

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

ĐỀ TÀI: QUẢN LÝ THÔNG TIN CỦA MỘT BỆNH VIỆN



Sinh viên thực hiện: 18120444 – Dương Thành Long

18120490 – Lăng Văn Nhàn

18120501 – Nguyễn Thành Phát

Giảng viên phụ trách: Cô Phạm Thị Bạch Huệ

ĐỒ ÁN MÔN HỌC - AN TOÀN VÀ BẢO MẬT DỮ LIỆU TRONG HỆ THỐNG THÔNG TIN

HỌC KỲ II – NĂM HỌC 2020 - 2021



MỤC LỤC

I. THÔNG TIN NHÓM VÀ ĐÁNH GIÁ HOÀN THÀNH CÔNG VIỆC.....	2
1. Bảng thông tin chi tiết nhóm.....	2
2. Bảng phân công và đánh giá mức độ hoàn thành công việc.....	2
II. BÁO CÁO ĐỒ ÁN.....	2
1. Thiết kế dữ liệu.....	2
1.1. Mô hình thực thể kết hợp.....	2
1.2. Mô hình cơ sở dữ liệu quan hệ.....	3
2. Các loại người dùng.....	3
3. Hiện thực các chính sách bảo mật.....	3
3.1. DAC và RBAC.....	3
3.2. Virtual Private Database (VPD).....	5
3.3. Mandatory Access Control (MAC).....	7
3.4. Encryption.....	9
3.5. Audit cơ bản và FGA.....	11
4. Xây dựng giao diện.....	16
III. TÀI LIỆU THAM KHẢO.....	20

I. THÔNG TIN NHÓM VÀ ĐÁNH GIÁ HOÀN THÀNH CÔNG VIỆC

1. Bảng thông tin chi tiết nhóm

Mã nhóm:	12	
Số lượng:	Nhóm 3 sinh viên	
MSSV	Họ tên	Email
18120444	Dương Thành Long	duongthanhlongk18hcmus@gmail.com
18120490	Lăng Văn Nhàn	nhanlang87@gmail.com
18120501	Nguyễn Thành Phát	phatt.ng.261@gmail.com

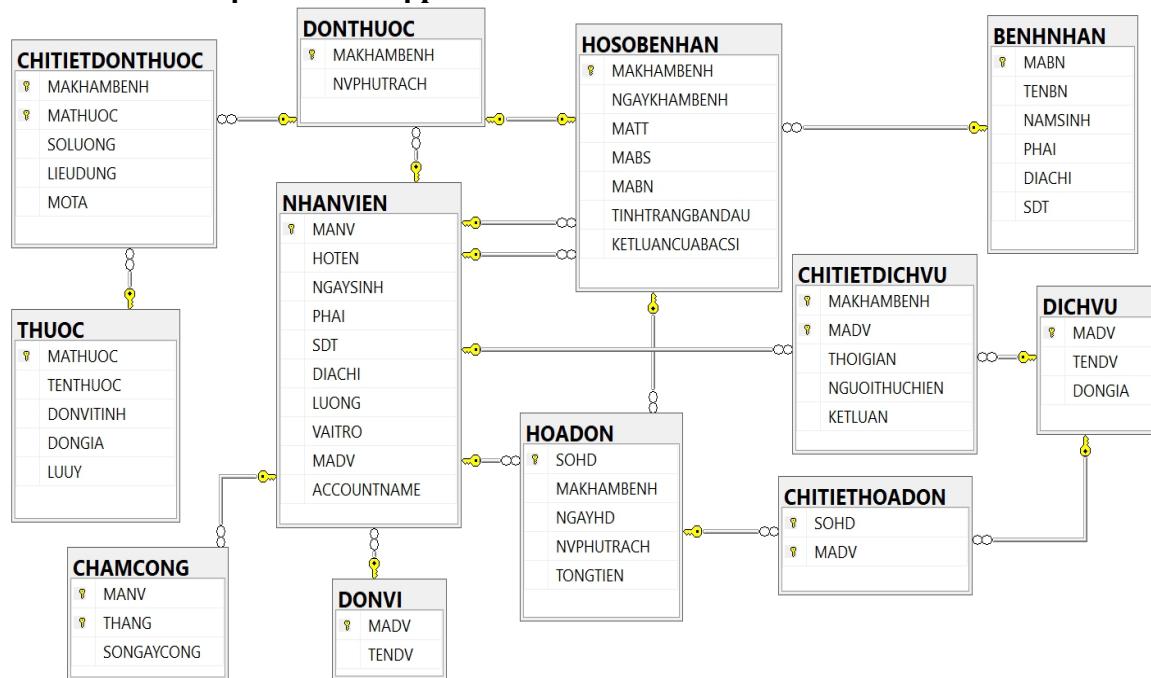
2. Bảng phân công và đánh giá mức độ hoàn thành công việc

Công việc thực hiện	Người thực hiện	Mức độ hoàn thành
Cài đặt chính sách OLS, Audit, thêm mới các đối tượng (user/ role) và xem danh sách đối tượng trên CSDL	18120444 – Dương Thành Long	100%
Cài đặt mã hóa, DAC, RBAC, phân quyền và lấy lại quyền của user/role	18120490 – Lăng Văn Nhàn	100%
Cài đặt chính sách VPD, xây dựng giao diện, xem quyền của một chủ thể, viết báo cáo	18120501 – Nguyễn Thành Phát	100%

II. BÁO CÁO ĐỒ ÁN

1. Thiết kế dữ liệu

1.1. Mô hình thực thể kết hợp





1.2. Mô hình cơ sở dữ liệu quan hệ

DONVI (MaDV, TenDV)

NHANVIEN (MaNV, HoTen, NgaySinh, Phai, SDT, DiaChi, Luong, VaiTro, MaDV, AccountName)

BENHNHAN (MaBN, TenBN, NamSinh, Phai, DiaChi, SDT)

HOSOBENHAN (MaKhamBenh, NgayKhamBenh, MaTT, MaBS, MaBN, TinhTrangBanDau, KetLuanCuaBacSi)

DICHVU (MaDV, TenDV, DonGia)

CHITIETDICHVU (MaKhamBenh, MaDV, ThoiGian, NguoiThucHien, KetLuan)

THUOC (MaThuoc, TenThuoc, DonViTinh, DonGia, LuuY)

DONTHUOC (MaKhamBenh, NVPhuTrach)

CHITIETDONTHUOC (MaKhamBenh, MaThuoc, SoLuong, LieuDung, MoTa)

HOADON (SoHD, MaKhamBenh, NgayHD, NVPhuTrach, TongTien)

CHITIETHOADON (SoHD, MaDV)

CHAMCONG (MaNV, Thang, SoNgayCong)

2. Các loại người dùng

- Quản lý: NHANVIEN, DONVI (thêm, xóa, sửa), CHAMCONG (xem)
- Kế toán: CHAMCONG (thêm, sửa), nhân viên kế toán không được xem bất cứ thông tin cá nhân hoặc những thông tin liên quan đến quá trình điều trị cho bệnh nhân của những bộ phận liên quan
- Bác sĩ: HOSOBENHAN (thêm, sửa trên những hồ sơ của bệnh nhân do bác sĩ đó phụ trách), CHITIETDICHVU (thêm, sửa), DONTHUOC, CHITIETDONTHUOC (thêm, chỉnh sửa)
- Tiếp tân: BENHNHAN (thêm, xóa, sửa), được điều phối bệnh nhưng không thể xem các thông tin liên quan đến số tiền cho từng thủ tục khám, xét nghiệm, chụp hình hoặc các thông tin điều trị bệnh của bệnh nhân
- Điều phối bệnh: DICHVU (xem), CHITIETDICHVU (thêm, sửa)
- Tài vụ: DICHVU (chỉnh sửa), HOADON, CHITIETHOADON (thêm, chỉnh sửa)
- Nhân viên bán thuốc: có thể xem thuốc và đơn thuốc mà bác sĩ kê cho bệnh nhân chứ không được xem thông tin bệnh hay các thông tin liên quan đến bệnh nhân

3. Hiện thực các chính sách bảo mật

3.1. DAC và RBAC

a. Khái niệm

- DAC (Discretionary access control): Điều khiển truy cập niêm ý dựa trên cá nhân, cho phép người dùng hoặc người quản trị xác định danh sách kiểm soát truy cập trên một tài nguyên cụ thể (ví dụ: file, bảng,...). Danh sách này sẽ xác định mỗi người dùng có quyền truy cập vào tài nguyên và đặc quyền của người dùng đối với tài nguyên đó.

- RBAC (Role-based access control): Điều khiển truy cập hướng vai trò dựa trên việc xác định danh sách các vai trò (role) và thêm từng người dùng trong hệ thống vào một hoặc nhiều vai trò. Quyền sau đó được cấp cho mỗi vai trò và người dùng nhận được chúng thông qua tư cách là thành viên của vai trò đó.

→ Đánh giá về DAC và RBAC:

- ✓ RBAC: dễ quản lý hơn DAC, và được quản lý tập trung, bất kể có bao nhiêu người dùng và vấn đề chỉ là trao cho mỗi người dùng vai trò chính xác.
- ✓ DAC: đơn giản và thường chi tiết hơn, đối với mỗi người dùng mới (hoặc thay đổi hay xóa người dùng) thì chúng ta cần phải xem xét tất cả các tài nguyên mà người dùng đó cần truy cập và thêm chúng vào danh sách.

b. Các chính sách DAC và RBAC được cài đặt

Policy 1 (DAC): Chỉ có admin mới được cấp quyền để cấp quyền cho các user khác

User admin được cấp quyền CREATE SESSION với chỉ thị [WITH ADMIN OPTION] để user admin có thể cấp tiếp quyền đó cho các user khác trong hệ thống:

```
GRANT EXECUTE ON DBMS_RLS TO AD1 WITH GRANT OPTION;  
GRANT CREATE SESSION TO AD1 WITH ADMIN OPTION;
```

User admin cấp quyền CREATE SESSION cho các user khác trong hệ thống:

```
GRANT CREATE SESSION TO ELIZABETH, SHERLOCK;  
GRANT EXECUTE ANY PROCEDURE TO ELIZABETH, SHERLOCK;
```

Policy 2 (DAC): Chỉ có admin mới được cấp quyền tạo user và role trong hệ thống

User admin được cấp quyền tạo user và tạo role:

```
GRANT CREATE USER TO AD1;  
GRANT CREATE ROLE TO AD1;
```

User admin tạo 2 role (bác sĩ, tiếp tân) và 2 user (KRIS, CONAN):

```
-- create a role  
CREATE ROLE DOCTOR;  
CREATE ROLE RECEPTION;  
-- create a user  
CREATE USER CONAN IDENTIFIED BY 123;  
CREATE USER KRIS IDENTIFIED BY 123;
```

Policy 3 (RBAC): Chỉ có role bác sĩ mới được quyền cập nhật trên bảng HOSOBENHAN

User admin cấp quyền SELECT, INSERT, UPDATE trên bảng HOSOBENHAN cho role DOCTOR:



```
GRANT SELECT ON AD1.NHANVIEN TO DOCTOR;  
GRANT SELECT, INSERT, UPDATE ON AD1.HOSOBENHAN TO DOCTOR;
```

Policy 4 (RBAC): Role tiếp tân được quyền xem thông tin bệnh nhân
User admin cấp quyền SELECT trên bảng BENHNHAN cho role RECEPTION:

```
GRANT SELECT ON BENHNHAN TO RECEPTION;
```

Policy 5 (RBAC): Role nhân viên phòng thuốc được quyền xem, chỉnh sửa thông tin THUOC

User admin cấp quyền SELECT, UPDATE trên bảng THUOC cho role MEDICINE:

```
GRANT SELECT, UPDATE ON THUOC TO MEDICINE;
```

3.2. Virtual Private Database (VPD)

a. Khái niệm

- VPD là một phương pháp hiệu quả và phổ biến để thực hiện bảo mật dữ liệu ở mức dòng (Row-level security)
- Row-level security (RLS) cho phép giới hạn việc truy xuất các hàng (record) dựa trên một chính sách bảo mật được thực hiện bằng PL/SQL. Một chính sách bảo mật mô tả các quy định quản lý việc truy xuất các dòng dữ liệu

b. Cơ chế thực hiện

- Đầu tiên, ta cần tạo 1 hàm (function) trả về một vị từ (predicate), vị từ này chứa các điều kiện của chính sách bảo mật mà ta muốn thực hiện
- Sau đó, ta dùng package PL/SQL DBMS_RLS để đăng ký function được tạo ở trên cho các table mà ta muốn bảo vệ
- Khi đó, một user bất kì nào thực hiện truy vấn trên đối tượng được bảo vệ, Oracle sẽ nối chuỗi được trả về từ function trên vào mệnh đề WHERE của câu lệnh SQL ban đầu, nhờ đó lọc được những dòng dữ liệu theo điều kiện của chính sách bảo mật

c. Một số lưu ý khi thực hiện RLS

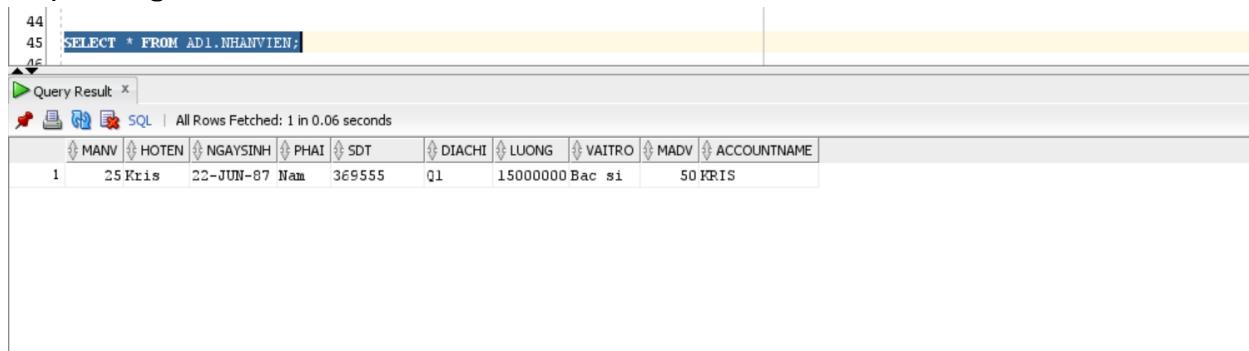
- Quyền sử dụng package DBMS_RLS không được gán cho mọi người dùng, nên phải cấp quyền EXECUTE ON DBMS_RLS để sử dụng nó (Cần quyền SYSDBA để thực hiện điều này)
- Những người có quyền EXEMPT ACCESS POLICY sẽ không bị ảnh hưởng bởi những cơ chế VPD
- DBMS_RLS.ADD_POLICY đòi hỏi ít nhất 3 tham số: object_name, policy_name, policy_function
- Policy function: 2 tham số truyền vào phải là kiểu VARCHAR2
- Mặc định, policy sẽ áp dụng cho hết tất cả các câu lệnh DML, nên có thể dùng thêm số STATEMENT_TYPES để chỉ rõ là áp dụng cho loại câu lệnh nào

- Để thực hiện được các chính sách bảo mật phức tạp một cách hiệu quả, thông thường người ta sẽ kết hợp RLS với Application context

d. Các chính sách VPD được cài đặt

Policy 1: Các nhân viên chỉ được xem thông tin cá nhân của mình

Ví dụ: Nhân viên KRIS đăng nhập vào hệ thống và select bảng NHANVIEN thì chỉ xem được thông tin của chính mình



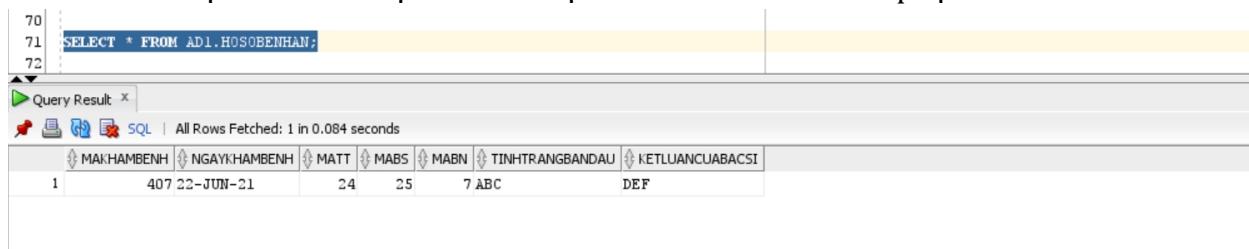
44
45 SELECT * FROM AD1.NHANVIEN;
46

Query Result x
SQL | All Rows Fetched: 1 in 0.06 seconds

	MANV	HOTEN	NGAYSINH	PHAI	SDT	DIACHI	LUONG	VAITRO	MADV	ACCOUNTNAME
1	25 Kris	22-JUN-87	Nam	369555	Q1	15000000	Bac si		50	KRIS

Policy 2: Bác sĩ chỉ được xem thông tin hồ sơ bệnh án của các bệnh nhân do bác sĩ đó phụ trách

Ví dụ: Nhân viên KRIS (bác sĩ) đăng nhập vào hệ thống và select bảng HOSOBENHAN thì chỉ xem được các hồ sơ bệnh án của bệnh nhân do bác sĩ KRIS phụ trách



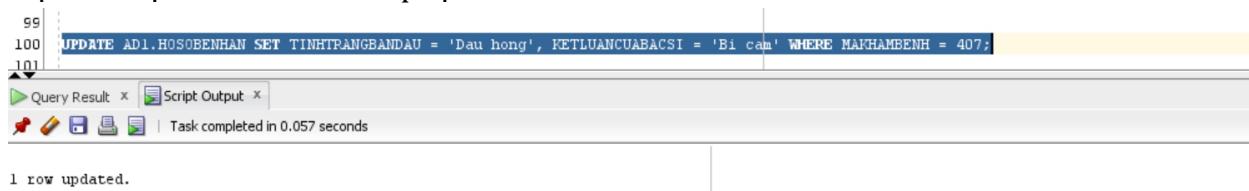
70
71 SELECT * FROM AD1.HOSOBENHAN;
72

Query Result x
SQL | All Rows Fetched: 1 in 0.08 seconds

	MAKHAMBENH	NGAYKHAMBNH	MATT	MABS	MABN	TINHTRANGBANDAU	KETLUANCUABACSI
1	407	22-JUN-21	24	25	7	ABC	DEF

Policy 3: Bác sĩ được phép cập nhật thông tin Tình trạng ban đầu và Kết luận của hồ sơ bệnh án

Ví dụ: Bác sĩ KRIS đăng nhập vào hệ thống và cập nhật lại Tình trạng ban đầu và Kết luận của bệnh nhân do mình phụ trách



99
100 UPDATE AD1.HOSOBENHAN SET TINHTRANGBANDAU = 'Dau hong', KETLUANCUABACSI = 'Bi cam' WHERE MAKHAMBENH = 407;
101

Query Result x Script Output x
Task completed in 0.057 seconds

1 row updated.

Xem lại kết quả sau khi cập nhật:



71 SELECT * FROM AD1.HOSOBENHAN;

Script Output x Query Result x
SQL | All Rows Fetched: 1 in 0.006 seconds

	MAKHAMBENH	NGAYKHAMBNH	MATT	MABS	MABN	TINHTRANGBANDAU	KETLUANCUABACSI
1	407	22-JUN-21	24	25	7	Dau hong	Bi cam



3.3. Mandatory Access Control (MAC)

a. Khái niệm

Oracle Label Security (OLS) là một sản phẩm được hiện thực dựa trên nền tảng công nghệ Virtual Private Database (VPD), cho phép các nhà quản trị điều khiển truy xuất dữ liệu ở mức hàng (row-level) một cách tiện lợi và dễ dàng hơn. Nó điều khiển việc truy xuất nội dung của các dòng dữ liệu bằng cách so sánh nhãn của hàng dữ liệu với nhãn và quyền của user. Các nhà quản trị có thể dễ dàng tạo thêm các chính sách kiểm soát việc truy xuất các hàng dữ liệu cho các CSDL bằng giao diện đồ họa thân thiện người dùng có tên gọi là Oracle Policy Manager hoặc bằng các packages được xây dựng sẵn.

b. Cơ chế hoạt động

Trong OLS, ta dùng các policy để quản lý truy xuất. Đối với mỗi policy, ta cần định ra một tập nhãn để phân lớp dữ liệu từ cao xuống thấp dựa theo độ nhạy cảm của dữ liệu (ngoài ra các nhãn còn có những yếu tố khác mà ta sẽ bàn đến khi đi vào chi tiết). Các nhãn đó gọi là các nhãn dữ liệu - "data label". Ứng với mỗi user, ta gán một nhãn để cho biết những loại dữ liệu nào mà họ có quyền truy cập. Những nhãn này gọi là nhãn người dùng – "user label". Sau đó ta áp dụng các policy lên các table mà mình mong muốn bảo vệ. Khi một user truy xuất lên table được bảo vệ, data label của từng dòng trong table và user label của user đó sẽ được so sánh để quyết định xem user đó được xem những dòng dữ liệu nào.

c. Cài đặt chính sách OLS

- Policy:

Nội dung chính sách	Nhân viên tiếp cận chỉ được xem thông tin hóa đơn do chính mình phụ trách lập. Level: nhân viên(mỗi nhân viên là 1 level) Compartment: những nhân viên trong bộ phận tiếp cận. Group: mỗi nhân viên trong bộ phận tiếp cận.
Đối tượng người dùng áp dụng	Nhân viên tiếp cận
Đối tượng dữ liệu áp dụng	Hóa đơn (Bảng: HOADON)
Cơ chế bảo mật đã cài đặt	OLS

- Mô tả các level, compartment và group:
 - + Level của chính sách:



Level_num	Short_name	Long_name
20	S	Sensitive
10	C	Confidential

+ Compartiment của chính sách:

Comp_num	Short_name	Long_name
65	T19	TTa19 (Tiếp tân là nhân viên có mã là 19)
55	T24	TTa24 (Tiếp tân là nhân viên có mã là 24)

+ Group của chính sách:

Group_num	Short_name	Long_name
210	TT19	Tiếp tân 19
220	TT24	Tiếp tân 24

- Kết quả sau khi thực hiện chính sách:

Ví dụ:

Tiếp tân có mã là 19 đăng nhập vào hệ thống và select bảng HOADON thì chỉ nhìn thấy được các hóa đơn do tiếp tân đó phụ trách lập:

```

97
98 -- DANG NHAP TAI KHOAN DE CHECK CHINH SACH OLS
99 SELECT * FROM AD1.HOADON;

```

Query Result x | All Rows Fetched: 5 in 0.241 seconds

SOHD	MAKHAMBENH	NGAYHD	NVPHUTRACH	TONGTIEN	CO_LUMN
1	1	400 04-APR-21	19	1000000	160
2	2	401 04-APR-21	19	1500000	160
3	3	402 06-APR-21	19	1000000	160
4	4	403 05-APR-21	19	1500000	160
5	7	405 21-JUN-21	19	1500000	160



Tiếp tân có mã là 24 đăng nhập vào hệ thống và select bảng HOADON thì chỉ nhìn thấy được các hóa đơn do tiếp tân đó phụ trách lập:

```

97
98 -- DANG NHAP TAI KHOAN DE CHECK CHINH SACH OLS
99 SELECT * FROM AD1.HOADON;

```

SOHD	MAKHAMBENH	NGAYHD	NVPHUTRACH	TONGTIEN	CO_LUMN
1	5	404 19-JUN-21	24	1500000	170
2	6	405 20-JUN-21	24	1500000	170

DBA thì xem được tất cả các hóa đơn:

```

97
98 -- DANG NHAP TAI KHOAN DE CHECK CHINH SACH OLS
99 SELECT * FROM AD1.HOADON;

```

SOHD	MAKHAMBENH	NGAYHD	NVPHUTRACH	TONGTIEN	CO_LUMN
1	1	400 04-APR-21	19	1000000	160
2	2	401 04-APR-21	19	1500000	160
3	3	402 06-APR-21	19	1000000	160
4	4	403 05-APR-21	19	1500000	160
5	5	404 19-JUN-21	24	1500000	170
6	6	405 20-JUN-21	24	1500000	170
7	7	405 21-JUN-21	19	1500000	160

3.4. Encryption

a. Khái niệm

- Mã hóa là phương pháp che giấu dữ liệu, biến dữ liệu sang dạng mã không có ý nghĩa đối với kẻ tấn công
- Các phương pháp mã hóa hiện có:
 - + Phương pháp Mã hóa đối xứng
 - + Phương pháp Mã hóa bất đối xứng
 - + Phương pháp Mã hóa lai
 - + Phương pháp Hàm băm mật mã
- Trong đề án lần này nhóm chọn phương pháp mã hóa đối xứng. Cụ thể là ở đây sử dụng kỹ thuật mã hóa DES (Data Encryption Standard)
 - + NBS (National Bureau of Standards) – bây giờ là NIST (National Institute of Standards and Technology) (Mỹ) chọn DES làm tiêu chuẩn mã hóa vào năm 1977
 - + Mỗi thông điệp (message) được chia thành những khối (block) 64 bits
 - + Khóa có 56 bits
 - + Có thể bị tấn công bằng giải thuật vét cạn khóa (Brute-force or exhaustive key search)

b. Chính sách mã hóa được cài đặt

- **Policy:**

- + Kỹ thuật mã hóa DES được cài đặt cho đồ án này, sử dụng 1 khóa để vừa giải mã và mã hóa

```

2 CREATE OR REPLACE PACKAGE Tool_DES AS
3
4     FUNCTION encrypt (input_text  IN  VARCHAR2, key_in IN VARCHAR2) RETURN RAW;
5
6     FUNCTION decrypt (p_raw   IN  RAW, key_in IN VARCHAR2) RETURN VARCHAR2;
7
8 END Tool_DES;

```

- + Cụ thể, nhóm thực hiện mã hóa trường kết luận trên bảng chi tiết dịch vụ. Key dùng để mã hóa do người dùng nhập, cụ thể ở đây là nhân viên dịch vụ sẽ nhập. Và chỉ nhân viên dịch vụ mới có thể update thông tin trên trường kết luận ở bảng chi tiết dịch vụ. Các user khác chỉ có thể xem

- Kết quả sau khi thực hiện chính sách:

Mã hóa:

```

EXECUTE MAHOA_CTDV (401, 'GAN PHU NE', 'TRONG1234');
SELECT* FROM CHITIETDICHVU

```

MAKHAMBENH	MADV	THOIGIAN	NGUOIDUCHIEN	KETLUAN
400	1001 04-APR-21		21	GAN BINH THUONG
401	1001 04-APR-21		22	EFA22598268C50178759CB5E71D9324
403	1001 04-APR-21		21	DA DAY BINH THUONH
402	1001 04-APR-21		22	MO MAU NHIEU

Giải mã:

```

EXECUTE GIAIMA_CTDV (401, 'TRONG1234');
SELECT* FROM CHITIETDICHVU

```

MAKHAMBENH	MADV	THOIGIAN	NGUOIDUCHIEN	KETLUAN
400	1001 04-APR-21		21	GAN BINH THUONG
401	1001 04-APR-21		22	GAN PHU NE
403	1001 04-APR-21		21	DA DAY BINH THUONH
402	1001 04-APR-21		22	MO MAU NHIEU



3.5. Audit cơ bản và FGA

a. Tổng quan về auditing

- Audit là một trong 4 cơ chế bảo mật được cung cấp bởi hệ quản trị cơ sở dữ liệu Oracle, audit giúp giám sát và ghi nhận lại các hoạt động đã và đang xảy ra trên cơ sở dữ liệu một cách có chọn lọc vì các tài khoản luôn có nguy cơ bị xâm nhập và sử dụng sai mục đích nên audit có thể giúp cho chúng ta cải thiện việc tuân thủ quy định.
- Oracle khuyên người dùng nên kích hoạt và thiết lập auditing, vì auditing là một phương pháp hiệu quả để thực thi kiểm soát nội bộ mạnh mẽ, giám sát và tìm ra các hoạt động nào làm trái lại chính sách đã đề ra.
- Audit thường dùng để:
 - ✓ Kích hoạt giải trình cho các hoạt động
 - ✓ Ngăn user khỏi các hành động không thích hợp dựa trên trách nhiệm phải giải trình đó
 - ✓ Điều tra các hoạt động đáng ngờ của người dùng trên hệ thống: ví dụ, khi có một user đang thực hiện hành động delete trên các bảng trong hệ thống, thì người quản trị bảo mật có thể dựa vào kinh nghiệm của bản thân mà sẽ quyết định audit tất cả các connection, tất cả hành động xóa dữ liệu thành công và không thành công khỏi các bảng
 - ✓ Phát hiện các vấn đề trong quá trình điều khiển truy cập và định quyền: có thể trong quá trình hiện thực các chính sách bảo mật bằng điều khiển truy cập thì người quản trị gặp một số sai sót và audit giúp họ nhận biết sai sót kịp thời để có thể điều chỉnh lại hệ thống cho phù hợp
 - ✓ Thông báo cho người giám sát về các hoạt động của user bất hợp pháp: ví dụ, một user bất hợp pháp có thể thay đổi hay xóa dữ liệu, hay user có nhiều quyền hệ thống hơn sự cho phép
 - ✓ Giám sát và thu thập dữ liệu về các hoạt động CSDL cụ thể: ví dụ như người quản trị hệ thống có thể thu thập các số liệu về số người dùng truy cập vào cơ sở dữ liệu trong giờ cao điểm hay những table nào đang được update,...
 - ✓ Giải quyết các nhu cầu đánh giá về sự tuân thủ

b. Fine-Grained Auditing - FGA

- Giới thiệu:
 - ✓ Fine-Grained Auditing là một loại audit cho phép chúng ta tạo ra một chính sách xác định rõ điều kiện mà điều kiện đó phải thỏa thì



audit mới có thể diễn ra. Điều này cho phép audit dựa vào nội dung của bản ghi.

- ✓ Nhìn chung, các chính sách Fine-Grained Audit dựa trên các vị từ SQL đơn giản do người dùng tự định nghĩa trên các đối tượng bảng làm điều kiện để audit có chọn lọc. Bất cứ khi nào các điều kiện chính sách được đáp ứng cho 1 hàng thì truy vấn sẽ được audit.
- ✓ Khi sử dụng chính sách, ta có thể chỉ rõ cột nào và điều kiện khi nào ta mới cần phải ghi lại việc truy xuất đó. Ngoài ra, ta còn có thể cung cấp thêm tên hàm mà ta muốn thực thi khi sự kiện audit diễn ra. Hàm này có thể nhắc nhở hoặc báo động cho người quản trị.
- Lưu trữ:
 - ✓ Những bản ghi của FGA sẽ được lưu trong bảng SYS.FGA_LOG\$ và được truy cập thông qua view DBA_FGA_AUDIT_TRAIL và DBA_COMMON_AUDIT_TRAIL (chứa thông tin của cả standard audit và fine-grained audit).
 - ✓ Ngoài ra, ta có thể truy cập view V\$XML_AUDIT_TRAIL để tìm kiếm thông tin các bản ghi của fine-grained audit được viết dưới dạng file XML.
 - ✓ Các câu lệnh INSERT, UPDATE, DELETE thường được audit. Câu lệnh SELECT ít được audit hơn cho chi phí cao (được sử dụng thường xuyên)
- Ưu điểm:
 - ✓ Có sử dụng kiểm tra tính đúng sai của điều kiện, đánh giá các bản ghi trên nội dung → Audit mịn đến đến cấp hàng và cột
 - ✓ Bắt được lệnh SQL trigger quá trình audit và tất cả các biến thông tin có liên quan được sử dụng
 - ✓ Thêm tính an toàn cho cột các thông tin nhạy cảm: có thể audit các cột cụ thể liên quan có chứa thông tin nhạy cảm
 - ✓ Cung cấp một event handler: sử dụng một cơ chế để tiếp nhận và xử lý event khi có xảy ra audit như một hàm gửi email thông báo đến cho quản trị viên về sự thay đổi trái phép trong cơ sở dữ liệu
 - ✓ Không cần thiết lập tham số audit_trail initialization parameters để bật chế độ fine-grained audit, chỉ cần sử dụng package DBMS_FGA PL/SQL để tạo và xóa các chính sách áp dụng lên các đối tượng hay các hoạt động cụ thể ta cần giám sát
 - ✓ So với standard audit thì fine-grained audit tối thiểu những giám sát không cần thiết, và chỉ ra những truy cập gây hại. Cơ chế này giúp ngăn chặn người dùng khỏi việc cố gắng tìm cách truy vấn vòng để không bị giám sát

c. Các chính sách audit được cài đặt

Policy 1 (Standard audit): Giám sát những truy cập trên bảng DICHVU

```
27
28 -- Audit1: GIAM SAT NHUNG TRUY CAP TREN BANG DICHVU
29 AUDIT SELECT, INSERT, UPDATE, DELETE ON DICHVU BY ACCESS WHENEVER SUCCESSFUL;
30 AUDIT SELECT, INSERT, UPDATE, DELETE ON DICHVU BY ACCESS WHENEVER NOT SUCCESSFUL;
```

User có username là ELIZABETH đã đăng nhập vào hệ thống và select bảng DICHVU:

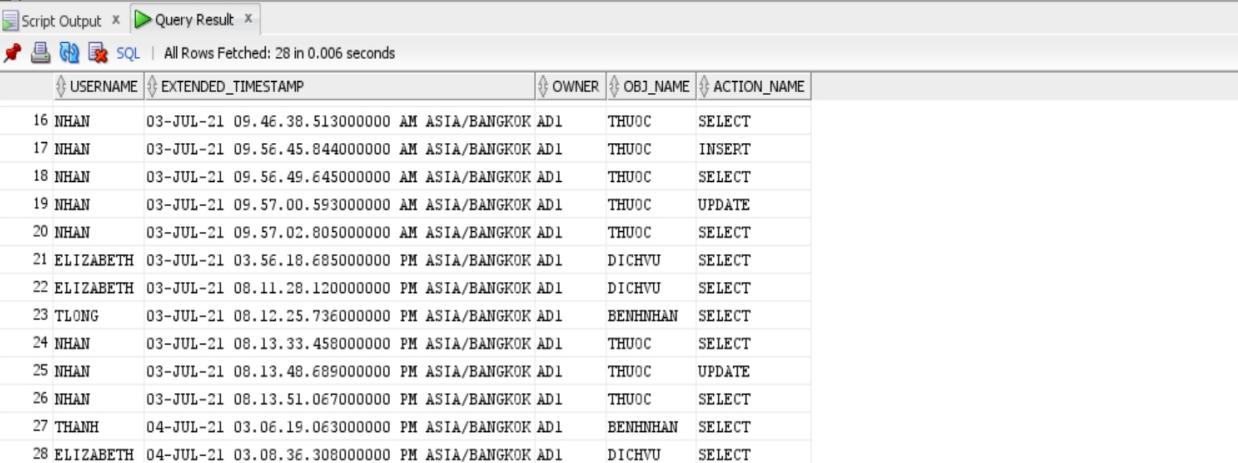


Script Output | Query Result | All Rows Fetched: 4 in 0.007 seconds

	MADV	TENDV	DONGIA
1	1001	Chup X quang	500000
2	1002	Sieu am	300000
3	1003	Xet nghiem mau	450000
4	1004	Noi soi	300000

Hành động đó được audit lại ở dòng số 28:

```
53 SELECT USERNAME, EXTENDED_TIMESTAMP, OWNER, OBJ_NAME, ACTION_NAME
54 FROM DBA_AUDIT_TRAIL
55 WHERE OWNER = 'AD1' -- SCHEMA CHUA BANG
56 ORDER BY TIMESTAMP;
```



Script Output | Query Result | All Rows Fetched: 28 in 0.006 seconds

USERNAME	EXTENDED_TIMESTAMP	OWNER	OBJ_NAME	ACTION_NAME	
16 NHAN	03-JUL-21 09.46.38.513000000 AM	ASIA/BANGKOK	AD1	THUOC	SELECT
17 NHAN	03-JUL-21 09.56.45.844000000 AM	ASIA/BANGKOK	AD1	THUOC	INSERT
18 NHAN	03-JUL-21 09.56.49.645000000 AM	ASIA/BANGKOK	AD1	THUOC	SELECT
19 NHAN	03-JUL-21 09.57.00.593000000 AM	ASIA/BANGKOK	AD1	THUOC	UPDATE
20 NHAN	03-JUL-21 09.57.02.805000000 AM	ASIA/BANGKOK	AD1	THUOC	SELECT
21 ELIZABETH	03-JUL-21 03.56.18.685000000 PM	ASIA/BANGKOK	AD1	DICHVU	SELECT
22 ELIZABETH	03-JUL-21 08.11.28.120000000 PM	ASIA/BANGKOK	AD1	DICHVU	SELECT
23 TLONG	03-JUL-21 08.12.25.736000000 PM	ASIA/BANGKOK	AD1	BENHNHAN	SELECT
24 NHAN	03-JUL-21 08.13.33.458000000 PM	ASIA/BANGKOK	AD1	THUOC	SELECT
25 NHAN	03-JUL-21 08.13.48.689000000 PM	ASIA/BANGKOK	AD1	THUOC	UPDATE
26 NHAN	03-JUL-21 08.13.51.067000000 PM	ASIA/BANGKOK	AD1	THUOC	SELECT
27 THANH	04-JUL-21 03.06.19.063000000 PM	ASIA/BANGKOK	AD1	BENHNHAN	SELECT
28 ELIZABETH	04-JUL-21 03.08.36.308000000 PM	ASIA/BANGKOK	AD1	DICHVU	SELECT

Policy 2 (Standard audit): Giám sát những truy cập trên bảng BENHNHAN

```
1
2 -- Audit2: GIAM SAT NHUNG TRUY CAP TREN BANG BENHNHAN
3 AUDIT SELECT, INSERT, UPDATE, DELETE ON BENHNHAN BY ACCESS WHENEVER NOT SUCCESSFUL;
4 AUDIT SELECT, INSERT, UPDATE, DELETE ON BENHNHAN BY ACCESS WHENEVER SUCCESSFUL;
```

User có username là THANH đã đăng nhập vào hệ thống và select bảng BENHNHAN và hành động đó được audit lại ở dòng số 27:



```
52 -- KIỂM TRA 2 CHINH SÁCH AUDIT (DÀNG NHẬP = AD1)
53 SELECT USERNAME, EXTENDED_TIMESTAMP, OWNER, OBJ_NAME, ACTION_NAME
54 FROM DBA_AUDIT_TRAIL
55 WHERE OWNER = 'AD1' -- SCHEMA CHUA BANG
56 ORDER BY TIMESTAMP;
```

Script Output x | Query Result x
SQL | All Rows Fetched: 27 in 0.031 seconds

USERNAME	EXTENDED_TIMESTAMP	OWNER	OBJ_NAME	ACTION_NAME
16 NHAN	03-JUL-21 09.46.38.513000000 AM	ASIA/BANGKOK	AD1	THUOC
17 NHAN	03-JUL-21 09.56.45.844000000 AM	ASIA/BANGKOK	AD1	THUOC
18 NHAN	03-JUL-21 09.56.49.645000000 AM	ASIA/BANGKOK	AD1	THUOC
19 NHAN	03-JUL-21 09.57.00.593000000 AM	ASIA/BANGKOK	AD1	THUOC
20 NHAN	03-JUL-21 09.57.02.805000000 AM	ASIA/BANGKOK	AD1	THUOC
21 ELIZABETH	03-JUL-21 03.56.18.685000000 PM	ASIA/BANGKOK	AD1	DICHVU
22 ELIZABETH	03-JUL-21 08.11.28.120000000 PM	ASIA/BANGKOK	AD1	DICHVU
23 TLONG	03-JUL-21 08.12.25.736000000 PM	ASIA/BANGKOK	AD1	BENHNHAN
24 NHAN	03-JUL-21 08.13.33.458000000 PM	ASIA/BANGKOK	AD1	THUOC
25 NHAN	03-JUL-21 08.13.48.689000000 PM	ASIA/BANGKOK	AD1	THUOC
26 NHAN	03-JUL-21 08.13.51.067000000 PM	ASIA/BANGKOK	AD1	THUOC
27 THANH	04-JUL-21 03.06.19.063000000 PM	ASIA/BANGKOK	AD1	BENHNHAN

Policy 3 (FGA audit): Giám sát những truy cập trên bảng THUOC

```
60 BEGIN
61   DBMS_FGA.ADD_POLICY (
62     OBJECT_SCHEMA      => 'AD1',
63     OBJECT_NAME        => 'THUOC',
64     POLICY_NAME        => 'AUDIT_THUOC',
65     ENABLE              => TRUE,
66     STATEMENT_TYPES    => 'UPDATE',
67     AUDIT_COLUMN       => 'MATHUOC, DONGIA, LUUY'
68   );
69 END;
70 /
```

User có username là NHAN đã đăng nhập vào hệ thống và update lưu ý của một thuốc trong bảng THUOC:

```
100 --- UPDATE
101 UPDATE AD1.THUOC SET LUUY = 'ABC' WHERE MATHUOC = 105;
```

Script Output x | Query Result x
Task completed in 0.06 seconds
Audit succeeded.

Audit succeeded.

Audit succeeded.

1 row updated.

Hành động đó đã được audit lại ở dòng được bôi đỏ:



```

132 -- AD1 CHECK THONG TIN AUDIT
133 SELECT * FROM DBA_FGA_AUDIT_TRAIL;
134

```

Script Output | Query Result | All Rows Fetched: 99 in 0.047 seconds

OBJECT_NAME	POLICY_NAME	SCN	SQL_TEXT
87 HOSOBENHAN	AUDIT_HSBA	2440241	SELECT * FROM AD1.HOSOBENHAN
88 HOSOBENHAN	AUDIT_HSBA	2440280	SELECT HS.MAKHAMBENH FROM NHANVIEN NV, HOSOBENHAN HS WHERE NV.ACCTNAME = :B1 AND NV.MANV = HS.MABS
89 HOSOBENHAN	AUDIT_HSBA	2440283	SELECT HS.MAKHAMBENH FROM NHANVIEN NV, HOSOBENHAN HS WHERE NV.ACCTNAME = :B1 AND NV.MANV = HS.MABS
90 HOSOBENHAN	AUDIT_HSBA	2440286	UPDATE AD1.HOSOBENHAN SET TINHTRANGBANDAU = 'XYZ', KETLUANCUABACSI = 'YYY' WHERE MAKHAMBENH = 406
91 HOSOBENHAN	AUDIT_HSBA	2440292	SELECT * FROM AD1.HOSOBENHAN
92 HOSOBENHAN	AUDIT_HSBA	2441697	SELECT * FROM AD1.HOSOBENHAN
93 HOSOBENHAN	AUDIT_HSBA	2441714	SELECT HS.MAKHAMBENH FROM NHANVIEN NV, HOSOBENHAN HS WHERE NV.ACCTNAME = :B1 AND NV.MANV = HS.MABS
94 HOSOBENHAN	AUDIT_HSBA	2441717	SELECT HS.MAKHAMBENH FROM NHANVIEN NV, HOSOBENHAN HS WHERE NV.ACCTNAME = :B1 AND NV.MANV = HS.MABS
95 HOSOBENHAN	AUDIT_HSBA	2441720	UPDATE AD1.HOSOBENHAN SET TINHTRANGBANDAU = 'ABC', KETLUANCUABACSI = 'ABC' WHERE MAKHAMBENH = 403
96 THUOC	AUDIT_THUOC	2484561	UPDATE AD1.THUOC SET LUUY = 'ABC' WHERE MATHUOC = 105
97 HOSOBENHAN	AUDIT_HSBA	2484605	SELECT HS.MAKHAMBENH FROM NHANVIEN NV, HOSOBENHAN HS WHERE NV.ACCTNAME = :B1 AND NV.MANV = HS.MABS
98 HOSOBENHAN	AUDIT_HSBA	2484608	SELECT HS.MAKHAMBENH FROM NHANVIEN NV, HOSOBENHAN HS WHERE NV.ACCTNAME = :B1 AND NV.MANV = HS.MABS
99 HOSOBENHAN	AUDIT_HSBA	2484611	UPDATE AD1.HOSOBENHAN SET KETLUANCUABACSI = 'SOT XUAT HUYET' WHERE MAKHAMBENH = 407

Policy 4 (FGA audit): Giám sát những truy cập trên bảng HOSOBENHAN

```

117 BEGIN
118     DBMS_FGA.ADD_POLICY (
119         OBJECT_SCHEMA      => 'AD1',
120         OBJECT_NAME        => 'HOSOBENHAN',
121         POLICY_NAME        => 'AUDIT_HSBA',
122         ENABLE              => TRUE,
123         STATEMENT_TYPES    => 'UPDATE',
124         AUDIT_COLUMN        => 'MABS, TINHTRANGBANDAU, KETLUANCUABACSI'
125     );
126 END;

```

User có username là KRIS đã đăng nhập vào hệ thống và update Kết luận của một bệnh nhân do bác sĩ KRIS phụ trách ở bảng HOSOBENHAN:

```
130 UPDATE AD1.HOSOBENHAN SET KETLUANCUABACSI = 'SOT XUAT HUYET' WHERE MAKHAMBENH = 407;
```

Script Output | Query Result | Task completed in 0.078 seconds

Audit succeeded.

Audit succeeded.

1 row updated.

1 row updated.

Hành động đó đã được audit lại ở dòng được bôi đỏ:



```

132 -- AD1 CHECK THONG TIN AUDIT
133 SELECT * FROM DBA_FGA_AUDIT_TRAIL;
134

Script Output x Query Result x
SQL | All Rows Fetched: 99 in 0.047 seconds
+-----+-----+-----+-----+
| OBJECT_NAME | POLICY_NAME | SCN | SQL_TEXT |
+-----+-----+-----+-----+
87 HOSOBENHAN AUDIT_HSBA 2440241 SELECT * FROM AD1.HOSOBENHAN
88 HOSOBENHAN AUDIT_HSBA 2440280 SELECT HS.MAKHAMBENH FROM NHANVIEN NV, HOSOBENHAN HS WHERE NV.ACCOUNTNAME = :B1 AND NV.MANV = HS.MABS
89 HOSOBENHAN AUDIT_HSBA 2440283 SELECT HS.MAKHAMBENH FROM NHANVIEN NV, HOSOBENHAN HS WHERE NV.ACCOUNTNAME = :B1 AND NV.MANV = HS.MABS
90 HOSOBENHAN AUDIT_HSBA 2440286 UPDATE AD1.HOSOBENHAN SET TINHTRANGBANDAU = 'XYZ', KETLUANCUABACSI = 'YYY' WHERE MAKHAMBENH = 406
91 HOSOBENHAN AUDIT_HSBA 2440292 SELECT * FROM AD1.HOSOBENHAN
92 HOSOBENHAN AUDIT_HSBA 2441697 SELECT * FROM AD1.HOSOBENHAN
93 HOSOBENHAN AUDIT_HSBA 2441714 SELECT HS.MAKHAMBENH FROM NHANVIEN NV, HOSOBENHAN HS WHERE NV.ACCOUNTNAME = :B1 AND NV.MANV = HS.MABS
94 HOSOBENHAN AUDIT_HSBA 2441717 SELECT HS.MAKHAMBENH FROM NHANVIEN NV, HOSOBENHAN HS WHERE NV.ACCOUNTNAME = :B1 AND NV.MANV = HS.MABS
95 HOSOBENHAN AUDIT_HSBA 2441720 UPDATE AD1.HOSOBENHAN SET TINHTRANGBANDAU = 'ABC', KETLUANCUABACSI = 'ABC' WHERE MAKHAMBENH = 403
96 THUOC AUDIT_THUOC 2484561 UPDATE AD1.THUOC SET LUUUY = 'ABC' WHERE MATHUOC = 105
97 HOSOBENHAN AUDIT_HSBA 2484605 SELECT HS.MAKHAMBENH FROM NHANVIEN NV, HOSOBENHAN HS WHERE NV.ACCOUNTNAME = :B1 AND NV.MANV = HS.MABS
98 HOSOBENHAN AUDIT_HSBA 2484608 SELECT HS.MAKHAMBENH FROM NHANVIEN NV, HOSOBENHAN HS WHERE NV.ACCOUNTNAME = :B1 AND NV.MANV = HS.MABS
99 HOSOBENHAN AUDIT_HSBA 2484611 UPDATE AD1.HOSOBENHAN SET KETLUANCUABACSI = 'SOT XUAT HUYET' WHERE MAKHAMBENH = 407

```

4. Xây dựng giao diện

- Giao diện Login:**



Please Login !

Username:

Password:

LOG IN

- Giao diện cho người quản trị:**

- ✓ Tab Users: Ở đây, người quản trị có thể xem các đối tượng như user, quyền của các user, các table, view và có thể tạo mới user, chỉnh sửa user, và xóa user ra khỏi hệ thống

Users	Roles	Grant Privileges	Revoke Privileges	Auditing
View Users	Users' Prvls			
See Tables	See Views			
Alter user: Username: <input type="text"/> Old pswd: <input type="text"/> New pswd: <input type="text"/> Alter Create user: Username: <input type="text"/> Add Password: <input type="text"/> Drop user: Username: <input type="text"/> Drop				
Username: <input type="text"/> User's Sys User's Obj Role: <input type="text"/> CONNECT Role's Sys Role's Obj				

- ✓ Tab Roles: Ở đây, người quản trị có thể xem các role, quyền của các role và có thể tạo mới, chỉnh sửa và xóa một role nào đó trong hệ thống

The screenshot shows the 'Roles' tab of a database management system. On the left, there are three main sections: 'Alter role' (with fields for Role and Password, and a green 'Alter' button), 'Create role' (with a field for Role and a green 'Add' button), and 'Drop role' (with a field for Role and a green 'Drop' button). To the right of these is a large, mostly empty central panel. On the far right, there is a sidebar with dropdown menus for 'Username' (set to 'SYS'), 'Role' (set to 'CONNECT'), and two sets of buttons for 'User's Sys', 'User's Obj', 'Role's Sys', and 'Role's Obj'.

- ✓ Tab Grant Privileges: Ở đây, người quản trị có thể thực hiện gán quyền hệ thống, quyền đối tượng cho user, role, gán role cho các user và xem các quyền của một user hoặc role cụ thể

The screenshot shows the 'Grant Privileges' tab. It features five separate grant sections, each with its own set of input fields and a 'Grant' button. From top-left to bottom-right, the sections are: 'Grant Sys To User' (Username, Privileges, Flag Ad, Grant button), 'Grant Sys To Role' (Role, Privileges, Flag Ad, Grant button), 'Grant Obj To User' (Username, Privilis Obj, Object, Grant button), 'Grant Obj To Role' (Role, Privilis Obj, Object, Grant button), and 'Grant Role To User' (Username, Role, Grant button). To the right of these sections is a large, mostly empty central panel. On the far right, there is a sidebar with dropdown menus for 'Username' (set to 'SYS'), 'Role' (set to 'CONNECT'), and two sets of buttons for 'User's Sys', 'User's Obj', 'Role's Sys', and 'Role's Obj'.

- ✓ Tab Revoke Privileges: Ở đây, người quản trị có thể thu hồi hoặc chỉnh sửa lại các quyền hệ thống, quyền đối tượng cho user, role và xem các quyền của một user hoặc role cụ thể



Users Roles Grant Privileges Revoke Privileges Auditing

Revoke User:
Username:
Privil Sys:
Privil Obj:
Table:

Revoke Role:
Role:
Privil Sys:
Privil Obj:
Object:

Edit Privil Obj:
User/Role:
New Privils:
Object:
Flag:
Old Privils:

Edit Privil Sys:
User/Role:
New Privils:
Flag:
Old Privils:

Username:

User's Sys
User's Obj

Role:

Role's Sys
Role's Obj

- ✓ Tab Auditing: Ở đây, người quản trị có thể giám sát các hành động đã được cài chính sách audit

Users Roles Grant Privileges Revoke Privileges Auditing

Standard:

Fine-Grained:

- **Giao diện cho bác sĩ:** Ở đây, bác sĩ có thể thực hiện các chức năng của bác sĩ đã được cài đặt trên hệ thống, cụ thể ở đây bác sĩ có thể xem thông tin cá nhân của mình, xem hồ sơ bệnh án của các bệnh nhân do mình phụ trách và cập nhật lại trường Tình trạng ban đầu và Kết luận của các hồ sơ bệnh án của bệnh nhân do mình phụ trách

Thông tin

Hồ sơ bệnh án

Write outcome:
Ma khám bệnh:
Tình trạng ban đầu:
Kết luận:



- Giao diện cho tiếp tân:** Ở đây, nhân viên tiếp tân có thể thực hiện các chức năng của mình đã được cài đặt trên hệ thống, cụ thể ở đây nhân viên tiếp tân có thể xem thông tin cá nhân của mình, xem thông tin bệnh nhân và xem thông tin các hóa đơn

Thông tin	Hóa Đơn	Bệnh Nhân	X
[Large empty gray box]			

- Giao diện cho nhân viên thuốc:** Ở đây, nhân viên phòng thuốc có thể thực hiện các chức năng của mình đã được cài đặt trên hệ thống, cụ thể ở đây là có thể xem thông tin cá nhân của mình, có thể thêm mới, chỉnh sửa xem thông tin các loại thuốc

Thông tin	Thuốc	X
<p>Add a drug:</p> <p>Mã thuốc: [Input]</p> <p>Tên thuốc: [Input]</p> <p>Đơn vị tính: [Input]</p> <p>Đơn giá: [Input]</p> <p>Lưu ý: [Input] <input type="button" value="Save"/></p> <p>Update a drug:</p> <p>Mã thuốc: [Input]</p> <p>Lưu ý: [Input] <input type="button" value="Save"/></p> [Large empty gray box]		

- Giao diện cho nhân viên thực hiện các dịch vụ của bệnh viện:** Ở đây, nhân viên thực hiện dịch vụ có thể thực hiện các chức năng của mình đã được cài đặt trên hệ thống, cụ thể ở đây là có thể xem thông tin cá nhân của mình, có thể xem các dịch vụ và có thể xem, chỉnh sửa trường Kết luận của các dịch vụ do mình thực hiện và mã hóa chúng, xem lại các key mà nhân viên đó đã dùng mã hóa

Thông tin	
Chi tiết dịch vụ	See Key
Dịch vụ	

Write outcome:

Ma kham benh:

Ket luan:

Key: 

Decode:

Ma kham benh:

Key: 

III. TÀI LIỆU THAM KHẢO

- Slide bài giảng:
https://drive.google.com/drive/folders/1jog8tV6nySw6IggT2b5E9GyyCx_S3EtB
- <http://www4.hcmut.edu.vn/~anhht/Slidesss/182ISS/Lab6.pdf>
- <https://viblo.asia/p/audit-database-p1-1Je5E8pGlnL>
- <https://viblo.asia/p/audit-database-p2-cac-dang-audit-chuan-trong-oracle-Do754W43lM6>
- Lab05-ISS-OLS trên Moodle (ở phần Thực hành)
- <https://docs.oracle.com/database/121/ASOAG/introduction-to-transparent-data-encryption.htm>
- <https://oracle-base.com/articles/8i/data-encryption>