TRƯỜNG ĐẠI HỌC KHOA HỌC TỰ NHIÊN ĐHQG – HCM

KHOA CÔNG NGHỆ THÔNG TIN

----------∞O∞----------

BÁO CÁO ĐỒ ÁN MÔN HỌC LẦN 2

Môn học: AN TOÀN VÀ BẢO MẬT DỮ LIỆU TRONG HTTT

Sinh viên thực hiện:

22127115 – Trần Trung Hiếu

22127138 – Đào Ngọc Hưng

22127329 – Phạm Ngọc Phú

22127354 – Phan Vũ Anh Quang

Giảng viên:

TS. Phạm Thị Bạch Huệ

ThS. Lương Vĩ Minh

ThS. Tiết Gia Hồng

1. Phân công & Các chức năng thực hiện

MSSV	Họ Tên	Chức năng	Phần trăm công việc được giao đã hoàn thành (%)	Phần trăm đóng góp vào hoàn thành đồ án
22127115	Trần Trung Hiếu	Tất cả chức năng phân hệ 1	100%	25%
22127138	Đào Ngọc Hưng	Hoàn thiện cài đặt các chính sách bảo mật (DAC, RBAC, VPD)	100%	25%
22127329	Phạm Ngọc Phú	Cài đặt chức năng OLS	100%	25%
22127354	Phan Vũ Anh Quang	Cài đặt chức năng Audit	100%	25%
	Tất cả thành viên	Viết báo cáo	100%	

2. Giải pháp lý thuyết & Đánh giá

2.1. Phân hệ 1

a) Tóm lược giải pháp

Giải pháp xây dựng ứng dụng WinForm tích hợp với Oracle DB Server nhằm hỗ trợ quản trị viên thực hiện các tác vụ quản lý người dùng, vai trò (role) và quyền truy cập trên cơ sở dữ liệu Oracle. Các chức năng chính bao gồm:

- Quản lý user/role: Tạo, sửa, xóa user/role thông qua các package PL/SQL (PKG_USER_MANAGEMENT, PKG_ROLE_MANAGEMENT).
- Xem danh sách: Liệt kê user/role và thông tin chi tiết từ các view hệ thống như DBA_USERS, DBA_ROLES.
- Cấp quyền:
    - Cấp quyền cho user/role trên các đối tượng như table, view, stored procedure, function.
    - Hỗ trợ cấp quyền chi tiết đến mức cột cho SELECT, UPDATE.
    - Tùy chọn WITH GRANT OPTION để cho phép người được cấp quyền cấp tiếp quyền đó.
- Thu hồi quyền: Thu hồi quyền từ user/role trên các đối tượng.
- Xem thông tin quyền: Truy vấn quyền của user/role từ view DBA_TAB_PRIVS.

Các package PL/SQL được thiết kế để xử lý logic phía server, giảm tải cho ứng dụng WinForm. WinForm sẽ gọi các procedure trong package thông qua kết nối Oracle (ODP.NET) để thực thi lệnh.

b) Nhận xét và Đánh giá

Ưu điểm:

- Tính module: Các package (PKG_USER_MANAGEMENT, PKG_ROLE_MANAGEMENT, PKG_USER_ROLES, PKG_OBJECT_MANAGEMENT) được tổ chức rõ ràng, dễ bảo trì và mở rộng.
- Bảo mật: Sử dụng tài khoản ADMIN với quyền hạn cụ thể, tránh lạm dụng quyền SYS/SYSTEM. Các lệnh động (EXECUTE IMMEDIATE) được kiểm soát chặt chẽ.
- Hiệu quả: Sử dụng REF CURSOR để trả về danh sách dữ liệu linh hoạt, phù hợp với giao diện WinForm.
- Hỗ trợ chi tiết: Cấp quyền đến mức cột và tùy chọn WITH GRANT OPTION đáp ứng yêu cầu phức tạp của quản trị Oracle.

Hạn chế: Chưa có

2.2. Phân hệ 2

a) Yêu cầu 1:

Câu 1: Bảo mật quan hệ NHANVIEN bằng RBAC

Chính sách:

- Người dùng có VAITRO = 'NVCB': chỉ được phép xem và cập nhật số điện thoại của chính mình.
- Các nhân viên còn lại (GV, TRGĐV, NV...) kế thừa quyền của NVCB.
- Người dùng có vai trò TRGĐV: xem được nhân viên trong đơn vị mình (trừ LUONG, PHUCAP).
- Người dùng có vai trò NV TCHC: toàn quyền (SELECT, INSERT, UPDATE, DELETE) trên bảng NHANVIEN.

Thực hiện:

- Tạo các VIEW: VW_NHANVIEN_NVCB, VW_NHANVIEN_TRGDV.
- Tạo các ROLE: ROLE_NVCB, ROLE_TRGDV, ROLE_TCHC.
- Tạo thủ tục: UPDATE_NHANVIEN_DT để kiểm tra mã nhân viên và cập nhật ĐT.

Giao diện:

- Giao diện cho NVCB: Chỉ chỉnh sửa được số điện thoại.
- Giao diện cho TRGĐV: Xem danh sách nhân viên trong đơn vị.
- Giao diện cho NV TCHC: CRUD toàn bộ bảng NHANVIEN.

Câu 2: Bảo mật quan hệ MOMON bằng RBAC

Chính sách:

- Giảng viên (GV): chỉ được xem phân công giảng dạy của chính mình.
- Nhân viên phòng đào tạo (NV PĐT): được xem, thêm, sửa, xóa MOMON trong học kỳ hiện tại.
- Trưởng đơn vị (TRGĐV): xem các dòng liên quan đến giảng viên trong đơn vị.
- Sinh viên: chỉ được xem các học phần thuộc khoa của mình đang được mở.

Thực hiện:

- Tạo các VIEW: VW_MOMON_GV, VW_MOMON_PDT, VW_MOMON_SV, VW_MOMON_TRGDV.
- Phân quyền SELECT/UPDATE/... theo vai trò tương ứng.
- Ràng buộc học kỳ hiện tại bằng các điều kiện SYSDATE trong VIEW.

Giao diện:

- Giao diện riêng cho mỗi vai trò:
    - GV: xem danh sách lớp học phần được phân công.
    - NV PĐT: cập nhật toàn bộ dữ liệu của học kỳ hiện tại.
    - SV: chỉ xem dữ liệu phù hợp với khoa.

Câu 3: Bảo mật quan hệ SINHVIEN bằng VPD

Chính sách:

- Sinh viên được phép xem và cập nhật địa chỉ + số điện thoại của chính mình.
- NV PCTSV: Toàn quyền CRUD trên SINHVIEN, ngoại trừ không được cập nhật TINHTRANG.

- NV PĐT: Được cập nhật cột TINHTRANG.
- GV: chỉ được xem các sinh viên thuộc khoa của mình.

Thực hiện:

- Tạo hàm POLICY_SINHVIEN để lọc dữ liệu theo người dùng.
- Áp dụng VPD qua DBMS_RLS.ADD_POLICY với điều kiện kiểm tra VAITRO, khoa, MASV.
- Tạo thủ tục UPDATE_SINHVIEN_INFO để cập nhật địa chỉ và điện thoại.

Giao diện:

- Giao diện sinh viên: chỉ cập nhật ĐCHI, ĐT.
- Giao diện NV PCTSV: Thêm, sửa, xóa sinh viên, nhưng không đụng đến TINHTRANG.
- Giao diện GV: chỉ xem danh sách sinh viên thuộc khoa.

Câu 4: Bảo mật quan hệ DANGKY bằng VPD

Chính sách:

- Sinh viên được:
    - Xem dữ liệu của chính mình.
    - Thêm/sửa/xóa đăng ký học phần trong 14 ngày đầu học kỳ, chỉ khi điểm = NULL.
- NV PĐT có quyền tương tự sinh viên, nhưng thực hiện thay mặt sinh viên.
- GV: xem danh sách lớp học phần mà mình dạy.
- NV PKT: cập nhật cột điểm của các dòng DANGKY.

Thực hiện:

- Tạo các hàm:
    - POLICY_DANGKY_SELECT: lọc dữ liệu phù hợp người dùng.
    - POLICY_DANGKY_MODIFY: kiểm tra thời gian 14 ngày đầu kỳ.
    - POLICY_DANGKY_DIEM: hạn chế NV PĐT sửa điểm.
- Áp dụng DBMS_RLS.ADD_POLICY với cột liên quan đến điểm.
- Tạo CHECK_INVALID_DANGKY_TIME cho FGA/Audit.

Giao diện:

- Sinh viên: chỉ thao tác trong 14 ngày đầu, khi chưa có điểm.
- GV: chỉ xem lớp học phần mình dạy.
- NV PKT: chỉnh sửa điểm.
- NV PĐT: thao tác đăng ký giúp sinh viên nhưng không được sửa điểm.

b) Yêu cầu 2: Nhãn bảo mật (Oracle Label Security)

Oracle Label Security (OLS) là một tính năng trong hệ thống quản lý cơ sở dữ liệu Oracle Database. Nó cung cấp các công cụ và khả năng để triển khai và quản lý việc bảo mật dữ liệu trên cấp độ nhãn (label-level) trong hệ thống cơ sở dữ liệu.

OLS cho phép bạn xác định và gắn nhãn cho các đối tượng dữ liệu, chẳng hạn như bảng, cột, dòng, hoặc thậm chí từng giá trị riêng lẻ. Nhãn được sử dụng để đại diện cho các cấp độ bảo mật khác nhau, ví dụ như "cực kỳ bảo mật" (top secret), "bảo mật" (secret), "nội bộ" (internal), và "công khai" (public). Bằng cách gắn nhãn cho dữ liệu, bạn có thể áp dụng các chính sách bảo mật nhằm kiểm soát truy cập dựa trên các quyền và nhãn đã được xác định.

Oracle Label Security hỗ trợ tích hợp với các tính năng khác của Oracle Database như quản lý người dùng và vai trò, quyền hạn. Nó cung cấp khả năng thực hiện kiểm tra kiểm soát truy cập để đảm bảo rằng chỉ những người có quyền được phép xem, sửa đổi, hoặc truy cập vào các đối tượng dữ liệu có nhãn tương ứng.

OLS thường được sử dụng trong các môi trường có yêu cầu bảo mật cao như trong ngành chính phủ, lĩnh vực quân sự, hoặc các tổ chức có nhu cầu bảo vệ dữ liệu nhạy cảm.

Trong đồ án này, nhóm đã cấu hình OLS để kiểm soát quyền truy cập vào bảng **THONGBAO** nơi chứa 9 thông báo gửi đến 8 người dùng khác nhau trong Trường đại học X nhằm đảm bảo rằng các thông báo chỉ được truy cập bởi những người dùng có quyền hợp lệ, dựa trên vai trò, phòng ban và cơ sở. OLS mang lại khả năng kiểm soát truy cập chi tiết hơn ở cấp độ dữ liệu, giúp ngăn chặn truy cập trái phép và đảm bảo tính bảo mật của các thông báo nhạy cảm.

Cấu trúc nhãn trong OLS

Chính sách OLS sử dụng các nhãn để phân loại dữ liệu và người dùng. Mỗi nhãn bao gồm ba thành phần chính:

- **Level:** Đại diện cho cấp độ bảo mật của dữ liệu. Trong hệ thống này, các mức độ được định nghĩa như sau:
    - TRDV: Trưởng đơn vị – cấp độ cao nhất.
    - NV: Nhân viên – cấp độ trung bình.
    - SV: Sinh viên – cấp độ thấp nhất.
- **Compartment:** Xác định các nhóm dữ liệu riêng biệt, tương ứng với các lĩnh vực hoặc phòng ban. Các ngăntrong hệ thống này bao gồm:
    - TOAN: Toán
    - LY: Lý
    - HOA: Hóa
    - HC: Hành chính
- **Group:** Xác định các nhóm dữ liệu có thể được chia sẻ, thường liên quan đến địa điểm hoặc cơ sở. Các nhóm trong hệ thống này là:
    - CS1: Cơ sở 1
    - CS2: Cơ sở 2

Nguyên tắc hoạt động

Để một người dùng có thể truy cập dữ liệu trong bảng THONGBAO, nhãn của người dùng phải lớn hơn hoặc bao gồm (nhãn dữ liệu là con của nhãn người dùng) nhãn của dữ liệu, dựa trên các quy tắc sau:

- **Level:** Mức độ của người dùng phải lớn hơn hoặc bằng mức độ của dữ liệu. Ví dụ, trưởng đơn vị (TRDV, 300) có thể truy cập dữ liệu dành cho nhân viên (NV, 200) hoặc sinh viên (SV, 100), nhưng sinh viên không thể truy cập dữ liệu của trưởng đơn vị.
- **Compartment:** Người dùng phải có tất cả các ngăn được gán cho dữ liệu. Nếu một thông báo có ngăn TOAN và LY, người dùng cũng phải có cả hai khoang này trong nhãn của mình.
- **Group:** Người dùng phải có ít nhất một nhóm trùng với nhóm của dữ liệu, hoặc dữ liệu không được gán nhóm nào. Ví dụ, một thông báo chỉ dành cho CS1 sẽ không thể truy cập bởi người dùng chỉ có nhóm CS2.

Ứng dụng vào bảng THONGBAO

- Bảng THONGBAO có một cột đặc biệt là OLS_LABEL, nơi lưu trữ nhãn của từng thông báo. Nhãn này xác định đối tượng nhận thông báo (ví dụ: trưởng đơn vị của khoa Toán ở cơ sở 1).
- Mỗi người dùng trong hệ thống được gán một nhãn riêng, phản ánh vai trò, phòng ban và cơ sở của họ.
- Khi người dùng truy vấn bảng THONGBAO, OLS tự động so sánh nhãn của họ với nhãn của từng thông báo để quyết định dữ liệu nào họ được phép xem.

Ví dụ:

- Một thông báo có nhãn TRDV:TOAN:CS1 chỉ có thể được xem bởi trưởng đơn vị của khoa Toán tại cơ sở 1.
- Một sinh viên (SV) ở cơ sở 2 (CS2) với nhãn SV::CS2 sẽ không thấy thông báo này vì mức độ (SV, 100) thấp hơn TRDV (300) và không có nhãn TOAN.

Đánh giá giải pháp

OLS cho phép phân quyền rất cụ thể dựa trên ba yếu tố (level, compartment, group), đảm bảo rằng thông báo chỉ đến đúng đối tượng cần nhận. Điều này giúp người dùng kiểm soát truy cập chi tiết. Nhãn có thể được điều chỉnh dễ dàng để thay đổi quyền truy cập mà

không cần sửa đổi cấu trúc bảng hoặc mã ứng dụng, mang tính linh hoạt cao. Dữ liệu nhạy cảm được bảo vệ chặt chẽ, ngăn chặn truy cập trái phép từ các đối tượng không đủ quyền, mang tính bảo mật cao. Một hạn chế của OLS là nó có thể phức tạp khi quản lý trong hệ thống lớn với nhiều người dùng và nhãn, đồng thời việc kiểm tra nhãn có thể ảnh hưởng đến hiệu suất truy vấn. Tuy nhiên với quy mô trong đồ án tương đối nhỏ, những hạn chế của nó không đáng kể.

c) Yêu cầu 3: Chính sách Audit (ghi vết trên dữ liệu)

Kích hoạt và Cấu hình Ghi Nhật ký

Hệ thống ghi nhật ký được kích hoạt và tùy chỉnh thông qua các lệnh SQL và các gói PL/SQL được cung cấp bởi Oracle:

- Standard Audit: Các chính sách được định nghĩa và kích hoạt bằng lệnh AUDIT. Các bản ghi được tạo ra bởi các chính sách này sẽ được lưu trữ dựa trên cấu hình tham số AUDIT_TRAIL của hệ thống
- Fine-Grained Audit (FGA): Các chính sách được tạo và quản lý thông qua gói DBMS_FGA, cụ thể là thủ tục DBMS_FGA.ADD_POLICY. Các bản ghi FGA được cấu hình để lưu vào bảng audit của cơ sở dữ liệu (DBMS_FGA.DB) và bao gồm thông tin SQL chi tiết (DBMS_FGA.EXTENDED), được truy vấn qua view DBA_FGA_AUDIT_TRAIL.

Thực hiện ghi nhật ký hệ thống dùng Standard Audit

Standard Audit được cấu hình để cung cấp một cái nhìn tổng quan về các hoạt động diễn ra trên các đối tượng và quyền hạn quan trọng. Các chính sách Standard Audit sau đã được thiết lập trong schema ADMIN:

- **Theo dõi DML trên các bảng quan trọng:**
    - **AUDIT INSERT, UPDATE, DELETE ON ADMIN.DANGKY BY ACCESS;**: Ghi lại mọi thao tác thêm, sửa, xóa trên bảng Đăng Ký, bất kể thành công hay thất bại. Điều này quan trọng để giám sát mọi thay đổi liên quan đến việc đăng ký học phần của sinh viên.
    - **AUDIT SELECT, UPDATE ON ADMIN.NHANVIEN BY ACCESS WHENEVER SUCCESSFUL;**: Ghi lại các hành động xem và cập nhật

thành công trên bảng Nhân Viên. Giám sát việc truy cập và sửa đổi thông tin nhân sự là cần thiết.
    - **AUDIT SELECT, INSERT, UPDATE, DELETE ON ADMIN.VW_MOMON_PDT BY ACCESS WHENEVER SUCCESSFUL;**: Ghi lại các thao tác DML thành công trên view VW_MOMON_PDT (dành cho Nhân viên Phòng Đào Tạo). Điều này giúp giám sát việc quản lý mở môn học trong học kỳ hiện tại.
- **Theo dõi hoạt động hệ thống và bảo mật:**
    - **AUDIT SESSION WHENEVER NOT SUCCESSFUL;**: Ghi lại tất cả các lần đăng nhập thất bại vào hệ thống, giúp phát hiện các cuộc tấn công dò mật khẩu.
    - **AUDIT ROLE BY ACCESS;**: Ghi lại các thao tác tạo, sửa, xóa, và gán vai trò (role), quan trọng cho việc quản lý phân quyền.
    - **AUDIT GRANT ANY ROLE, GRANT ANY PRIVILEGE BY ACCESS;**: Ghi lại việc gán các quyền hệ thống mạnh, giúp kiểm soát các thay đổi đặc quyền cấp cao.
    - **AUDIT TABLE BY ACCESS;**: Ghi lại các thao tác DDL quan trọng như tạo, sửa, xóa, cắt bảng (CREATE/ALTER/DROP/TRUNCATE TABLE), giúp giám sát thay đổi cấu trúc dữ liệu.

Thực hiện ghi nhật ký hệ thống dùng Fine-Grained Audit (FGA)

FGA được sử dụng để giám sát các hành vi cụ thể, có điều kiện phức tạp, đặc biệt là các hành vi vi phạm chính sách bảo mật hoặc quy tắc nghiệp vụ nhạy cảm. Các tình huống sau được giám sát bằng FGA:

- Hành vi cập nhật điểm trên DANGKY bởi người không thuộc vai trò “NV PKT”:
    - Triển khai: Sử dụng chính sách FGA tên AUDIT_UPDATE_DIEM_NOT_NV_PKT áp dụng cho bảng ADMIN.DANGKY.
    - Đối tượng theo dõi: Các cột điểm ĐIEMTH, ĐIEMQT, ĐIEMCK, ĐIEMTK.
    - Hành động theo dõi: UPDATE.
    - Điều kiện kích hoạt (audit_condition): ADMIN.CHECK_NOT_NV_PKT = 0. Hàm ADMIN.CHECK_NOT_NV_PKT sẽ kiểm tra xem user thực hiện

hành động có sở hữu ROLE_NV_PKT hay không. Nếu không có vai trò này, hàm trả về 0, và policy FGA sẽ được kích hoạt, ghi lại hành động cập nhật điểm trái phép.

- Hành vi đọc hoặc cập nhật LUONG, PHUCAP của người khác bởi người không thuộc vai trò "NV TCHC":

    - Triển khai: Sử dụng hai chính sách FGA trên bảng ADMIN.NHANVIEN:
        - AUDIT_SELECT_LUONG_PHUCAP_NOT_TCHC: Cho hành động SELECT.
        - AUDIT_UPDATE_LUONG_PHUCAP_NOT_TCHC: Cho hành động UPDATE.
    - Đối tượng theo dõi: Các cột LUONG, PHUCAP.
    - Điều kiện kích hoạt (audit_condition):
        - Đối với SELECT: MANV != SYS_CONTEXT('USERENV', 'SESSION_USER') AND ADMIN.CHECK_NOT_TCHC = 0. Điều kiện này đảm bảo chỉ audit khi user xem lương/phụ cấp của người khác (MANV != SESSION_USER) VÀ user đó không có vai trò ROLE_TCHC (hàm CHECK_NOT_TCHC trả về 0).
        - Đối với UPDATE: ADMIN.CHECK_NOT_TCHC = 0. Audit mọi hành động cập nhật lương/phụ cấp nếu user không có vai trò ROLE_TCHC.
- Hành vi thêm, xóa, sửa trên DANGKY của sinh viên nhưng trên dòng dữ liệu của sinh viên khác hoặc ngoài thời gian cho phép:

    - Triển khai: Sử dụng chính sách FGA tên AUDIT_DANGKY_INVALID_SV áp dụng cho bảng ADMIN.DANGKY.
    - Hành động theo dõi: INSERT, UPDATE, DELETE.
    - Điều kiện kích hoạt (audit_condition): ADMIN.CHECK_INVALID_DANGKY(DANGKY.MASV, DANGKY.MAMM) = 1. Hàm ADMIN.CHECK_INVALID_DANGKY được thiết kế để:
        - Chỉ áp dụng kiểm tra chi tiết nếu user thực thi có vai trò ROLE_SV.
        - Kiểm tra xem mã sinh viên trên dòng dữ liệu (p_masv) có khớp với user đang thực thi (SYS_CONTEXT('USERENV', 'SESSION_USER')) hay không. Nếu không khớp, trả về 1 (audit).

    - Kiểm tra xem ngày hiện tại (SYSDATE) có nằm trong khoảng 14 ngày đầu của học kỳ tương ứng với p_mamm hay không. Nếu nằm ngoài khoảng thời gian này, trả về 1 (audit).
    - Nếu các điều kiện trên không bị vi phạm (đúng sinh viên, trong thời hạn), hàm trả về 0 (không audit).

Truy xuất Dữ liệu Nhật ký

Dữ liệu nhật ký hệ thống được truy xuất thông qua các view từ điển dữ liệu chuẩn của Oracle:

- Standard Audit Data: Truy vấn từ view DBA_AUDIT_TRAIL.
- Fine-Grained Audit Data: Truy vấn từ view DBA_FGA_AUDIT_TRAIL.

3. Nguồn tham khảo

[1] Micro Focus, n.d. *Oracle Backups*. Available at: https://www.microfocus.com/documentation/borland-connect/3.1/install-help/STARTEAM-DC9FDDDA-ORACLEBACKUPS-CON.html

[2] Oracle, n.d. *Overview of Backups*. Available at: https://docs.oracle.com/en-us/iaas/mysql-database/doc/overview-backups.html

[3] Oracle Corporation, n.d. *Auditing in Oracle Database*. Available at: https://docs.oracle.com/cd/E11882_01/server.112/e10575/tdpsg_auditing.html

[4] Oracle Label Security(OLS): https://oracle--base-com.translate.goog/articles/9i/oracle-label-security-9i?_x_tr_sl=en&_x_tr_tl=vi&_x_tr_hl=vi&_x_tr_pto=tc