**BÁO CÁO ĐỒ ÁN LÝ THUYẾT**

**AN TOÀN BẢO MẬT DỮ LIỆU TRONG HỆ THỐNG THÔNG TIN**

*LỚP 19HTTT1 - NHÓM 01*

*GIẢNG VIÊN HƯỚNG DẪN*

* *TS.*Phạm Thị Bạch Huệ
* *Ths.*Lương Vĩ Minh

Mục lục

[**A.** **Thông tin chung** 3](#_Toc103192281)

[**I.** **Thông tin nhóm** 3](#_Toc103192282)

[**II.** **Thông tin đồ án** 3](#_Toc103192283)

[**B.** **Kết quả đồ án** 3](#_Toc103192284)

[**I.** **Phân hệ 1** 3](#_Toc103192285)

[**1.** **Lý thuyết** 3](#_Toc103192286)

[**a.** **Người dùng (User)** 3](#_Toc103192287)

[**b.** **Vai trò (Role)** 4](#_Toc103192288)

[**c.** **Khung nhìn (View)** 4](#_Toc103192289)

[**d.** **Quyền người dùng (Privilege)** 6](#_Toc103192290)

[**2.** **Triển khai cài đặt** 7](#_Toc103192291)

[**a.** **Xem thông tin các đối tượng** 7](#_Toc103192292)

[**b.** **Tạo/xóa các đối tượng** 10](#_Toc103192293)

[**c.** **Quản lý quyền truy cập** 10](#_Toc103192294)

[**II.** **Phân hệ 2** 12](#_Toc103192295)

[**1.** **Tóm tắt lý thuyết** 12](#_Toc103192296)

[**a.** **DAC** 12](#_Toc103192297)

[**b.** **RBAC** 13](#_Toc103192298)

[**c.** **VPD** 13](#_Toc103192299)

[**d.** **OLS** 14](#_Toc103192300)

[**e.** **Mã hóa** 15](#_Toc103192301)

[**f.** **Audit** 15](#_Toc103192302)

[**2.** **Các chính sách bảo mật trong đồ án** 16](#_Toc103192303)

[**2.1** **Kết nối dòng dữ liệu với tài khoản người dùng** 16](#_Toc103192304)

[**2.2** **Ứng dụng DAC + RBAC** 16](#_Toc103192305)

[**2.3** **Ứng dụng VPD** 17](#_Toc103192306)

[**2.4** **Ứng dụng OLS** 19](#_Toc103192307)

[**2.5** **Ứng dụng mã hóa** 20](#_Toc103192308)

[**2.6** **Ứng dụng Audit** 20](#_Toc103192309)

[**C.** **Tham khảo** 21](#_Toc103192310)

1. **Thông tin chung**
2. **Thông tin nhóm**

Nhóm 01

Số lượng thành viên: 3

**Thông tin thành viên**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **STT** | **MSSV** | **Họ tên** | **Email** | **Ghi chú** |
| 1 | 19127652 | Hồ Nhật Linh | 19127652@student.hcmus.edu.vn | Nhóm trưởng |
| 2 | 19127512 | Lâm Hoàng Phúc | 19127512@student.hcmus.edu.vn |  |
| 3 | 19127507 | Nguyễn Quang Phú | 19127507@student.hcmus.edu.vn |  |

1. **Thông tin đồ án**

Hệ quản trị CSDL: Oracle database 18c.

Nền tảng ứng dụng: Windows, MacOS, Linux.

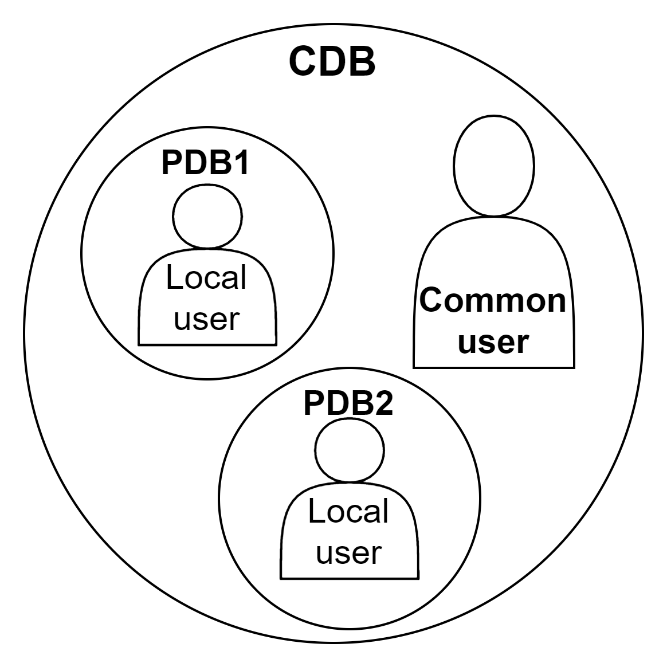
Ngôn ngữ lập trình: Java.

Framework: Java swing.  
API kết nối database: JDBC (Java Database Connectivity) sử dụng **công nghệ SSL** để bảo mật thông tin trên đường truyền.

1. **Kết quả đồ án**
2. **Phân hệ 1**
3. **Lý thuyết**
4. **Người dùng (User)**

User sở hữu 1 tài khoản trên HQTCSDL, user có thể dùng tài khoản này để đăng nhập và thực hiện các công việc (thêm, sửa, xóa dữ liệu, cấu trúc dữ liệu,…) được cho phép thực thi.

Oracle lưu trữ cơ sở dữ liệu trong 1 **CDB** (Container database hay Root) lớn để quản lý tất cả dữ liệu, trong CDB có chứa các **PDB** (Pluggable database), PDB chứa các lược đồ, dữ liệu của riêng nó.

Trong Oracle, có 2 loại user là common user và local user

(Mô tả common user và local user trong Oracle)

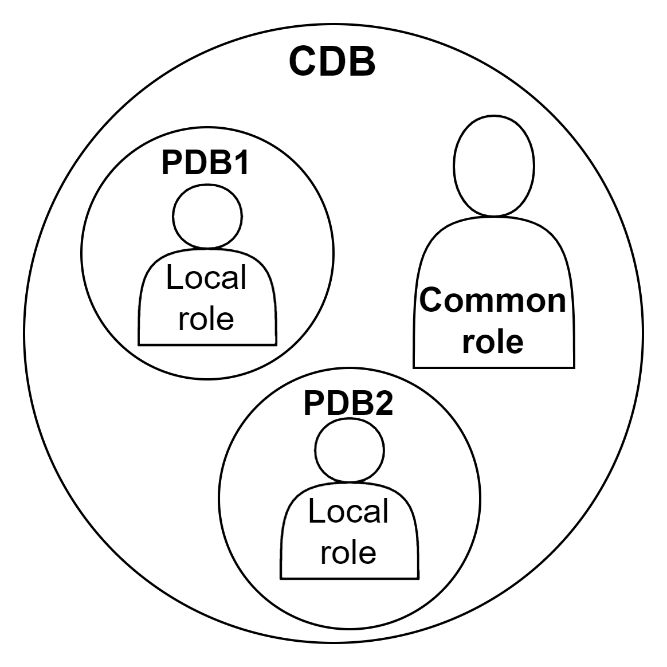
* **Common user**: Có thể sử dụng tài nguyên trên toàn bộ CDB (toàn bộ CSDL), tên người dùng phải bắt đầu bằng kí tự “C##” và không được trùng nhau.
* **Local user**: Chỉ có thể sử dụng tài nguyên ở 1 PDB nó thuộc về, tên user có thể khác nhau nếu không cùng PDB.

Trong Oracle, **1 user tương ứng 1 schema**, chứa tất cả những đối tượng (table, view, procedure) của riêng schema đó, những đối tượng khác schema có thể khác tên.

Ví dụ ta có 1 user C##NHOM1 thì tuong ứng ta sẽ có 1 schema C##NHOM1, ta có thể tạo các đối tượng trên shema (sử dụng toán tử ‘.’ để truy cập vào các đối tượng), chẳng hạn C##NHOM1.BANG\_1, C##NHOM1.KHUNG\_NHIN\_1.

1. **Vai trò (Role)**

Role là 1 tập hợp những quyền liên quan với nhau. Role có thể được sử dụng để gán cho 1 user hay 1 role khác để user hay role đó kế thừa những quyền của role gán.

Tương tự như user, role cũng có 2 loại là **Common role** (có thể truy cập trên CDB, tên phải bắt đầu là “C##”) và **Local role** (chỉ được truy cập PDB của mình). 

(Mô tả common role và local role trong Oracle)

1. **Khung nhìn (View)**

**Khung nhìn (View)** là một bảng ảo, nó không chứa dữ liệu mà chỉ là đối tượng trung gian để tương tác với các bảng thật. View được tạo từ câu truy vấn dữ liệu

Ví dụ:Tạo view để xem thông tin giáo viên thuộc bộ môn HTTT

CREATE VIEW GIAO\_VIEN\_HTTT

AS

SELECT \*

FROM GIAO\_VIEN

**WHERE MA\_BM = ‘HTTT’;**

Thực chất, View trong Oracle chỉ là những câu truy vấn đã được xác thực được lưu lại trong data dictionary.Ảnh có chứa văn bản

Mô tả được tạo tự động

(Cách Oracle lưu view)

Bên cạnh việc tăng hiệu năng truy vấn. Thì mục đích chính của việc dùng View là để thực hiện các chính sách bảo mật trong CSDL

* **Bảo vệ dữ liệu mức dòng:** ta dùng điều kiện WHERE để loại những dòng dữ liệu cần bảo vệ khỏi View. Chẳng hạn, ta tạo View để truy vấn thông tin nhân viên kế toán (KT), những nhân viên khác sẽ không được xem

CREATE VIEW NHAN\_VIEN\_KE\_TOAN

AS

SELECT \*

FROM NHAN\_VIEN

**WHERE LOAI\_NHAN\_VIEN = ‘KE TOAN’;**

* **Bảo vệ dữ liệu mức cột**: ta có thể chọn ra những cột dữ liệu cần thiết cho View và ẩn những cột còn lại đi. Chẳng hạn, ta tạo View để truy vấn thông mã nhân viên và họ tên nhân viên, các trường còn lại (ngày sinh, số CMND, lương,…) sẽ bị ẩn đi khỏi View.

CREATE VIEW NHAN\_VIEN\_THONG\_TIN

AS

**SELECT MA\_NHAN\_VIEN, HO\_TEN**

FROM NHAN\_VIEN;

1. **Quyền người dùng (Privilege)**

**Quyền người dùng (privilege)** là sự cho phép người dùng thực hiện một câu lệnh SQL cụ thể hoặc thực hiện truy cập đến các objects của các người dùng khác (hay schema khác).

Có 2 loại quyền trong Oracle:

* **Quyền hệ thống (System privilege):** Cho phép người dùng thực hiện hành động trên đối tượng (table, view, index,…) của **bất kì schema nào**. Loại quyền này chỉ nên cấp cho những user có độ tin cậy và quyền hành cao. Ảnh có chứa văn bản

  Mô tả được tạo tự động

*(Ví dụ 1 số quyền hệ thống. Nguồn:* [*Privileges (oracle.com)*](https://docs.oracle.com/database/121/TTSQL/privileges.htm#TTSQL339)*)*

* **Quyền đối tượng (Object privilege):** Cho phép 1 user có thể thực hiện hành động hoặc truy cập vào các **đối tượng của 1 user khác** (schema khác). **User sẽ có toàn bộ quyền đối tượng trên schema của mình**Ảnh có chứa văn bản

  Mô tả được tạo tự động *(Ví dụ 1 số quyền đối tượng. Nguồn:* [*Privileges (oracle.com)*](https://docs.oracle.com/database/121/TTSQL/privileges.htm#TTSQL339)*)*

**Cú pháp câu lệnh cấp quyền:**

* **GRANT <PRIVILLEGE> ON <OBJECT> TO <USER>** (với những câu lệnh có mức cột thì privilege cần có thêm thông tin cột)
* Ví dụ:
  + **GRANT SELECT ON ANOTHER.TABLE\_TEST TO USER\_TEST**: cấp quyền SELECT trên bảng TABLE\_TEST của schema ANOTHER cho user USER\_TEST.
  + **GRANT UPDATE(COLUMN\_1, COLUMN\_2) ON ANOTHER.TABLE\_TEST TO USER\_TEST**: cấp quyền UPDATE trên các cột COLUMN\_1, COLUMN\_2 của bảng TABLE\_TEST thuộc schema ANOTHER cho user USER\_TEST.

**Cú pháp câu lệnh thu hồi quyền đã cấp:**

* **REVOKE <PRIVILLEGE> ON <OBJECT> FROM <USER>** (khi thu hồi chỉ thu hồi toàn bộ quyền, không thu hồi trên chi tiết từng cột)
* Ví dụ:
  + **REVOKE UPDATE(COLUMN\_1) ON ANOTHER.TABLE\_TEST FROM USER\_TEST**: Đây là **câu lệnh sai** do tiến hành thu hồi trên cột.
  + **REVOKE UPDATE ON ANOTHER.TABLE\_TEST FROM USER\_TEST**: Đây là câu lệnh đúng, tiến hành thu hồi quyền UPDATE trên bảng TABLE\_TEST thuộc shema ANOTHER của user USER\_TEST.

1. **Triển khai cài đặt**
2. **Xem thông tin các đối tượng**

**Xem các users trong hệ thống:** ta sử dụng view **DBA\_USERS** để lấy thông tin các user Ảnh có chứa bàn

Mô tả được tạo tự động

*(Tất cả user trong hệ thống)*

**Xem các roles trong hệ thống:** ta sử dụng view **DBA\_ROLES** để lấy tất cả roleẢnh có chứa văn bản

Mô tả được tạo tự động

*(Tất cả role trong hệ thống)*

**Xem các roles đã được cấp cho 1 user hoặc các users trong 1 role:** ta sử dụng view **DBA\_ROLE\_PRIVS** với cột **GRANTEE** là user hoặc role được gán, và **GRANTED\_ROLE** là role gán.

Ảnh có chứa văn bản

Mô tả được tạo tự động

*(Liệt kê những role/user được cấp role)*

1. **Tạo/xóa các đối tượng**

Để tạo các đối tượng ta cần lấy thông tin về tin về schema và tên của đối tượng đó.

Đầu tiên cần kiểm tra tên đối tượng đã tồn tại chưa

* **Đối với user, role** thì sử dụng view DBA\_ROLES và DBA\_USERS.
* **Đối với table** thì truy vấn view DBA\_TABLES (lấy ra thuộc tính OWNER và TABLE\_NAME) để xác nhận điều này.

Ta tiến hành tạo các đối tượng

* **Đối với role**, chỉ cần tên và schema của role đó: CREATE ROLE <schema>.<role>.
* **Đối với user**, ta cần thêm thông tin mặt khẩu của user: CREATE USER <user> IDENTIFIED BY <password>.
* **Đối với table**, cần cung cấp thông tin về các thuộc tính (kiểu dữ liệu, chiều dài dữ liệu, khóa chính, khóa ngoại (thuộc tính tham chiếu), cho phép null): Ta tạo 1 câu lệnh SQL để từ những thuộc tính đó theo mẫu (thế chuỗi):

CREATE TABLE <SCHEMA\_NAME>.<TABLE\_NAME> (

<COLUMN\_NAME> <DATA\_TYPE>(<DATA\_LENGTH>, <DATA\_PRECISION>) <NOT NULL> <UNIQUE>,

--Nếu thuộc tính là khóa ngoại

FOREIGN KEY (<COLUMN\_NAME>) REFERENCES <REF\_TABLE>(<REF\_COLUMN>)

…

PRIMARY KEY (<COLUMN\_NAME>,…));

1. **Quản lý quyền truy cập**

Ta đã điểm qua cú pháp cấp quyền và thu hồi quyền ở phần 1, ta chỉ cần lập trình để tạo những câu lệnh SQL dựa vào yêu cầu của DBA.

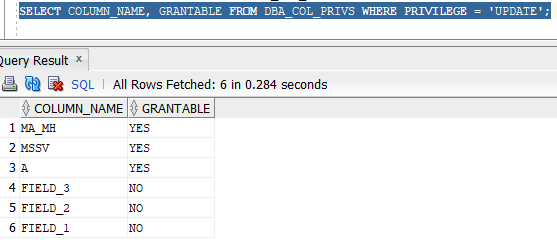
Để xem quyền của user, role trên các bảng:

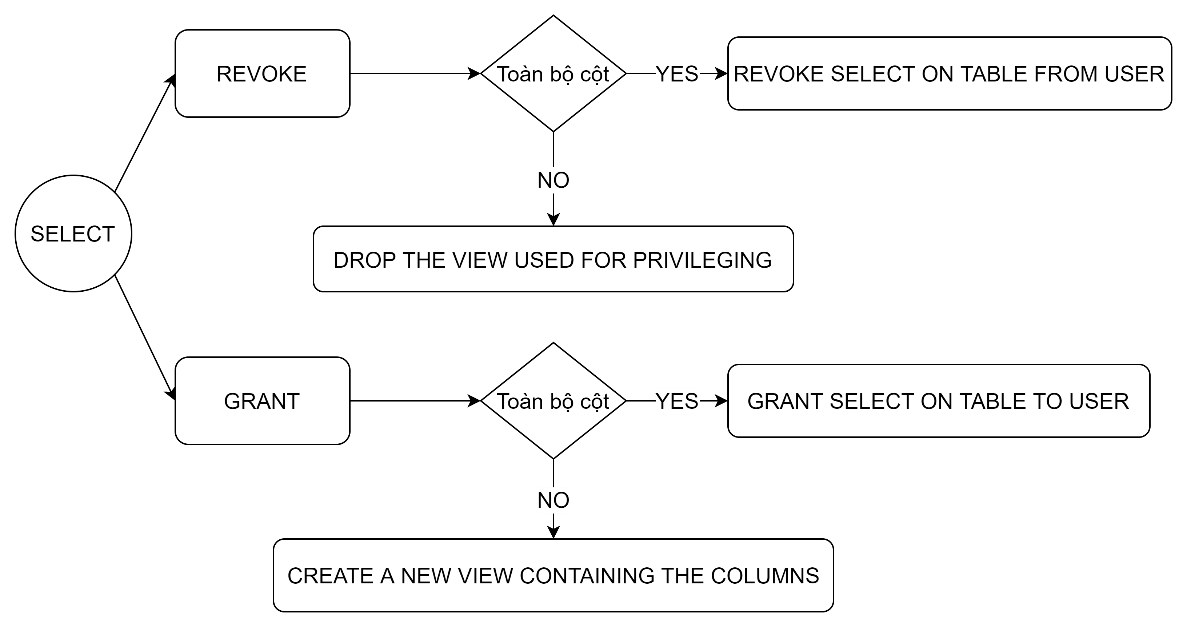
* Đối với quyền không chi tiết trên cột **(INSERT, DELETE)**, ta dùng view **DBA\_TAB\_PRIVS** để lấy thông tin về quyền, với PRIVILEGE là hành động, GRANTABLE là chỉ định WITH GRANT OPTION:

Ảnh có chứa bàn

Mô tả được tạo tự động

*(Liệt kê quyền trên bảng của user)*

* Đối với quyền chi tiết trên cột **(UPDATE),** ta dùng view **DBA\_COL\_PRIVS** để lấy thông tin về quyền trên các cột, với COLUMN\_NAME là tên cột, PRIVILEGE là hành động, GRANTABLE là chỉ định WITH GRANT OPTION: 

Đặc biệt chú ý, đối với quyền SELECT, do **Oracle không hỗ trợ cấp quyền SELECT chi tiết đến mức cột,** nên ta sẽ sử dụng View thay thế. Nếu DBA cấp quyền cho toàn bộ cột thì ta cấp bằng câu lệnh GRANT SELECT như bình thường, còn nếu cấp chi tiết đến cột thì ta sẽ tạo View mới có tên là <schema>.<user>\_SELECT\_ON\_<table> với những cột đã chọn. Khi thu hồi quyền ta sẽ tiến hành thu hồi quyền SELECT trên bảng đi (nếu user có quyền trên toàn bộ cột) hoặc xóa hẳn View dùng cho việc cấp quyền đi (nếu user có quyền trên 1 số cột). 

(Mô tả việc cấp/thu hồi quyền SELECT)

1. **Phân hệ 2**
2. **Tóm tắt lý thuyết**
3. **DAC**

**Mô hình DAC (Discretionary Access Control - Điều khiển truy cập tùy quyền)** thực hiện phân quyền dựa trên mỗi người dùng, xem xét người dùng U có quyền P gì trên đối tượng O của cơ sở dữ liệu. DAC cho phép người dùng có thể cấp quyền truy cập vào những đối tượng mà họ có quyền cho người dùng khác.

Ví dụ, ta cấp quyền cho user GROUP\_1 để đọc trên bảng NHAN\_VIEN, và cho phép GROUP\_1 có thể cấp quyền đọc cho bất kì user nào khác trên bảng NHAN\_VIEN

GRANT SELECT ON NHAN\_VIEN TO GROUP\_1 WITH GRANT OPTION

Sau đó, GROUP\_1 cấp quyền đọc cho GROUP\_2, tuy nhiên không muốn cho GROUP\_2 cấp quyền này cho ai

GRANT SELECT ON NHAN\_VIEN TO GROUP\_2;

Khi quyền đọc trên NHAN\_VIEN của GROUP\_1 bị thu hồi, thì GROUP\_2 cũng bị mất quyền này đi trong trường hợp là Oracle database, tuy nhiên sự thu hồi này có thể khác đi ở những RDBMS khác (có thể là GROUP\_2 vẫn còn giữ được quyền của mình).

REVOKE SELECT ON NHAN\_VIEN FROM GROUP\_1

* Có thể dẫn đến:REVOKE SELECT ON NHAN\_VIEN FROM GROUP\_2

**Mô hình DAC tập trung vào cá nhân hóa của mỗi người dùng,** thường là cho phép họ truy cập vào những dòng dữ liệu có liên quan đến chính bản thân mình. DAC thường sử dụng View (đã đề cập ở phần I) như cơ chế bảo mật để ép thỏa.

Ví dụ, ta có 1 View

CREATE VIEW NHAN\_VIEN\_KE\_TOAN

AS

SELECT \*

FROM NHAN\_VIEN

**WHERE MA\_NHAN\_VIEN = USER;**

View này được sử dụng để mỗi nhân viên chỉ có thể truy cập vào dòng dữ liệu của chính mình.

Nhận xét về DAC, thì đây là mô hình cấp quyền rất linh hoạt, mỗi người dùng có thể có những quyền đa dạng tùy vào vai trò của họ trong hệ thống. Tuy nhiên, mô hình này sẽ trở nên cồng kền và khó quản lý khi mà số lượng người dùng trong hệ thống quá lớn, việc cấp những quyền thích hợp cho mỗi người dùng là rất tốn chi phí và thời gian, dẫn đến sự ra đời của mô hình có tính thực tế hơn là RBAC.

1. **RBAC**

Để nói về RBAC, đầu tiên ta cần phải hiểu về role (vai trò). Như đã đề cập ở phần I, role là một tập những quyền trong hệ thống, những người dùng ở trong role bất kì sẽ được thực hiện tất cả những quyền của role đó. Chẳng hạn, ta có role NHAN\_VIEN\_ROLE

CREATE ROLE NHAN\_VIEN

Ta cấp quyền SELECT, UPDATE cho role NHAN\_VIEN\_ROLE trên bảng NHAN\_VIEN

GRANT SELECT, UPDATE ON NHAN\_VIEN TO NHAN\_VIEN\_ROLE

Lúc này, những người dùng nằm trong role NHAN\_VIEN sẽ có quyền SELECT, UPDATE trên bảng NHAN\_VIEN. Ví dụ, ta thêm người dùng GROUP\_1 vào role NHAN\_VIEN\_ROLE

GRANT NHAN\_VIEN\_ROLE TO GROUP\_1

RBAC cho thấy tính hiệu quả của nó trong những hệ thống lớn, khi mà số lượng người dùng lên đến 5, 6 con số (thậm chí là lớn hơn), thì tất cả những gì ta cần làm là đưa họ vào những role thích hợp.

1. **VPD**

Ở phần trên, khi đề cập đến DAC ta có điểm qua cách sử dụng View để bảo mật dữ liệu cấp dòng (chỉ cấp quyền truy cập trên những dòng dữ liệu thích hợp với mỗi người dụng cụ thể, hay còn gọi là Row-Level Security).

Tuy nhiên, ta có thể nhìn ra điểm yếu của việc ép thỏa bằng View, đó chính là số lượng View sẽ “bùng nổ” khi mà ta có quá nhiều vai trò khác nhau trong hệ thống, chẳng hạn như trong đồ án này, ta có các người dùng “Thanh tra”, “Nghiên cứu”, “Cơ sở y tế”, “Bác sĩ” khi xem thông tin trên bảng HSBA (Hồ sơ bệnh án) sẽ ra những dòng khác nhau, điều đó đồng nghĩa với việc ta phải 4 View khác nhau và cấp quyền cho từng role trên những View thích hợp. Việc này sẽ trở nên khó khăn hơn trong việc quản lý và gây tốn chi phí, thử tưởng tượng ta có thêm 10 hay 20 vai trò trong hệ thống thì lại tạo thêm 10 hay 20 View, và khi yêu cầu nghiệp vụ thay đổi thì ta phải đi chỉnh sửa từng View cho phù hợp. Khái niệm VPD ra đời nhằm giải quyết tình huống này.

VPD là cơ chế bảo mật (thường dùng cho các chính sách bảo mật dữ liệu cấp dòng), nó hoạt động bằng cách tự động thêm các vị từ trong truy vấn của người dùng.

Vị từ đơn giản là những câu điều kiện nằm sau mệnh đề WHERE trong câu truy vấn, chẳng hạn ta có câu truy vấn

SELECT \* FROM NHAN\_VIEN WHERE MANV != 10

Thì vị tự ở đây là ‘MANV != 10’

Vậy, rất đơn giản, ta sẽ tạo ra các vị từ cho VPD để nó tự động thêm vào trong các câu truy vấn (thêm điều kiện WHERE hoặc AND với những điều kiện đã có trong câu)

Để tạo vị từ, ta sẽ sử dụng các hàm (Function) để trả về vị từ, chẳng hạn ta có 1 hàm để trả về toàn bộ nhân viên nếu người đọc là DBA, hoặc trả về các nhân viên không phải là ‘Giám đốc’ nếu người đọc là người khác.

CREATE OR REPLACE FUNCTION LAY\_VI\_TU (

schema\_name IN VARCHAR2 DEFAULT NULL,

object\_name IN VARCHAR2 DEFAULT NULL)

AS

BEGIN

IF USER = ‘SYS’

THEN

RETURN ‘1 = 1’; --Trả ra tất cả các dòng

END IF;

RETURN ‘VAITRO != ‘’’GIAMDOC’’’’;

END;

Ta tiến hành áp dụng VPD trên bảng NHAN\_VIEN

DBMS\_RLS.ADD\_POLICY(

object\_name => ‘NHAN\_VIEN',

policy\_name => ‘SELECT\_NV',

policy\_function => 'LAY\_VI\_TU’);

Khi đó, ví dụ ta truy vấn

SELECT \* FROM NHAN\_VIEN

Oracle sẽ tự động thêm điều kiện cho câu truy vấn

Nếu người dùng hiện tại là DBA thì câu truy vấn thực sự sẽ trở thành

SELECT \* FROM NHAN\_VIEN WHERE 1 = 1 --Trả về mọi dòng

Nếu người dùng hiện tại là người nào khác ngoài DBA, thì câu truy vấn thực sự sẽ trở thành

SELECT \* FROM NHAN\_VIEN WHERE VAITRO != ‘GIAMDOC’

1. **OLS**

Ngoại trừ View và VPD, ta vẫn còn 1 cơ chế bảo mật dữ liệu cấp độ dòng rất hiệu quả là **OLS (Oracle label security).**

OLS hoạt động bằng cách sử dụng các khái niệm level, compartment, group của người dùng, tiến hành đánh nhãn dữ liệu (thành phần của nhãn bao gồm level, compartment và group đó), khi người dùng truy cập dữ liệu, Oracle sẽ đánh giá so sánh nhãn của dữ liệu và nhãn của người dùng dựa vào thuật toán để xác định có cho phép truy cập hay không.

Level (cấp độ): dùng để đánh giá cấp bậc của người dùng (biểu thị mức độ quan trọng của họ trong hệ thống), ví dụ ta có các level ‘Nhân viên tập sự’, ‘Nhân viên chính thức’, ‘Quản lý’, level là tiêu chí quan trọng đầu tiên quan trọng nhất để xem xét khả năng truy cập của người dùng.

**Compartment:** đề cập tiêu chí lĩnh vực của người dùng trong hệ thống, chẳng hạn ta có các lĩnh vực trong đồ án là ‘Khoa nội’, ‘Khoa ngoại’ và ‘Chuyên sâu’. Compartment là tiêu chí không bắt buộc khi gán nhãn dữ liệu.

**Group:** đề cập tiêu chí khu vực hoạt động của người dùng trong hệ thống, chẳng hạn ta có các khu vực trong đồ án là ‘Cận trung tâm’, ‘Ngoại thành’ và ‘Cận thành’. Group là tiêu chí không bắt buộc khi gán nhãn dữ liệu.

**Nhãn được ghi như sau:** ‘Level:Compartment\_1,Compartment\_2,…,Compartment\_n:Group\_1,Group\_2,…,Group\_n’

**Thuật toán để Oracle xem xét cho phép truy cập dữ liệu (đọc dữ liệu)**

* Level của người dùng phải lớn hơn hoặc bằng level của dữ liệu
* Compartment của người dùng phải bao gồm toàn bộ compartment của dữ liệu
* Group của người dùng phải bao gồm ít nhất 1 group của dữ liệu

Chẳng hạn, ta có các level YBS < GDS; compartment KN, CS; Group CTT, NT

Nếu một dữ liệu có nhãn ‘YBS:KN:CTT’ thì yêu cầu người dùng phải có ít nhất level YBS (YBS hay GDS), compartment phải có KN, group phải có ít nhất CTT

Nếu một dữ liệu có nhãn ‘GDS:KN,CS:CTT,NT’ thì yêu cầu người dùng phải có ít nhất level GDS (hiện tại chỉ có GDS), compartment phải có KN, CS; group phải có CTT hoặc NT (1 trong 2).

Ta có thể thấy, so với VPD, OLS dễ thực hiện hơn rất nhiều, cách hoạt động cũng rất đơn giản và dễ hiểu, không cần phải code dài dòng và tính toán nhiều trường hợp như VPD. Tuy nhiên cũng có hạn chế, ví dụ ta phải xác định rõ ràng và chặt chẽ các level, compartment và group của từng người dùng trong hệ thống, đôi khi có những trường hợp đặc biệt ta muốn người dùng level thấp đọc những dữ liệu có level cao thì cũng khó khăn để thực hiện.

1. **Mã hóa**

Mã hóa là quá trình ẩn dữ liệu đi, biến nó thành dạng không thể đọc được (thường là trở thành chuỗi byte)

Mã hóa là lá chắn cuối cùng trong quá trình bảo mật cơ sở dữ liệu, dù cho kẻ xấu có đi qua những bước cấp quyền bên trên thì cũng không thể khai thác dữ liệu của hệ thống

Để thực hiện mã hóa, ta cần có khóa, tùy vào cơ chế mã hóa mã có thể xuất hiện thêm nhiều khóa. Có 2 cách mã hóa cơ bản nhất; Đầu tiên là mã hóa sử dụng khóa đối xứng, nghĩa là ta sử dụng cùng 1 khóa cho quá trình mã hóa và giải mã dữ liệu, cách làm này giúp đẩy mạnh hiệu năng của quá trình mã hóa nhờ sử dụng thuật toán đơn giản và khóa ngắn, ta cũng phải đối diện với sự khó khăn của việc phân phối khóa; Cách thứ 2 là mã hóa bằng khóa bất đối xứng, nghĩa là ta sử dụng 1 khóa (gọi là public key) cho quá trình mã hóa và sử dụng 1 khóa khác cho quá trình giải mã (gọi là private key), cách làm này giúp giải quyết vấn đề phân phối tuy nhiên lại gây ảnh hưởng về mặt hiệu năng do thuật toán phức tạp.

Vấn đề rất quan trọng trong mã hóa, đó là quản lý khóa (lưu trữ, phân phối, thay đổi khóa, làm mới khóa), điều này phụ thuộc phần lớn vào nơi chúng ta mã hóa (mức ứng dụng, mức hệ điều hành hay mức CSDL), 1 trong những cách mã hóa phổ bên nhất là mã hóa mức CSDL, việc mã hóa ở mức CSDL đem lại cho ta nhiều lợi ích: bảo mật dữ liệu khỏi những kẻ xâm nhập, kể cả DBA, có thể chia sẻ dữ liệu giữa nhiều ứng dụng với nhau; Đương nhiên, phương pháp này vẫn có những nhược điểm nhất định, như là làm chậm hoạt động của DB Server, không thể bảo vệ được tấn công ở mức ứng dụng.

1. **Audit**

Audit không phải là một cơ chế dùng để thực hiện cấp quyền truy cập cho người dùng.

Audit là cơ chế bảo mật hoạt động bằng cách ghi lại các hoạt động đã xảy ra trong cơ sở dữ liệu (tương tự như một nhật kí).

Mục đích chính của audit là để phát hiện ra những hoạt động bất thường trong hệ thống (phát hiện ra những lỗ hỏng bảo mật) và ai là người gây ra sự bất thường này (tránh sự thoái thác trách nhiệm), audit còn dùng để truy vết những lần cập nhật dữ liệu.

Trong Oracle ta có 2 loại audit chính là **Standard audit** và **Fine-grained audit.**

Standard là audit chuẩn của Oracle, sẽ ghi nhận lại toàn bộ hoạt động mà ta đã chỉ định, ta có thể thực hiện audit trên table, view, procedure,…

Chẳng hạn ta thực hiện audit cho hành động SELECT trên bảng NHAN\_VIEN khi không thành công (BY ACCESS là chỉ định ghi trên mỗi lần truy cập, nếu dùng BY SESSION thì chỉ ghi trên mỗi session dù có truy cập bao nhiêu lần)

AUDIT SELECT ON NHAN\_VIEN BY ACCESS WHENEVER NOT SUCCESSFUL

Fine-grained audit hỗ trợ nhiều hơn so với Standard audit, ta sẽ nghĩ đến những trường hợp khi mà chỉ cần audit ở 1 điều kiện cụ thể, hay chỉ audit khi truy cập lên những cột nào đó.

Chẳng hạn ta thực hiện audit khi người đọc bảng NHAN\_VIEN không phải là chính họ

dbms\_fga.add\_policy(object\_schema => 'C##QLKCB',

object\_name => 'NHANVIEN',

policy\_name => 'audit\_nhanvien\_another\_pol',

audit\_condition => 'USERNAME != USER',

statement\_types => 'SELECT');

Thực hiện audit khi có cập nhật trên trường lương của nhân viên

dbms\_fga.add\_policy(object\_schema => 'C##QLKCB',

object\_name => 'NHANVIEN',

policy\_name => 'audit\_nhanvien\_salary\_pol',

audit\_column => ‘LUONG’

statement\_types => ‘UPDATE');

1. **Các chính sách bảo mật trong đồ án**
2. **Kết nối dòng dữ liệu với tài khoản người dùng**

Ta cần kết nối dòng dữ liệu với tài khoản người dùng, ta có 2 bảng NHANVIEN và BENHNHAN cần thực hiện điều này.

Ta có thể thực hiện điều này bằng cách cho trường mã (nhân viên/bệnh nhân) chính là username của người dùng. Tuy nhiên, điều này có thể làm lộ username của người dùng khi mã của họ bị lộ, nên ta sẽ dùng cách thứ 2. Ta sẽ chèn thêm 1 trường USERNAME cho 2 bảng NHANVIEN và BENHNHAN (tất nhiên là thuộc tính UNIQUE) **Ảnh có chứa văn bản

Mô tả được tạo tự động**

1. **Ứng dụng DAC + RBAC**

**Xem thông tin bệnh nhân: ta có yêu cầu nghiệp vụ**

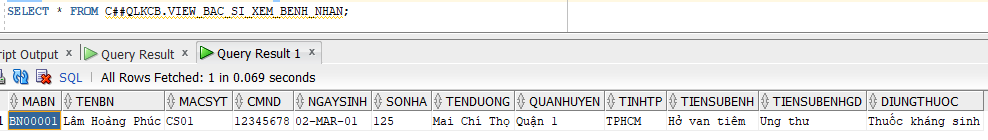
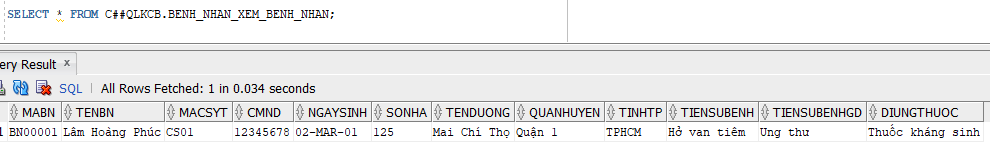
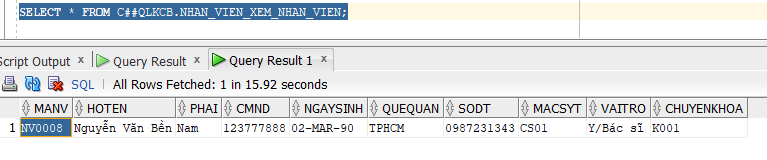
* Thanh tra có thể xem thông tin toàn bộ bệnh nhân trong hệ thống
* Bệnh nhân có thể xem thông tin của chính mình
* Bác sĩ có thể xem thông tin bệnh nhân mà mình đã chữa trị

**Xem thông tin nhân viên:**

* Nhân viên có thể xem thông tin của chính mình
* Thanh tra có thể xem thông tin của toàn bộ nhân viên trong hệ thống

Ta có thể thấy trước mặt, ta cần tạo ra 2 View để xem thông tin bệnh nhân và 1 View để xem thông tin nhân viên, xét thấy số lượng này là không lớn, hơn nữa cũng không yêu cầu thuật toán quá khó khăn nên ta vẫn sẽ áp dụng cơ chế View để ép thỏa các chính sách này thay vì dùng VPD.

Ngoài Thanh tra viên có thể đọc thẳng trên bảng gốc (xem toàn bộ), thì với nhân viên thường, bác sĩ và bệnh nhân cần phải tạo 3 View

* View cho bác sĩ xem thông tin bệnh nhân: chỉ lấy những bệnh nhân có hồ sơ bệnh án có mã bác sĩ trùng với bác sĩ đang truy cập. Ví dụ khi bác sĩ có mã ‘NV0008’ xem thông tin bệnh nhân 
* View cho bệnh nhân xem thông tin cá nhân: chỉ lấy bệnh nhân có USERNAME trùng với USER hiện tại đang truy cập. Ví dụ khi bệnh nhân ‘BN00001’ xem thông tin cá nhân
* View cho nhân viên xem thông tin cá nhân: chỉ lấy nhân viên có USERNAME trùng với USER hiện tại đang truy cập. Ví dụ khi nhân viên ‘NV0008’ xem thông tin cá nhân 

**Số lượng người dùng trong hệ thống là rất lớn nên ta cần tạo các role cho họ. Ta có các role như sau**

* BENHNHAN: cho toàn bộ người dùng bệnh nhân
* NHANVIEN: cho toàn bộ người dùng nhân viên
* THANHTRA: cho các nhân viên thanh tra
* BACSI: cho các nhân viên bác sĩ
* CSYT: cho các nhân viên cơ sở y tế
* NGHIENCUU: cho các nhân viên nghiên cứu

1. **Ứng dụng VPD**

**Xem hồ sơ bệnh án**

* Nhân viên Thanh tra và DBA có thể xem thông tin toàn bộ hồ sơ bệnh án
* Nhân viên Cơ sở y tế có thể đọc, thêm, xóa hồ sơ bệnh án thuộc cơ sở y tế của họ trong vòng từ ngày 5 đến ngày 27 tháng này
* Nhân viên Y/Bác sĩ có thể đọc hồ sơ bệnh án mà họ chữa trị (có mã bác sĩ trùng với mã nhân viên)
* Nhân viên Nghiên cứu có thể đọc hồ sơ bệnh án có thuộc cơ sở y tế và chuyên khoa của họ

**Xem hồ sơ bệnh án dịch vụ**

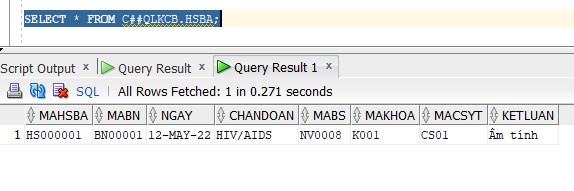
* Người dùng chỉ có thể đọc, thêm, xóa các dòng dịch vụ trong hồ sơ bệnh án nếu có quyền tương tự trên hồ sơ bệnh án của dòng dữ liệu này (nghĩa là có chính sách tương tự như hồ sơ bệnh án)

Phân tích vấn đề này, ta thấy rằng có thể tiếp cận được bằng cơ chế View, tuy nhiên ta sẽ phải tạo ít nhất 3 View cho bảng HSBA và 3 View cho bảng HSBA\_DV nếu muốn ép thỏa các chính sách một cách chặt chẽ. Xét thấy số lượng view này là khá lớn, hơn nữa các view bảng HSBA\_DV sẽ phải sử dụng các phép truy vấn để JOIN với bảng HSBA khá phức tạp, nên ta sẽ sử dụng 1 giải pháp hợp lí hơn là VPD.

**Ta cần 2 hàm trả ra vị từ cho 2 bảng HSBA và HSBA\_DV**

* **Hàm trả ra vị từ cho bảng HSBA**
* Nếu người dùng là DBA hoặc Thanh tra viên thì trả ra ‘1 = 1’ (toàn bộ dòng)
* Nếu người dùng là Cơ sở y tế thì trả ra 'MACSYT = MACSYT\_CUA\_NGUOI\_DUNG AND NGAY thuộc vào tháng này (ngày 5 – 27)’
* Nếu người dùng là Y/Bác sĩ thì trả ra ‘MABS = MANV’
* Nếu người dùng là Cơ sở y tế thì trả ra ‘MACSYT = MACSYT\_CUA\_NGUOI\_DUNG AND MAKHOA = MAKHOA\_CUA\_NGUOI\_DUNG’
* **Hàm trả ra vị từ cho bảng HSBA\_DV**: ta sẽ dùng điều kiện EXISTS để tìm dòng HSBA kết nối với nó và dùng điều kiện tương tự như hàm vị từ của HSBA đối với HSBA vừa tìm được

**Khi Thanh tra đọc bảng HSBA**Ảnh có chứa bàn

Mô tả được tạo tự động **Khi Bác sĩ ‘NV0008’ đọc bảng HSBA**

1. **Ứng dụng OLS**

Ta xét yêu cầu nghiệp vụ xem thông báo của người dùng. Có các cấp bậc người dùng: Y bác sĩ, Giám đốc cơ sở y tế, Giám đốc sở; Có các lĩnh vực Ngoại trú, Nội trú, Chuyên khoa; Có các khu vực Ngoại thành, Cận trung tâm, Trung tâm. Khi mà các yếu tố này đã được xác định rõ ràng, thì OLS là một lựa chọn tối ưu cho chính sách này, mặc dù VPD vẫn có thể được ứng dụng, tuy nhiên OLS sẽ dễ triển khai hơn rất nhiều, hơn nữa nếu thêm các vai trò này vào trong dữ liệu ban đầu có thể khiến ta phải chỉnh sửa các hàm vị từ VPD đã tạo.

**Đầu tiên, ta có các level trong hệ thống**

* YBS: Y bác sĩ, 7000
* GDCSYT: Giám đốc cơ sở y tế, 8000
* GDS: Giám đốc sở, 9000

**Ta có các compartments:**

* Ngoai: Ngoại trú
* Noi: Nội trú
* Sau: Điều trị chuyên sâu

**Ta có các group:**

* NT: Ngoại thành
* CTT: Cận trung tâm
* TT: Trung tâm

**Ta tạo 1 số nhãn cho dữ liệu trong bảng THONGBAO**

* (1) YBS: Toàn bộ user level ít nhất là YBS
* (2) YBS:noi,ngoai:ctt,tt: Toàn bộ user level ít nhất là YBS; bao gồm compartments Noi,Ngoai; ít nhất phải có group ctt hoặc tt
* (3) YBS:noi,sau:tt: Toàn bộ user level ít nhất là YBS; bao gồm compartments Noi,Sau; ít nhất phải có group tt
* (4) GDCSYT: Toàn bộ user có level ít nhất là GDCSYT
* (5) GDCSYT:noi,ngoai:tt: Toàn bộ user level ít nhất là GDSYT; bao gồm compartments Noi,Ngoai; ít nhất phải có group tt
* (6) GDS: Toàn bộ user có level ít nhất là GDS

**Ta thiết lập 1 số loại người dùng trong hệ thống**

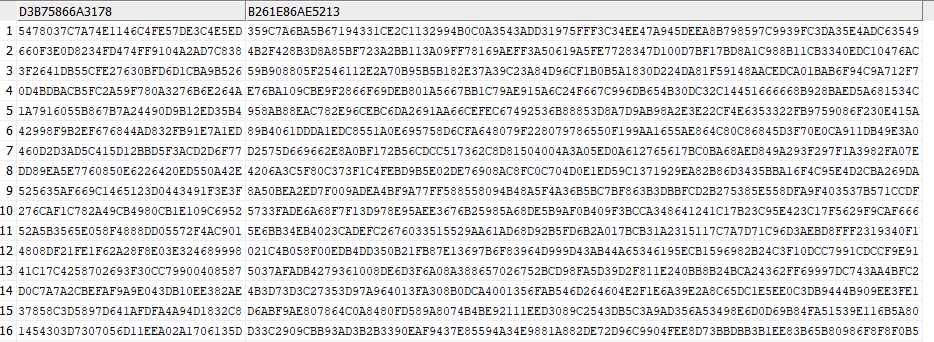
* YBS: có thể đọc (1)
* YBS:noi,ngoai:ctt: có thể đọc (1), (2)
* YBS:noi,ngoai,sau:tt: có thể đọc (1), (2), (3)
* GDCSYT:noi:tt: có thể đọc (1), (4)
* GDCSYT:noi,ngoai:nt: có thể đọc (1), (4)
* GDCSYT:noi,ngoai,sau:ctt,tt: có thể đọc (1), (2), (3), (4)
* GDS::nt: có thể đọc (1), (4), (6)
* GDS: ngoai,noi,sau:tt: có thể đọc toàn bộ dữ liệu

1. **Ứng dụng mã hóa**

Trong đồ án này, ta sẽ tiến hành **mã hóa dữ liệu CMND của bệnh nhân và nhân viên**.

Do ứng dụng của chúng ta không có 1 web server cố định, mà sử dụng Database như một server chính quản lý các hoạt động, nên ta sẽ tiến hành mã hóa ở mức CSDL.

Đầu tiên ta cần đề cập đến cách lưu trữ khóa. Do mã hóa mức CSDL, nên tốt nhất ta sẽ lưu trong cơ sở dữ liệu (bảng chứa khóa nằm trong schema khác) để tăng hiệu năng và dễ dàng trong việc giải mã. Trong hệ thống, mỗi nhân viên hay bệnh nhân có 1 khóa riêng, được tạo bằng hàm tạo byte ngẫu nhiên của Oracle, mỗi dòng trong bảng chứa khóa tương ứng với 1 khóa, gồm 2 thuộc tính là mã nhân viên/bệnh nhân và giá trị của khóa.

Bảng chứa khóa cũng là một yếu tố đáng quan tâm, nếu dữ liệu của bảng này bị truy cập bất hợp lệ thì coi như việc mã hóa thành “công cốc”. Do đó, ta sẽ chồng thêm 1 lớp bảo mật nữa, bằng cách mã hóa bảng chứ khóa, mỗi dòng khóa (thuộc về 1 bệnh nhân hay nhân viên) được mã hóa bằng key là 'mããm' (ví dụ BN001 có khóa của dòng khóa là 'BN0001100NB'), key này là do chúng ta tự suy diễn ra (sẽ viết thành thuật toán trong các function, procedure giải mã). Chú ý rằng, chúng ta không chỉ mã hóa trường khóa, mà còn mã hóa cả trường mã nhân viên/bệnh nhân trong bảng khóa, ta làm điều này là do nếu trường mã không bị ẩn đi, kẻ tấn công có thể dùng cột mã để suy diễn ra thuật toán mã hóa trong bảng chứa khóa. 

(Hình ảnh bảng chứa khóa)

Mỗi khi cần đọc, thêm, cập nhật CMND bảng nhân viên, bệnh nhân cần giải mã khóa trong bảng khóa rồi mới dùng khóa đó giải mã tìm ra CMND, có thể thấy cách mã hóa của chúng ta dù an toàn nhưng đã làm tốn chi phí của hệ thống khá nhiều.

Do khóa được lưu trong cơ sở dữ liệu, ta không cần bận quá tâm quá nhiều đến việc phân phối khóa, mất khóa, tuy nhiên phải bảo mật thật cẩn thận bảng chứa khóa, vì mất khóa thì coi như dữ liệu cũng “đi” theo.

Để thay đổi khóa cần cần giải mã ra CMND, xóa dòng trong bảng khóa, tạo khóa mới ngẫu nhiên, mã hóa lại CMND và insert khóa mới vào lại bảng chứa khóa.

1. **Ứng dụng Audit**
2. **Standard audit**

Bênh nhân và nhân viên là những người dùng trực tiếp trong hệ thông. Việc thêm, xóa nhân viên hay bênh nhân cần phải được ghi nhận lại

* Audit INSERT, DELETE trên bảng BENHNHAN và NHANVIEN

Các hoạt động khám chữa bệnh hàng ngày cần phải được ghi nhận lại (HSBA, HSBA\_DV), tránh những cập nhật không hợp lệ làm ảnh hưởng hoạt động của hệ thống, nếu có xảy ra thì cũng phải xem xét trách nhiệm của người đó

* Audit INSERT, DELETE, UPDATE trên bảng HSBA và HSBA\_DV

Bảng chứa khóa rất quan trọng, việc mất khóa hay sửa khóa có thể làm mất hẳn dữ liệu đã mã hóa, cần ghi nhận lại các hành động thêm, sửa, xóa trên bảng này

* Audit INSERT, DELETE, UPDATE trên bảng khóa

Hành động đọc không thành công trên bảng chứa khóa có thể là dấu hiệu cho kẻ xấu cố tình truy cập, cần ghi nhân lại.

* Audit hành động SELECT không thành công trên bảng khóa

Chúng ta có sử dụng khóa tự suy diễn (thuật toán được ghi lại trong các procedure và function), do đó cần ghi nhận lại khi có người cố tình truy cập xem mã nguồn của các procedure và function

* Audit SELECT trên view mà hệ thống cho xem thông tin các procedure (ALL\_SOURCE)

1. **Fine-grained audit**

Cần ghi nhận lại khi có người dùng bảng nhân viên hay bệnh nhân mà không phải là chính họ

* Fine-grained audit trên bảng nhân viên và bệnh nhân khi người truy xuất không phải chính họ (USER != USERNAME trong bảng)

Cần ghi nhận lại khi thông tin VAITRO, USERNAME, CMND của nhân viên được cập nhật, đây là những thông tin quan trọng, có thể làm ảnh hưởng đến quá trình hoạt động của hệ thống, chẳng hạn chỉnh sửa VAITRO có thể khiến cho nhân viên có thể xem mọi thông tin họ muốn nếu chỉnh thành Thanh tra viên.

* Fine-grained audit trên bảng nhân viên cho hành động UPDATE trên các trường VAITRO, USERNAME, CMND

Cần ghi nhận lại khi thông tin USERNAME, CMND của bệnh nhân được cập nhật, đây là những thông tin quan trọng nhất của bệnh nhân, chỉ có thể bị chỉnh sửa bởi nhân viên, nếu bị chỉnh sửa không hợp lệ cần truy ra ai là người thực hiện

* Fine-grained audit trên bảng bệnh nhân cho hành động UPDATE trên các trường USERNAME, CMND

1. **Tham khảo**

McGraw-Hill Osborne - Effective Oracle Database 10g Security by Design

Slide môn học của thầy Lương Vĩ Minh và cô Phạm Thị Bạch Huệ