ĐẠI HỌC QUỐC GIA THÀNH PHỐ HỒ CHÍ MINH

ĐẠI HỌC KHOA HỌC TỰ NHIÊN

**KHOA CÔNG NGHỆ THÔNG TIN**

AN TOÀN VÀ BẢO MẬT TRONG HỆ THỐNG THÔNG TIN

BÁO CÁO ĐỒ ÁN CUỐI KÌ

NHÓM 22

1412101 – Võ Minh Duy

1412689 – Hoàng Thị Bích Vân

# **Mục lục**

[**Mục lục** 2](#_Toc12663401)

[**1.** **Đánh giá đồ án:** 3](#_Toc12663402)

[**2.** **Thiết kế cơ sở dữ liệu:** 3](#_Toc12663403)

[**2.1.** **Mô hình quan hệ** 3](#_Toc12663404)

[**2.2.** **Lược đồ CSDL:** 4](#_Toc12663405)

[**2.3.** **Access Controls:** 4](#_Toc12663406)

[**2.3.1.** **DAC:** 4](#_Toc12663407)

[**2.3.2.** **VPD:** 7](#_Toc12663408)

[**2.3.3.** **OLS:** 11](#_Toc12663409)

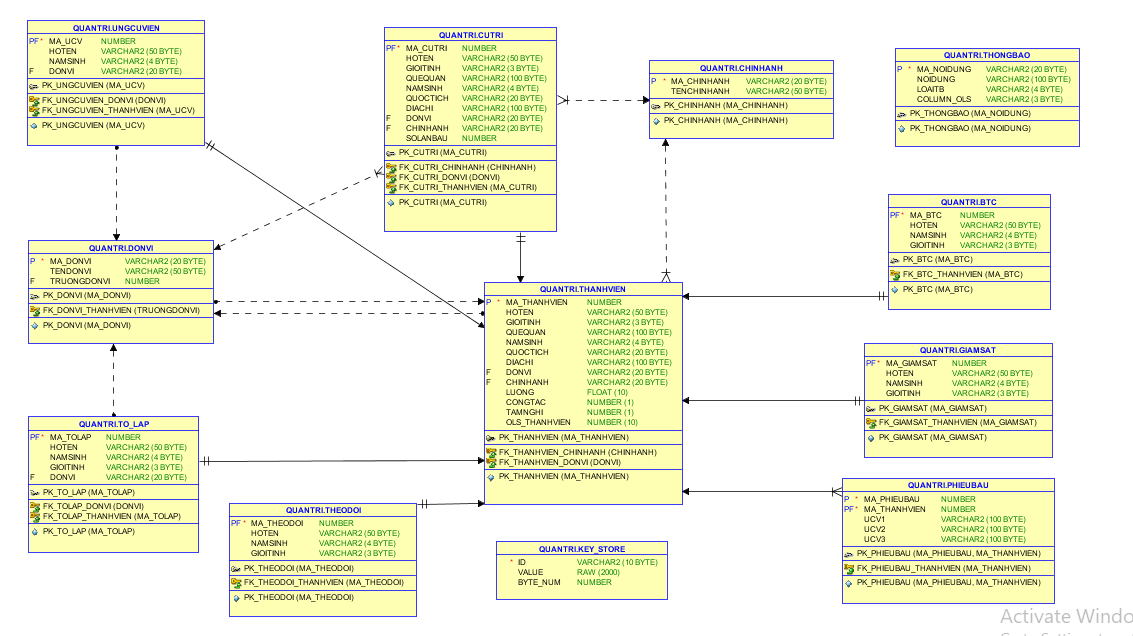
[**2.3.4.** **Mã hóa:** 14](#_Toc12663410)

[**2.4.** **Chức năng:** 20](#_Toc12663411)

[**3.** **Giao diện:** 21](#_Toc12663412)

1. **Đánh giá đồ án:**

|  |  |  |
| --- | --- | --- |
| **STT** | **Nội dung** | Đánh giá |
| **1** | **PHẦN 1: HỆ THỐNG DÀNH CHO NGƯỜI QUẢN TRỊ BẢO MẬT Yêu cầu: Xây dựng giao diện cho phép người quản trị** | |
| 1.1 | Xem danh sách các đối tượng hiện có trên CSDL (user, role, table, view, ….) |  |
| 1.2 | Thêm mới đối tượng (table, user, role, …) |  |
| 1.3 | Phân quyền/ lấy lại quyền của một user/ role. |  |
| 1.4 | Xem quyền của một chủ thể cụ thể. |  |
| **2** | **PHẦN 2: HIỆN THỰC CÁC CHÍNH SÁCH BẢO MẬT** | |
| 2.1 | Báo cáo: Lược đồ CSDL sẽ dùng, liệt kê chính sách bảo mật, phân tích và phân loại. Liệt kê đầy đủ nhưng chỉ cần phân tích và cài đặt **tối thiểu mỗi cơ chế 2 chính sách.** |  |
| 2.2 | DAC + RBAC |  |
| 2.3 | VPD |  |
| 2.4 | MAC (chỉ cần cài đặt 1 chính sách) |  |
| 2.5 | Mã hóa (chỉ cần cài đặt 1 chính sách) |  |
| 2.6 | Audit |  |
| 2.7 | Giao diện cho ứng dụng liên quan các chính sách được cài đặt bởi các cơ chế bảo mật trên. |  |

1. **Thiết kế cơ sở dữ liệu:**
   1. **Mô hình quan hệ**
   2. **Lược đồ CSDL:**
   3. **Access Controls:**
      1. **DAC:**

|  |  |  |  |
| --- | --- | --- | --- |
| STT | Role | Quyền | Cài đặt |
| 1 | Nhân viên | * Tạo kết nối vào CSDL * Truy vấn bảng THANHVIEN | ✔ |
| 2 | Ban tổ chức | * Truy vấn, thêm, cập nhật bảng UNGCUVIEN,GIAMSAT,TO\_LAP,THEDOI | ✔ |
| 3 | Tổ lập | * Truy vấn, thêm, xóa, cập nhật bảng CUTRI | ✔ |
| 4 | Giám sát | * Truy vấn tất cả các bảng trong CSDL | ✔ |
| 5 | Theo dõi kết quả | * Truy vấn bảng PHIEUBAU, CUTRI, UNGVIEN | ✔ |
| 6 | Cử tri | * Thêm, cập nhật bảng PHIEUBAU | ✔ |

* Source-code: /code/oracle\_script/access\_control.sql

/\*

Tạo role trong hệ thống

\*/

CREATE ROLE NHANVIEN;

CREATE ROLE BTC;

CREATE ROLE TOLAP;

CREATE ROLE THEODOIKQ;

CREATE ROLE GIAMSAT;

CREATE ROLE CUTRI;

/\*

Cấp quyền cho role NHANVIEN

\*/

GRANT CREATE SESSION TO NHANVIEN;

GRANT SELECT ON THANHVIEN TO NHANVIEN;

/\*

Cấp quyền cho role CUTRI

\*/

GRANT INSERT, UPDATE ON PHIEUBAU TO CUTRI;

/\*

Cấp quyền cho role BTC

\*/

GRANT SELECT, INSERT, UPDATE ON UNGCUVIEN TO BTC;

GRANT SELECT, INSERT, UPDATE ON GIAMSAT TO BTC;

GRANT SELECT, INSERT, UPDATE ON TO\_LAP TO BTC;

GRANT SELECT, INSERT, UPDATE ON THEODOI TO BTC;

/\*

Cấp quyền cho role TOLAP

\*/

GRANT SELECT, UPDATE, INSERT, DELETE on CUTRI TO TOLAP

/\*

Cấp quyền cho role THEODOIKQ

\*/

GRANT SELECT ON PHIEUBAU TO THEODOIKQ;

GRANT SELECT ON CUTRI TO THEODOIKQ;

GRANT SELECT ON UNGCUVIEN TO THEODOIKQ;

/\*

Cấp quyền cho role GIAMSAT

\*/

GRANT SELECT ON CHINHANH TO GIAMSAT;

GRANT SELECT ON DONVI TO GIAMSAT;

GRANT SELECT ON THANHVIEN TO GIAMSAT;

GRANT SELECT ON BTC TO GIAMSAT;

GRANT SELECT ON TO\_LAP TO GIAMSAT;

GRANT SELECT ON GIAMSAT TO GIAMSAT;

GRANT SELECT ON UNGCUVIEN TO GIAMSAT;

GRANT SELECT ON THEODOI TO GIAMSAT;

GRANT SELECT ON THONGBAO TO GIAMSAT;

GRANT SELECT ON PHIEUBAU TO GIAMSAT;

GRANT SELECT ON CUTRI TO GIAMSAT;

* + 1. **VPD:**

|  |  |  |  |
| --- | --- | --- | --- |
| STT | Tên chính sách | Mô tả | Cài đặt |
| 1 | Quản lý truy cập thành viên | Thành viên chỉ được truy vấn thông tin của bản thân | ✔ |
| 2 | Quản lý cập nhật phiếu bầu | Cử tri chỉ được phép cập nhật phiếu bầu của bản thân | ✔ |

* Source-code: /code/oracle\_script/access\_control.sql

/\*

Chính sách cho phép :

NHANVIEN : chỉ xem được thông tin của bản thân

\*/

create or replace FUNCTION f\_select\_thanhvien (

p\_schema VARCHAR2,

p\_obj VARCHAR2

)

Return VARCHAR2

AS

m\_user VARCHAR2(128);

m\_donvi VARCHAR2(20);

user\_role VARCHAR2(128);

stm VARCHAR2(100);

begin

select user into m\_user from dual;

create or replace FUNCTION f\_select\_thanhvien (

p\_schema VARCHAR2,

p\_obj VARCHAR2

)

Return VARCHAR2

AS

m\_user VARCHAR2(128);

m\_donvi VARCHAR2(20);

user\_role VARCHAR2(128);

stm VARCHAR2(100);

begin

select user into m\_user from dual;

--Kiểm tra là QUANTRI hoặc người dùng TOLAP

select granted\_role into user\_role from BINHBAU\_USER\_ROLES where grantee = to\_char(m\_user) AND granted\_role != 'NHANVIEN';

if user = 'QUANTRI' or user\_role = 'TOLAP' then

return '';

end if;

--Nếu là role khác

stm := 'MA\_THANHVIEN = ' || m\_user;

return stm;

end f\_select\_thanhvien; end f\_select\_thanhvien;

BEGIN

dbms\_rls.add\_policy (

object\_schema => 'QUANTRI',

object\_name => 'THANHVIEN',

policy\_name => 'Xem\_thanhvien\_donvi',

function\_schema => 'QUANTRI',

policy\_function => 'f\_select\_thanhvien\_donvi',

statement\_types => 'select'

);

END;

/\*

Chính sách cho phép :

CUTRI : update thông tin phiếu bầu của bản thân

\*/

create or replace FUNCTION f\_update\_cutri\_phieubau (

p\_schema VARCHAR2,

p\_obj VARCHAR2

)

Return VARCHAR2

AS

m\_user VARCHAR2(128);

stm VARCHAR2(100);

begin

select user into m\_user from dual;

stm := 'ma\_thanhvien = ' || to\_char(user);

return stm;

end f\_update\_cutri\_phieubau;

BEGIN

dbms\_rls.add\_policy (

object\_schema => 'QUANTRI',

object\_name => 'PHIEUBAU',

policy\_name => 'Capnhat\_phieubau',

function\_schema => 'QUANTRI',

policy\_function => 'f\_update\_cutri\_phieubau',

statement\_types => 'update'

);END;

* + 1. **OLS:**

|  |  |  |  |
| --- | --- | --- | --- |
| STT | Tên chính sách | Mô tả | Cài đặt |
| 1 | Thanhvien\_policy | Gán nhán cho bảng thành viên với các component:   * Level: NHANVIEN, TOLAP * Compartment: DONVI(N) * GROUP:CHINHANH(N)   Cho phép người dùng TOLAP truy vấn bảng THANHVIEN và lấy những người dùng thuộc cùng đơn vị | ✖ |

* Source-code: /code/oracle\_script/access\_control.sql

execute sa\_sysdba.drop\_policy('thanhvien\_policy');

execute sa\_sysdba.create\_policy( 'thanhvien\_policy', 'ols\_thanhvien' );

--Tạo thành phần policy

execute sa\_components.create\_level('thanhvien\_policy',10,'NV','NHAN VIEN');

execute sa\_components.create\_level('thanhvien\_policy',20,'TL','TO LAP');

execute sa\_components.create\_compartment('thanhvien\_policy',1,'DV1','DONVI 1');

execute sa\_components.create\_compartment('thanhvien\_policy',2,'DV2','DONVI 2');

execute sa\_components.create\_compartment('thanhvien\_policy',3,'DV3','DONVI 3');

execute sa\_components.create\_compartment('thanhvien\_policy',4,'DV4','DONVI 4');

execute sa\_components.create\_group('thanhvien\_policy',100,'CN1','CHI NHANH 1');

execute sa\_components.create\_group('thanhvien\_policy',200,'CN2','CHI NHANH 2');

--Function tự gán nhãn cho dữ liệu

create or replace function tao\_nhan\_OLS\_thanhvien (

p\_mtv in number,

p\_donvi in varchar2,

p\_chinhanh in varchar2

)

return lbacsys.lbac\_label as

v\_label varchar2(100);

m\_donvi varchar(20);

m\_chinhanh varchar(20);

begin

FOR u IN (select granted\_role from BINHBAU\_USER\_ROLES where grantee = TO\_CHAR(p\_mtv))

LOOP

if u.granted\_role = 'TOLAP' then

v\_label := v\_label || 'TL:';

else

v\_label := 'NV:';

end if;

END LOOP;

if p\_donvi = '1' then

v\_label := 'DV1:';

elsif p\_donvi = '2' then

v\_label := 'DV2:';

elsif p\_donvi = '3' then

v\_label := 'DV3:';

else

v\_label := 'DV4:';

end if;

if p\_chinhanh = '1' then

v\_label := v\_label || 'CN1';

else

v\_label := v\_label || 'CN2';

end if;

return TO\_LBAC\_DATA\_LABEL('thanhvien\_policy',v\_label);

end tao\_nhan\_OLS\_thanhvien;

BEGIN

sa\_policy\_admin.apply\_table\_policy (

policy\_name => 'thanhvien\_policy',

schema\_name => 'QUANTRI',

table\_name => 'THANHVIEN',

table\_options => ' READ\_CONTROL,WRITE\_CONTROL,CHECK\_CONTROL ',

label\_function => 'QUANTRI.tao\_nhan\_OLS\_thanhvien(:new.ma\_thanhvien,:new.donvi,:new\_chinhanh)',

predicate => NULL

);

END;

* + 1. **Mã hóa:**

|  |  |  |  |
| --- | --- | --- | --- |
| STT | Mô tả | Hoạt động | Cài đặt |
| 1 | Mã hóa thông tin ứng cử viên trên phiếu bầu.  Tổ theo dõi chỉ có thể xem thông tin ứng cử viên trên phiếu bầu nhưng không xem được ai bỏ phiếu đó. | 1. Trigger ALTER\_PHIEUBAU\_TRIGGER khi thêm 1 dòng vào bảng PHIEUBAU 2. Tổ theo dõi dùng lệnh:   select \* from table(query\_ungvien());  để xem giải mã. | ✔ |
| 2 | Mã hóa thông tin lương của thành viên. |  | ✖ |

* Source-code: /code/oracle\_script/mahoa.sql

--Trigger mã hóa thông tin UCV được thêm vào phiếu bầu

create or replace TRIGGER alter\_phieubau\_trigger

BEFORE UPDATE OR INSERT ON PHIEUBAU

FOR EACH ROW

declare

ciphertext RAW(2000);

current\_user VARCHAR(50);

m\_key RAW(32);

BEGIN

select KEY\_STORE.value

into m\_key

from KEY\_STORE

where ID = '1';

ciphertext := encrypt\_data\_AES128( in\_data => UTL\_I18N.STRING\_TO\_RAW(:new.UCV1,'AL32UTF8'),

in\_key => m\_key

);

:new.UCV1 := UTL\_RAW.CAST\_TO\_VARCHAR2(ciphertext);

ciphertext := encrypt\_data\_AES128( in\_data => UTL\_I18N.STRING\_TO\_RAW(:new.UCV2,'AL32UTF8'),

in\_key => m\_key

);

:new.UCV2 := UTL\_RAW.CAST\_TO\_VARCHAR2(ciphertext);

ciphertext := encrypt\_data\_AES128( in\_data => UTL\_I18N.STRING\_TO\_RAW(:new.UCV3,'AL32UTF8'),

in\_key => m\_key

);

:new.UCV3 := UTL\_RAW.CAST\_TO\_VARCHAR2(ciphertext);

END;

INSERT INTO PHIEUBAU

VALUES ('1','TDA01','Jacquenetta Jenoure','Annabel Dunlop','Gisele Grice');

SELECT \* FROM PHIEUBAU;

--Tạo function để lấy thông tin phiếu bầu

create or replace TYPE PHIEUBAU\_TYPE

AS OBJECT (

UCV1 VARCHAR2(100),

UCV2 VARCHAR2(100),

UCV3 VARCHAR2(100),

);

create or replace TYPE PHIEUBAU\_TABLE

AS TABLE OF PHIEUBAU\_TYPE;

CREATE OR REPLACE FUNCTION QUERY\_UNGVIEN

RETURN PHIEUBAU\_TABLE

PIPELINED

AS

plaintext VARCHAR2(100);

ciphertext RAW(2000);

m\_key RAW(32);

curr\_user VARCHAR2(128);

user\_role VARCHAR2(128);

BEGIN

curr\_user := SYS\_CONTEXT('userenv','SESSION\_USER');

select granted\_role into user\_role

from BINHBAU\_USER\_ROLES

where grantee = curr\_user AND granted\_role != 'NHANVIEN';

exception

when NO\_DATA\_FOUND then

user\_role := '';

IF user\_role = 'THEODOIKQ' THEN

--select key

select KEY\_STORE.value

into m\_key

from KEY\_STORE

where ID = '1';

FOR pb IN (select UCV1, UCV2, UCV3 from PHIEUBAU)

LOOP

--decrypt UCV1

pb.UCV1 := UTL\_RAW.CAST\_TO\_NUMBER(decrypt\_data\_AES128(UTL\_I18N.STRING\_TO\_RAW(pb.UCV1),m\_key));

--decrypt UCV2

pb.UCV2 := UTL\_RAW.CAST\_TO\_NUMBER(decrypt\_data\_AES128(UTL\_I18N.STRING\_TO\_RAW(pb.UCV2),m\_key));

--decrypt UCV3

pb.UCV3 := UTL\_RAW.CAST\_TO\_NUMBER(decrypt\_data\_AES128(UTL\_I18N.STRING\_TO\_RAW(pb.UCV3),m\_key));

PIPE ROW (PHIEUBAU\_TYPE(pb.UCV1,pb.UCV2,pb.UCV3));

END LOOP;

ELSE

raise\_application\_error(-20000,'User authority level is not sufficient');

END IF;

END;

--Cho phép người dùng THEODOIKQ sử dụng function decrypt

create or replace trigger capquyen\_mahoa\_phieubau

AFTER INSERT ON THEODOI

FOR EACH ROW

DECLARE

PRAGMA AUTONOMOUS\_TRANSACTION;

stm varchar2(100);

BEGIN

stm := 'GRANT EXECUTE ON QUANTRI.QUERY\_UNGVIEN TO "' || :new.ma\_theodoi || '"';

execute immediate stm;

commit;

END capquyen\_mahoa\_phieubau;

select \* from table(query\_ungvien());

* 1. **Chức năng:**
* Procedure : P
* Function: F
* Trigger: T

|  |  |  |  |
| --- | --- | --- | --- |
| STT | Loại | Tên | Hoạt động |
| 1 | P | CAPNHAT\_ROLE | Tự động cập nhật lại Role của người dùng tương ứng với bảng |
| 2 | P | TAO\_USER | Tạo user trong CSDL  Gán quyền NHANVIEN khi thêm 1 dòng dữ liệu vào bảng THANHVIEN  Mật khẩu mặc định: 123456 |
| 3 | F | ENCRYPT\_DATA\_AES128 | Mã hóa thông tin sử dụng thuật toán AES128 |
| 4 | F | DECRYPT\_DATA\_AES128 | Giải mã thông tin sử dụng thuật toán AES128 |
| 5 | F | F\_SELECT\_THANHVIEN | Sử dụng trong VPD 1  Trả về rỗng nếu người dùng là QUANTRI hoặc TOLAP |
| 6 | F | F\_UPDATE\_CUTRI\_PHIEUBAU | Sử dụng trong VPD 2 |
| 7 | F | HASH\_DATA |  |
| 8 | F | QUERY\_UNGVIEN | Trả về giải mã thông tin ứng cử viên của bảng PHIEUBAU |
| 9 | T | ALTER\_PHIEUBAU\_TRIGGER | Điều kiện: SELECT | UPDATE bảng PHIEUBAU  Mã hóa thông tin ứng cử viên trước khi thêm dữ liệu vào bảng |
| 10 | T | CAPQUYEN\_MAHOA\_PHIEUBAU | Điều kiện: INSERT bảng THEODOI  Cấp quyền thực thi chức năng QUERY\_PHIEUBAU |
| 12 | T | TAO\_CONNECTION | Điều kiện: INSERT bảng THANHVIEN  Lấy năm hệ thống và thêm vào trước MATHANHVIEN sao đó gọi TAO\_USER |
| 13 | T | THEM\_( BTC|CUTRI|  GIAMSAT|THEODOI|  TOLAP) | Điều kiện: INSERT bảng (BTC|CUTRI|GIAMSAT|THEODOI|TOLAP)  Gọi procedure CAPNHAT\_ROLE |

1. **Giao diện:**