|  |  |  |
| --- | --- | --- |
|  | **Đại học Quốc gia Thành phố Hồ Chí Minh**  **Trường Đại học Khoa học Tự nhiên**  **Khoa Công nghệ Thông tin** | |
| **AN TOÀN VÀ BẢO MẬT DỮ LIỆU TRONG HỆ THỐNG THÔNG TIN** | |
| **BÁO CÁO ĐỒ ÁN THỰC HÀNH** | |
| **| CHỦ ĐỀ |**  **XÂY DỰNG HỆ THỐNG THÔNG TIN**  **QUẢN LÝ CHUỖI TIỆM CẮT TÓC VĂN MINH** | |
| **Giảng viên hướng dẫn:**  **TS. Phạm Thị Bạch Huệ**  **ThS. Tiết Gia Hồng**  **ThS. Lương Vĩ Minh** | |
| Thành phố Hồ Chí Minh – 07/2022 | |

**Đồ án thực hành – xây dựng hệ thống thông tin**

**Nhóm thực hiện: ATBMCQ-4**

**HỌC KỲ II – NĂM HỌC 2021-2022**

**an toàn và bảo mật dữ liệu trong hệ thống thông tin**

**ĐẠI HỌC QUỐC GIA THÀNH PHỐ HỒ CHÍ MINH**

**ĐẠI HỌC KHOA HỌC TỰ NHIÊN THÀNH PHỐ HỒ CHÍ MINH**

**KHOA CÔNG NGHỆ THÔNG TIN**



# LỜI CẢM ƠN

Lời đầu tiên, nhóm chúng em xin gửi lời cảm ơn chân thành đến trường Đại học Khoa học Tự nhiên đã đưa môn An toàn và bảo mật dữ liệu trong hệ thống thông tin vào chương trình giảng dạy. Đặc biệt, nhóm chúng em xin gửi lời cảm ơn sâu sắc đến cô Phạm Thị Bạch Huệ, cô Tiết Gia Hồng và thầy Lương Vĩ Minh đã truyền đạt những kiến thức quý báu cho chúng em trong suốt thời gian học tập. Thầy cô không chỉ mang đến cho chúng em vốn kiến thức về lý thuyết mà còn là những kinh nghiệm trong thực hành, làm cho chúng em có cái nhìn khách quan hơn và sâu hơn về an toàn và bảo mật dữ liệu trong hệ thống thông tin. Trong thời gian qua, chúng em đã có thêm kiến thức lẫn thực hành thực tiễn với một tinh thần học tập hiệu quả, nghiêm túc. Đây chắc chắn là hành trang cực kì bổ ích hỗ trợ cho chúng em sau này. An toàn và bảo mật dữ liệu trong hệ thống thông tin là môn học thú vị, bổ ích và thực tiễn. Đảm bảo cung cấp đủ kiến thức cần có cho sinh viên khoa công nghệ thông tin.

Tuy nhiên, do vốn kiến thức hạn hẹp cũng như khả năng tiếp thu kiến thức còn nhiều hạn chế mặc dù nhóm chúng em đã cố gắng hết sức mình để có thực hiện đồ án và báo cáo một cách chỉnh chu nhất, tuy nhiên không thể tránh được những thiếu sót. Chúng em rất mong nhận được sự chỉ bảo, đóng góp ý kiến của thầy cô để chúng em có điều kiện bổ sung, nâng cao kiến thức của mình, phục vụ tốt hơn công tác thực tế sau này.

Nhóm chúng em xin chân thành cảm ơn!

# MỤC LỤC

# BẢNG THÔNG TIN NHÓM

|  |  |  |
| --- | --- | --- |
| **Mã nhóm** | 4 | |
| **Số lượng** | 4 | |
| **MSSV** | **Họ tên** | **Email** |
| 18120289 | Lâm Quốc Bình | [18120289@student.hcmus.edu.vn](mailto:18120289@student.hcmus.edu.vn) |
| 19120640 | Trần Minh Sơn | [19120640@student.hcmus.edu.vn](mailto:19120640@student.hcmus.edu.vn) |
| 19120674 | Phạm Tân Tị | [19120674@student.hcmus.edu.vn](mailto:19120674@student.hcmus.edu.vn) |
| 19120714 | Trần Tín Văn | [19120714@student.hcmus.edu.vn](mailto:19120714@student.hcmus.edu.vn) |

# BẢNG PHÂN CÔNG CÔNG VIỆC

|  |  |  |
| --- | --- | --- |
| **Người thực hiện** | **Công việc** | **Mức độ hoàn thành** |
| Trần Tín Văn | Xem danh sách người dùng trong hệ thống. | 100% |
| Trần Tín Văn | Thông tin về quyền (privileges) của mỗi user/ role trên các đối tượng dữ liệu. | 100% |
| Phạm Tân Tị | Cho phép tạo mới, xóa, sửa (hiệu chỉnh) user hoặc role | 100% |
| Trần Minh Sơn  Phạm Tân Tị | Cho phép thực hiện việc cấp quyền: cấp quyền cho user, cấp quyền cho role, cấp role cho user  Quá trình cấp quyền có tùy chọn là có cho phép người được cấp quyền có thể cấp quyền đó cho user/ role khác hay không (có chỉ định WITH GRANT OPTION hay không)  Quyền, select, update thì cho phép phân quyền tinh đến mức cột; quyền insert, delete thì không | 100% |
| Trần Minh Sơn  Phạm Tân Tị | Cho phép thu hồi quyền từ người dùng / role | 100% |
| Lâm Quốc Bình | Cho phép kiểm tra quyền của các chủ thể vừa được cấp quyền | 100% |
| Phạm Tân Tị | Cho phép chỉnh sửa quyền của user/role | 100% |
| Lâm Quốc Bình | Chỉnh sửa tất cả giao diện và chức năng đăng nhập | 100% |
| Trần Tín Văn  Lâm Quốc Bình | Kiểm thử hệ thống | 100% |

# KẾT QUẢ BÁO CÁO

|  |  |
| --- | --- |
| **Loại đồ án** | Đồ án thực hành |
| **Ngày kết thúc** | 30/06/2022 |

## Tổng quan

Trong những năm gần đây, các chương trình quản lí dữ liệu không còn xa lạ với chúng ta. Việc quản lý người dùng và dữ liệu là rất cần thiết. Đặc biệt là trong lĩnh vực y tế, công tác quản lý thông tin là rất quan trọng và đòi hỏi độ chính xác cao. Ứng dụng công nghệ thông tin vào trong việc quản lý giúp người dùng giảm thiểu đi việc quản lý thủ công mất nhiều thời gian và tiết kiệm chi phí. Từ đó có thể nâng cao hiệu quả công việc và chất lượng dịch vụ.

Nắm bắt xu thế đó cùng với đồ án thực hành của môn An toàn và bảo mật dữ liệu trong hệ thống thông tin, nhóm chúng em đã tìm hiểu và xây dựng chương trình Quản lý thông tin y tế cho một sở y tế.

## Sản phẩm

### Các công cụ dùng để xây dựng chương trình:

**Oracle Database Sever:** Thiết kế cơ sở dữ liệu

**Microsoft Visual Studio**: Lập trình ứng dụng

**GitHub:** Quản lý dự án – Link

**Youtube:** Video demo – Link

### Chính sách bảo mật

Với phân hệ 1, nhóm chúng em đã áp dụng được 2 chính sách bảo mật cụ thể là DAC và RBAC. Admin là siêu người dùng có thể tạo mới user/role và cấp quyền cũng như chỉnh sửa quyền cho mỗi user/role.

Với phân hệ 2, nhóm chúng em đã hoàn thiệt và áp dụng thêm các chính sách bảo mật.

#### DAC – RBAC:

Danh sách các role:

* CSYT\_ROLE\_THANHTRA

TC#2: Có 5 nhân viên thuộc sở y tế với vai trò “Thanh tra”. Các nhân viên giữ vai trò thanh tra có thể đọc dữ liệu trên tất cả các quan hệ được mô tả để kết xuất báo cáo định kỳ, mà không có quyền thêm, xóa, sửa trên bất cứ quan hệ nào.

Tạo role CSYT\_ROLE\_THANHTRA và gán các quyền select trên tất cả các bảng.

|  |
| --- |
| **CREATE ROLE** CSYT\_ROLE\_THANHTRA;  **GRANT SELECT ON** CSYT\_Admin.HSBA **TO** CSYT\_ROLE\_THANHTRA;  **GRANT SELECT ON** CSYT\_Admin.HSBA\_DV **TO** CSYT\_ROLE\_THANHTRA;  **GRANT SELECT ON** CSYT\_Admin.BenhNhan **TO** CSYT\_ROLE\_THANHTRA;  **GRANT SELECT ON** CSYT\_Admin.CSYT **TO** CSYT\_ROLE\_THANHTRA;  **GRANT SELECT ON** CSYT\_Admin.NhanVien **TO** CSYT\_ROLE\_THANHTRA; |

* CSYT\_ROLE\_QUANLIDULIEU

Áp dụng TC#3 tạo role CSYT\_ROLE\_QUANLIDULIEU và cấp quyền select các view và thực thi các procedure cho role CSYT\_ROLE\_QUANLIDULIEU theo tiêu chí 3:

* Thêm, xóa dòng trên hồ sơ bệnh án (HSBA)
* Thêm, xóa dòng dịch vụ (HSBA\_DV) liên quan 1 hồ sơ bệnh án.

|  |
| --- |
| **CREATE ROLE** CSYT\_ROLE\_QUANLIDULIEU;  **GRANT SELECT ON** CSYT\_Admin.View\_QuanLiDuLieu\_HSBA **TO** CSYT\_ROLE\_QUANLIDULIEU;  **GRANT SELECT ON** CSYT\_Admin.View\_QuanLiDuLieu\_HSBA\_DV **TO** CSYT\_ROLE\_QUANLIDULIEU;  **GRANT EXECUTE ON** CSYT\_Admin.QLDL\_Insert\_HSBA **TO** CSYT\_ROLE\_QUANLIDULIEU;  **GRANT EXECUTE ON** CSYT\_Admin.QLDL\_Insert\_HSBA\_DV **TO** CSYT\_ROLE\_QUANLIDULIEU;  **GRANT EXECUTE ON** CSYT\_ADMIN.QLDL\_Delete\_HSBA **TO** CSYT\_ROLE\_QUANLIDULIEU;  **GRANT EXECUTE ON** CSYT\_ADMIN.QLDL\_Delete\_HSBA\_DV **TO** CSYT\_ROLE\_QUANLIDULIEU; |

* CSYT\_ROLE\_BACSI

Y sĩ/ Bác sĩ có quyền xem hồ sơ bệnh án (HSBA) mà họ đã chữa trị và kết quả về các dịch vụ đã sử dụng (HSBA\_DV) và thông tin bệnh nhân (BỆNHNHÂN) khi nhập thông tin mã bệnh nhân hoặc số CMND. Áp dụng TC#4 tạo role CSYT\_ROLE\_BACSI và cấp quyền cho role CSYT\_ROLE\_BACSI:

|  |
| --- |
| **CREATE ROLE** CSYT\_ROLE\_BACSI;  **GRANT SELECT ON** CSYT\_ADMIN.VIEW\_BACSI\_HSBA **TO** CSYT\_ROLE\_BACSI;  **GRANT SELECT ON** CSYT\_ADMIN.VIEW\_BACSI\_HSBA\_DV **TO** CSYT\_ROLE\_BACSI;  **GRANT SELECT ON** CSYT\_ADMIN.VIEW\_BACSI\_BENHNHAN **TO** CSYT\_ROLE\_BACSI;  **GRANT EXECUTE ON** CSYT\_ADMIN.BACSI\_SELECT\_BENHNHAN **TO** CSYT\_ROLE\_BACSI; |

* CSYT\_ROLE\_NGHIENCUU

Nhân viên ở vai trò “Nghiên cứu” ở mỗi cơ sở y tế, chỉ có thể xem các hồ sơ bệnh án được điều trị tại cùng cơ sơ y tế với nhân viên nghiên cứu đó), tại khoa giống chuyên khoa ghi trên bằng cấp của nhân viên nghiên cứu đó. Áp dụng TC#5 tạo role CSYT\_ROLE\_NGHIENCUU và cấp quyền cho role CSYT\_ROLE\_NGHIENCUU sao cho phù hợp với TC#5:

|  |
| --- |
| **CREATE ROLE** CSYT\_ROLE\_NGHIENCUU;  **GRANT SELECT ON** CSYT\_ADMIN.VIEW\_NGHIENCUU\_HSBA **TO** CSYT\_ROLE\_NGHIENCUU;  **GRANT SELECT ON** CSYT\_ADMIN.VIEW\_NGHIENCUU\_HSBA\_DV **TO** CSYT\_ROLE\_NGHIENCUU; |

* CSYT\_ROLE\_BENHNHAN

TC#5: Mỗi nhân viên hoặc bệnh nhân đăng nhập chỉ có thể xem thông tin của chính mình và có thể chỉnh sửa các trường (trừ trường mã) liên quan đến chính người đó. Áp dụng TC#5 tạo role CSYT\_ROLE\_BENHNHAN và cấp quyền cho role CSYT\_ROLE\_BENHNHAN sao cho phù hợp:

|  |
| --- |
| **CREATE ROLE** CSYT\_ROLE\_BENHNHAN;  **GRANT SELECT ON** CSYT\_ADMIN.VIEW\_BENHNHAN\_SELFVIEW **TO** CSYT\_ROLE\_BENHNHAN;  **GRANT UPDATE ON** CSYT\_ADMIN.VIEW\_BENHNHAN\_SELFVIEW **TO** CSYT\_ROLE\_BENHNHAN; |

* CSYT\_ROLE\_NHANVIEN

CSYT\_ROLE\_NHANVIEN cũng giống như các quyền role CSYT\_ROLE\_BENHNHAN được cấp theo TC#5:

|  |
| --- |
| **CREATE ROLE** CSYT\_ROLE\_NHANVIEN;  **GRANT SELECT ON** CSYT\_ADMIN.VIEW\_NHANVIEN\_SELFVIEW **TO** CSYT\_ROLE\_NHANVIEN;  **GRANT UPDATE ON** CSYT\_ADMIN.VIEW\_NHANVIEN\_SELFVIEW **TO** CSYT\_ROLE\_NHANVIEN; |

#### OLS

Cấp độ (level) được chia làm 3:

* Giám đốc sở
* Giám đốc cơ sở
* Y bác sĩ

Câu lệnh khởi tạo 3 cấp độ:

|  |
| --- |
| **EXEC** SA\_COMPONENTS.CREATE\_LEVEL('ACCESS\_THONGBAO',150,'GDS','GIAM\_DOC\_SO');  **EXEC** SA\_COMPONENTS.CREATE\_LEVEL('ACCESS\_THONGBAO',100,'GDCS','GIAM\_DOC\_CSYT');  **EXEC** SA\_COMPONENTS.CREATE\_LEVEL('ACCESS\_THONGBAO',50,'YBS','Y\_BSI'); |

3 tuyến tương đương với 3 compartment:

* Chuyên sâu
* Nội trú
* Ngoại trú

Câu lệnh khởi tạo 3 compartment:

|  |
| --- |
| **EXEC** SA\_COMPONENTS.CREATE\_COMPARTMENT('ACCESS\_THONGBAO',80,'CS','CHUYEN\_SAU');  **EXEC** SA\_COMPONENTS.CREATE\_COMPARTMENT('ACCESS\_THONGBAO',70,'NT','NOI\_TRU');  **EXEC** SA\_COMPONENTS.CREATE\_COMPARTMENT('ACCESS\_THONGBAO',60,'NGT','NGOAI\_TRU'); |

Vị trí địa lý tương đương gồm 3 khu vực với 3 group:

* Trung tâm
* Cận trung tâm
* Ngoại thành

Câu lệnh khởi tạo 3 compartment:

|  |
| --- |
| **EXEC** SA\_COMPONENTS.CREATE\_GROUP('ACCESS\_THONGBAO',120,'TT','TRUNG\_TAM');  **EXEC** SA\_COMPONENTS.CREATE\_GROUP('ACCESS\_THONGBAO',200,'CTT','CAN\_TRUNG\_TAM','TT');  **EXEC** SA\_COMPONENTS.CREATE\_GROUP('ACCESS\_THONGBAO',300,'NTH','NGOAI\_THANH','TT'); |

Nhãn của 3 người dùng:

* Giám đốc sở: có toàn quyền coi thông báo
* Giám đốc cơ sở chuyên sâu và nội trú ở ngoại thành: có quyền coi các thông báo từ có nội dung "cơ sở y tế" đổ xuống
* Các y bác sĩ ở cấp chuyên sâu và trung tâm: có thể coi các thông báo có nội dung "y bác sĩ" và có địa điểm là trung tâm

#### Data Encryption – Mã hóa dữ liệu

Vì các thông tin cá nhân là các thông tin nhạy cảm và không được phép cho người khác truy cập nên nhóm đã tiến hành 2 chính sách mã hóa:

* Chính sách 1: Bệnh nhân
* Mã hóa các trường: CMND, số nhà, tên đường, quận huyện và tỉnh thành.
* Key → mã bệnh nhân + mã cơ sở
* Chính sách 2: Nhân viên
* Mã hóa các trường: CMND và quê quán.
* Key → mã nhân viên + mã cơ sở

Dữ liệu mã hóa và giải mã được xử lý ở cấp DBMS. Sử dụng trigger được lưu trữ để triển khai:

* CSYT\_ADMIN.ENCRYPT\_I\_BN
* CSYT\_ADMIN.ENCRYPT\_U\_BN
* CSYT\_ADMIN.ENCRYPT\_I\_NV
* CSYT\_ADMIN.ENCRYPT\_U\_NV

Hàm mã hóa dữ liệu:

|  |
| --- |
| **CREATE OR REPLACE FUNCTION** CSYT\_ADMIN.**ENCRYPT**(pi\_input **VARCHAR2**,pi\_key **VARCHAR2**)  **RETURN RAW**  **AS**  input\_string **VARCHAR2**(16) := pi\_input;  raw\_input **RAW**(128) := utl\_raw.cast\_to\_raw(**CONVERT**(input\_string,'AL32UTF8','US7ASCII'));  key\_string **VARCHAR2**(100) := pi\_key;  raw\_key **RAW**(128) :=utl\_raw.cast\_to\_raw(**CONVERT**(key\_string,'AL32UTF8','US7ASCII'));  encrypted\_raw **RAW**(2048);  encrypted\_string **VARCHAR2**(2048);  **BEGIN**  dbms\_output.put\_line('key:'||raw\_key);  encrypted\_raw := dbms\_crypto.**ENCRYPT**(src => raw\_input, typ => dbms\_crypto.des\_cbc\_pkcs5,  **KEY** => raw\_key);  **RETURN** encrypted\_raw;  **END**;  / |

Hàm giải mã dữ liệu:

|  |
| --- |
| **CREATE OR REPLACE FUNCTION** csyt\_admin.**DECRYPT**(pi\_input **RAW**,pi\_key **VARCHAR2**)  **RETURN VARCHAR2**  **AS**  key\_string **VARCHAR2**(100) := pi\_key;  raw\_key **RAW**(128) :=utl\_raw.cast\_to\_raw(**CONVERT**(key\_string,'AL32UTF8','US7ASCII'));  decrypted\_raw **RAW**(2048);  decrypted\_string **VARCHAR2**(2048);  **BEGIN**  dbms\_output.put\_line('key:'||raw\_key);  **BEGIN**  decrypted\_raw := dbms\_crypto.**DECRYPT**(src => pi\_input, typ => dbms\_crypto.des\_cbc\_pkcs5,  **KEY** => raw\_key);  decrypted\_string:=**CONVERT**(utl\_raw.cast\_to\_varchar2(decrypted\_raw),'US7ASCII','AL32UTF8');  **RETURN** decrypted\_string;  **EXCEPTION**  **WHEN OTHERS THEN**  **RETURN NULL**;  **END**;  **END**;  / |

Graphical user interface, application

Description automatically generated

Graphical user interface, application

Description automatically generated

Database Encryption Levels: Attribute value (cấp độ giá trị thuộc tính)

**Ưu điểm:**

* Có thể chọn dữ liệu để bảo vệ ở các đơn vị dữ liệu khác nhau (bảng, hàng, cột, giá trị, tất cả cơ sở dữ liệu,…).
* Dễ dàng chia sẻ dữ liệu được mã hóa giữa các ứng dụng khác nhau.

**Hạn chế:**

* Khi thay đổi kiểu dữ liệu hoặc kích thước dữ liệu của các thuộc tính được mã hóa sẽ phải thay đổi trigger được lưu trữ cùng một lúc.
* Làm chậm hệ thống cơ sở dữ liệu đáng kể do tốn thời gian cho mã hóa và giải mã dữ liệu.
* Không thể ngăn chặn tấn công ở cấp ứng dụng.

Sử dụng des\_cbc\_pkcs5

DES-Data Encryption Standard.

Block cipher. Sử dụng khóa có độ dài 56 bits

Cipher Block Chaining.

Khối Plaintext kế tiếp được XOR với khối

ciphertext trước đó trước khi nó được mã hóa. Vector khởi tạo (IV) được xem như khối plaintext đầu tiên.

PAD\_PKCS5 Cung cấp cơ chế đệm thêm tuân theo chuẩn PKCS #5: Password-Based Cryptography Standard: thêm vào n số, chỉ n byte còn thiếu của khối cuối cùng. Nếu khối cuối cùng đủ, vẫn đệm thêm toàn bộ khối.

Phương pháp quản lý khóa: sử dụng khóa suy diễn

#### Standard Audit

Vì các thông tin cá nhân là các thông tin nhạy cảm nên nhóm đã tạo 2 chính sách audit:

* Giám sát các trường hợp cố gắng xem thông tin của bệnh nhân một cách bất hợp pháp.
* Giám sát các trường hợp cố gắng xem thông tin của nhân viên một cách bất hợp pháp.

|  |
| --- |
| **ALTER SYSTEM SET** audit\_sys\_operations=**TRUE** **SCOPE**=**SPFILE**;  --Ghi lai cac hanh vi xem thong tin benh nhan/nhan vien bat hop phap  **AUDIT** **SELECT** **on** CSYT\_ADMIN.BenhNhan **BY ACCESS WHENEVER NOT SUCCESSFUL**;  **AUDIT** **SELECT** **on** CSYT\_ADMIN.NhanVien **BY ACCESS WHENEVER NOT SUCCESSFUL**; |

#### Fine-Grained Audit

Tương tự với Standard Audit. Tuy nhiên, ở đây nhóm chúng em có thêm điều kiện là người thay đổi dữ liệu không phải là bản thân người dùng:

* Chính sách 1: Thông tin bị thay đổi không phải do chính bệnh nhân chỉnh sửa

### Chính sách 2: Thông tin bị thay đổi không phải do chính nhân viên chỉnh sửa



|  |
| --- |
| --Chính sách 1:  **create or replace procedure** CSYT\_ADMIN.InvalidAccessAudit(cur **out SYS\_REFCURSOR**)  **as**  **begin**  **OPEN** cur **FOR**  **select distinct** USERID,obj$name **AS** tbl,**TO\_char**(Ntimestamp#,'dd-mon-yyyy hh:mi:ss') **AS** TIME  **from sys**.aud$ **where** obj$creator='CSYT\_ADMIN';  --DBMS\_SQL.return\_result(cur);  **end**;  /  --Chính sách 2:  **create or replace procedure** CSYT\_ADMIN.IllegalAccessAudit(cur **out SYS\_REFCURSOR**)  **as**  **begin**  **OPEN** cur **FOR**  **select distinct** DB\_USER,OBJECT\_NAME **AS** tbl,**TO\_char**(timestamp,'dd-mon-yyyy hh:mi:ss') **AS** TIME,  SQL\_TEXT as ViecLam  **from sys**.DBA\_FGA\_AUDIT\_TRAIL **where** OBJECT\_SCHEMA='CSYT\_ADMIN';  --DBMS\_SQL.return\_result(cur);  **end**; |

### Các chức năng của ứng dụng

#### Phân hệ 1

Danh sách chức năng đã thực hiện:

* Xem danh sách người dùng trong hệ thống.
* Thông tin về quyền (privileges) của mỗi user/ role trên các đối tượng dữ liệu.
* Cho phép tạo mới, xóa, Sửa (hiệu chỉnh) user hoặc role.
* Cho phép thực hiện việc cấp quyền: cấp quyền cho user, cấp quyền cho role, cấp role cho user. Quá trình cấp quyền có tùy chọn là có cho phép người được cấp quyền có thể cấp quyền đó cho user/ role khác hay không (có chỉ định WITH GRANT OPTION hay không). Quyền, select, update thì cho phép phân quyền tinh đến mức cột; quyền insert, delete thì không.
* Cho phép thu hồi quyền từ người dùng/ role.
* Cho phép kiểm tra quyền của các chủ thể vừa được cấp quyền.
* Cho phép chỉnh sửa quyền của user/ role.

#### Phân hệ 2

Danh sách chức năng đã thực hiện:

### Giao diện ứng dụng

Có cần để giao diện theo tiêu chí ko?

##### Giao diện đăng nhập

Graphical user interface, text, application

Description automatically generated

Bước 1: Nhập Username và Password với tài khoản admin có username là “admin” và password là “a”.

Bước 2: Nhấn Login để đăng nhập. Nếu đúng tài khoản ứng dụng sẽ hiển thị giao diện chính. Nếu sai ứng dụng sẽ xuất hiện thông báo. Nhấn ESC để thoát ứng dụng.

##### Giao diện chính của ứng dụng

Graphical user interface, text, application, email

Description automatically generated

Đây là giao diện chính của chương trình sau khi đăng nhập thành công.

Chương trình gồm các mục chính:

* User: Gồm các thao tác xem danh sách User, tạo User mới, xóa User, chỉnh sửa User và xem quyền của User.
* Role: Gồm các thao tác xem danh sách Role, tạo Role mới, xóa Role, chỉnh sửa Role và xem quyền của Role.
* Cấp quyền: Thực hiện thao tác cấp quyền cho một User hoặc một Role .
* Đăng xuất: Đăng xuất khỏi ứng dụng

##### Giao diện User

Tại giao diện User, quản trị viên có thể xem danh sách các User trên hệ thống và thêm User mới (Nhân viên, Bệnh nhân).

Graphical user interface, text

Description automatically generated

Giao diện thêm Nhân viên mới:

Graphical user interface, application, Word

Description automatically generated

Giao diện thêm Bệnh nhân mới:

Graphical user interface, application

Description automatically generated

##### Giao diện Role

Tại giao diện Role, quản trị viên có thể xem danh sách các Role trên hệ thống và thêm Role mới.

Graphical user interface, text, application, email

Description automatically generated

Giao diện thêm Role mới:

Graphical user interface, text, application, chat or text message

Description automatically generated

##### Giao diện cấp quyền

Tại giao diện cấp quyền, quản trị viên có thể xem và xóa quyền của một User hoặc một Role.

Table

Description automatically generated

Giao diện xem quyền của một chủ thể cụ thể:

Table

Description automatically generated

# TÀI LIỆU THAM KHẢO

**[1] Slide bài giảng**

**[2] docs.oracle.com**

**[3] tranvanbinh.vn**

**[4] stackoverflow.com**

**[5] dba-oracle.com**

**[6] community.oracle.com**

|  |
| --- |
| Do cùng một trang web tham khảo nhiều bài viết dựa vào từ khóa nên không thể để đường dẫn cụ thể đến bài viết. |