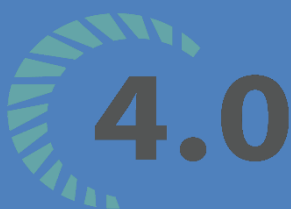


BỘ MÔN HỆ THỐNG THÔNG TIN – KHOA CÔNG NGHỆ THÔNG TIN
ĐẠI HỌC KHOA HỌC TỰ NHIÊN THÀNH PHỐ HỒ CHÍ MINH, ĐẠI HỌC QUỐC
GIÁ TP HCM

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



Nhóm thực hiện: ATBMCQ-20

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

HỌC KỲ II – NĂM HỌC 2021-2022



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 Lâm	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 phân hệ 1

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 Lâm	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

Bảng phân công & đánh giá hoàn thành công việc phân hệ 2

Công việc thực hiện	Người thực hiện	Mức độ hoàn thành	Đánh giá của nhóm
TC#4, TC#7 + OLS + Giao diện	19120677- Nguyễn Diệp Minh Tiến	70%	7/10
TC#3, TC#1, TC#6 + Audit + Giao diện	19120559 - Hà Duy Lâm	70%	7/10
TC#5, TC#2 + Mã hóa + Giao diện	19120661 - Lê Mai Nguyên Thảo	70%	7/10
Vẽ ERD, Tạo CSDL, Tạo dữ liệu mẫu, tạo báo cáo	19120545 - Lê Ngọc Khoa	80%	8/10

THÔNG TIN ĐỒ ÁN - BÀI TẬP

Đồ án – Bài tập	AN TOÀN VÀ BẢO MẬT DỮ LIỆU TRONG HTTT PHẦN HỆ 1
Loại bài tập	Đồ án - Nhóm



MỤC LỤC

I. MÔ TẢ ĐỒ ÁN	3
II. BÁO CÁO ĐỒ ÁN	3
PHÂN HỆ 1: HỆ THỐNG DÀNH CHO NGƯỜI QUẢN TRỊ VIÊN:	3
1. Xem danh sách các đối tượng hiện có trên CSDL.....	3
2. Thêm mới đối tượng	4
3. Phân quyền/ lấy lại quyền của một user/ role.	5
4. Xem quyền của một chủ thể cụ thể.	6
5. Giao diện ứng dụng:.....	8
6. Video demo:	13
PHÂN HỆ 2: HIỆN THỰC CÁC CHÍNH SÁCH BẢO MẬT	13
1. Thiết kế cơ sở dữ liệu:.....	13
2. Các chính sách bảo mật:	17
2.1 Chính sách DAC (<i>Direct access control</i>):	17
2.2 Chính sách RBAC(<i>Role-based access control</i>):	17
2.3 Chính sách VPD (<i>Virtual Private Database</i>):.....	18
2.4 Chính sách OLS(<i>Oracle label security</i>):.....	18
2.5 Chính sách mã hóa (Encrypt).....	20
2.6 Chính sách Audit:.....	21

I. 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.

II. 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:



USERNAME
37 KHOA
38 C##LEKHQA3
39 C##LEKHQA4
40 AUDSYS
41 DIP
42 C##THUTHU5
43 C##QUANLI1
44 C##THUTHU2
45 SYSRM

- Danh sách role:



ROLE
1 CONNECT
2 RESOURCE
3 DBA
4 FDB_DBA
5 AUDIT_ADMIN
6 AUDIT_VIEWER
7 SELECT_CATALOG_ROLE
8 EXECUTE_CATALOG_ROLE
9 CAPTURE_ADMIN
10 EXP_FULL_DATABASE
11 IMP_FULL_DATABASE
12 CDB_DBA

- Danh sách table



select table_name from all_tables
Script Output x Query Result x
SQL Fetched 300 rows in 0.161 seconds
TABLE_NAME
19 FET\$
20 SEG\$
21 UET\$
22 USER\$
23 TSQ\$
24 UNDO\$
25 FILE\$
26 OBJ\$
27 PROXY_DATA\$
28 PROXY_ROLE_DATA\$
29 CON\$
30 CDEF\$

2. Thêm mới đối tượng

- Tạo mới user

```
----- Tao moi user
create or replace procedure Grant_NewUser(User_name in nvarchar2,Pass_Word in nvarchar2)
authid current_user
as
    Tmp_count int;
Begin
    select count(*) into Tmp_count from all_users where username = User_name;
    If(Tmp_count != 0) then
        RAISE_APPLICATION_ERROR(-20000,'User da ton tai');
    ELSE
        execute immediate('Create user '|| User_name||' identified by '||Pass_Word);
        execute immediate('grant create session to '||User_name);
    END IF;
End;
```

- Tạo mới role

```
-----Tao role moi
create or replace procedure Grant_NewRole(Role_name in varchar2,Pass_Word in varchar2)
authid current_user
as
    Tmp_query varchar(100);
Begin
    IF(Pass_Word = ' ') THEN
        Tmp_query := 'Create role '|| Role_name;
    END IF;
    Tmp_query := 'Create role '|| Role_name||' identified by '||Pass_Word;
    execute IMMEDIATE (Tmp_query);
    exception
    when others then
        RAISE_APPLICATION_ERROR(-20000,'Role da ton tai');
End;
```

- Chỉnh sửa Role

```
-----Chinh sua role
create or replace procedure Alter_Role(Role_name in varchar2,Pass_Word in varchar2)
authid current_user
is
    Tmp_count int;
    Tmp_query varchar2(100);
begin
    if(Pass_Word=' ') then
        Tmp_query :='ALTER ROLE '|| Role_Name|| ' Not IDENTIFIED';
        execute immediate(Tmp_query);
    elsif(pass_word!=' ') then
        Tmp_query :='ALTER ROLE '|| Role_Name|| ' IDENTIFIED BY' || Pass_Word;
    end if;
end;
```

- Chỉnh sửa password user



```
-----Chỉnh sửa password user
create or replace procedure Alter_User(User_name in varchar2,Pass_Word in varchar2)
authid current_user
is
Tmp_count int;
Begin
select count(*) into Tmp_count from all_users where username = User_name;
If(Tmp_count != 0) then
    execute immediate('alter user '|| User_name||' identified by '||Pass_Word);
ELSE
    RAISE_APPLICATION_ERROR(-20000,'User không tồn tại');
END IF;
END;
```

- Xóa role:

```
-----Xóa role
create or replace procedure Drop_Role(Role_name in varchar2)
authid current_user
as
    Tmp_query varchar(100);
Begin
    Tmp_query := 'Drop role '|| Role_name;
    execute IMMEDIATE (Tmp_query);
exception
    when others then
        RAISE_APPLICATION_ERROR(-20000,'Role không tồn tại');
End;
```

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

- Phân quyền cho user :

```
--Cap quyền cho user
create or replace procedure Grant_Privs_toUser(User_Name in varchar2, Privs_name in varchar2,Table_Name in varchar2,grant_option in Varchar2 )
authid current_user
is
Tmp_count int;
Tmp_Query varchar2(100);
begin
select count(*) into Tmp_count from all_users where username=User_name;
if(Tmp_count!=0) then
    if(grant_option='NO') then
        Tmp_Query:='Grant '||Privs_name|| ' on ' ||Table_Name ||' to ' ||User_Name;
        execute immediate (Tmp_query);

        elsif(grant_option='YES') then
            Tmp_Query:='Grant '||Privs_name|| ' on ' ||Table_Name ||' to ' ||User_Name||' With grant option' ;
            end if;
        execute immediate (Tmp_query);
    else
        RAISE_APPLICATION_ERROR(-20000,'User chưa tồn tại');
    end if;
end;
```

- Thu hồi quyền user:



```
--Thu hoi quyen cho user
create or replace procedure Revoke_Object_Privs_User(User_Name in varchar2, priv in varchar2, a_object in varchar2)
authid current_user is
Tmp_query varchar(100);
Tmp_count int;
exception_username exception;
Begin

select count(*) into Tmp_count from all_users where UserName=User_Name;
if(Tmp_count != 0) then
Tmp_query:='REVOKE '||priv||' ON ' ||a_object||' FROM ' ||User_name;
execute IMMEDIATE (Tmp_query);
elsif(Tmp_count=0) then
raise exception_username;
end if;

Exception
when exception_username then
RAISE_APPLICATION_ERROR(-20000,'User chua ton tai');
WHEN OTHERS THEN
    IF SQLCODE != -942 THEN
        RAISE;
    END IF;
End;
```

- Phân quyền cho role:

```
-----Phân quyền cho Role
create or replace procedure Grant_Privs_toRole(Role_Name in varchar2, Privs_name in varchar2,Table_Name in varchar2)
authid current_user
is
Tmp_Query varchar2(100);
begin
    Tmp_Query := 'Grant '||Privs_name|| ' on ' ||Table_Name ||' to ' ||Role_Name;
    execute immediate (Tmp_Query);
end;
```

- Thu hồi quyền role:

```
-----Thu hồi quyền của Role
create or replace procedure Revoke_Privs_toRole(Role_Name in varchar2, Privs_name in varchar2,Table_Name in varchar2)
authid current_user
is
Tmp_Query varchar2(100);
begin
    Tmp_Query := 'Revoke '||Privs_name|| ' on ' ||Table_Name ||' from ' ||Role_Name;
    execute immediate (Tmp_Query);
end;
```

4. Xem quyền của một chủ thể cụ thể.

- Xem quyền của user:



-- XEM QUYỀN USER

```
select A.*
from (select grantee username,
             granted_role privilege,
             '--' owner,
             '--' table_name,
             '--' column_name,
             admin_option admin_option,
             'ROLE' access_type
       from dba_role_privs RP
       join dba_roles R on RP.granted_role = R.role
       where grantee in (select username from dba_users)
      union
      select grantee username,
             privilege privilege,
             '--' owner,
             '--' table_name,
             '--' column_name,
             admin_option admin_option,
             'SYSTEM' access_type
       from dba_sys_privs
       where grantee in (select username from dba_users)
      union
      select grantee username,
             privilege privilege,
             owner owner,
             table_name table_name,
             '--' column_name,
             grantable admin_option,
             'TABLE' access_type
       from dba_tab_privs
       where grantee in (select username from dba_users)
      union
```

```
select DP.grantee username,
       privilege privilege,
       owner owner,
       table_name table_name,
       column_name column_name,
       '--' admin_option,
       'ROLE' access_type
from role_tab_privs RP, dba_role_privs DP
where RP.role = DP.granted_role and DP.grantee in (select username from dba_users)
union
select grantee username,
       privilege privilege,
       grantable admin_option,
       owner owner,
       table_name table_name,
       column_name column_name,
       'COLUMN' access_type
from dba_col_privs
where grantee in (select username from dba_users)) A
order by username, A.table_name, case
    when A.access_type = 'SYSTEM' then 1
    when A.access_type = 'TABLE' then 2
    when A.access_type = 'COLUMN' then 3
    when A.access_type = 'ROLE' then 4
end,
case
    when A.privilege in ('EXECUTE') then 1
    when A.privilege in ('SELECT', 'INSERT', 'DELETE') then 3
    else 2
end,
A.column_name, A.privilege;
```

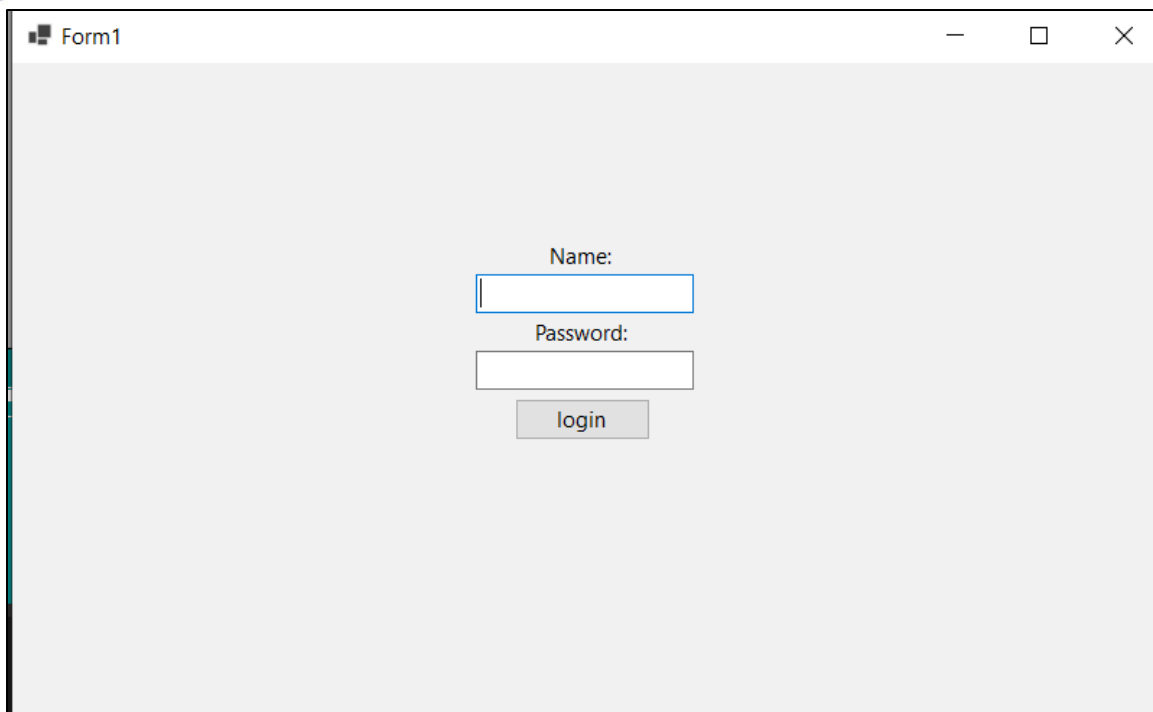
- Xem quyền của role



<pre>-- XEM QUYỀN ROLE select A.* from (select grantee role, granted_role privilege, '---' owner, '---' table_name, '---' column_name, admin_option admin_option, 'ROLE' access_type from dba_role_privs RP join dba_roles R on RP.granted_role = R.role where grantee in (select role from dba_roles) union select grantee role, privilege privilege, '---' owner, '---' table_name, '---' column_name, admin_option admin_option, 'SYSTEM' access_type from dba_sys_privs where grantee in (select role from dba_roles) union select grantee role, privilege privilege, owner owner, table_name table_name, '---' column_name, granttable admin_option, 'TABLE' access_type from dba_tab_privs where grantee in (select role from dba_roles) union select DP.grantee role,</pre>	
<pre> privilege privilege, owner owner, table_name table_name, column_name column_name, '---' admin_option, 'ROLE' access_type from role_tab_privs RP, dba_role_privs DP where RP.role = DP.granted_role and DP.grantee in (select role from dba_roles) union select grantee role, privilege privilege, granttable admin_option, owner owner, table_name table_name, column_name column_name, 'COLUMN' access_type from dba_col_privs where grantee in (select role from dba_roles)) A order by role, A.table_name, case when A.access_type = 'SYSTEM' then 1 when A.access_type = 'TABLE' then 2 when A.access_type = 'COLUMN' then 3 when A.access_type = 'ROLE' then 4 end, case when A.privilege in ('EXECUTE') then 1 when A.privilege in ('SELECT', 'INSERT', 'DELETE') then 3 else 2 end, A.column_name, A.privilege;</pre>	

5. Giao diện ứng dụng:

- Giao diện login:



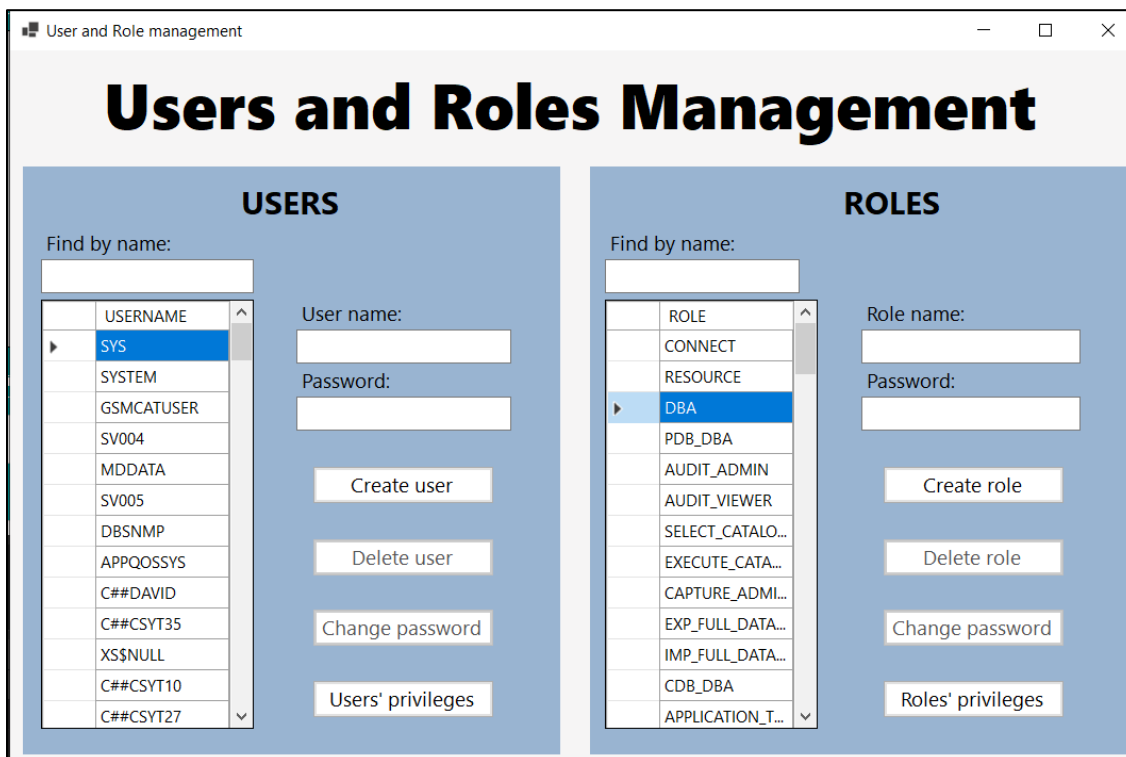
Form1

Name:

Password:

login

- Giao diện thêm, xóa, sửa user:



User and Role management

Users and Roles Management

USERS

Find by name:

USERNAME
SYS
SYSTEM
GSMCATUSER
SV004
MDDATA
SV005
DBSNMP
APPQOSSYS
C##DAVID
C##CSYT35
X\$NULL
C##CSYT10
C##CSYT27

User name:

Password:

Create user

Delete user

Change password

Users' privileges

ROLES

Find by name:

ROLE
CONNECT
RESOURCE
DBA
PDB_DBA
AUDIT_ADMIN
AUDIT_VIEWER
SELECT_CATALO...
EXECUTE_CATA...
CAPTURE_ADML...
EXP_FULL_DATA...
IMP_FULL_DATA...
CDB_DBA
APPLICATION_T...

Role name:

Password:

Create role

Delete role

Change password

Roles' privileges

- Giao diện xem quyền của tất cả user:



Form1

List privileges of user

	GRANTEE	OWNER	TABLE_NAME	GRANTOR	PRIVILEGE	GRANTABLE	HIERARCHY
▶	SYSTEM	SYS	ORASBASE	SYS	USE	YES	NO
	PUBLIC	SYS	DUAL	SYS	SELECT	YES	NO
	PUBLIC	SYS	SYSTEM_PRIVI...	SYS	READ	NO	NO
	PUBLIC	SYS	TABLE_PRIVILE...	SYS	READ	NO	NO
	PUBLIC	SYS	USER_PRIVILE...	SYS	READ	NO	NO
	PUBLIC	SYS	STMT_AUDIT_O...	SYS	READ	NO	NO
	PUBLIC	SYS	FINALHIST\$	SYS	INSERT	NO	NO
	PUBLIC	SYS	DM\$EXPIMP_ID...	SYS	SELECT	NO	NO

Search

Load

Grant Priviledges

User:
Table:
Priviledges:
Grant option:

Revoke Priviledges

User:
Table:
Priviledges:

- Giao diện tìm xem quyền của 1 user:

Form1

List privileges of user

	GRANTEE	OWNER	TABLE_NAME	GRANTOR	PRIVILEGE	GRANTABLE	HIERARCHY
▶	C##LEKHOA1	SYSTEM	SACH	SYSTEM	DELETE	NO	NO
	C##LEKHOA1	SYSTEM	SACH	SYSTEM	SELECT	YES	NO
	C##LEKHOA1	SYSTEM	DOCGIA	SYSTEM	SELECT	YES	NO
	C##LEKHOA1	SYSTEM	SACH	SYSTEM	SELECT	YES	NO
*							

Search

Load

Grant Priviledges

User:
Table:
Priviledges:
Grant option:

Revoke Priviledges

User:
Table:
Priviledges:

- Giao diện thêm quyền cho user:



Form1

List privileges of user

	GRANTEE	OWNER	TABLE_NAME	GRANTOR	PRIVILEGE	GRANTABLE	HIERARCHY
▶	C##LEKHOA1	SYSTEM	SACH	SYSTEM	DELETE	NO	NO
	C##LEKHOA1	SYSTEM	THUVIEN	SYSTEM	DELETE	NO	NO
	C##LEKHOA1	SYSTEM	SACH	SYSTEM	SELECT	YES	NO
	C##LEKHOA1	SYSTEM	DOCGIA	SYSTEM	SELECT	YES	NO
	C##LEKHOA1	SYSTEM	SACH	SYSTEM	SELECT	YES	NO
*							

Search

Load

Grant Privileges

User:
Table:
Privileges:
Grant option:

Revoke Privileges

User:
Table:
Privileges:

- Giao diện thu quyền user:

Form1

List privileges of user

	GRANTEE	OWNER	TABLE_NAME	GRANTOR	PRIVILEGE	GRANTABLE	HIERARCHY
▶	C##LEKHOA1	SYSTEM	SACH	SYSTEM	DELETE	NO	NO
	C##LEKHOA1	SYSTEM	SACH	SYSTEM	SELECT	YES	NO
	C##LEKHOA1	SYSTEM	DOCGIA	SYSTEM	SELECT	YES	NO
	C##LEKHOA1	SYSTEM	SACH	SYSTEM	SELECT	YES	NO
*							

Search

Load

Grant Privileges

User:
Table:
Privileges:
Grant option:

Revoke Privileges

User:
Table:
Privileges:



- Giao diện xem quyền của tất cả role

Admin

QuyềnCuaRole

ROLE	OWNER	TABLE_NAME	COLUMN_NAME	PRIVILEGE
C##BENHNHAN	SYSTEM	BENHNHAN	SONHA	INSERT
AQ_ADMINISTR...	WMSYS	AQ\$WMSEVENT...		SELECT
SELECT_CATAL...	SYS	KU\$_XMLSCHE...		SELECT
C##BENHNHAN	SYSTEM	BENHNHAN	QUANHUYEN	INSERT
SELECT_CATAL...	SYS	KU\$_TABLE_XM...		SELECT
C##BENHNHAN	SYSTEM	BENHNHAN	DIUNGTHUOC	INSERT

Role

ROLE	ROLE_ID	PASSWORD
CONNECT	2	NO
RESOURCE	3	NO
DBA	4	NO
PDB_DBA	5	NO
AUDIT_ADMIN	6	NO
AUDIT_VIEWER	7	NO

Button

Grant

Role name

Privilege name

Table name

Revoke

Search

Role name

Load

- Giao diện tìm xem quyền của 1 role

Admin

QuyềnCuaRole

ROLE	OWNER	TABLE_NAME	COLUMN_NAME	PRIVILEGE
C##BENHNHAN	SYSTEM	BENHNHAN	SONHA	INSERT
C##BENHNHAN	SYSTEM	BENHNHAN	QUANHUYEN	INSERT
C##BENHNHAN	SYSTEM	BENHNHAN	NGAYSINH	INSERT
C##BENHNHAN	SYSTEM	BENHNHAN	TINHTP	INSERT
C##BENHNHAN	SYSTEM	BENHNHAN	TIENSUBENH	INSERT
C##BENHNHAN	SYSTEM	BENHNHAN	TIENSUBENHGD	INSERT

Role

ROLE	ROLE_ID	PASSWORD_RE
C##BENHNHAN	243	NO

Button

Grant

Role name

Privilege name

Table name

Revoke

Search

Role name

Load

- Giao diện cấp/thu quyền cho role:

Admin

QuyềnCuaRole

ROLE	OWNER	TABLE_NAME	COLUMN_NAME	PRIVILEGE
C##BENHNHAN	SYSTEM	BENHNHAN	SONHA	INSERT
C##BENHNHAN	SYSTEM	BENHNHAN	QUANHUYEN	INSERT
C##BENHNHAN	SYSTEM	BENHNHAN		SELECT
C##BENHNHAN	SYSTEM	BENHNHAN	NGAYSINH	INSERT
C##BENHNHAN	SYSTEM	BENHNHAN	TINHTP	INSERT
C##BENHNHAN	SYSTEM	BENHNHAN	TIENSUBENH	INSERT

Role

ROLE	ROLE_ID	PASSWORD_RE
C##BENHNHAN	243	NO

Button

Grant

Role name

Privilege name

Table name

Revoke

Search

Role name

Load

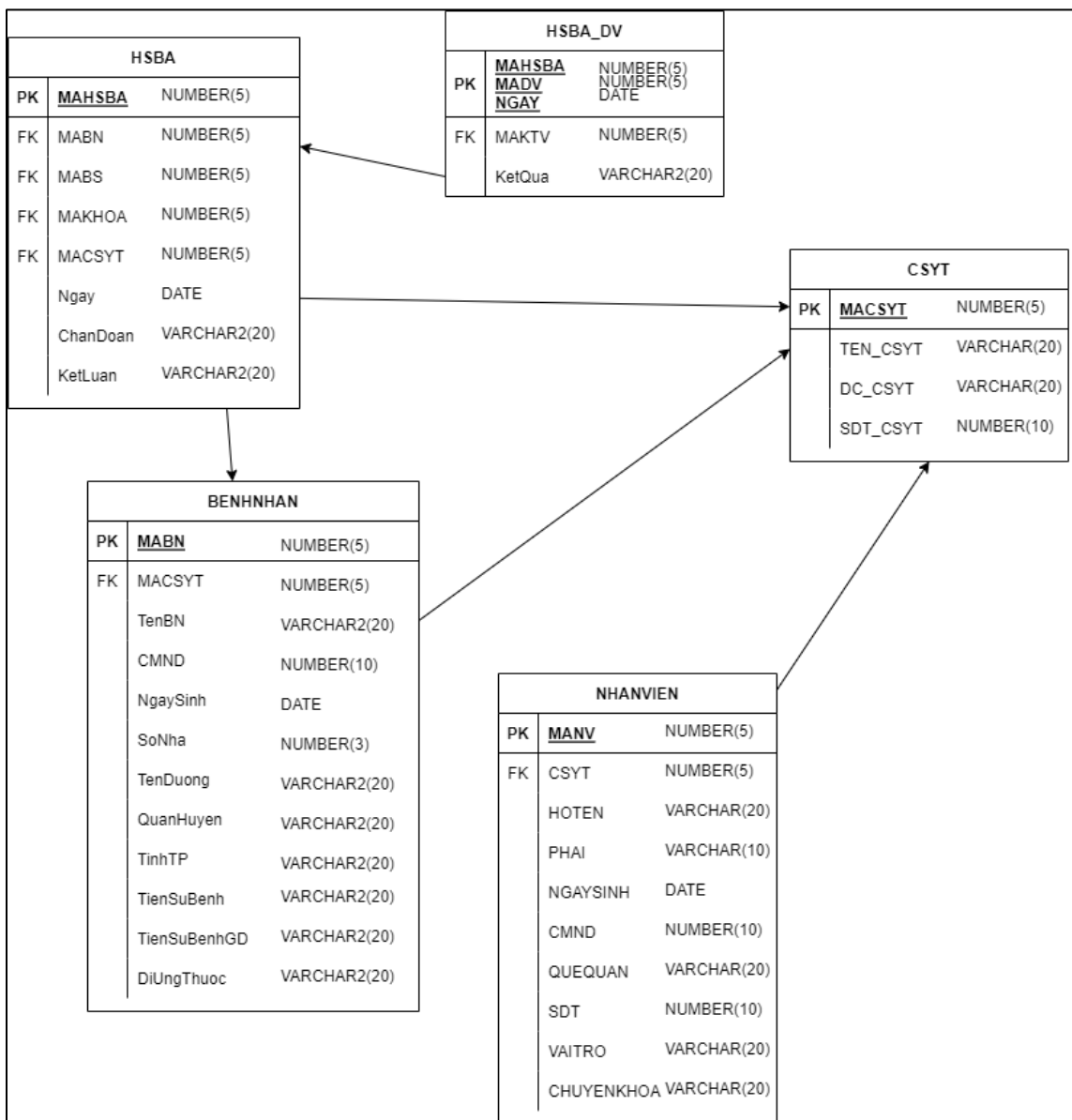
6. Video demo:

<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:

a) Mô hình:



b) 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
<u>MABN</u>	NUMBER (5)	Mã bệnh nhân tiếp nhận điều trị	Khóa ngoại
<u>MABS</u>	NUMBER (5)	Mã bác sĩ điều trị	Khóa ngoại
<u>MACSYT</u>	NUMBER (5)	Cơ sở y tế mà bệnh nhân điều trị	Khóa ngoại
<u>MAKHOA</u>	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
<u>MACSYT</u>	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 bệnh nhân	
SONHA	NUMBER (3)	Số nhà của bệnh nhân	
TENDUONG	VARCHAR (20)	Tên đường nơi bệnh nhân ở	
QUANHUYEN	VARCHAR (20)	Tên quận huyện nơi bệnh 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 bệnh của gia đình 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 tính 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	
<u>CSYT</u>	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	Khóa chính

		định CSYT	
MADV	NUMBER (5)	Tên CSYT	Khóa chính
NGAY	DATE	Ngày lập hồ sơ	Khóa chính
<u>MAKTV</u>	NUMBER (5)	Mã người thực hiện dịch vụ	Khóa ngoại
KETQUA	VARCHAR (20)	Kết quả dịch vụ	

2. Các chính sách bảo mật:

2.1 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)

2.2 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 BENHNNHAN
 - Ở #TC5:

- RL_NghienCuu được cấp quyền Select trên View để xem HSBA và HSBA_DV

2.3 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 BENHNNHAN.
 - 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.

2.4 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.

2.5 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 ký 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).

2.6 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 bệnh án của năm 2019.