Trường Đại học Khoa học Tự nhiên, ĐHQG HCM

Khoa Công nghệ thông tin

NĂM HỌC 2023-2024

ĐỒ ÁN MÔN HỌC

CSC12001 - AN TOÀN VÀ BẢO MẬT DỮ LIỆU TRONG HTTT

Giáo viên: TS. Phạm Thị Bạch Huệ

ThS. Lương Vĩ Minh

ThS. Tiết Gia Hồng

Nội dung

PHÂN HỆ 1: ỨNG DỤNG QUẢN TRỊ CSDL ORACLE.

Dành cho người quản trị cơ sở dữ liệu

Sinh viên hãy xây dựng ứng dụng ***Window Form*** cho phép người dùng có quyền quản trị trên Oracle DB Server thực hiện được các thao tác sau:

1. Xem danh sách tài khoản người dùng trong hệ thống Oracle DB Server.
2. Xem thông tin về quyền (privileges) của mỗi *user*/ *role* trên các đối tượng dữ liệu.
3. Cho phép Tạo mới, Xóa, Sửa (hiệu chỉnh) user hoặc role.
4. Cho phép thực hiện việc cấp quyền:
    a. Cấp quyền cho user, cấp quyền cho role, cấp role cho user.
    b. 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).
    c. Quyền select, update phải cho phép phân quyền tính đến mức cột; quyền insert, delete thì không.
5. Cho phép thu hồi quyền hạn từ user/role.
6. Cho phép kiểm tra quyền của các chủ thể vừa được cấp quyền.

PHÂN HỆ 2: ỨNG DỤNG QUẢN LÝ DỮ LIỆU NỘI BỘ

Khoa Công nghệ thông tin một trường Đại học X cần xây dựng ứng dụng *Windows Form* A để quản lý dữ liệu nội bộ. Sau đây là trích một phần lược đồ CSDL mà khoa đang sử dụng:

NHANSU (MANV, HOTEN, PHAI, NGSINH, PHUCAP, ĐT, VAITRO, MAĐV)

Quan hệ *NHANSU* lưu lại dữ liệu về tất cả nhân viên trong khoa. Nhân sự trong khoa có thể phụ trách các công việc sau: *nhân viên cơ bản, giảng viên, giáo vụ*, ...

Mỗi nhân viên có mã nhân viên (MANV), có họ tên (HOTEN), thuộc phái (PHAI), có ngày sinh (NGSINH), phụ cấp (PHUCAP), số điện thoại liên lạc (ĐT), đảm nhận một vai trò (VAITRO) và thuộc về 1 đơn vị (MAĐV).

SINHVIEN (MASV, HOTEN, PHAI, NGSINH, ĐCHI, ĐT, MACT, MANGANH, SOTCTL, ĐTBTL)

Mỗi sinh viên có mã duy nhất (MASV), họ tên (HOTEN), phái (PHAI), ngày sinh (NGSINH), địa chỉ (ĐCHI), số điện thoại (ĐT), sinh viên thuộc một chương trình đào tạo (MACT), theo học một ngành (MANGANH), số tín chỉ của chương trình đào tạo mà sinh viên đã tích lũy được (SOTCTL) và điểm trung bình tích lũy (ĐTBTL).

Hệ thống hiện có khoảng 4.000 sinh viên đang học tại khoa.

ĐONVI (MAĐV, TENĐV, TRGĐV)

Mỗi đơn vị có mã đơn vị (MAĐV), tên đơn vị (TENĐV), người làm trưởng đơn vị (TRGĐV) – cũng là nhân sự của Khoa.

Các đơn vị là: *Văn phòng khoa*, *Bộ môn HTTT*, *Bộ môn CNPM*, *Bộ môn KHMT*, *Bộ môn CNTT*, *Bộ môn TGMT* và *Bộ môn MMT và Viễn thông*.

Mỗi đơn vị có một nhân sự làm trưởng (TRGĐV). Trưởng đơn vị của đơn vị *Văn phòng khoa* chính là nhân sự có vai trò trưởng khoa.

HOCPHAN (MAHP, TENHP, SOTC, STLT, STTH, SOSVTĐ, MAĐV)

Mỗi học phần có mã học phần (MAHP), tên học phần (TENHP), số tín chỉ (SOTC), số tiết lý thuyết (STLT), số tiết thực hành (STTH), số sinh viên tối đa tiếp nhận vào mỗi lớp học phần mỗi khi học phần được mở.

Theo phân công của trưởng khoa, mỗi học phần do một đơn vị (MAĐV) phụ trách chuyên môn và do người làm trưởng đơn vị đó phân công giảng dạy.

Với các học phần do đơn vị *Văn phòng khoa* phụ trách phân công giảng dạy thì các nhân sự *giáo vụ* thừa hành trưởng khoa phân công giảng dạy.

KHMO (MAHP, HK, NAM, MACT)

Mỗi dòng trong quan hệ KHMO (kế hoạch mở môn) cho biết trong năm học NAM, học kỳ HK đối với chương trình đào tạo MACT thì có mở học phần có mã là MAHP.

Các chương trình đào tạo có thể gồm: chính quy ('CQ'), chất lượng cao ('CLC'), chương trình tiên tiến ('CTTT'), Việt - Pháp ('VP').

Mỗi năm học có 3 học kỳ bắt đầu tương ứng vào ngày đầu tiên các tháng 1, 5, 9.

PHANCONG (MAGV, MAHP, HK, NAM, MACT)

Mỗi dòng trong quan hệ PHANCONG cho biết một giảng viên (MAGV, cũng là một nhân sự) được phân công giảng dạy học phần (MAHP) được mở cho chương trình đào tạo (MACT) trong học kỳ HK của năm học NAM theo Kế hoạch mở môn.

ĐANGKY (MASV, MAGV, MAHP, HK, NAM, MACT, ĐIEMTH, ĐIEMQT, ĐIEMCK, ĐIEMTK)

Mỗi dòng trong quan hệ ĐANGKY cho biết một sinh viên (MASV) đăng ký lớp học phần (đã được mở trong quan hệ KHMO và đã được phân công cho giáo viên trong quan hệ PHANCONG) được xác định bởi các thông tin gồm: mã giảng viên (MAGV), mã học phần (MAHP), mã chương trình đào tạo (MACT), học kỳ (HK), năm học (NAM).

Kết quả học tập của sinh viên được ghi lại ở các cột điểm thực hành (ĐIEMTH), điểm quá trình (ĐIEMQT), điểm cuối kỳ (ĐIEMCK) và điểm tổng kết (ĐIEMTK) theo một công thức tỉ lệ cho trước.

Thuộc tính *VAITRO* trong quan hệ **NHANSU**:

- Cho biết nhiệm vụ của một nhân sự được tổ chức phân công, có thể nhận các giá trị sau: "*Nhân viên cơ bản*" (có 10 người), "*Giảng viên*" (có 80 người), "*Giáo vụ*" (có 10 người), "*Trưởng đơn vị*" (có 6 người), "*Trưởng khoa*" (có 1 người). Quyền tương ứng

với từng vai trò được mô tả dưới dạng các chính sách được đánh mã **CS#i** và mô tả bên dưới.

- Thuộc tính *VAITRO* phản ánh đúng vai trò của từng nhân sự, do trưởng khoa phân công. Người quản trị bảo mật trong hệ thống gán các quyền truy cập dữ liệu cho từng nhân sự theo đúng vai trò (*VAITRO*), được liệt kê bên dưới.

CS#1: Người dùng có VAITRO là "**Nhân viên cơ bản"** có quyền truy cập dữ liệu:

- Xem dòng dữ liệu của chính mình trong quan hệ NHANSU, có thể chỉnh sửa số điện thoại (ĐT) của chính mình (nếu số điện thoại có thay đổi).
- Xem thông tin của tất cả SINHVIEN, ĐƠNVỊ, HOCPHAN, KHMO.

CS#2: Người dùng có VAITRO là "**Giảng viên**" có quyền truy cập dữ liệu:

- Như một người dùng có vai trò **"Nhân viên cơ bản"** (xem mô tả **CS#1**).
- Xem dữ liệu phân công giảng dạy liên quan đến bản thân mình (PHANCONG).
- Xem dữ liệu trên quan hệ ĐANGKY liên quan đến các lớp học phần mà giảng viên được phân công giảng dạy.
- Cập nhật dữ liệu tại các trường liên quan điểm số (trong quan hệ ĐANGKY) của các sinh viên có tham gia lớp học phần mà giảng viên đó được phân công giảng dạy. Các trường liên quan điểm số bao gồm: ĐIEMTH, ĐIEMQT, ĐIEMCK, ĐIEMTK.

CS#3: Người dùng có VAITRO là "**Giáo vụ"** có quyền:

- Như một người dùng có vai trò **"Nhân viên cơ bản"** (xem mô tả **CS#1**).
- Xem, Thêm mới hoặc Cập nhật dữ liệu trên các quan hệ SINHVIEN, ĐONVI, HOCPHAN, KHMO, theo yêu cầu của trưởng khoa.
- Xem dữ liệu trên toàn bộ quan hệ PHANCONG. Tuy nhiên, chỉ được sửa trên các dòng dữ liệu phân công liên quan các học phần do "*Văn phòng khoa*" phụ trách phân công giảng dạy, thừa hành người trưởng đơn vị tương ứng là trưởng khoa.

- Xóa hoặc Thêm mới dữ liệu trên quan hệ ĐANGKY theo yêu cầu của sinh viên trong khoảng thời gian còn cho hiệu chỉnh đăng ký, *xem điều kiện có thể hiệu chỉnh đăng ký học phần được mô tả bên dưới.*

CS#4: Người dùng có VAITRO là "**Trưởng đơn vị"**, gồm trưởng các bộ môn (không bao gồm trưởng khoa), có quyền truy cập dữ liệu:

- Như một người dùng có vai trò "**Giảng viên"** (xem mô tả **CS#2**).
- Thêm, Xóa, Cập nhật dữ liệu trên quan hệ PHANCONG, đối với các học phần được phụ trách chuyên môn bởi đơn vị mà mình làm trưởng,
- Được xem dữ liệu phân công giảng dạy của các giảng viên thuộc các đơn vị mà mình làm trưởng.

CS#5: Người dùng có VAITRO là "**Trưởng khoa"** có quyền hạn:

- Như một người dùng có vai trò "**Giảng viên"**
- Thêm, Xóa, Cập nhật dữ liệu trên quan hệ PHANCONG đối với các học phần quản lý bởi đơn vị "*Văn phòng khoa*".
- Được quyền Xem, Thêm, Xóa, Cập nhật trên quan hệ NHANSU.
- Được quyền Xem (không giới hạn) dữ liệu trên toàn bộ lược đồ CSDL.

CS#6: Người dùng có VAITRO là "**Sinh viên"** có quyền hạn:

- Trên quan hệ SINHVIEN, sinh viên chỉ được xem thông tin của chính mình, được Chỉnh sửa thông tin địa chỉ (ĐCHI) và số điện thoại liên lạc (ĐT) của chính sinh viên.
- Xem danh sách tất cả học phần (HOCPHAN), kế hoạch mở môn (KHMO) của chương trình đào tạo mà sinh viên đang theo học.
- Thêm, Xóa các dòng dữ liệu đăng ký học phần (ĐANGKY) liên quan đến chính sinh viên đó trong học kỳ của năm học hiện tại (nếu thời điểm hiệu chỉnh đăng ký còn hợp lệ).
- Sinh viên **không** được chỉnh sửa trên các trường liên quan đến điểm.

- Sinh viên được Xem tất cả thông tin trên quan hệ ĐANGKY tại các dòng dữ liệu liên quan đến chính sinh viên.

Sinh viên có thể hiệu chỉnh đăng ký học phần (thêm, xóa) nếu ngày hiện tại không vượt quá 14 ngày so với ngày bắt đầu học kỳ (xem thêm thông tin về học kỳ trong quan hệ KHMO) mà sinh viên đang hiệu chỉnh đăng ký học phần.

*Giả sử cơ sở dữ liệu được khai báo trên HQT CSDL Oracle, hãy đề xuất cách ép thỏa các chính sách bảo mật **CS#i** được mô tả ở trên.*

Sinh viên có thể mô tả lại ngữ cảnh bài toán hoặc các chính sách bảo mật cho phù hợp với thực tế, hoặc có thể bổ sung thêm thuộc tính cho lược đồ CSDL đã cho (nếu cần thiết).

Yêu cầu 1: Cấp quyền truy cập

Với vai trò là người quản trị bảo mật trong hệ thống A, em hãy trình bày cách thực hiện việc cấp quyền cho nhân sự trong toàn hệ thống theo từng chính sách bảo mật ***CS#i*** và cài đặt chức năng minh hoạ trên ứng dụng.

- Yêu cầu bắt buộc: CS#6 sử dụng cơ chế VPD của Oracle để cài đặt.
- Nếu sinh viên cài đặt thêm các chính sách bảo mật có ứng dụng thực tế trong ngữ cảnh ứng dụng trên thì sẽ được xem xét cộng điểm.

Yêu cầu 2: Vận dụng mô hình điều khiển truy cập OLS

Giả sử nhân sự của khoa được bổ sung thêm người để vận hành tại 2 cơ sở khác nhau gồm: *Cơ sở 1* và *Cơ sở 2*. Khoa muốn thiết lập cho hệ thống chức năng phát tán thông báo, được lưu ở bảng THÔNGBÁO(NỘIDUNG), đến những người dùng trong hệ thống tùy vào cấp bậc, lĩnh vực hoạt động và vị trí địa lý.

Cho biết nhân sự và các dòng thông báo được chia ra làm các cấp bậc sau: *Trưởng khoa, Trưởng đơn vị, Giảng viên, Giáo vụ và Nhân viên*; Độ ưu tiên giảm dần tương ứng là: *Trưởng khoa > Trưởng đơn vị > Giảng viên > Giáo vụ > Nhân viên > Sinh viên*.

Nội dung thông báo thường tùy thuộc vào lĩnh vực hoạt động của các bộ môn có liên quan, gồm: *HTTT, CNPM, KHMT, CNTT, TGMT, MMT*.

Hãy thiết lập hệ thống nhãn gồm 03 thành phần và điều chỉnh mô hình dữ liệu (nếu cần thiết) để hệ thống có thể đáp ứng các yêu cầu sau. Đồng thời, cài đặt chức năng minh hoạ trên ứng dụng.

a) Hãy gán nhãn cho người dùng là *Trưởng khoa* có thể đọc được toàn bộ thông báo.
b) Hãy gán nhãn cho các *Trưởng bộ môn* phụ trách *Cơ sở 2* có thể đọc được toàn bộ thông báo. dành cho trưởng bộ môn không phân biệt vị trí địa lý.
c) Hãy gán nhãn cho 01 *Giáo vụ* có thể đọc toàn bộ thông báo dành cho giáo vụ
d) Hãy cho biết nhãn của dòng thông báo t1 để t1 được phát tán (đọc) bởi tất cả *Trưởng đơn vị.*
e) Hãy cho biết nhãn của dòng thông báo t2 để phát tán t2 đến *Sinh viên* thuộc ngành *HTTT* học ở *Cơ sở 1*.
f) Hãy cho biết nhãn của dòng thông báo t3 để phát tán t3 đến *Trưởng bộ môn KHMT* ở *Cơ sở 1*.
g) Cho biết nhãn của dòng thông báo t4 để phát tán t4 đến *Trưởng bộ môn KHMT* ở *Cơ sở 1 và Cơ sở 2*.
h) Em hãy cho thêm 3 chính sách phát tán dòng dữ liệu nữa trên mô hình OLS đã cài đặt.

Yêu cầu 3: Ghi nhật ký hệ thống

Sinh viên hãy thực hiện cài đặt trên Oracle và Ứng dụng:

1. Kích hoạt việc ghi nhật ký hệ thống.
2. Thực hiện ghi nhật ký hệ thống dùng *Standard audit*: theo dõi hành vi của những user nào trên những đối tượng cụ thể, trên các đối tượng khác nhau (table, view, stored procedure, function), hay chỉ định theo dõi các hành vi hiện thành công hay không thành công.

3. Thực hiện *Fine-grained Audit* các tình huống sau và tạo ngữ cảnh để có thể ghi vết được (có dữ liệu ghi vết) các hành vi sau:
    a. Hành vi Cập nhật quan hệ ĐANGKY tại các trường liên quan đến điểm số nhưng người đó không thuộc vai trò **Giảng viên**.
    b. Hành vi của người dùng này có thể đọc trên trường PHUCAP của người khác ở quan hệ NHANSU.
4. Kiểm tra (đọc xuất) dữ liệu nhật ký hệ thống.

Yêu cầu 4: Sao lưu và phục hồi dữ liệu

Sinh viên hãy tìm hiểu về cơ chế sao lưu và phục hồi dữ liệu do các HQT CSDL cung cấp và cài đặt chức năng sao lưu (chủ động, tự động) và khôi phục dữ liệu dự vào nhật ký hệ thống ở Yêu cầu 3 (sau khi có sự cố).

1. Tìm hiểu các phương pháp thực hiện sao lưu và phục hồi dữ liệu.
2. Hãy hiện thực các phương pháp đó trên HQT CSDL Oracle.
3. Đánh giá ưu khuyết điểm các phương pháp đã tìm hiểu và thử nghiệm.
4. Kết luận.

MỘT SỐ QUY ĐỊNH:

1. Nhóm phải thực hiện cả hai phân hệ, cùng ứng dụng.
2. Chấm đồ án vào ngày thi theo lịch thi chung của Trường (Giữa kỳ, Cuối kỳ).
3. **Cuốn báo cáo đồ án:**
    a. Trình bày giải pháp lý thuyết ngắn gọn, dễ hiểu, ghi rõ tài liệu tham khảo, không dịch lại tài liệu, chủ yếu là phần tóm lược những gì tìm hiểu được, nhận xét, đánh giá, thuyết minh các kết quả đạt được.
    b. Nhóm trưởng làm bảng phân công công việc và đánh giá thành viên trong nhóm (đóng chung trong cuốn đồ án).
4. Nhóm ghi rõ đã cài đặt những chính sách bảo mật cụ thể nào với kịch bản gì. Nhóm *phải* vận dụng và cài đặt *tất cả các cơ chế bảo mật đã học* vào các chính sách bảo mật của đồ án.
5. Nộp cuối kỳ:
    a. Bản in Báo cáo trên giấy nộp vào ngày chấm đồ án; nộp trên Moodle (trước deadline).
    b. Gồm các tập tin MS Word báo cáo (báo cáo cuốn đồ án), Source code, Script CSDL (gồm script schema, data). Tên tập tin đặt theo quy định là *mã sinh viên của các thành viên trong nhóm, cách nhau bởi dấu '_'*. Tất cả tập tin được lưu trong thư mục với tên theo quy định: **ATBM-2024-MãNhóm** (Mã Nhóm xem trong danh sách phân công nhóm đồ án trên Moodle).
6. Tất cả các thành viên của nhóm đều phải có khả năng thực hiện các yêu cầu của đồ án. Bất kỳ sinh viên nào đều có thể được Giáo viên chấm yêu cầu phải thực hiện tại chỗ yêu cầu cài đặt một số chính sách bảo mật.
7. **Bài giống nhau: tất cả thành viên đều 0 điểm môn học.**

Hết