bookmark16) [Oracle](#_bookmark16) [13](#_bookmark16)

[Câu 18: Nêu ví dụ về đặc quyền hệ thống (system prilvilege) và đặc quyền đối tượng (object](#_bookmark17) [privilega). Viết câu lệnh SQL cho các ví dụ đó. Nêu sự khác nhau giữa admin option và grant](#_bookmark17) [option. Ví dụ các câu lệnh SQL](#_bookmark17) [14](#_bookmark17)

[Câu 19: Mô tả chính sách DAC, trong DAC ai là người có thẩm quyền cao nhất để trao quyền trên](#_bookmark18) [một đối tượng cơ sở dữ liệu?](#_bookmark18) [15](#_bookmark18)

[Câu 20: Mô tả các mô hình xử lý CSDL (vẽ hình minh họa), lưu ý trong từng mô hình, dữ liệu nằm](#_bookmark19) [ở](#_bookmark19) [đâu?](#_bookmark19) [16](#_bookmark19)

[Câu 21 : Địa chỉ rào là gì. Ưu- nhược điểm](#_bookmark20) [17](#_bookmark20)

[Câu 22 : Tái định vị? Tái định vị động – tĩnh có thể thực hiện trong những thời điểm nào.](#_bookmark21) [18](#_bookmark21)

[Câu 23: So sánh phương pháp kiểm soát dựa vào hạn chế và phương pháp dựa vào gây nhiễu trong](#_bookmark22) [cơ sở dữ liệu thống kê](#_bookmark22) [18](#_bookmark22)

[**Câu 24 : Tìm hiểu những vấn đề cần thiết khi mã hóa CSDL (vấn đề mã hóa ở đâu, bảo vệ khóa,**](#_bookmark23)[**phân phối khóa như thế nào)**](#_bookmark23)[19](#_bookmark23)

[**Câu 25: Thực hiện các thiết kế an toàn. Các bước để thiết kế cơ sở dữ liệu (mô tả).**](#_bookmark24)[19](#_bookmark24)

[**Câu 26: Trình bày các yêu cầu bảo vệ CSDL**](#_bookmark25)[20](#_bookmark25)

[**Câu 27: Nêu rõ đặc điểm của kiểm soát truy nhập MAC và DAC trong CSDL, nêu sự khác nhau**](#_bookmark26)[**giữa chúng. Ứng dụng 2 chính sách này trong thực tế các hệ quản trị như thế nào?**](#_bookmark26)[21](#_bookmark26)

[**Câu 28: Nêu đặc điểm cơ bản về Tấn công dựa vào Trình theo dõi (trình bày được ý tưởng của 2**](#_bookmark27)[**kiểu tấn công này) , và tấn công dựa vào Hệ tuyến tính,ví dụ**](#_bookmark27) [23](#_bookmark27)

[**Câu 29: Tìm hiểu các kỹ thuật chống suy diễn trong CSDL thống kê, nêu ưu nhược điểm của từng**](#_bookmark28)[**phương pháp. (Chú ý tìm hiểu kỹ các kiểm soát này)**](#_bookmark28)[25](#_bookmark28)

[**Câu 30 : Trình bày việc gán và thu hồi quyền trong MAC, DAC**](#_bookmark29)[28](#_bookmark29)

[**Câu 31 : Tìm hiểu kỹ thuật SQL Injection**](#_bookmark30)[29](#_bookmark30)

[**Câu 32 : So sánh hệ thống HIDS(máy trạm) và NIDS(mạng)**](#_bookmark31)[29](#_bookmark31)

[**Câu 33 :Trình bày 2 mô hình phát hiện xâm nhập trong IDS. Nêu ưu-nhược điểm từng mô hình.**](#_bookmark32)[**Cho ví dụ**](#_bookmark32) [30](#_bookmark32)

[**Câu 34 : Tìm hiểu 2 cơ chế phân trang, phân đoạn và so sánh (vẽ hình) . Thế nào là phân mảnh nội**](#_bookmark33)[**vi, phân mảnh ngoại vi. Ví dụ**](#_bookmark33) [30](#_bookmark33)

# Câu 1 : Thế nào là mô hình an toàn? Có mấy loại? Cho ví dụ. Sự khác nhau giữa mô hình an toàn và chính sách an toàn

* 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.
* Hai loại mô hình an toàn là:
  + ***Mô hình an toàn tùy ý*** *(Discretionary security models)*

Ví dụ: Mô hình ma trận truy nhập, mô hình Take-Grant, mô hình Action-Entity

* + ***Mô hình an toàn bắt buộc*** *(Mandatory security models).*

Ví dụ: mô hình Bell – Lapadula, mô hình Sea View, mô hình Dion,

* **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. |

# Câu 2: Nêu đặc điểm của mô hình Bell-Lapadula. Mô hình này thường áp dụng cho những loại dữ liệu nào?

* 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 hoặc thương mại: Access, SQL, SQL Server,

**Câu 3: 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 NV(…….)

DML (Data Manipulation Language) 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 congnhan where name=”nam”

# Câu 4: Thế nào là thống kê nhạy cảm với một cơ sở dữ liệu thống kê? 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 5: 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 pháp ( 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 6: 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 mang tính cấu trúc.
* Nó được thiết kế để quản lý dữ liệu trong một hệ thống quản lý cơ sở dữ liệu quan hệ (RDBMS).
* SQL là ngôn ngữ cơ sở dữ liệu, được sử dụng để tạo, xóa trong cơ sở dữ liệu, lấy các hàng và sửa đổi các hàng, …

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

* + 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

**MySQL** là [hệ quản trị cơ sở dữ liệu](https://vi.wikipedia.org/wiki/H%E1%BB%87_qu%E1%BA%A3n_tr%E1%BB%8B_c%C6%A1_s%E1%BB%9F_d%E1%BB%AF_li%E1%BB%87u) [tự do nguồn mở](https://vi.wikipedia.org/wiki/Ph%E1%BA%A7n_m%E1%BB%81m_ngu%E1%BB%93n_m%E1%BB%9F) phổ biến nhất thế giới và được các nhà phát triển rất ưa chuộng trong quá trình phát triển ứng dụng.

# Câu 7: 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:

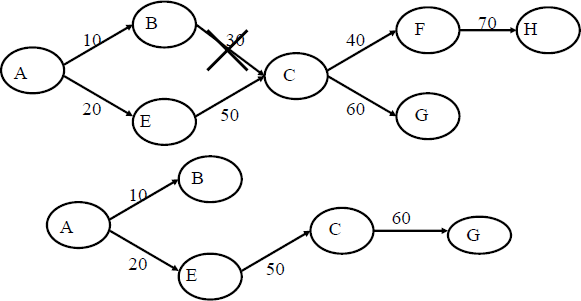
* + - * Sử dụng cơ chế thu hồi đệ quy.

+ 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.

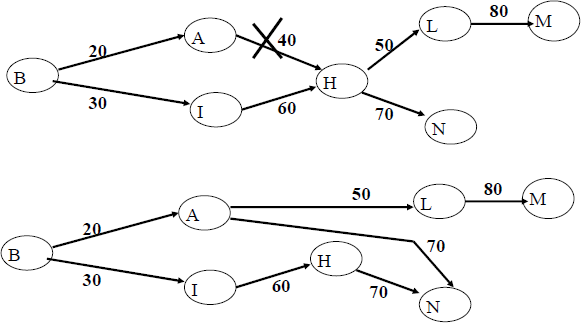
+ Người dùng (người trao đặc quyền trên 1 bảng) cũng có thể ghi rõ từ khóa Public, thay cho users. Khi đó, tất cả những người dùng của CSDL đều được trao đặc quyền trên bảng.

+ 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 8: 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 (statistical database - 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.

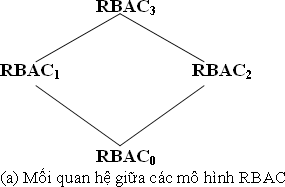
* + Sự khác biệt chính với CSDL quan hệ thông thường đó là
    - Khả năng truy vấn bị giới hạn (với một SDB những câu truy vấn thống kê mới đc phép truy vấn, những câu truy vấn vào từng trường hợp dữ liệu riêng lẻ đều coi không hợp lệ.)
    - Việc truy vấn chỉ được giới hạn ở một vài phép toán thống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

# Câu 9: Vẽ sơ đồ mối quan hệ giữa các mô hình RBAC? Giải thích

\*Mô hình RBAC(Role based Access Control)

* Được áp dụng vào đầu những năm 1970s.
* Khái niệm chính của RBAC là những quyền hạn được liên kết với những vai
* trò.
* Khi số lượng chủ thể và đối tượng lớn số lượng quyền hạn có thể trở nên vô
* cùng lớn.
* Nếu người dùng có nhu cầu cao, số lượng cấp và thu hồi quyền diễn ra thường
* xuyên.
* Với RBAC thì có thể giới hạn trước các mối quan hệ vai trò – quyền hạn, làm
* cho việc phân công người dùng đến các vai trò được xác định trước dễ dàng
* hơn.
* Không có RBAC sẽ khó khăn cho việc xác định quyền hạn nào được quy định
* đến người dùng nào.
* Những người dùng được chỉ định những vai trò thích hợp. Điều này làm đơn
* giản cho việc quản lí quyền hạn.
* Trong một tổ chức, những chức năng công việc khác nhau được phân thành những vai trò và người dùng được chỉ định vai trò dựa vào trách nhiệm và năng lực của họ.

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



-Mô hình nền tảng *RBAC0* thì ở dưới cùng, nó 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 nhưng có thêm các điểm đặc trưng cho từng mô hình.

+ *RBAC1* thêm vào khái niệm của hệ thống phân cấp vai trò (các trạng thái trong đó vai trò có thể thừa kế quyền hạn từ vai trò khác).

*+ RBAC2* thêm vào các ràng buộc (áp dụng ràng buộc để có thể thừa nhận cấu hình của các thành phần khác nhau của RBAC). RBAC1 , RBAC2 không liên quan nhau.

* RBAC3 là mô hình tổng hợp của ba mô hình RBAC0 , RBAC1 và RBAC2.

# Câu 10: 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 (Data Type)**: kiểu dữ liệu cũng có thể đảm bảo tính toàn vẹn dư 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.
  + **Đặt Not Null**: Null là một loại giá trị đặc biệt, nó không tương đương với zero, blank hay empty string ” ” mà có nghĩa là không biết (unknown) hay chưa được định nghĩa (undefined). Khi thiết kế CSDL nên cẩn thận trong việc cho phép một cột được Null hay Not Null vì việc chứa dữ liệu Null có thể làm cho một số ứng dụng không xử lý dữ liệu null kỹ lưỡng bị lỗi.
  + **Đặt giá trị Default**: 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.
  + **Thuộc tính Identity**: dữ liệu thuộc dạng ID sẽ đảm bảo tính duy nhất của dữ liệu trong bảng dữ liệu.
  + **Các ràng buộc (Constraints)**: Các ràng buộc dùng để đảm bảo tính toàn vẹn của 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.
  + **Các luật (Rules)**: là một đối tượng tương đương với CHECK Constraint trong SQL,rule là một object riêng và sau đó liên kết với một cột nào đó của bảng trong khi CHECK constraint là một thuộc tính của bảng nên có thể được tạo ra với lệnh CREATE TABLE.
  + **Triggers**: Một loại *stored procedure* đặc biệt được thực thi một cách tự động khi một bảng được Update, Insert hoặc Delete.
  + **Indexes**: sẽ được bàn đến trong bài nói về Indexes.

# Câu 11: 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**

**-** 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. Trong mỗi mô hình an toàn, có hai khái niệm cần quan tâm đó là: chủ thể (subject) và đối tượng (object)

+ Chủ thể là một thực thể chủ động, chẳng hạn: người dùng và các tiến trình.

+ Đối tượng là các thực thể bị động, như: các file, bảng, khung nhìn,…

+ Trong CSDL đa mức, chúng ta còn quan tâm đến các đối tượng mịn hơn như: các hàng, các cột, các ô.

# - Đặc điểm của hệ thống dựa trên 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.

+ Mục đích: phân loại các mục thông tin khác nhau, đồng thời phân quyền cho các mức truy cập khác nhau vào các mục riêng biệt để đảm bảo tính bí mật. Thường áp dụng trong các lĩnh vực quân sự.

+ 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.

+ 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.

**- Trong 2 chính sách MAC và DAC thì chỉ có chính sách MAC có dùng hệ thống Multi-level chẳng hạn như mô hình Bell Lapadula.**

# Câu 12: Những vấn đề cần giải quyết khi mã hóa CSDL.

* **Phương pháp mã hóa CSDL cần giải quyết:**
  + **Mã hóa file 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 truy cập 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 13 : 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) gồm: count, sum,min,max,avg
* X(C) là tập truy vấn trên C là tập tất cả các bản ghi trong SDB thỏa mãn C
* |X(C)| là lực lượng của X(C): số lượng bản ghi thỏa mãn C với |X(C)|=count(C)

Một thống kê *q*(C) chỉ được phép truy xuất vào cơ sở dữ liệu thống kê nếu tập truy vấn của nó (*X(C)*) thoả mãn quan hệ sau: 

***N*** là tổng số bản ghi trong SDB, ***K*** do DBA định nghĩa.

*Ví dụ*:

+ Xét một SDB về công nhân như sau: Tự vẽ bảng

Giả sử công thức đặc trưng có dạng: *C = (ChucVu=‘Trường phòng)*

Ta có N = 5 và chọn k =2, khi đó ta có |X(C)| = 1 <k, nên tập truy vấn của C không thỏa mãn điều kiện của Kiểm soát kích cỡ tập truy vấn. Do đó, tất cả cá thống kê trên C đều bị chặn.

# Câu 14 : Có mấy giao đoạn để hoàn tất một giao dịch? Giả sử có một giao dịch (transaction) như sau

**{accountA = accountA – X(N) accountB = accountB + X(N)}**

Mô tả ngắn gọn quá trình thực hiện giao dịch này trong DBMS

* Có 5 giai đoạn để hoàn tất một giao dịch:
  + Bắt đầu transaction với câu lệnh:

START TRANSACTION; BEGIN;

* + 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.
* Mô tả: Chuyển tiền từ tài khoản A vào tài khoản B, giao dịch bao gồm 3 thao tác riêng: giảm số tiền trong tài khoản A, tăng số tiền trong tài khoản B, ghi nhận giao dịch trong nhật ký

UPDATE account\_A

SET balance = balance – X(N) WHERE account = 3209;

UPDATE account\_B

SET balance = balance + X(N) WHERE account = 3208;

INSERT INTO journal VALUES (journal\_seq.NEXTVAL, ‘1B’, 3209, 3208, X(N));

COMMIT WORK;

* Oracle phải đảm bảo rằng cả 3 lệnh SQL đều được thực hiện để bảo đảm tài khoản được cân đối đúng. Khi có điều gì đó ngăn cản một trong 3 lệnh trong giao dịch (như lỗi phần cứng), thì những lệnh khác của giao dịch phải bị hủy bỏ quá trình này được gọi là rolling back. Nếu như lỗi xảy ra trong bất cứ thao tác cập nhật nào thì không thực hiện các thao tác cập nhật khác.

# Câu 15: Trình bày những lớp người dùng chính của một hệ thống ATCSDL, 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 16: Mô tả kiến trúc Integrity Lock, nó được dùng cho DBMS nào? Tại sao gọi kiến trúc này là khóa toàn vẹn?

* **Mô tả kiến trúc Integrity Lock:**

+ *Khoá toàn vẹn* được đề xuất lần đầu tiên tại Viện nghiên cứu của Lực lượng Không quân về An toàn cơ sở dữ liệu [AF83], được dùng để kiểm soát *tính toàn vẹn* và sự *truy nhập* cho cơ sở dữ liệu.

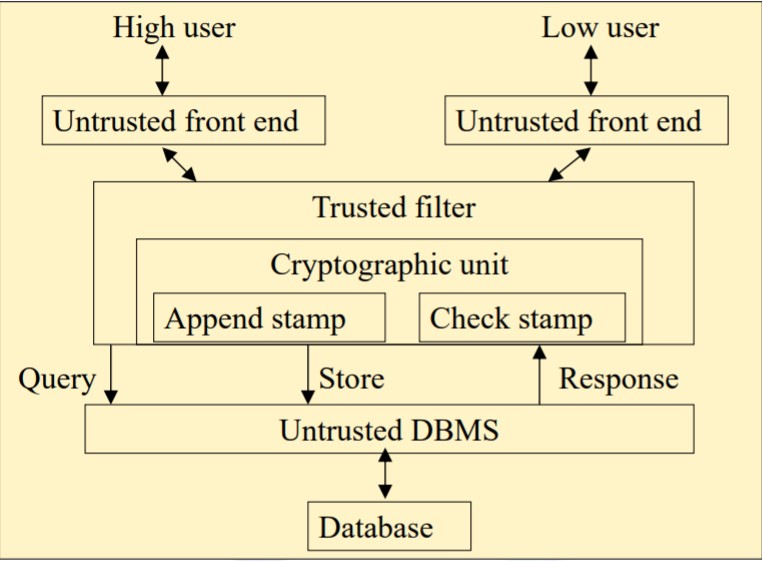
+ Kiến trúc Integrity lock đã có trong hệ quản trị thương mại TRUDATA.

* Đặc điểm:

+ TFE thực thi bảo vệ nhiều mức bằng cách gắn các nhãn an toàn vào các đối tượng CSDL dưới dạng các *tem – Stamps.*

+ 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 Integrity 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 thể tạo ra dựa vào tổng kiểm tra (checksum).

+ Khóa bí mật chỉ có TFE biết.

* Kiến trúc Integrity Lock được sử dụng trong hệ quản trị thương mại TRUDATA (công nghệ cơ sở dữ liệu tin cậy) và mẫu thử nghiên cứu Mitre
* Tính toàn vẹn nằm ở chỗ dữ liệu dù bị sửa đổi hay bị lỗi trên đường truyền thì kẻ tấn công không thể tính ra được tem hợp lệ.

# Câu 17: 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 18: Nêu ví dụ về đặc quyền hệ thống (system prilvilege) và đặc quyền đối tượng (object privilege). 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 DEFAULT CREATE RULE CREATE VIEW BACKUP DATABASE BACKUP LOG

**Ví dụ**

Create table SinhVien (

MaSV varchar(10) not null primary key,

Hoten varchar(30) not null, GioiTinh varchar (20), Quequan varchar(40), MaLop varchar(10),

FOREIGN KEY(MaLop) REFERENCES Lop(MaLop))

* 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 Reference

**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 19: 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:
  + 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 được biểu diễn bởi ma trận truy nhập (ACM).
* Trong DAC, **người sở hữu có thẩm quyền cao nhất** để trao quyền trên một đối tượng cơ sở dữ liệu mà người đó tạo ra, không phải nhân viên quản trị có quyền này.

# Câu 20: Mô tả các mô hình xử lý CSDL (vẽ hình minh họa), lưu ý trong từng mô hình, dữ liệu nằm ở đâu?

- Mọi ứng dụng cơ sở dữ liệu đều bao gồm 3 thành phần:

+ Thành phần xử lý ứng dụng

+ Thành phần phần mềm cơ sở dữ liệu (DBMS)

+ Bản thân cơ sở dữ liệu (DB)

- Các mô hình xử lý cơ sở dữ liệu phụ thuộc vào định vị của 3 thành phần trên, có 3 mô hình chính là:

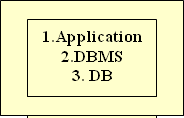
+ Mô hình cơ sở dữ liệu tập trung (Centralized database model)

+ Mô hình cơ sở dữ liệu phân tán (Distributed database model)

+ Mô hình cơ sở dữ liệu Client/Server (Client/Server database model)

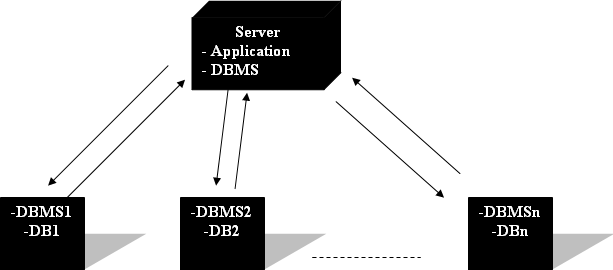
# Mô hình cơ sở dữ liệu tập trung:

* Cả 3 thành phần: xử lý ứng dụng, phần mềm cơ sở dữ liệu và bản thân cơ sở dữ liệu đều nằm trên một máy.
* Ví dụ các ứng dụng trên một máy sử dụng phần mềm cơ sở dữ liệu Oracle, cơ sở dữ liệu nằm trong máy đó.



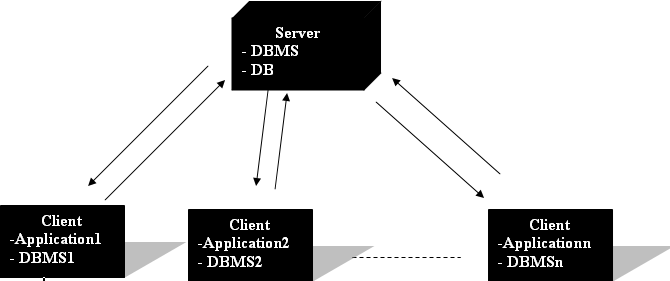
# Mô hình cơ sở dữ liệu phân tán:

* Trong mô hình này, cơ sở dữ liệu nằm trên nhiều máy khác nhau. Khi máy chủ cần truy xuất dữ liệu, nó sẽ gọi đến các máy này, và cần quá trình đồng bộ dữ liệu
* Mô hình này phù hợp cho các công ty có nhiều chi nhánh khác



# Mô hình cơ sở dữ liệu 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 nằm trên các client.



# Câu 21 : Địa chỉ rào là gì. Ưu- nhược điểm

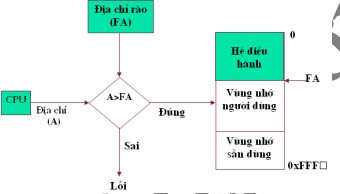
## Địa chỉ rào:

## 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. Cơ 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

Các 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 22 : 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: địa chỉ 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 phải biên dịch lại ctrinh.

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

Biên dịch-> mã lệnh thực thi tương đối(object code) chứa các địa chỉ tương đối . Thời điểm nạp biết 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*

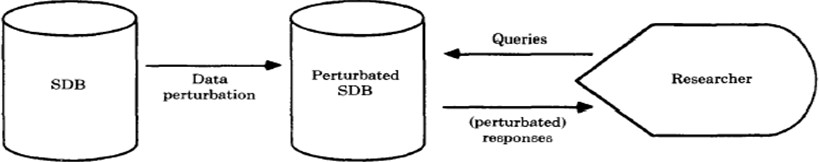
* **Tái định vị động:** các đ/c logic chỉ dc chuyển thành đ/c tuyệt đối tại thời điểm chạy chương trình. Khi đó cần sd cơ chế phần cứng đặc biệt(MMU) bằng cách thay đổi đ/c rào K. Đ/c của chương trình khi đc nạp vào bộ nhớ cha phải là đ/c tuyệt đối, nó có thể đc tái định vị. tái định vị chưa bảo vệ được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

# Câu 23: So sánh phương pháp kiểm soát dựa vào hạn chế và phương pháp dựa vào gây nhiễu trong cơ sở dữ liệu thống kê

* + Các kỹ thuật dựa vào hạn chế: chống suy diễn bằng cách hạn chế một số câu truy vấn thống kê (chẳng hạn như các câu truy vấn mà tập truy vấn của nó chứa một số lượng nhỏ/ lớn các bản ghi, hoặc các tập truy vấn chứa một vài bản ghi chung). Mặc dù chống suy diễn được một phần, nhưng nhược điểm của kỹ thuật này là hạn chế số lượng lớn các câu tryu vấn thống kê và do đó làm hạn chế phần lớn khả năng sử dụng của SDB
  + Các kỹ thuật dựa vào gây nhiễu: chống suy diễn bằng cách đưa ra các sửa đổi đối với thông tin được dùng khi trả lời các câu truy vấn thống kê. Việc sửa đổi có thể được thực hiện với dữ liệu lưu giữ trong SDB, hoặc không sửa đổi dữ liệu trong SDB nhưng sửa đổi kết quả tính toán trước khi chuyển tới người sử dụng. Ưu điểm của kỹ thuật này là chống được suy diễn nhưng hạn chế là đưa ra các kết quả truy vấn không chính xác. Vấn đề chủ yếu đối với các kỹ

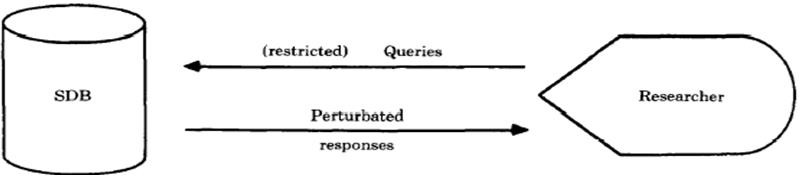
thuật này là độ lệch (bias). Do việc sửa đổi gây mất mát thông tin, chính vì vậy phải sửa đổi sao cho vẫn đảm bảo được tính tương thích của các kết quả.

1. Phương pháp gây nhiễu dữ liệu và gây nhiễu đầu ra có gì khác nhau (vẽ hình)
   * Phương pháp gây nhiễu dữ liệu:

+ Tiến hành trên các giá trị của bản ghi (được lưu giữ trong SDB) và sinh ra một dữ liệu mới – “dữ liệu bị sửa đổi”. Dữ liệu này được sử dụng khi tính toán các câu truy vấn thống kê.

* + Phương pháp gây nhiễu đầu ra:

+ Thực hiện sửa đổi trên các kết quả được tính toán chính xác của một câu truy vấn thống kê yêu cầu, trước khi chuyển nó cho người sử dụng. Về cơ bản, kỹ thuật dựa trên một số kiểu làm tròn trên các kết quả chính xác.



# Câu 24 : 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 ở: Mã hóa khi dữ liệu lưu trữ trên các hệ thống máy tính và truyền qua Internet hay các mạng máy tính khác,mã hóa ổ đĩa,file,email, điện mật
* Bảo vệ khóa: tăng cường độ khó các thuật toán, đảm bảo tính bí mật toàn vẹn và xác thực, làm khó viêc phân tích thành thừa số nguyên tố.
* Phân phối khoá được định nghĩa là cơ chế một nhóm chọn khoá mật và sau đó truyền nó đến các nhóm khác. Còn thoả thuận khoá là giao thức để hai nhóm (hoặc nhiều hơn) liên kết với nhau cùng thiết lập một khoá mật bằng cách liên lạc trên kênh công khai

# Câu 25: 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:

+Dùng chính sách cấp quyền DAC, MAC

+Dùng cơ chế sao lưu phục hồi dữ liệu

+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

# Câu 26: Trình bày các 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 mức thấp hơn file: bản ghi, thuộc tính.
  + Kiểm soát truy nhập CSDL phức tạp hơn kiểm soát file.

Bảo vệ chống suy diễn

Suy diễn là khả năng có được các thông tin bí mật từ những thông tin không bí mật.

* + Suy diễn trong CSDL quan hệ bình thường.
  + Suy diễn trong các CSDL thống kê (quan trọng)

Bảo vệ toàn vẹn cơ sở dữ liệu

Bảo vệ CSDL khỏi những người dùng không hợp pháp, tránh sửa đổi nội dung dữ liệu trái phép.

DBMS đưa ra các kiểm soát bằng các ràng buộc DL, thủ tục sao lưu, phục hồi và các thủ tục an toàn đặc biệt.

Hệ thống phục hồi của DBMS sử dụng các file nhật ký, ghi lại tất cả các phép toán được thực hiện trên dữ liệu: đọc, ghi, xóa, chèn.

*+Toàn vẹn dữ liệu thao tác*

*+Toàn vẹn ngữ nghĩa của dữ liệu:*

Khả năng lưu vết và kiểm tra

Là khả năng ghi lại mọi truy nhập tới dữ liệu (với các phép toán read và write). Khả năng kiểm tra và lưu vết đảm bảo tính toàn vẹn dữ liệu vật lý và trợ giúp cho việc phân tích dãy truy nhập vào CSDL

Xác thực người dùng

Yêu cầu này thực sự cần thiết để xác định tính duy nhất của người dùng. Định danh người dùng làm cơ sở cho việc trao quyền. Người dùng được phép truy nhập dữ liệu, khi hệ thống xác định được người dùng này là hợp pháp

Quản lý và bảo vệ dữ liệu nhạy cảm

Dữ liệu nhạy cảm là dữ liệu không được để công khai

Dữ liệu nhạy cảm chỉ được cấp cho người dùng hợp pháp Bảo vệ nhiều mức

Bao gồm một tập các yêu cầu bảo vệ: dữ liệu được phân loại thành nhiều mức nhạy cảm.

Mục đích của bảo vệ nhiều mức là phân loại các mục thông tin khác nhau, đồng thời phân quyền cho các mức truy nhập khác nhau vào các mục riêng biệt. Một yêu cầu nữa đối với bảo vệ nhiều mức là khả năng gán mức cho các thông tin.

# Câu 27: Nêu rõ đặc điểm của kiểm soát truy nhập MAC và DAC trong CSDL, nêu sự khác nhau giữa chúng. Ứng dụng 2 chính sách này trong thực tế các hệ quản trị như thế nào?

# *Đặc điểm của kiểm soát truy nhập MAC:*

# Được áp dụng cho các thông tin có yêu cầu bảo vệ nghiêm ngặt, hạn chế truy nhập của các chủ thể vào các đối tượng bằng cách sử dụng các *nhãn an toàn (label).*

*Ví dụ:*



*Đặc điểm của kiểm soát truy nhập DAC:*

+ Chỉ rõ những đặc quyền mà mỗi chủ thể có thể có được trên các đối tượng và trên hệ thống (object prilvilege, system prilvilege).

+ Các yêu cầu truy nhập được kiểm tra, thông qua một cơ chế kiểm soát tuỳ ý, truy nhập chỉ được trao cho các chủ thể thoả mãn các quy tắc cấp quyền của hệ thống.

*+ Được định nghĩa trên một tập*

* Các đối tượng an toàn (security objects)
* Các chủ thể an toàn (security subjects)
* Và các đặc quyền truy nhập (access prilvilege)

(Quyền truy nhập gồm: object prilvilege, system prilvilege).

*+* Người dùng có thể bảo vệ dữ liệu mà họ sở hữu

+ Người chủ sở hữu (owner) có thể gán quyền truy nhập (read, write, execute…) tới các user khác.

+ Việc gán và thu hồi quyền truy nhập là “tùy ý” do những người dùng này.

*\*\*Sự khác nhau giữa MAC và DAC*

|  |  |
| --- | --- |
| MAC | DAC |
| - Kiểm soát quyền dựa vào các nhãn an toàn gắn với chủ thể và đối tượng | - Kiểm soát quyền dựa trên quyền sở hữu đối tượng |
| - Việc trao, hủy bỏ quyền chỉ do một nhân viên an toàn | - Việc trao, hủy bỏ quyền là túy ý với những user có đặc quyền |
| - User không thể thay đổi nhãn hay quyền, chỉ do một nhân viên an toàn cao nhất. | - User có thể thay đổi quyền tùy vào đặc quyền của user đó. |

|  |  |
| --- | --- |
| - Dùng cho các hệ thống yêu cầu bảo vệ nghiêm ngặt như: quân sự, quốc phòng | - Dùng được cho mọi hệ thống, |
| - Độ an toàn cao nhưng phức tạp | - Linh hoạt, nhưng độ an toàn không cao |

Ví dụ một số hệ quản trị

* Có chính sách DAC như: Access, MySQL, SQL Server, Oracle
* Có chính sách MAC như: Oracle, DB2, Sybase

# Câu 28: Nêu đặc điểm cơ bản về Tấn công dựa vào Trình theo dõi (trình bày được ý tưởng của 2 kiểu tấn công này) , và tấn công dựa vào Hệ tuyến tính,ví dụ.

\**Trình theo dõi (Tracker):*

* + Là một tập các công thức đặc trưng, có thể được sử dụng để đưa thêm bản ghi vào các 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

Kiểu 1 K=2

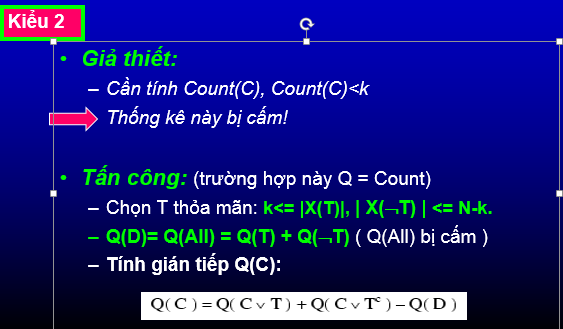
* + *Giả thiết:*
    - User cần tính Count(C), Sum(C, Luong)
    - Công thức *C = (AB)*, và Count (C) = 1.

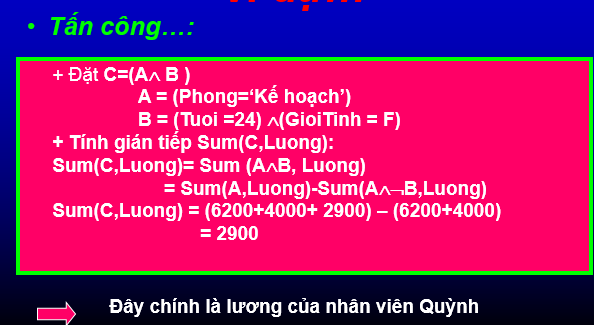
*Câu truy vấn này bị cấm!*

* + *Tấn công:*
    - Tính T = *A* *B* thỏa mãn k<=|X(T)|<= N-k.
    - Tính gián tiếp Count (C):

*Q*(C)= *Q* (AB) = *Q* (A)- *Q* (AB)

=> *Q* (C) = *Q* (A) - *Q* (T)





cách thức tấn công dựa vào Hệ tuyến tính.

* + Là loại tấn công bằng cách giải một hệ phương trình có dạng: *HX* = *Q*

*1,1x1 + 1,2x2 + . . . + 1,nxN = q1*

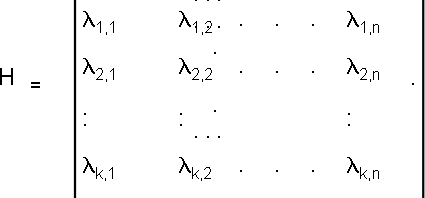
*2,1x1 + 2,2x2 + . . . + 2,NxN = q2*

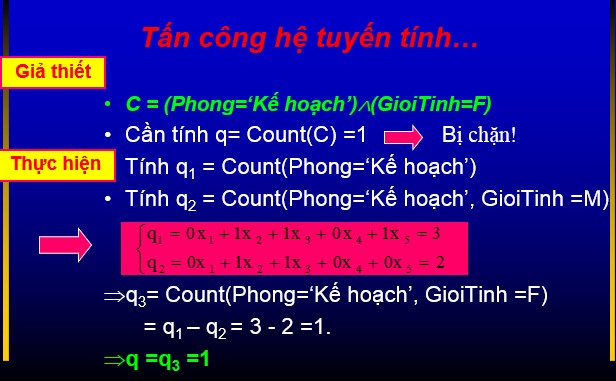
*.*

*k,1x1 + k,2x2 + . . . + k,nxN = qK*

Mỗi phương trình tương ứng một câu truy vấn

* + *H* là ma trận truy vấn
    - *H*[*i,j*] = 1 nếu bản ghi *xj*X(Ci), (tương ứng qi)
    - *H*[*i,j*] = 0 nếu ngược lại



* + - *x*1 ,..., *x*N là giá trị của N bản ghi
  + *Q* = (*q1*, ..., *qk*) là vector của các thống kê đưa ra
  + *C = (Phong=‘Kế hoạch’)* *(GioiTinh=F)*
    - Cần tính q= Sum(Luong, C)
    - Tính q1=X(C1) = Count(Phong=‘Kế hoạch’) = 3
    - Tính q2 =X(C2) = Count(Phong=‘Kế hoạch’, GioiTinh =M)=2
    - Sum(Luong, C) = Sum(Luong, C1) – Sum(Luong,C2)

= (6200+4000+2900) – (6200+4000) = 2900.

* + - Như vậy, kẻ tấn công đã tìm ra lương của người thỏa mãn C.

# Câu 29: Tìm hiểu các kỹ thuật chống suy diễn trong CSDL thống kê, nêu ưu nhược điểm của từng phương pháp. (Chú ý tìm hiểu kỹ các kiểm soát này)

* Kiểm soát kích cỡ tập truy vấn
* Kỹ thuật giấu ô
* Kỹ thuật gây nhiễu

# \*Kiểm soát kích cỡ tập truy vấn

Một thống kê *q*(C) chỉ được phép nếu tập truy vấn của nó, *X(C)*, thoả mãn quan hệ sau:

*k*  *X*(C) *N*-*k*

**0**  *k*  *N/2*

Trong đó, *N* là tổng số bản ghi trong SDB, *k* do DBA định nghĩa.

Kiểm soát này ngăn chặn các tấn công đơn giản, dựa vào các tập truy vấn rất nhỏ hoặc rất lớn.

*Ưu điểm:*

* + - Đưa ra kêt quả chính xác
    - Chỉ chống được tấn công suy diễn đơn giản

*Nhựơc điểm:*

* + - Không chống được một số tấn công phức tạp như: Trình theo dõi, Hệ tuyến tính.
    - Hạn chế khả năng hữu ích của SDB (vì hạn chế nhiều câu truy vấn)

*Ví dụ:* Người dùng yêu cầu thống kê *q*1 = *Count* (C) =1, => có một cá nhân A thỏa mãn C. Đưa ra thống kê *q*2 = *Count* (C  C')

* Nếu *q2 = 1 => A* thỏa mãn *C’*
* Ngược lại, A không thỏa mãn C’ Đưa ra thống kê khác, ví dụ Sum(C, *Ai*)

=> Kiểm soát kích cỡ tập truy vấn không cho phép đưa ra *q1, q2.*

\***Kiểm soát kích cỡ tập truy vấn mở rộng:**

-Nhược điểm của kiểm soát kích cỡ tập truy vấn là do các công thức đặc trưng liên quan đến nhau (ví dụ: C và T).

-*Cải tiến*: tăng số lượng các tập truy vấn cần được kiểm soát.

* Cho công thức đặc trưng C
* *Tìm tập truy vấn ngầm định* của C

-Cho trước một thống kê bậc *m* có dạng như sau:

* *q*(*A1* = *a1* *A2*= *a2* ...  *Am* =*am*) Hoặc:

*- q*(*A1* = *a1* *A2*= *a2* ...  *Am* =*am*)

-Khi đó, tồn tại 2m = Cm0 + Cm1 +Cm2 +…+ Cmm-1 tập truy vấn ngầm định, tương ứng với các thống kê sau đây:

*q*(*A1* = *a1* *A2*= *a2* ...  *Am* =*am*)

*Ưu điểm:*

*q*(*A1* = *a1* *A2*= *a2* ...  *Am* =*am*)

...

*q*(*A1*= *a1* *A2*= *a2* ...  *Am* =*am*)

*q*(*A1* = *a1* *A2*= *a2* ...  *Am* =*am*)

...

*q*(*A1* = *a1* *A2*= *a2* ...   *Am* =*am*)

Chống được các kiểu tấn công: Trình theo dõi, Hệ tuyến tính

*Nhược điểm:*

* Tốn công: phải kiểm tra *2m* tập truy vấn ngầm định (hàm mũ tăng rất lớn theo *m*).
* *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.

\***Kỹ thuật gộp**

-Các câu truy vấn thống kê được tính toán trên các cá thể tổng hợp. Dữ liệu riêng sẽ được nhóm lại thành một khối nhỏ trước khi đưa ra.

-*Giá trị trung bình* của nhóm gộp sẽ thay thế cho mỗi giá trị riêng của dữ liệu được gộp

-Kỹ thuật này giúp ngăn chặn khám phá dữ liệu riêng.

*Ưu điểm:*

* Tránh được việc để lộ thông tin nhạy cảm

*Nhựơc điểm:*

* Kết quả đưa ra không chính xác

*Ví dụ:* Cục thống kê nông nghiệp quốc gia (NASS) công bố dữ liệu về các nông trường, trang trại. Để bảo vệ chống lại sự khám phá dữ liệu, dữ liệu chỉ được đưa ra ở *mức vùng*. Dữ liệu tại các nông trại ở mỗi vùng sẽ được gộp để bảo vệ tính riêng tư và tránh bị khám phá.

# \*Kỹ thuật giấu ô

-*Giấu ô*: trong các bảng, giấu đi tất cả các ô tương ứng với các thống kê nhạy cảm và 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 bằng 1, nghĩa là Count(C) =1
  + Thống kê *Sum*, tiêu chuẩn nhạy cảm được sử dụng là quy tắc *«đáp ứng n, trội k% »* . Theo tiêu chuẩn này, 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* đó. Các tham số *n* và *k* được giữ bí mật và do DBA xác định.

*Ưu điểm:* Chống được các tấn công kết hợp dựa vào Count và Sum

*Nhược điểm:* Hạn chế khả năng hữu ích của SDB, vì phải che giấu một số ô trong CSDL.

# \*Kỹ thuật gây nhiễu

*Gây nhiễu cố định (fixed perturbation)*

* *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 một hàm gây nhiễu f, với gía trị nhiễu=> tốn công, giảm hiệu năng hệ thống.
    - Kết quả đưa ra không chính xác.

# Câu 30 : Trình bày việc gán và thu hồi quyền trong MAC, DAC.

* DAC
  + Trao quyền: 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 31 : 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.
* 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 Text và Input.
  + Mã hóa cơ sở dữ liệu ở các trường hoặc các bản ghi quan trọng.
  + …

# Câu 32 : 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 trên các 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 33 :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.

# Câu 34 : 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:

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

+Thanh ghi giới hạn: lưu chiều dài của phân đoạn

* Chia sẻ phân đoạn:các tiến trình có thể chia sẻ với nhau từng 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), mặc dù tổng các khối có thể đủ để cấp phát.

**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.