**BỘ MÔN HỆ THỐNG THÔNG TIN – KHOA CÔNG NGHỆ THÔNG TIN**

**ĐẠI HỌC KHOA HỌC TỰ NHIÊN THÀNH PHỐ HỒ CHÍ MINH, ĐẠI HỌC QUỐC GIA TP HCM**

Nhóm thực hiện: ATBMCQ-20

GV phụ trách: Phạm Thị Bạch Huệ - Lương Vĩ Minh

HỌC KỲ II – NĂM HỌC 2021-2022

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

**BẢNG THÔNG TIN CHI TIẾT NHÓM**

|  |  |  |
| --- | --- | --- |
| **Mã nhóm:** | ATBMCQ-20 | |
| **Tên nhóm:** | ATBMCQ-20 | |
| **Số lượng:** | **4** | |
| **MSSV** | **Họ tên** | **Email** |
| 19120677 | Nguyễn Diệp Minh Tiến | 19120677@student.hcmus.edu.vn |
| 19120559 | Hà Duy Lãm | 19120559@student.hcmus.edu.vn |
| 19120661 | Lê Mai Nguyên Thảo | 19120661@student.hcmus.edu.vn |
| 19120545 | Lê Ngọc Khoa | 19120545@student.hcmus.edu.vn |

|  |  |  |  |
| --- | --- | --- | --- |
| **Bảng phân công & đánh giá hoàn thành công việc** | | | |
| **Công việc thực hiện** | **Người thực hiện** | **Mức độ hoàn thành** | **Đánh giá của nhóm** |
| Câu 4,8,10 | 19120677- Nguyễn Diệp Minh Tiến | 100% | 10/10 |
| Câu 1,6 | 19120559 - Hà Duy Lãm | 100% | 10/10 |
| Câu 2,7 | 19120661 - Lê Mai Nguyên Thảo | 100% | 10/10 |
| Câu 3,5,9 | 19120545 - Lê Ngọc Khoa | 100% | 10/10 |
| |  |  | | --- | --- | | **THÔNG TIN ĐỒ ÁN - BÀI TẬP** | | | **Đồ án – Bài tập** | AN TOÀN VÀ BẢO MẬT DỮ LIỆU TRONG HTTT  PHÂN HỆ 1 | | **Loại bài tập** | Đồ án - Nhóm | | | | |

**MỤC LỤC**

[**I.** **MÔ TẢ ĐỒ ÁN** 2](#_Toc107442471)

[**II.** **BÁO CÁO ĐỒ ÁN** 3](#_Toc107442472)

[**PHÂN HỆ 1: HỆ THỐNG DÀNH CHO NGƯỜI QUẢN TRỊ VIÊN:** 3](#_Toc107442473)

[1. Xem danh sách các đối tượng hiện có trên CSDL 3](#_Toc107442474)

[2. Thêm mới đối tượng 3](#_Toc107442475)

[3. Phân quyền/ lấy lại quyền của một user/ role. 5](#_Toc107442476)

[4. Xem quyền của một chủ thể cụ thể. 6](#_Toc107442477)

[5. Giao diện ứng dụng: 8](#_Toc107442478)

[6. Video demo: 12](#_Toc107442479)

[**PHÂN HỆ 2: HIỆN THỰC CÁC CHÍNH SÁCH BẢO MẬT** 12](#_Toc107442480)

[1. Thiết kế cơ sở dữ liệu: 12](#_Toc107442481)

[2. Các chính sách bảo mật: 17](#_Toc107442482)

[2.1 Chính sách DAC (*Direct access control*): 17](#_Toc107442483)

[2.2 Chính sách RBAC(*Role-based access control):* 17](#_Toc107442484)

[2.3 Chính sách VPD (*Virtual Private Database*): 17](#_Toc107442485)

[2.4 Chính sách OLS(*Oracle label security*): 18](#_Toc107442486)

[2.5 Chính sách mã hóa (Encrypt) 20](#_Toc107442487)

[2.6 Chính sách Audit: 21](#_Toc107442488)

1. **MÔ TẢ ĐỒ ÁN**

Đồ án xây dựng ứng dụng quản lý quá trình bình bầu tín nhiệm có 2 phân hệ.

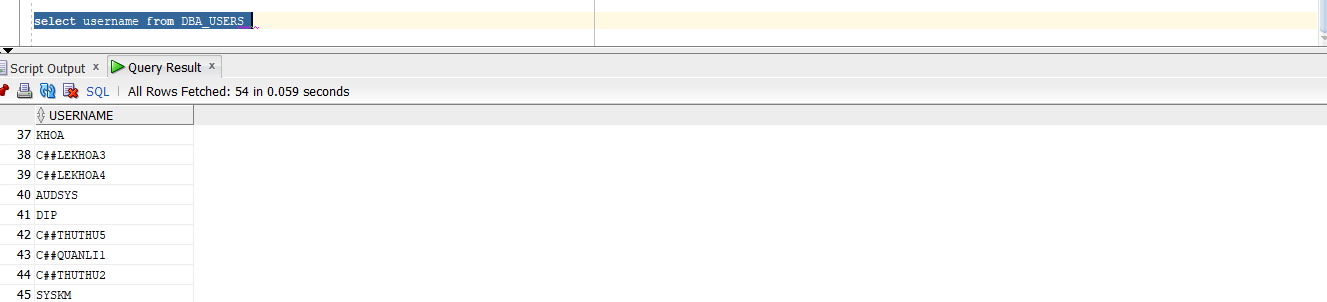
* **Phân hệ 1**: Dành cho người quản trị người dùng và điều khiển truy cập. Tạo các user, role, cấp quyền và thu quyền, xem quyền được cấp của một đối tượng cụ thể, …
* **Phân hệ 2**: Cấp quyền truy cập cho từng đối tượng, thiết lập cơ chế, chính sách bảo mật.

1. **BÁO CÁO ĐỒ ÁN**

## **PHÂN HỆ 1: HỆ THỐNG DÀNH CHO NGƯỜI QUẢN TRỊ VIÊN:**

1. Xem danh sách các đối tượng hiện có trên CSDL

* Danh sách user:



* Danh sách role:

Ảnh có chứa văn bản

Mô tả được tạo tự động

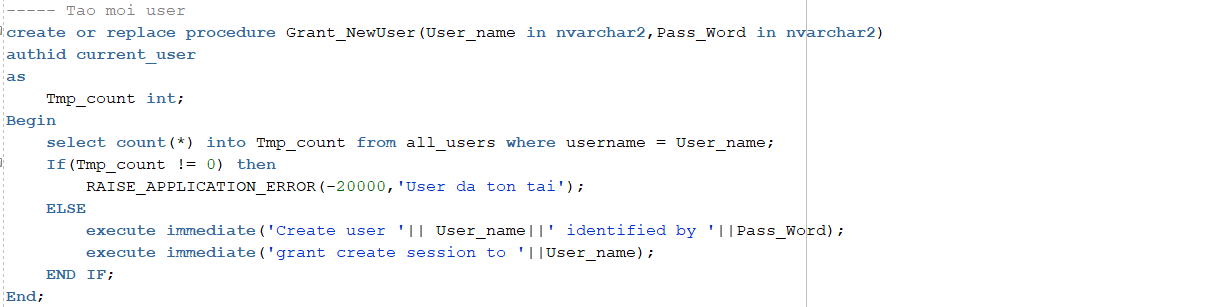
* Danh sách table

Ảnh có chứa bàn

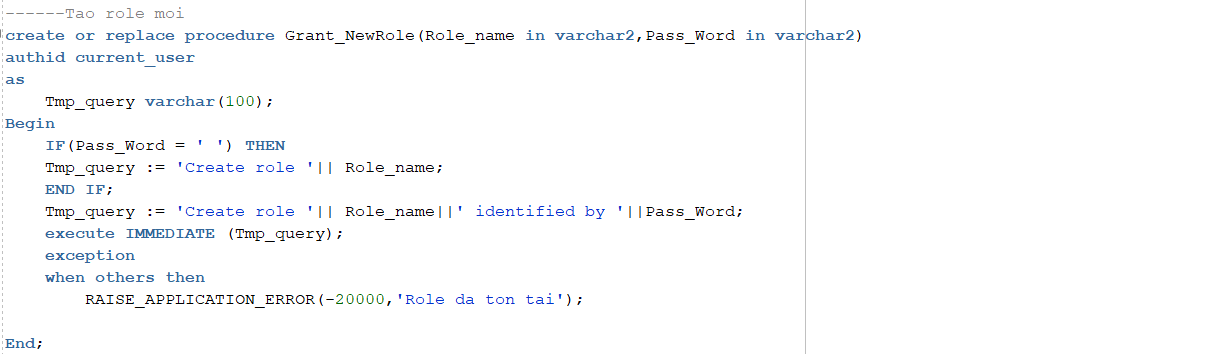
Mô tả được tạo tự động

1. Thêm mới đối tượng

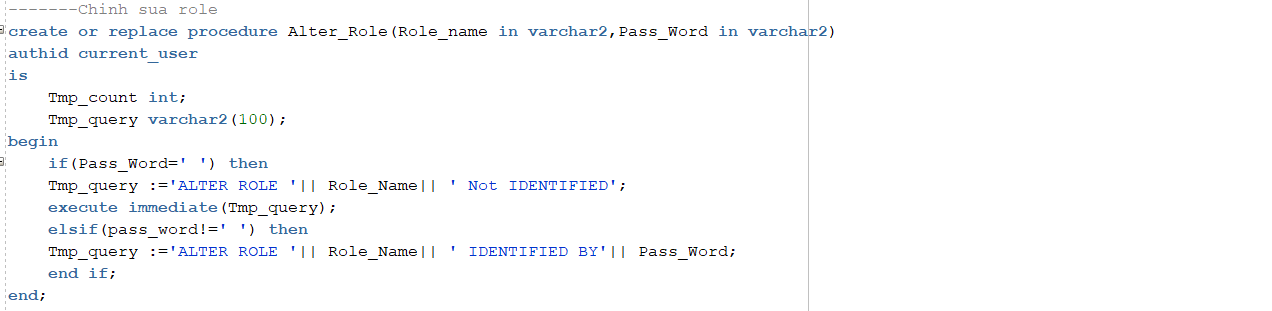
* Tạo mới user



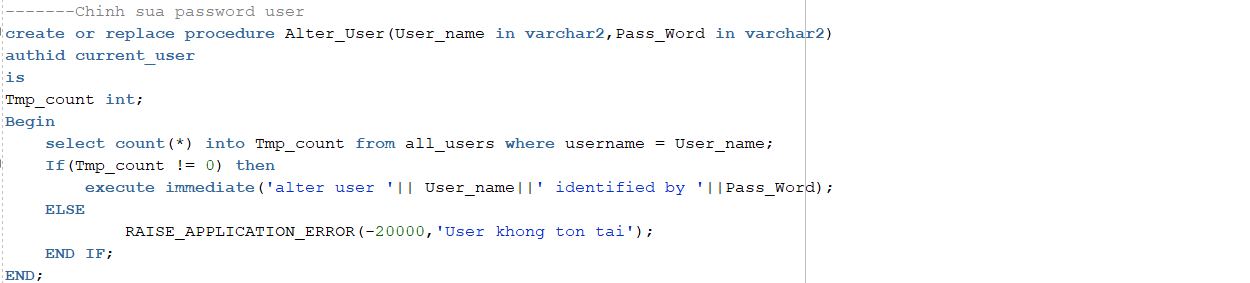
* Tạo mới role



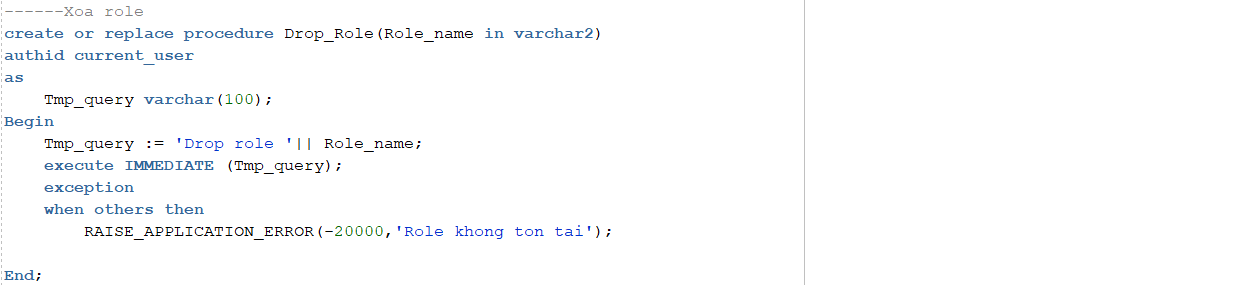
* Chỉnh sửa Role



* Chỉnh sửa password user

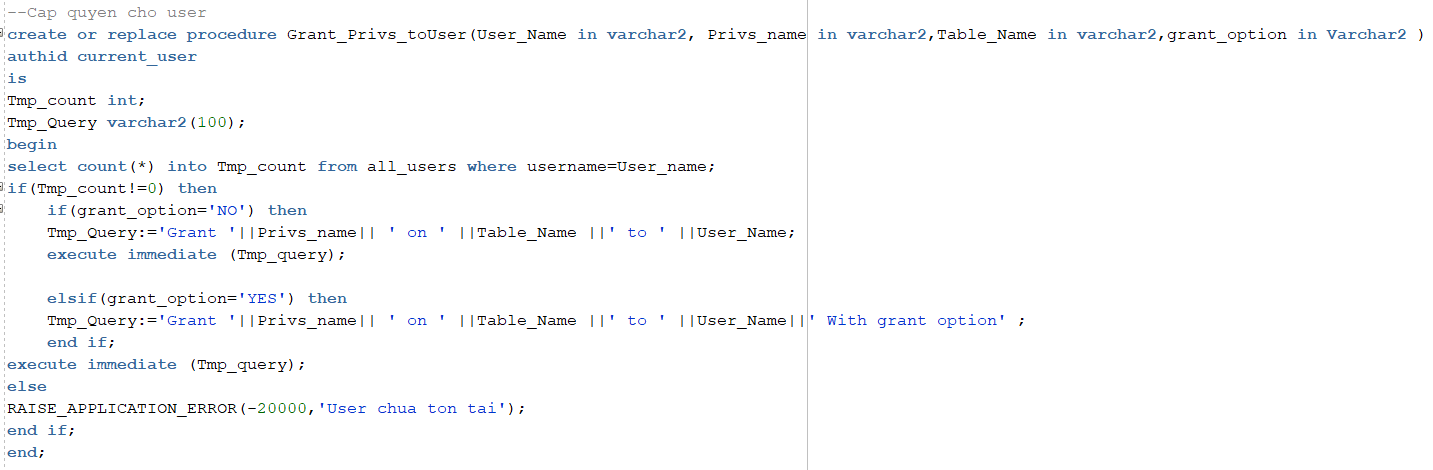


* Xóa role:

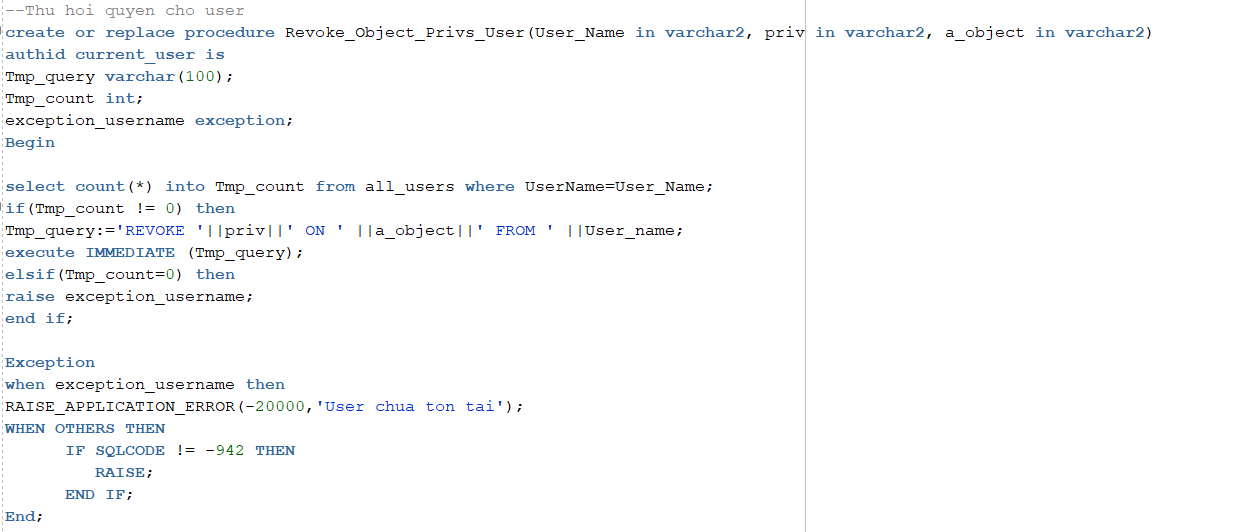


1. Phân quyền/ lấy lại quyền của một user/ role.

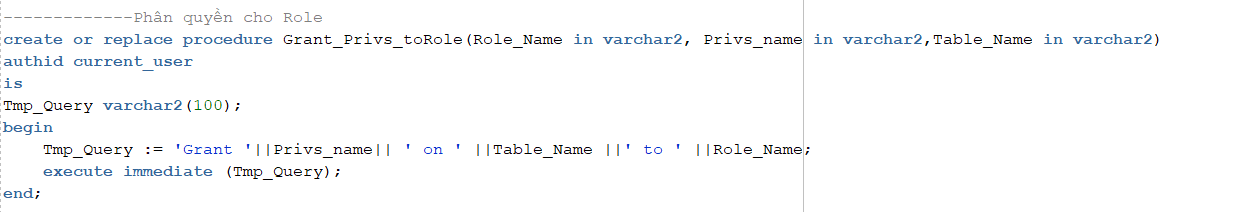
* Phân quyền cho user :



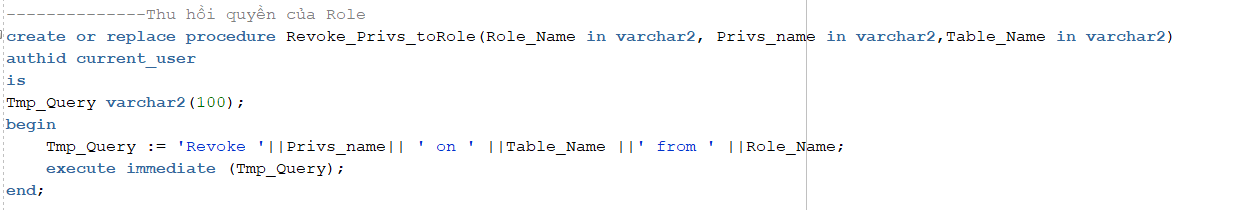
* Thu hồi quyền user:



* Phân quyền cho role:

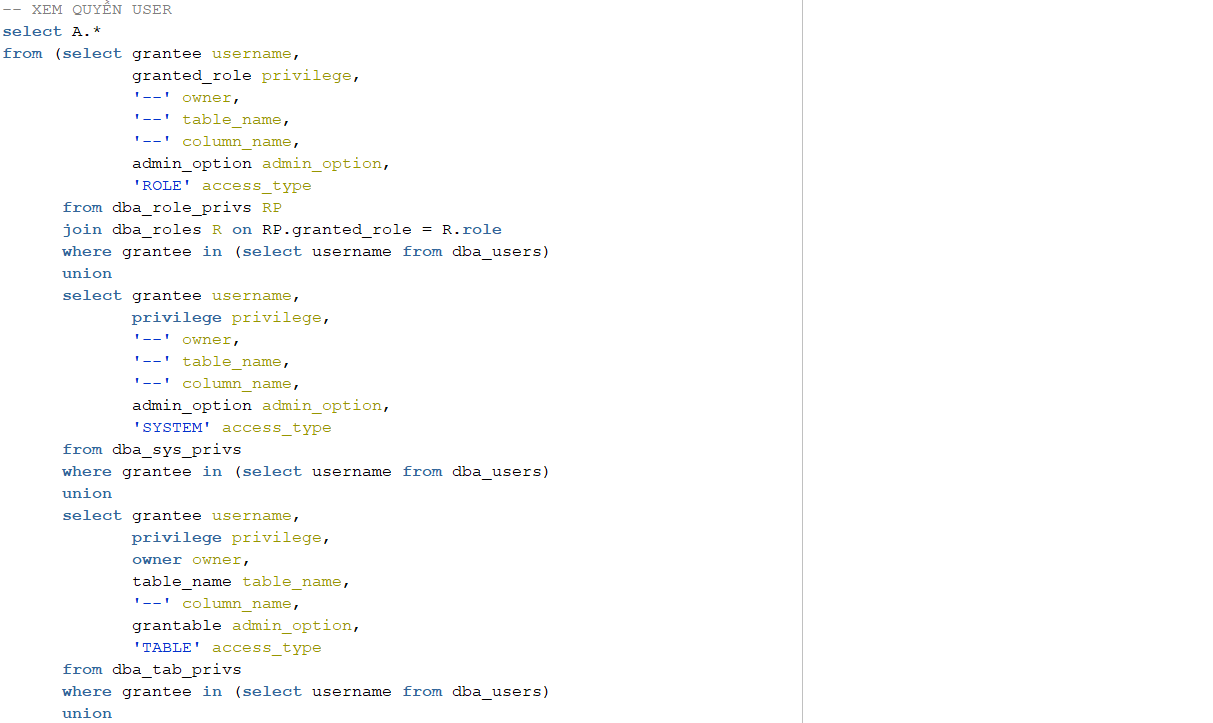


* Thu hồi quyền role:



1. Xem quyền của một chủ thể cụ thể.

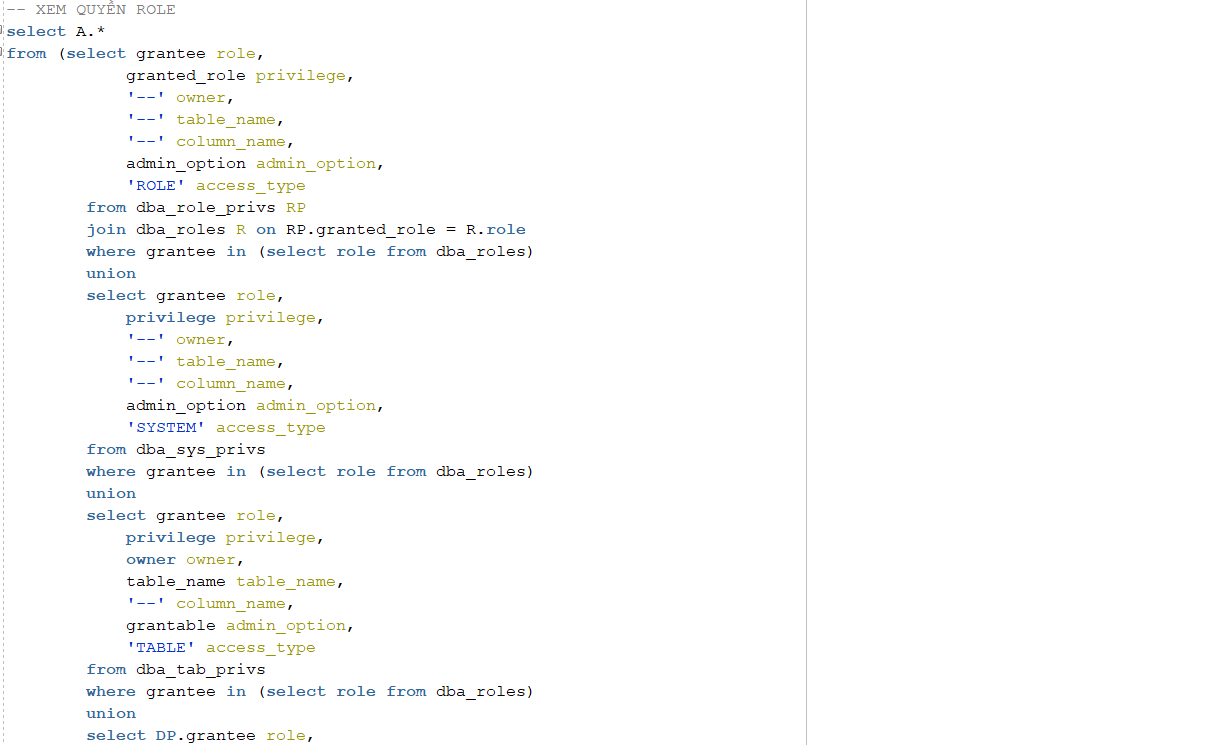
* Xem quyền của user:

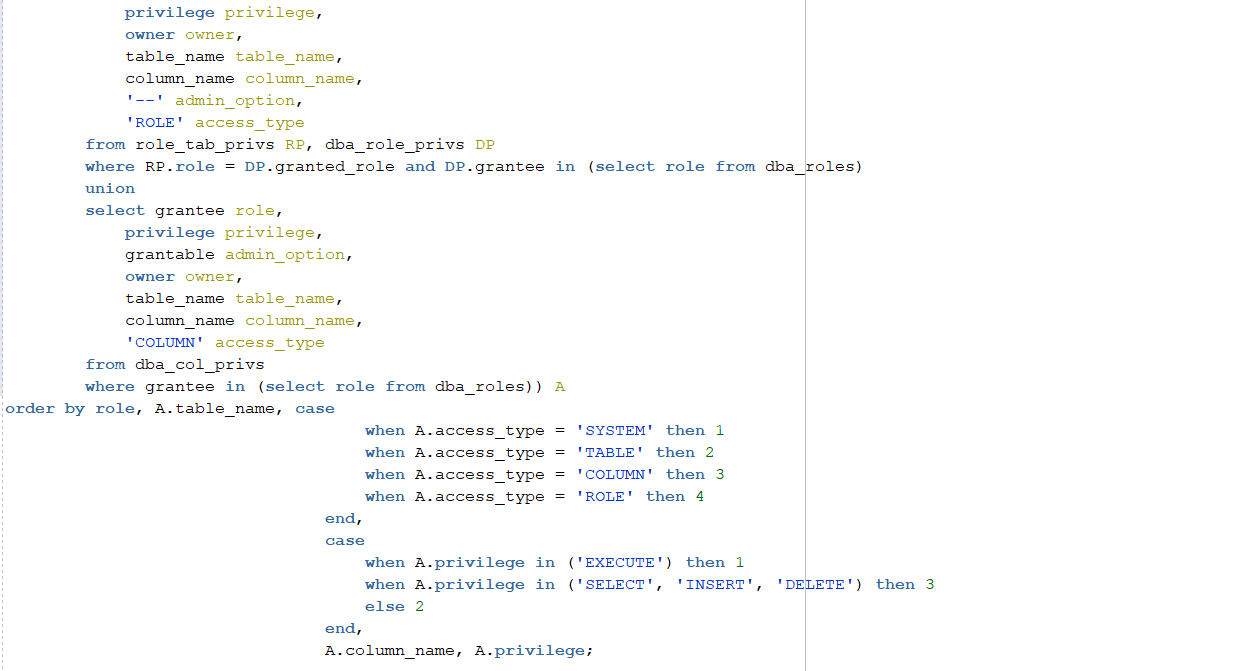


Ảnh có chứa văn bản

Mô tả được tạo tự động

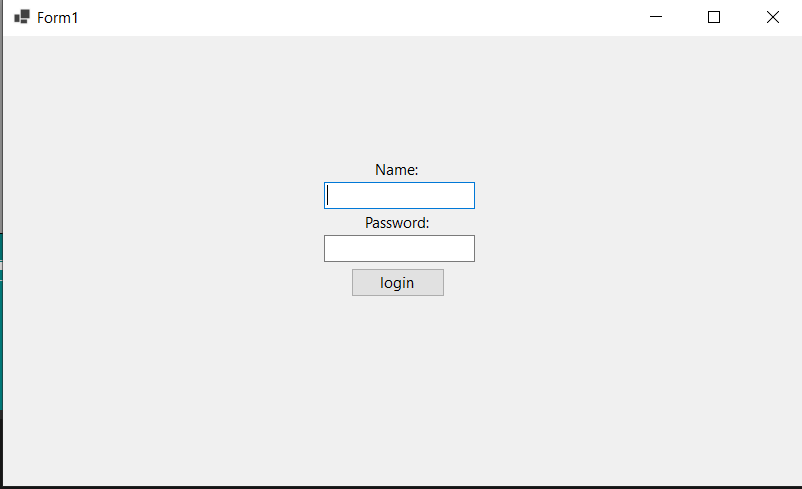
* Xem quyền của role



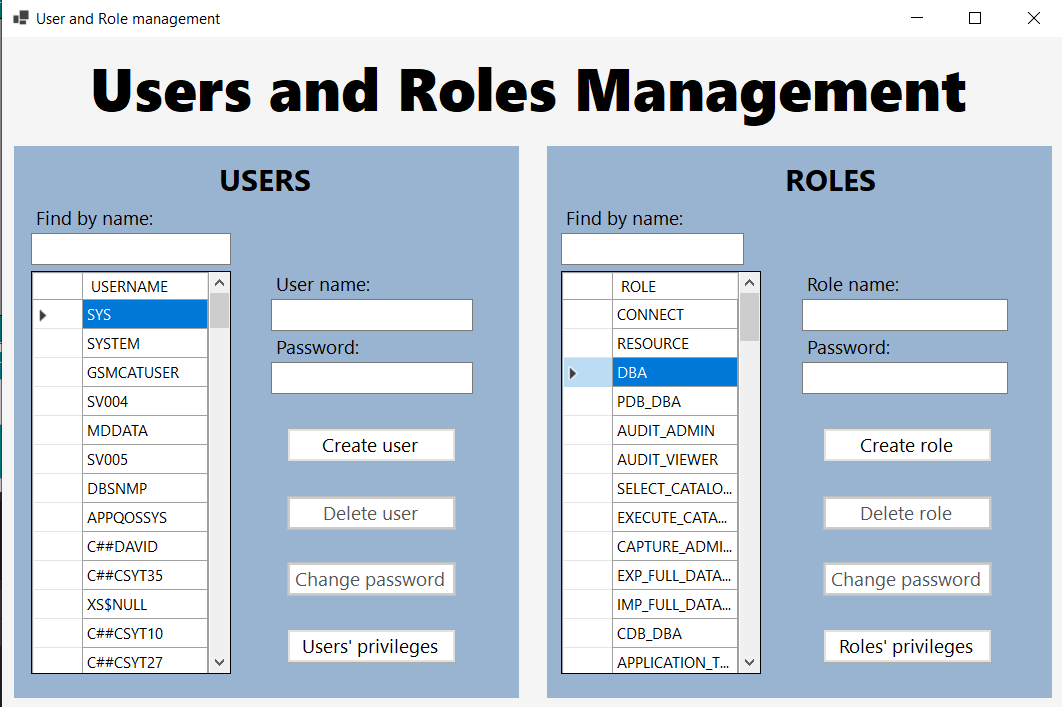


1. Giao diện ứng dụng:

* Giao diện login:



* Giao diện thêm, xóa, sửa user:



* Giao diện xem quyền của tất cả user:

Ảnh có chứa bàn

Mô tả được tạo tự động

* Giao diện tìm xem quyền của 1 user:

Ảnh có chứa bàn

Mô tả được tạo tự động

* Giao diện thêm quyền cho user:

Ảnh có chứa bàn

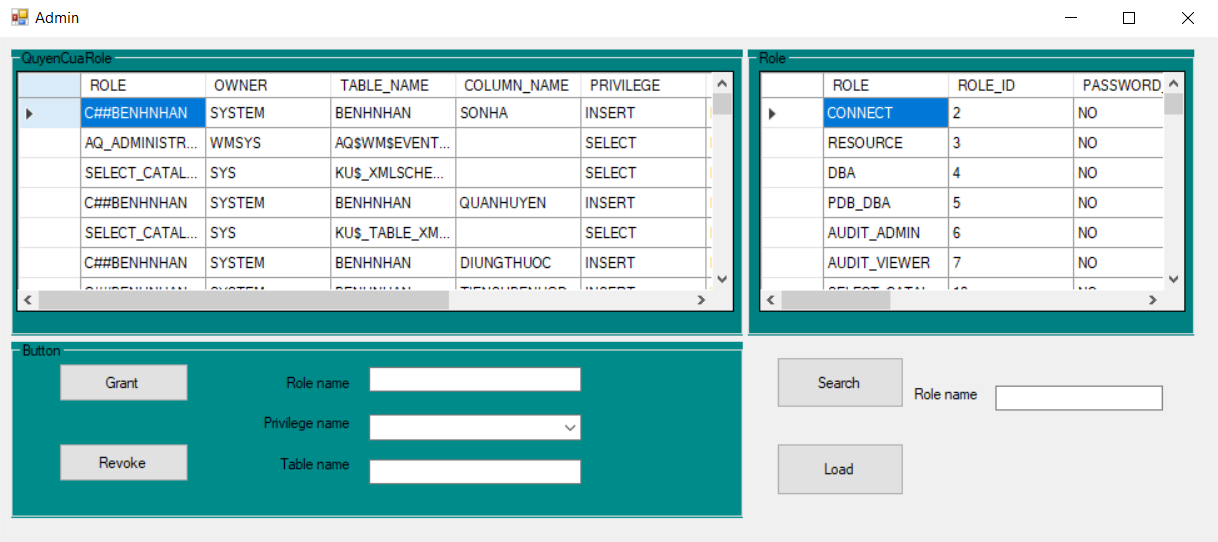
Mô tả được tạo tự động

* Giao diện thu quyền user:

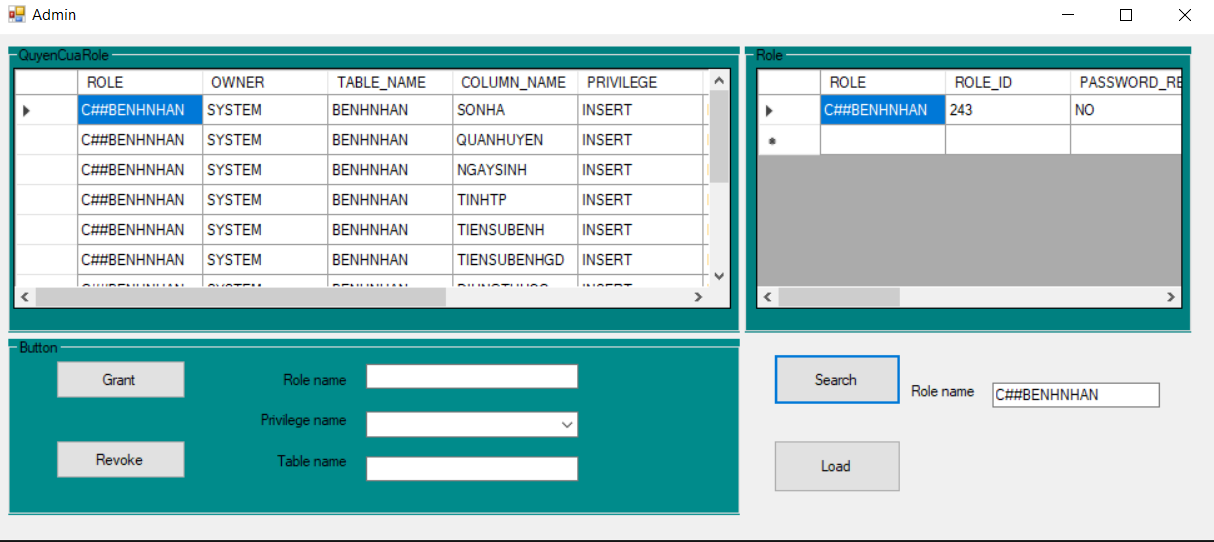
Ảnh có chứa bàn

Mô tả được tạo tự động

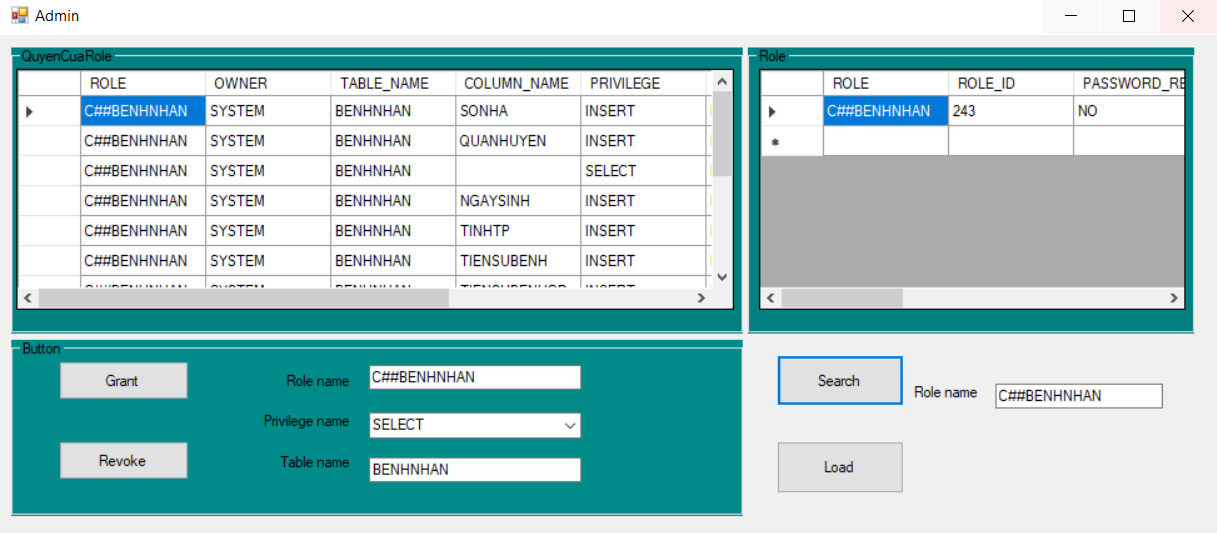
* Giao diện xem quyền của tất cả role



* Giao diện tìm xem quyền của 1 role



* Giao diện cấp/thu quyền cho role:

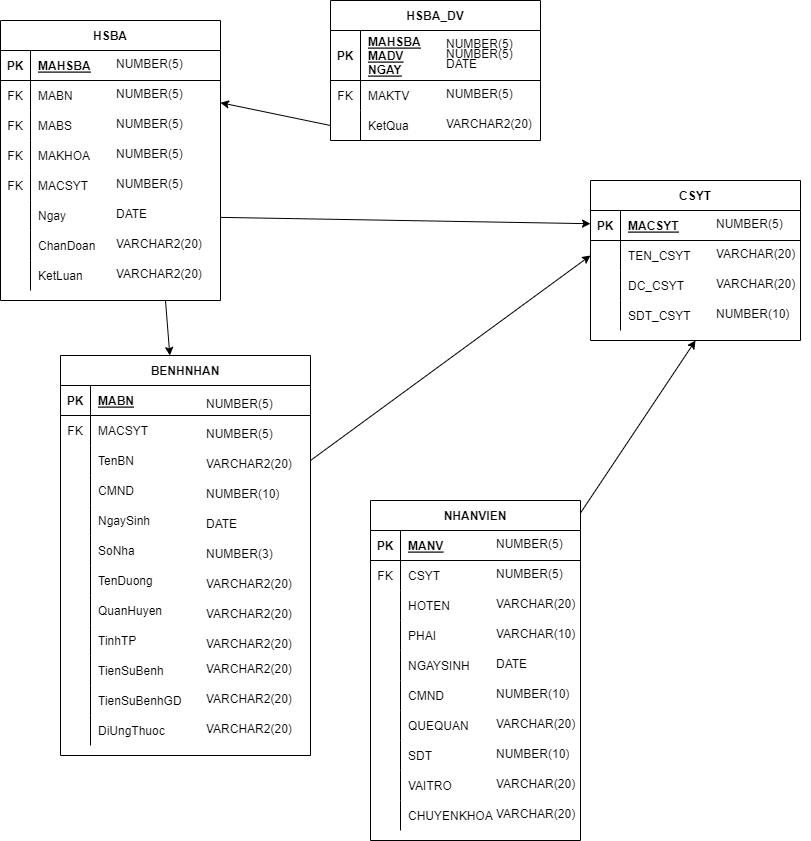


1. Video demo:

<https://drive.google.com/drive/folders/1zPnc9QzTpqtJEY01GgtDFbS1YhI6DrsT?usp=sharing>

## **PHÂN HỆ 2: HIỆN THỰC CÁC CHÍNH SÁCH BẢO MẬT**

1. Thiết kế cơ sở dữ liệu:
2. Mô hình:



1. Đặc tả:

* CSYT: Lưu trữ thông tin cơ sở y tế

|  |  |  |  |
| --- | --- | --- | --- |
| **Tên thuộc tính** | **Kiểu dữ liệu** | **Đặc tả** | **Ghi chú** |
| **MACSYT** | NUMBER (5) | Mã duy nhất xác định CSYT | Khóa chính |
| TEN\_CSYT | VARCHAR (20) | Tên CSYT |  |
| DC\_CSYT | VARCHAR (20) | Địa chỉ của CSYT |  |
| SDT\_CSYT | NUMBER (10) | Số điện thoại liên lạc của csyt |  |

* HSBA: Lưu thông tin hồ sơ bệnh án

|  |  |  |  |
| --- | --- | --- | --- |
| **Tên thuộc tính** | **Kiểu dữ liệu** | **Đặc tả** | **Ghi chú** |
| **MAHSBA** | NUMBER (5) | Mã duy nhất xác định HSBA. | Khóa chính |
| MABN | NUMBER (5) | Mã bệnh nhân tiếp nhận điều trị | Khóa ngoại |
| MABS | NUMBER (5) | Mã bác sĩ điều trị | Khóa ngoại |
| MACSYT | NUMBER (5) | Cơ sở y tế mà bệnh nhân điều trị | Khóa ngoại |
| MAKHOA | NUMBER (5) | Mã khoa mà bệnh nhân được tiếp và điều trị | Khóa ngoại |
| NGAY | DATE | Ngày lập HSBA |  |
| CHANDOAN | VARCHAR (20) | Chẩn đoán của bác sĩ |  |
| KETLUAN | VARCHAR (20) | Kết luận của bác sĩ |  |

* BENHNHAN: Lưu trữ thông tin của bệnh nhân

|  |  |  |  |
| --- | --- | --- | --- |
| **Tên thuộc tính** | **Kiểu dữ liệu** | **Đặc tả** | **Ghi chú** |
| **MABN** | NUMBER (5) | Mã duy nhất xác định bệnh nhân | Khóa chính |
| MACSYT | NUMBER (5) | Mã cơ sở y tế | Khóa ngoại |
| TENBN | VARCHAR (20) | Tên bệnh nhân |  |
| CMND | NUMBER (10) | CMND của bệnh nhân |  |
| NGAYSINH | DATE | Ngày sinh của bênh nhân |  |
| SONHA | NUMBER (3) | Số nhà của bênh nhân |  |
| TENDUONG | VARCHAR (20) | Tên đường nơi bênh nhân ở |  |
| QUANHUYEN | VARCHAR (20) | Tên quận huyện nơi bênh nhân ở |  |
| TINHTP | VARCHAR (20) | Tên Tỉnh/TP nơi bệnh nhân ở |  |
| TIENSUBENH | VARCHAR (20) | Tiền sử bệnh của bệnh nhân |  |
| TIENSUBENHGD | VARCHAR (20) | Tiền sử bênh của gia đinh bệnh nhân |  |
| DIUNGTHUOC | VARCHAR (20) | Thuốc mà bệnh nhân dị ứng |  |

* NHANVIEN: Lưu trữ thông tin của nhân viên

|  |  |  |  |
| --- | --- | --- | --- |
| **Tên thuộc tính** | **Kiểu dữ liệu** | **Đặc tả** | **Ghi chú** |
| **MANV** | NUMBER (5) | Mã duy nhất xác định mỗi nhân viên | Khóa chính |
| TENNV | VARCHAR (20) | Tên nhân viên |  |
| PHAI | VARCHAR (10) | Giới tinh nhân viên |  |
| CMND | NUMBER (10) | CMND của nhân viên |  |
| NGAYSINH | DATE | Ngày sinh của nhân viên |  |
| QUEQUAN | VARCHAR (20) | Quê quán nhân viên |  |
| SDT | VARCHAR (20) | SDT nhân viên |  |
| VAITRO | VARCHAR (20) | Vai trò của nhân viên |  |
| CHUYENKHOA | VARCHAR (20) | Chuyên khoa mà nhân viên được cấp bằng |  |
| CSYT | NUMBER (5) | CSYT mà nhân viên đang làm | Khóa ngoại |

* HSBA\_DV: Lưu trữ thông tin các hồ sơ bệnh án dịch vụ đã sử dụng theo chỉ định của bác sĩ địa chỉ

|  |  |  |  |
| --- | --- | --- | --- |
| **Tên thuộc tính** | **Kiểu dữ liệu** | **Đặc tả** | **Ghi chú** |
| **MAHSDA** | NUMBER (5) | Mã duy nhất xác định CSYT | Khóa chính |
| **MADV** | NUMBER (5) | Tên CSYT | Khóa chính |
| **NGAY** | DATE | Ngày lập hồ sơ | Khóa chính |
| MAKTV | NUMBER (5) | Mã người thực hiện dịch vụ | Khóa ngoại |
| KETQUA | VARCHAR (20) | Kết quả dịch vụ |  |

1. Các chính sách bảo mật:
2. Chính sách DAC (*Direct access control*):

* Là chính sách được sử dụng để phân quyền trên đối tượng dữ liệu cho từng người dùng khác nhau trong hệ thống thông qua các câu lệnh **GRANT (**Cấp quyền) và **REVOKE** (Thu hồi quyền).
* Các quyền ở đây có thể Select (Đọc), Insert (Thêm), Update (Sửa), Delete (Xóa), Execute (thực thi)

1. Chính sách RBAC(*Role-based access control):*

* Là một cơ chế phân quyền cho một nhóm người dùng có quyền tương tự nhau thông qua các role và cấp các role cho người dùng.
* Các chính sách RBAC được cài trong CSDL này là:
* Ở #TC2:
* RL\_YBS thì chỉ có quyền đọc dữ liệu trên tất cả quan hệ mà không được thêm, xóa, sửa.
* Ở #TC3:
* Nhân viên có vai trò “Admin\_CSYT” có quyền thêm, xóa trên một số trường của HSBA và HSBA\_DV
* Ở #TC4:
* RL\_YBS được cấp quyền xem trên bảng BENHNHAN
* Ở #TC5:
* RL\_NghienCuu được cấp quyền Select trên View để xem HSBA và HSBA\_DV

1. Chính sách VPD (*Virtual Private Database*):

* Là một cơ chế bảo mật, cho phép ta tạo các chính sách bảo mật để điều khiển việc truy cập ở mức hàng, cột. Bản chất thì VPD thêm một mệnh đề WHERE vào câu lệnh SQL được đưa ra đối với bảng (table), khung nhìn (view) hoặc synonym (tên thay thế cho các đối tượng như bảng, khung nhìn, các thủ tục được lưu và các đối tượng CSDL khác).
* VPD cung cấp giải pháp bảo mật tới mức mịn trực tiếp trên các table, view, synonym. Nó gán trực tiếp các chính sách bảo mật lên các đối tượng CSDL, và các chính sách sẽ tự động được thực hiện mỗi khi có một người dùng truy nhập dữ liệu đến các đối tượng đó.
* VPD được áp dụng trong #TC6 là:
* VPD cho role bệnh nhân: Chỉ được xem thông tin của mình, và được phép cập nhật một số trường dữ liệu(trừ trường mã) trên bảng BENHNHAN.
* VPD cho role nhân viên: Chỉ được xem thông tin của mình, và được phép cập nhật một số trường dữ liệu(trừ trường mã) trên bảng NHANVIEN.
* VPD được áp dụng trong #TC4 là:
* Các users được cấp role “Y/Bác sĩ” được cấp quyền xem trên view kết hợp giữa HSBA và HSBA\_DV (chỉ lấy các trường liên quan) → V\_HSBA\_KQDV.
* VPD được áp dụng vào V\_HSBA\_KQDV để user chỉ có thể xem được thông tin thuộc hồ sơ bệnh án mà họ đã chữa trị.

1. Chính sách OLS(*Oracle label security*):

* Khi người dùng nhập vào 1 câu truy vấn SQL, đầu tiên Oracle sẽ kiểm tra DẠC để bảo đảm rằng user đó có quyền truy vấn trên table được nhắc đến trong câu truy vấn. Kế tiếp Oracle sẽ kiểm tra xem có chính sách VPD nào được áp dụng cho table đó không. Nếu có, chuỗi điều kiện của chính sách VPD sẽ được nối thêm vào câu truy vấn gốc và sau đó ta có được 1 tập các hàng dữ liệu.Cuối cùng, Oracle sẽ kiểm tra các nhãn OLS trên mỗi hàng dữ liệu đó để xác định những hàng nào mà người dùng có thể truy xuất.
* Các nhãn được chia thành 3 mức độ là Level, Compartment và Group. Chính sách được cài đặt cụ thể như sau:
* Level: Giám đốc sở (GD) > Giám đốc cơ sở y tế (GĐCSYT) > Y bác sĩ (YBS)

|  |  |  |
| --- | --- | --- |
| LEVEL\_NUM | LONG\_NAME | SHORT\_NAME |
| 9000 | GIAM\_DOC\_CO\_SO | GDCS |
| 7000 | GIAM\_DOC\_CO\_SO\_Y\_TE | GDCSYT |
| 5000 | Y\_BAC\_SI | YBS |

* Compartment: Điều trị ngoại trú (DTNGT), điều trị nội trú (DTNT), điều trị chuyên sâu (DTCS)

|  |  |  |
| --- | --- | --- |
| LEVEL\_NUM | SHORT\_NAME | LONG\_NAME |
| 200 | DTCS | DIEU\_TRI\_CHUYEN\_SAU |
| 400 | DTNT | DIEU\_TRI\_NOI\_TRU |
| 800 | DTNGT | DIEU\_TRI\_NGOAI\_TRU |

* Group: Trung tâm (TT), cận trung tâm (CTT), ngoại thành (NT)

|  |  |  |
| --- | --- | --- |
| LEVEL\_NUM | SHORT\_NAME | LONG\_NAME |
| 10 | TT | TRUNG\_TAM |
| 20 | CTT | CAN\_TRUNG\_TAM |
| 30 | NT | NGOAI\_THANH |

* Ba người dùng có vai trò khác nhau trong hệ thống:
* Giám đốc cơ sở thuộc tuyến điều trị nội trú ở vùng trung tâm:

GD:DTNT:TT

* Giám đốc cơ sở y tế thuộc tuyến điều trị ngoại trú và điều trị chuyên sâu ở vùng cận trung tâm:

GĐCSYT:DTNGT,DTCS:CTT

* Y bác sĩ thuộc tuyến điều trị ngoại trú ở vùng ngoại thành:

YBS:DTNGT:NT

* Tạo bảng THONGBAO gồm các thông tin NOIDUNG, NGAYGIO, DIADIEM, OLS\_THONGBAO
* OLS\_THONGBAO được gán vào khi áp dụng chính sách.

1. Chính sách mã hóa (Encrypt)

* **Mã hóa (Encrypt)** là biến đổi dữ liệu ban đầu thành dữ liệu khác bằng các thuật toán để che giấu dữ liệu.
* Là rào cản cuối cùng của kẻ tấn công khi đã vượt qua các cơ chế bảo mật (xác thực người dùng, điều khiển truy cập,...).
* Trong đồ án Mã hóa các thuộc tính của các quan hệ:
* BENHNHAN(CMND, NGAYSINH, SONHA, TENDUONG, TIENSUBENH, TIENSUBENHGD, DIUNGTHUOC)
* HSBA(CHANDOAN, KETLUAN)
* HSBA\_DV(KETQUA)
* Mã hóa bằng thuật toán mã hóa đối xứng AES256 (1 khóa, độ dài khóa là 256 bit). Khóa được tạo cứng từ các kí tự ngẫu nhiên, đảm bảo đủ 256 bit (32 ký tự).
* Chỉ những người dùng có quyền truy xuất dữ liệu của thuộc tính đã được mã hóa mới có thể xem được bản rõ của dữ liệu
* Những người dùng không có quyền truy xuất dữ liệu thì không được xem (kể cả dữ liệu đã mã).

1. Chính sách Audit:

* Audit là hành động theo dõi, nó đóng vai trò như một chiếc camera ghi lại những thao tác, hành động tác động trực tiếp lên dữ liệu. Trong Oracle, người quản trị có thể cấu hình để thực hiện audit lại các hoạt động trong của cả người dùng trong CSDL và người dùng không có trong CSDL, giới hạn audit với 1 số lệnh cụ thể hay audit một số role cụ thể trong dữ liệu.
* Audit gồm: Standard Audit và Fine-grained Audit (FGA)
* Trong đồ án ta cài đặt:
* Standard Audit:
* Standard Auditing trên table CSYT khi một user thực hiện insert, update.
* Standard Auditing trên table NHANVIEN khi một user thực hiện insert.
* Fine-grained Audit (FGA)
* Fine-Grained Audit trên table BENHNHAN khi một user cập nhật lại trường dữ liệu(TIENSUBENH, TIENSUBENHGD, DIUNGTHUOC).
* Fine-Grained Audit trên table HSBA khi một user truy vấn các hồ sơ bênh án của năm 2019.