

TRƯỜNG ĐẠI HỌC KHOA HỌC TỰ NHIÊN
KHOA CÔNG NGHỆ THÔNG TIN



BÁO CÁO ĐỒ ÁN MÔN HỌC

BỘ MÔN: AN TOÀN BẢO MẬT HỆ THỐNG THÔNG TIN

Giảng viên: Phạm Thị Bạch Huệ
Lương Vĩ Minh

Sinh viên: Võ Minh Lâm 18120192
Vũ Phan Nhật Tài 18120545
Ngô Nhật Tân 18120547

Thành phố Hồ Chí Minh, ngày 22 tháng 05 năm 2021

MỤC LỤC

I.	Phân tích thiết kế cơ sở dữ liệu	3
1.	Phân tích cơ sở dữ liệu ở mức quan niệm	3
2.	Phân tích cơ sở dữ liệu ở mức logic	3
3.	Phân tích cơ sở dữ liệu ở mức vật lý	3
3.1.	Đặc tả các quan hệ	4
3.2.	Các ràng buộc toàn vẹn của cơ sở dữ liệu	6
3.3.	Xác định và phân quyền các loại người dùng	7
II.	Xây dựng các chức năng của hệ thống	9
1.	Phân hệ 1	9
1.1.	Giao diện đăng nhập	9
1.2.	Xem danh sách người dùng và role trong hệ thống	9
1.3.	Kiểm tra quyền của các người dùng/role	9
1.4.	Xem role của user	10
1.5.	Tạo user mới	10
1.6.	Xoá user	11
1.7.	Hiệu chỉnh user	11
1.8.	Tạo role mới	12
1.9.	Xoá role	12
1.10.	Cấp quyền cho user/role	13
1.11.	Cấp role cho user	14
1.12.	Thu hồi role từ user	14
1.13.	Audit	14
a.	Standard audit	14
b.	Fine-grained audit	15
2.	Phân hệ 2	15
2.1.	Các chính sách DAC	15
2.2.	Các chính sách RBAC	15
2.3.	Các chính sách VPD	15
2.4.	Các chính sách OLS	16
2.5.	Các chính sách mã hóa	16
III.	Đánh giá mức độ hoàn thành đồ án	17
IV.	Phân công và đánh giá công việc	17

3.1. Đặc tả các quan hệ

a. Bảng Nhân viên

Tên thuộc tính	Kiểu dữ liệu	Ràng buộc	Ghi chú
MaNhanVien	Varchar2 (30)	NOT NULL	Khóa chính
HoTen	Varchar2 (30)	NOT NULL	
SĐT	Varchar2 (15)	UNIQUE	
DiaChi	Varchar2 (50)	NOT NULL	
Email	Varchar2 (50)	UNIQUE	
D.O.B	Date	NOT NULL	
LuongCoBan	Int	NOT NULL	
PhuCap	Int	NOT NULL	
Username	Varchar2 (20)	NOT NULL	
MaBoPhan	Varchar2 (10)	NOT NULL	

b. Bảng Bộ phận

Tên thuộc tính	Kiểu dữ liệu	Ràng buộc	Ghi chú
MaBoPhan	Varchar2 (10)	NOT NULL	Khóa chính
TenBoPhan	Varchar2 (50)	NOT NULL	

c. Bảng Lịch trực phòng

Tên thuộc tính	Kiểu dữ liệu	Ràng buộc	Ghi chú
MaPhongKham	Varchar2 (10)	NOT NULL	Khóa chính
MaNhanVien	Varchar2 (30)	NOT NULL	Khóa chính
ThoiGianTruc	Date	NOT NULL	

d. Bảng Phòng khám

Tên thuộc tính	Kiểu dữ liệu	Ràng buộc	Ghi chú
MaPhongKham	Varchar2 (10)	NOT NULL	Khóa chính
TenPhongKham	Varchar2 (50)	NOT NULL	

e. Bảng Phiếu chăm công

Tên thuộc tính	Kiểu dữ liệu	Ràng buộc	Ghi chú
MaNhanVien	Varchar2 (20)	NOT NULL	Khóa chính
ThoiGianChamCong	Date	NOT NULL	Khóa chính
SoNgayCong	int	NOT NULL	
TienLuong	int	NOT NULL	

f. Bảng Hóa đơn

Tên thuộc tính	Kiểu dữ liệu	Ràng buộc	Ghi chú
MaHoaDon	Varchar2 (20)	NOT NULL	Khóa chính
NgayLapHoaDon	Date	NOT NULL	
TongTien	int	NOT NULL	
MaKhamBenh	Varchar2 (20)	NOT NULL	
MaNhanVien	Varchar2 (20)	NOT NULL	

g. Bảng Chi tiết hóa đơn

Tên thuộc tính	Kiểu dữ liệu	Ràng buộc	Ghi chú
MaHoaDon	Varchar2 (20)	NOT NULL	Khóa chính
MaDichVu	Varchar2 (20)	NOT NULL	Khóa chính

h. Bảng Phiếu khám bệnh

Tên thuộc tính	Kiểu dữ liệu	Ràng buộc	Ghi chú
MaKhamBenh	Varchar2 (20)	NOT NULL	Khóa chính
NgayKham	date	NOT NULL	
TrieuChung	Varchar2 (2048)	NOT NULL	
KetLuanCuaBacSi	Varchar2 (2048)	NOT NULL	
MaBenhNhan	Varchar2 (20)	NOT NULL	
MaNhanVien	Varchar2 (20)	NOT NULL	

i. Bảng Bệnh nhân

Tên thuộc tính	Kiểu dữ liệu	Ràng buộc	Ghi chú
MaBenhNhan	Varchar2 (20)	NOT NULL	Khóa chính
HoTenBenhNhan	Varchar2 (30)	NOT NULL	
NamSinh	int	NOT NULL	
DiaChi	Varchar2 (50)	NOT NULL	
SDT	Varchar2 (10)	NOT NULL	

j. Bảng Dịch vụ

Tên thuộc tính	Kiểu dữ liệu	Ràng buộc	Ghi chú
MaDichVu	Varchar2 (20)	NOT NULL	Khóa chính
TenDichVu	Varchar2 (20)	NOT NULL	
GiaTien	int	NOT NULL	

k. Bảng Phiếu yêu cầu dịch vụ

Tên thuộc tính	Kiểu dữ liệu	Ràng buộc	Ghi chú
MaKhamBenh	Varchar2 (20)	NOT NULL	Khóa chính
MaDichVu	Varchar2 (20)	NOT NULL	Khóa chính
KetQuaDichVu	Varchar2 (100)	NOT NULL	
MaNhanVien	Varchar2 (20)	NOT NULL	

l. Bảng Toa thuốc

Tên thuộc tính	Kiểu dữ liệu	Ràng buộc	Ghi chú
MaDonThuoc	Varchar2 (20)	NOT NULL	Khóa chính
NgayLapDon	Date	NOT NULL	
TongTien	int	NOT NULL	
MaKhamBenh	Varchar2 (20)	NOT NULL	

m. Bảng Chi tiết toa thuốc

Tên thuộc tính	Kiểu dữ liệu	Ràng buộc	Ghi chú
MaDonThuoc	Varchar2 (20)	NOT NULL	Khóa chính
MaThuoc	Varchar2 (20)	NOT NULL	Khóa chính
SoLuong	int	NOT NULL	
LieuLuong	Varchar2 (50)	NOT NULL	

n. Bảng Thuốc

Tên thuộc tính	Kiểu dữ liệu	Ràng buộc	Ghi chú
MaThuoc	Varchar2 (20)	NOT NULL	Khóa chính
TenThuoc	Varchar2 (50)	NOT NULL	
DonGia	int	NOT NULL	
DonViTinh	Varchar2 (10)	NOT NULL	
LuuY	Varchar2 (50)	NOT NULL	

3.2. Các ràng buộc toàn vẹn của cơ sở dữ liệu

- Lương cơ bản của của nhân viên phải là số nguyên dương.
- Nhân viên phải trên 18 tuổi.
- Phụ cấp của nhân viên phải là số nguyên dương.
- Số ngày công phải dương và không vượt quá số ngày trong tháng
- Phí dịch vụ phải là số dương
- Tổng tiền toa thuốc phải là số dương
- Số lượng và đơn giá thuốc phải là số dương

3.3. Xác định và phân quyền các loại người dùng

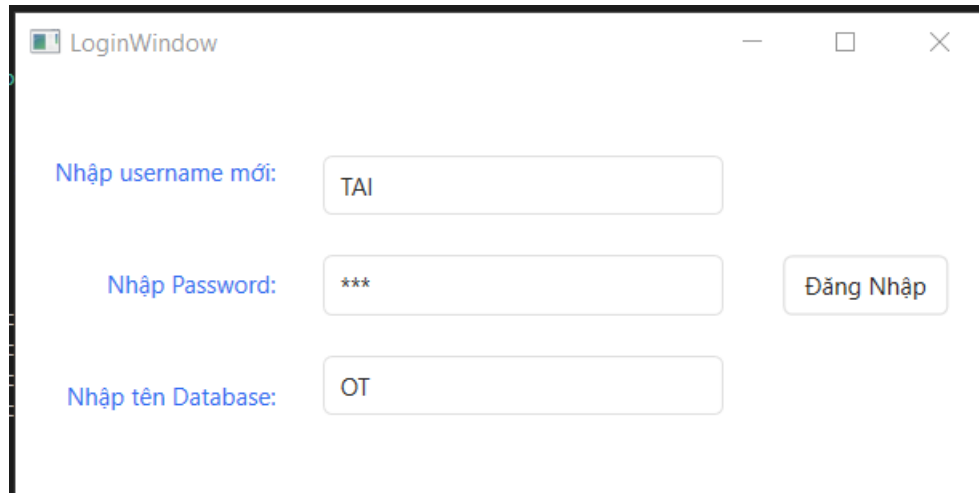
		Quản lý tài nguyên và nhân sự	Quản lý tài vụ	Quản lý chuyên môn	Tiếp tân và điều phối	Nhân viên phòng tài vụ	Bác sĩ	Nhân viên bán thuốc	Nhân viên kế toán
PHONG KHAM	I	X							
	R	X	X	X	X		X		
	U	X							
	D	X							
LICHTRUC PHONG	I	X							
	R	X	X	X	X		X		
	U	X							
	D	X							
PHIEUCHAM CONG	I								X
	R	X	X (Chỉ dữ liệu của mình)	X	X (Chỉ dữ liệu của mình)	X (Chỉ dữ liệu của mình)	X (Chỉ dữ liệu của mình)	X (Chỉ dữ liệu của mình)	X
	U								X
	D								
NHANVIEN	I	X							
	R	X	X	X	X (Chỉ dữ liệu của mình)	X (Chỉ dữ liệu của mình)	X (Chỉ dữ liệu của mình)	X (Chỉ dữ liệu của mình)	(LUONGCB, PHUCAP)
	U	X	X (Chỉ dữ liệu của mình) bao gồm (HoTen, SDT, DiaChi, Email, DOB)	X (Chỉ dữ liệu của mình) bao gồm (HoTen, SDT, DiaChi, Email, DOB)	X (Chỉ dữ liệu của mình) bao gồm (HoTen, SDT, DiaChi, Email, DOB)	X (Chỉ dữ liệu của mình) bao gồm (HoTen, SDT, DiaChi, Email, DOB)	X (Chỉ dữ liệu của mình) bao gồm (HoTen, SDT, DiaChi, Email, DOB)	X (Chỉ dữ liệu của mình) bao gồm (HoTen, SDT, DiaChi, Email, DOB)	X (Chỉ dữ liệu của mình) bao gồm (HoTen, SDT, DiaChi, Email, DOB)
	D	X							
BENHNHAN	I				X				
	R	X	X	X	X				
	U				X				
	D								
PHIEUKHAM BENH	I				X				
	R		X	X	X		Chỉ với bệnh nhân của mình		

	U						Chỉ với bệnh nhân của mình		
	D								
THUOC	I								
	R		X	X			X	X	
	U		(Đơn giá)						
	D								
CHITIETTOA THUOC	I						X		
	R		X	X			X	X	
	U						X		
	D						X		
TOATHUOC	I						X		
	R		X	X			X	X	
	U						X	(Tổng tiền)	
	D						X		
BOPHAN	I	X							
	R	X	X	X	X	X	X	X	X
	U	X							
	D	X							
CHITIET HOADON	I					X			
	R		X	X		X			
	U					X			
	D								
HOADON	I					X			
	R		X	X		X			
	U					X			
	D								
PHIEUYEU CAUDICHVU	I				X		X		
	R		X	X	Trừ (KQDICHVU)	Trừ (KQDICHVU)	X		
	U				Trừ (KQDICHVU)		X		
	D						X		
DICHVU	I								
	R		X	X	X (trừ giá tiền)	X	X		
	U		(Đơn giá)						
	D								

II. Xây dựng các chức năng của hệ thống

1. Phân hệ 1

1.1. Giao diện đăng nhập



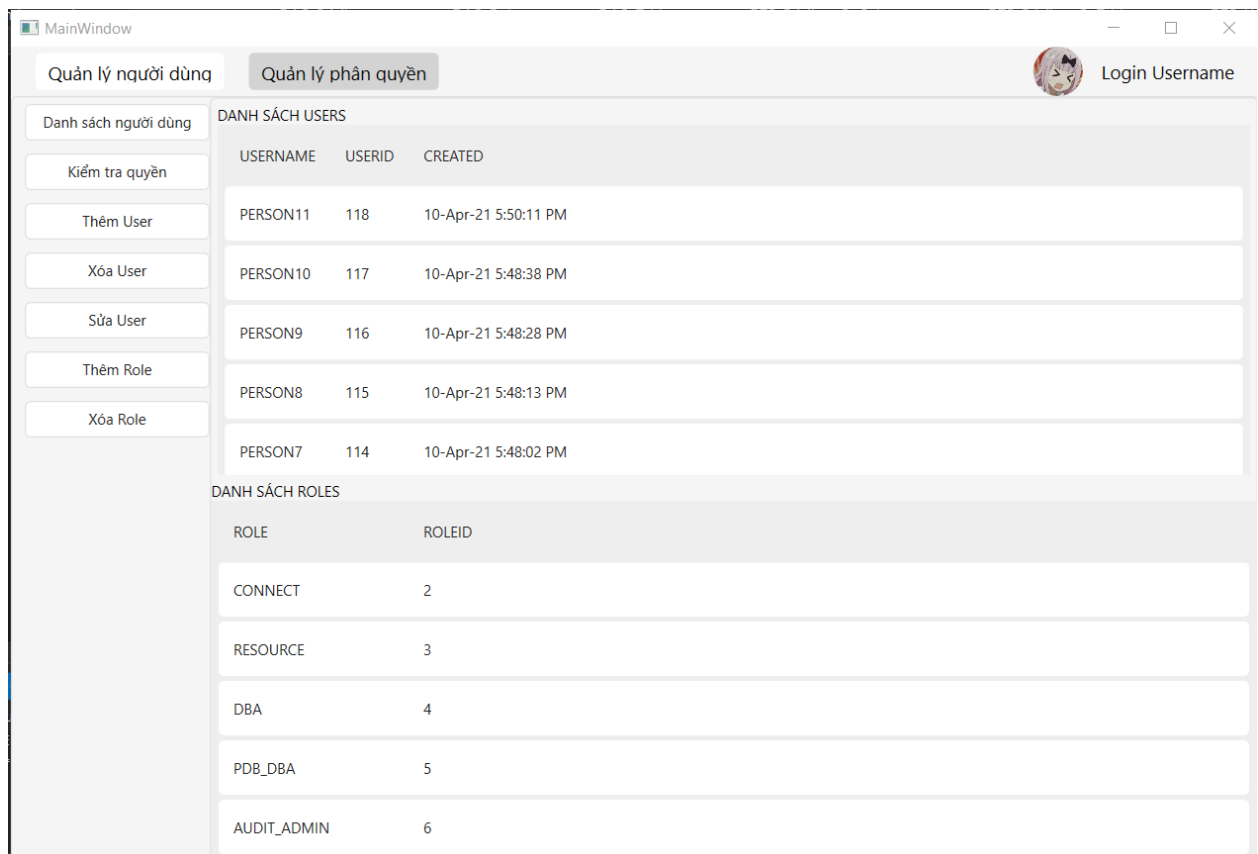
LoginWindow

Nhập username mới: TAI

Nhập Password: *** Đăng Nhập

Nhập tên Database: OT

1.2. Xem danh sách người dùng và role trong hệ thống



MainWindow

Quản lý người dùng Quản lý phân quyền Login Username

Danh sách người dùng

Kiểm tra quyền

Thêm User

Xóa User

Sửa User

Thêm Role

Xóa Role

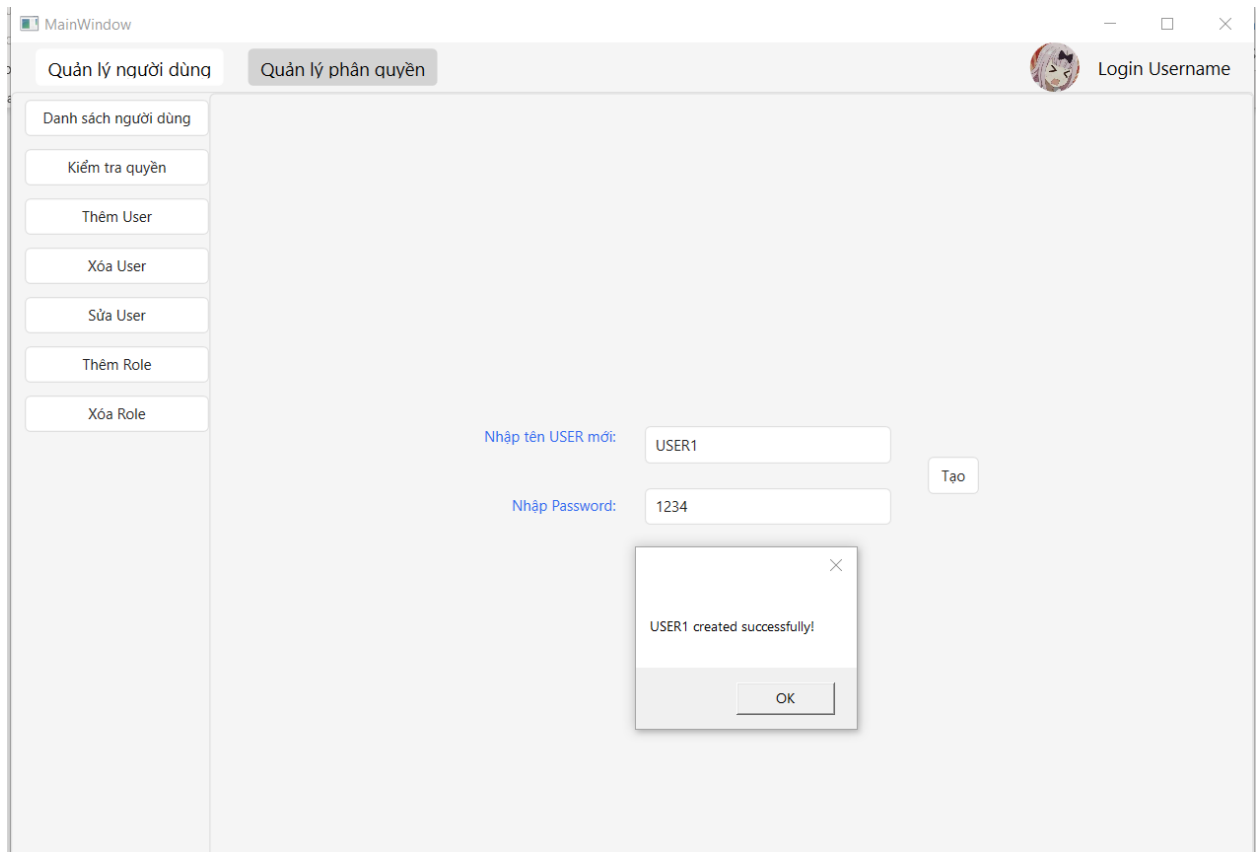
DANH SÁCH USERS

USERNAME	USERID	CREATED
PERSON11	118	10-Apr-21 5:50:11 PM
PERSON10	117	10-Apr-21 5:48:38 PM
PERSON9	116	10-Apr-21 5:48:28 PM
PERSON8	115	10-Apr-21 5:48:13 PM
PERSON7	114	10-Apr-21 5:48:02 PM

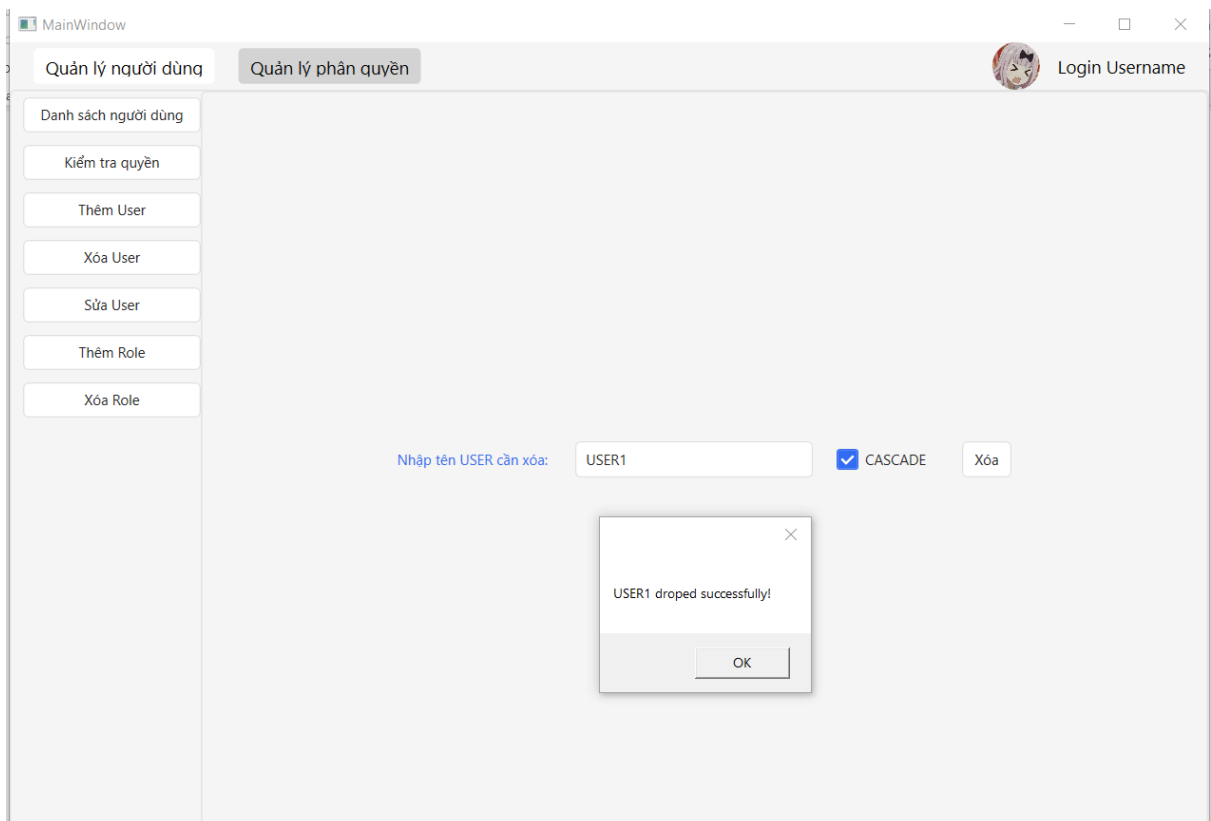
DANH SÁCH ROLES

ROLE	ROLEID
CONNECT	2
RESOURCE	3
DBA	4
PDB_DBA	5
AUDIT_ADMIN	6

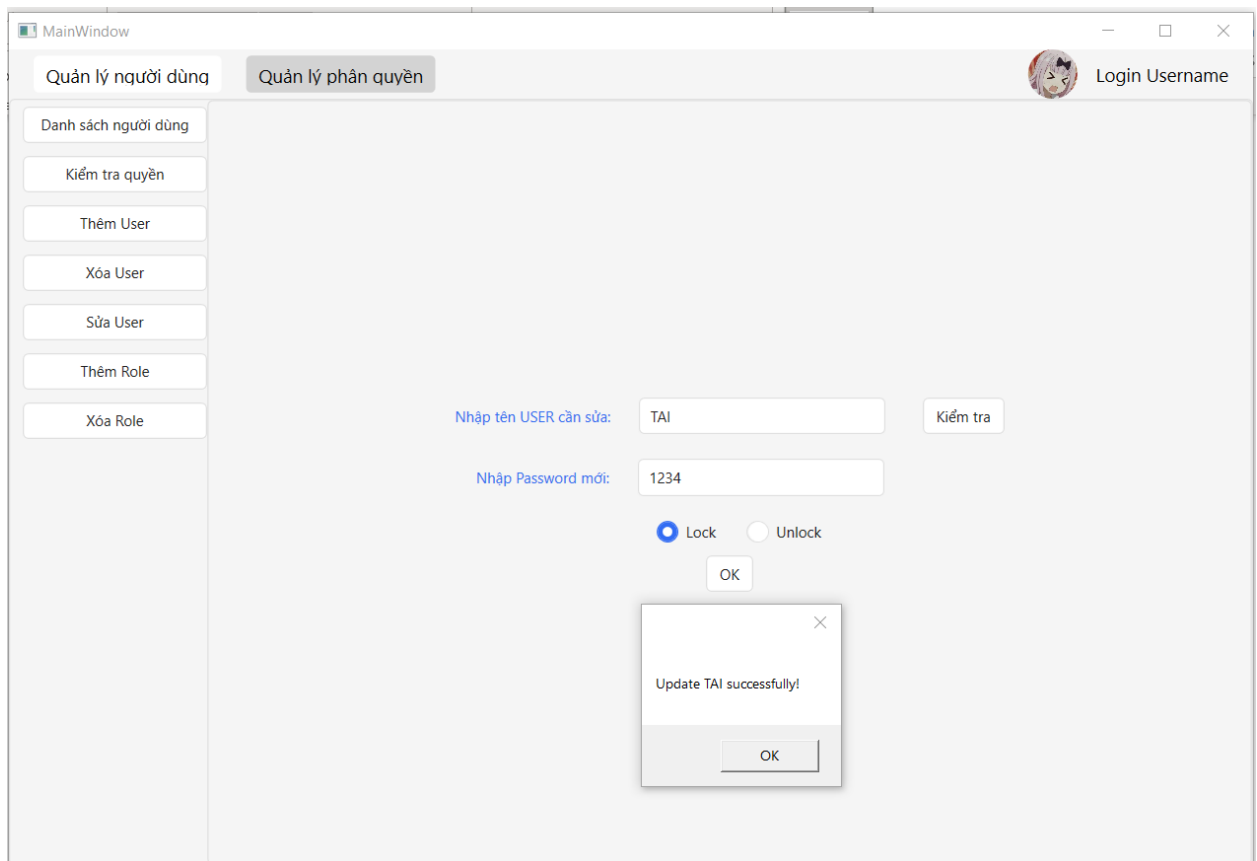
1.3. Kiểm tra quyền của các người dùng/role



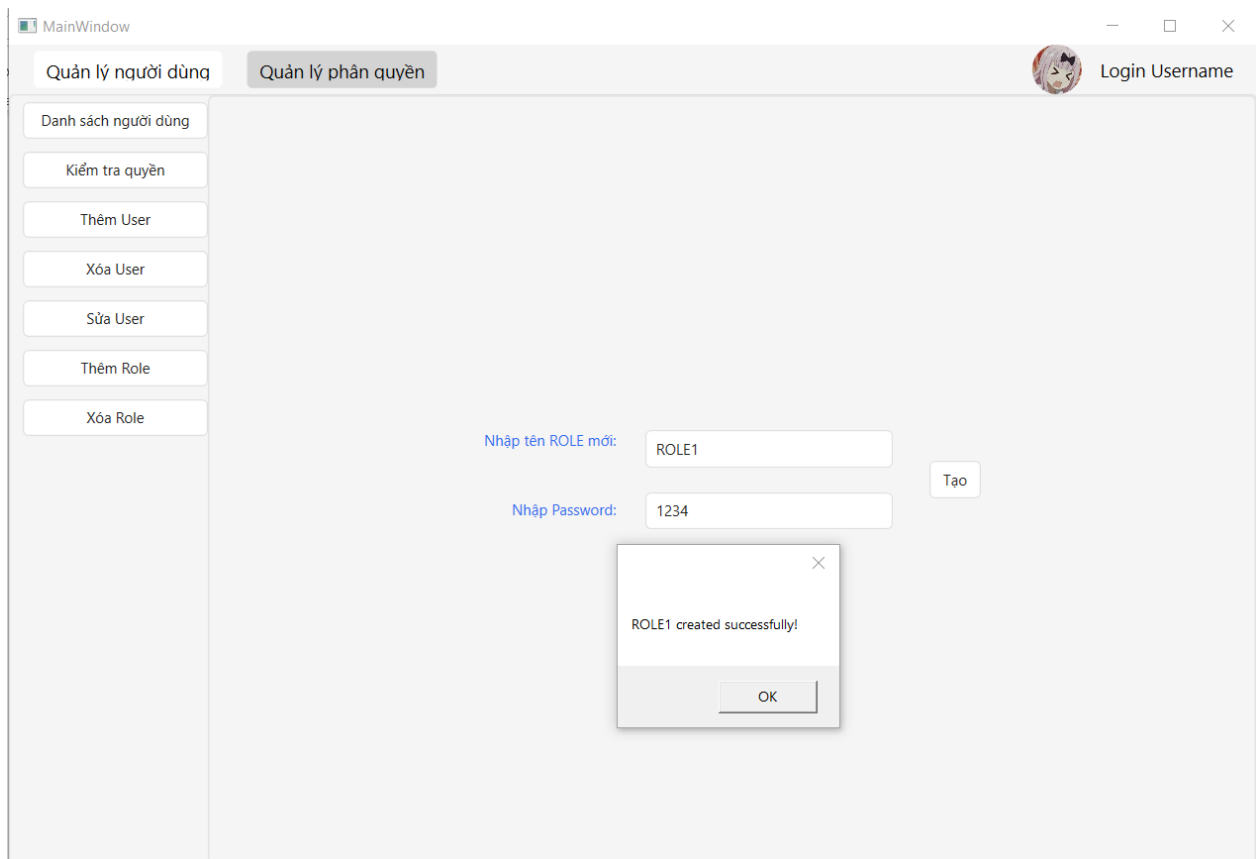
1.6. Xóa user



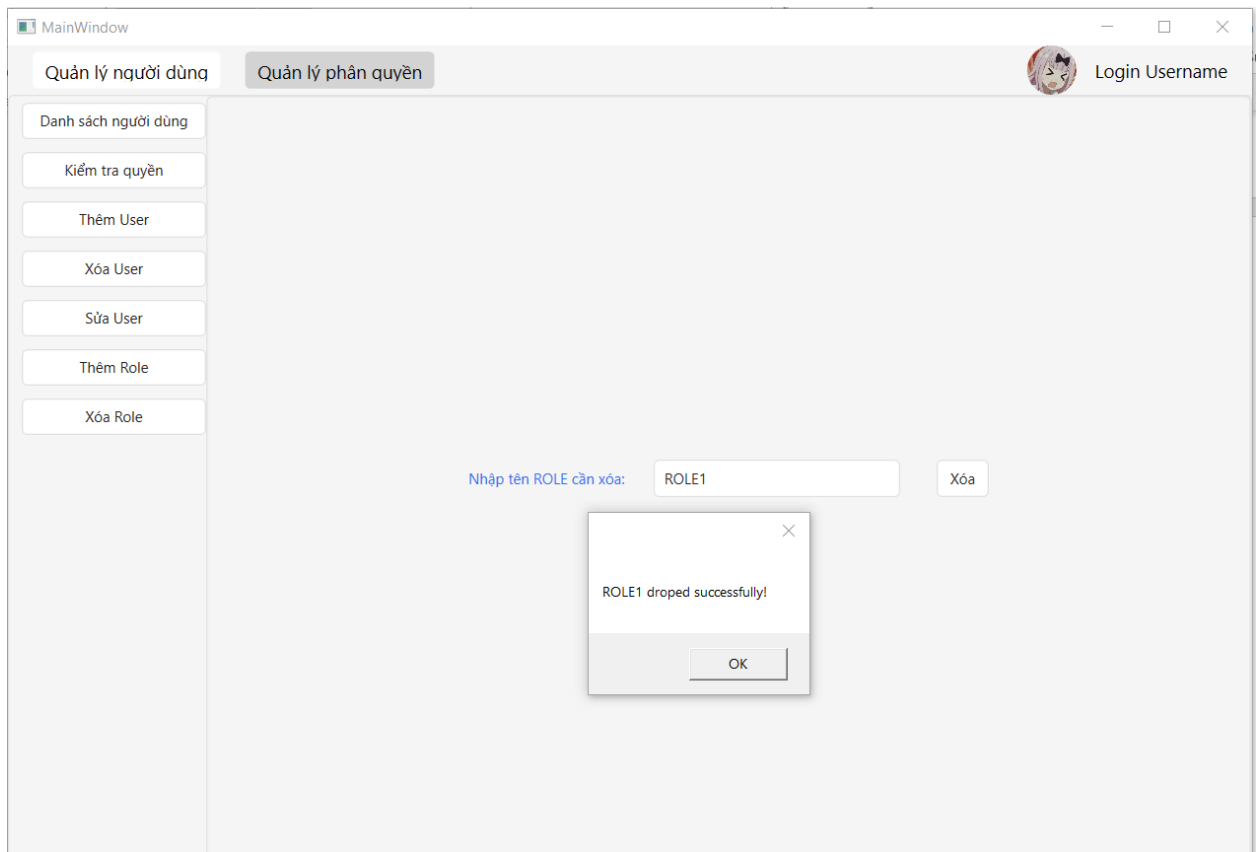
1.7. Hiệu chỉnh user



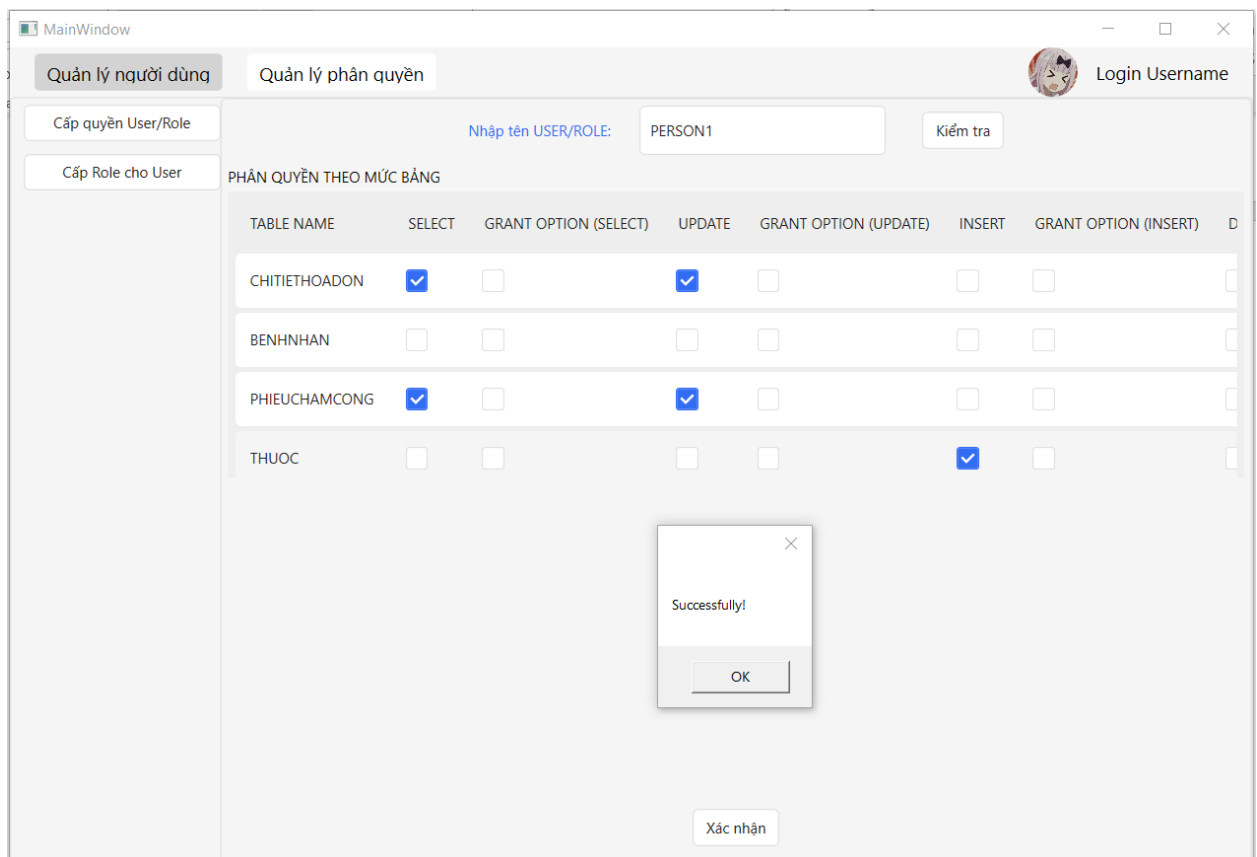
1.8. Tạo role mới



1.9. Xóa role



1.10. Cấp quyền cho user/role



1.11. Cấp role cho user

The screenshot shows a web application window titled 'MainWindow'. It has two tabs: 'Quản lý người dùng' and 'Quản lý phân quyền'. The 'Quản lý phân quyền' tab is active. On the left sidebar, there are two buttons: 'Cấp quyền User/Role' and 'Cấp Role cho User'. The main area displays a form with the text 'GRANT ROLE' followed by a dropdown menu showing 'BACSI', then 'TO' followed by a dropdown menu showing 'PERSON2', and a 'Confirm' button. A modal dialog box is open in the center, displaying the message 'Grant succeeded.' and an 'OK' button.

1.12. Thu hồi role từ user

The screenshot shows the same web application window. The left sidebar now includes four buttons: 'Cấp quyền User/Role', 'Cấp Role cho User', 'Xem Role của User', and 'Thu hồi Role của User'. The main area displays a form with the text 'REVOKE ROLE' followed by an empty dropdown menu, then 'FROM' followed by a dropdown menu showing 'TEST', and a 'Confirm' button. A modal dialog box is open in the center, displaying the message 'Revoke succeeded.' and an 'OK' button.

1.13. Audit

a. Standard audit

🚦 **Chính sách 1:** Những thông tin trên bảng Bệnh nhân được đánh giá là vô cùng nhạy cảm. Theo quy định được đề ra, hệ thống phải đảm bảo tính bảo mật đối với thông tin cá nhân của từng bệnh nhân. Vì vậy chính sách Standard audit được cài đặt trên bảng Bệnh nhân để

theo dõi tất cả hành vi của tất cả người dùng trên bảng dữ liệu này bao gồm như xem, thêm, sửa, xóa.

✚ **Chính sách 2:** hệ thống được xây dựng ra để dành cho đội ngũ nhân viên của bệnh viện sử dụng, bên cạnh đó thông tin cá nhân của mỗi nhân viên cũng được đánh giá cần được bảo vệ tránh khỏi việc đánh cắp thông tin. Vì vậy standard audit được cài đặt trên bảng nhân viên để theo dõi lại các hành vi nhằm ngăn chặn việc đánh cắp tài khoản cũng như đánh cắp thông tin cá nhân của nhân viên.

b. Fine-grained audit

✚ **Chính sách 1:** Trong quá trình khám bệnh, bác sĩ có thể yêu cầu bệnh nhân thực hiện một số dịch vụ khác (xét nghiệm, X-quang, ...) sau đó dựa vào kết quả của các dịch vụ ấy để có thể đưa ra những chẩn đoán về bệnh cho bệnh nhân. Theo nguyên tắc tất cả thông tin cá nhân và hồ sơ bệnh án của bệnh nhân phải được bảo vệ và giữ bí mật thì Fine – grained audit được cài đặt lên cột KetQuaDichVu trong bảng PhieuYeuCauDichVu để theo dõi hành vi của những người dùng trên đối tượng dữ liệu này.

✚ **Chính sách 2:** sau khi hoàn tất quá trình chẩn đoán của mình, bác sĩ sẽ ghi lại hồ sơ bệnh án cho bệnh nhân trong phiếu khám bệnh. Với ý tưởng tương tự ở chính sách 1, fine - grained audit được cài đặt trên cột KetLuanCuaBacSi trong bảng PhieuKhamBenh để ghi nhận tất cả hành vi của tất cả người dùng trên đối tượng dữ liệu này.

2. Phân hệ 2

2.1. Các chính sách DAC

DAC (*Direct access control*) 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** và **REVOKE**. Các quyền ở đây có thể **Select, Insert, Update, Delete, Execute**. Các chính sách đã được cài đặt cụ thể như sau:

✚ **Chính sách 1:** người dùng được xác định là Nhân viên tài vụ của bệnh viện sẽ được quyền truy cập và xem các thông tin trên bảng dịch vụ.

✚ **Chính sách 2:** người dùng được xác định là bác sĩ sẽ được phân quyền xem các thông tin trên bảng thuốc và dịch vụ.

2.2. Các chính sách RBAC

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 role đã được cài đặt và quyền của các role có thể tham khảo chi tiết tại mục 3.3 trong phần I. Để minh họa cho các role đã được cài đặt, nhóm đã demo trên 2 role cụ thể như sau:

✚ **Role Nhân viên bán thuốc:** có thể xem thông tin trên bảng Thuốc và bảng Toa thuốc

✚ **Role Nhân viên quản lý tài vụ:** có thể xem trên bảng Dịch vụ cũng như các thông tin thanh toán trong hóa đơn hiện có.

2.3. Các chính sách VPD

Sau khi người dùng được cấp các quyền trên cơ sở dữ liệu, hệ quản trị sẽ xét đến các chính sách **VPD** (*Virtual Private Database*) dùng để kiểm soát các dòng cụ thể trong 1 bảng bằng

cách thêm mệnh đề Where vào sau các câu truy vấn của người dùng, từ đó có thể giới hạn những dòng dữ liệu mà người dùng được phép coi. Các chính sách VPD đã được cài đặt được mô tả cụ thể như sau:

✚ **Đối với bảng Phiếu chăm công:** các role như Tiếp tân và điều phối, nhân viên tài vụ, bác sĩ, nhân viên bán thuốc chỉ được xem những thông tin của mình. Còn những role còn lại nếu được cấp quyền truy cập thì có thể xem tất cả các dòng trong bảng.

✚ **Đối với bảng Phiếu khám bệnh:** bác sĩ chỉ xem được những phiếu khám bệnh do mình chịu trách nhiệm. Các role ngoài bác sĩ nếu được cấp quyền thì sẽ truy cập tất cả các dòng dữ liệu.

2.4. Các chính sách OLS

OLS (*Oracle label security*) là một trong chính sách điều khiển quyền truy cập các dòng trong một bảng bằng cách dán nhãn lên các dòng dữ liệu và lên từng người dùng. Khi người dùng gọi đến bảng dữ liệu được cài đặt chính sách OLS thì chỉ xem được những dòng dữ liệu thỏa mãn nhãn của mình. Các nhãn được chia thành 3 mức độ là Level, Compartment và Group. Chính sách được cài đặt cụ thể như sau:

- ✚ **Level:** Quản lý, nhân viên
- ✚ **Compartment:** Nhân sự, chuyên môn
- ✚ **Group:** Chi nhánh A, chi nhánh B

Diễn giải: bệnh viện sẽ gồm 2 chi nhánh A và B. Tại mỗi chi nhánh sẽ gồm nhiều bộ phận khác nhau (cài đặt demo 2 phòng ban mẫu là nhân sự và chuyên môn) và trong mỗi phòng ban sẽ gồm 2 loại nhân viên là Quản lý và nhân viên thường. Chính sách OLS được cài đặt trên bảng Nhân viên với các chính sách cụ thể như sau:

- ✚ Nhân viên chỉ được các dòng dữ liệu ở chi nhánh của mình
- ✚ Quản lý nhân sự được nhìn thấy tất cả thông tin của trong bảng nhân viên bao gồm Giám đốc
- ✚ Nhân viên nhân sự có quyền tương tự như quản lý nhân sự trừ không thể xem được thông tin của Giám đốc vì lý do bảo mật
- ✚ Quản lý chuyên môn có thể nhìn thấy tất cả các nhân viên thuộc phòng ban của mình.

2.5. Các chính sách mã hóa

Như đã đề cập ở trên, theo quy định các thông tin liên quan đến hồ sơ bệnh án của bệnh nhân phải được bảo mật. Chính sách mã hóa được thực hiện trên cột Triệu chứng và Kết quả chẩn đoán của bảng Phiếu khám bệnh. Tuy nhiên nhóm không thực hiện việc mã hóa tại Oracle mà quyết định việc mã hóa và giải mã sẽ được tại client vì để đảm bảo cho việc dữ liệu không bị đánh cắp trên đường truyền.

Bằng thuật toán mã hóa Triple DES, việc mã hóa và giải mã sẽ được thực hiện ở client mỗi khi người dùng insert và hoặc gọi dữ liệu từ cơ sở dữ liệu lên. Điều đó đảm bảo cho dữ liệu trên đường truyền là dữ liệu đã được mã hóa và không thể giải mã được nếu không tìm được thuật toán và các yếu tố được cài đặt client.

✚ Mô tả cơ chế hoạt động của thuật toán

Thuật toán muốn mã hóa với giải mã cần 2 yếu tố là Init Vector và Key.

- Key được lưu trữ cố định tại client.
- InitVector là chuỗi random có 8 ký tự (8 bytes)

Dữ liệu sau khi được mã hóa thành dạng chuỗi sẽ được chèn thêm InitVector ở phía trước và được lưu xuống cơ sở dữ liệu. Lúc giải mã, client sẽ tách InitVector và cypher value ra và lấy InitVector với Key để giải mã dữ liệu.

III. Đánh giá mức độ hoàn thành đồ án

STT	Phân hệ	Tên chính sách	Số chính sách được cài đặt	Mức độ hoàn thành
1	1	Các chức năng của QTV	-	100%
2		Standard audit	2	100%
3		Fine – grained audit	2	100%
4	2	DAC	2	100%
5		RBAC	8 (trên Oracle) 2 (tại Giao diện)	100%
6		VPD	2	100%
7		OLS	1	100%
8		Mã hóa	1	100%

IV. Phân công và đánh giá công việc

STT	Công việc	Thành viên được phân công	Mức độ hoàn thành
1	Phân tích thiết kế hệ thống	Ngô Nhật Tân	100%
2	Cài đặt cơ sở dữ liệu	Vũ Phan Nhật Tài	100%
3	Cài đặt các RBTV	Ngô Nhật Tân	100%
4	Cài đặt các chức năng của Quản trị viên	Vũ Phan Nhật Tài Võ Minh Lâm	100%
5	Cài đặt các chính sách Audit	Võ Minh Lâm	100%
6	Cài đặt các role	Vũ Phan Nhật Tài	100%

7	Cài đặt các chính sách VPD	Ngô Nhật Tân	100%
8	Cài đặt các chính sách OLS	Ngô Nhật Tân	100%
9	Cài đặt các chính sách mã hóa	Võ Minh Lâm	100%
10	Thiết kế và cài đặt giao diện	Võ Minh Lâm	100%
		Vũ Phan Nhật Tài	