Trường Đại học Khoa học Tự nhiên

Khoa Công nghệ thông tin

LỚP CQ2018 – NĂM HỌC 2020 - 2021

ĐỒ ÁN MÔN HỌC

CSC12001 - AN TOÀN VÀ BẢO MẬT DỮ LIỆU TRONG HTTT

PHÂN HỆ 1: DÀNH CHO NGƯỜI QUẢN TRỊ CƠ SỞ DỮ LIỆU

Sinh viên hãy xây dựng ứng dụng cho phép các người dùng có quyền quản trị thực hiện công việc sau:

- 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.

Sinh viên hãy thực hiện chức năng ghi nhật ký hệ thống (chỉ yêu cầu thực hiện mức HQT CSDL Oracle):

- Admin có quyền enable/ disable việc ghi nhật ký toàn hệ thống.
- Admin được chỉ định ghi nhật ký của những hành động thực hiện bởi những user nào trên những đối tượng cụ thể. Các hành động đó là: đăng nhập, thay đổi thông tin user account, select, insert, update, delete, execute.; các đối tượng là table, view, stored procedure, function. Admin cũng được quyền chọn ghi nhật ký hành động được thực hiện thành công hay không thành công.
- Kiểm tra dữ liệu nhật ký hệ thống. Sinh viên nên đề ra một số kịch bản theo dõi hệ thống để phân tích dữ liệu nhật ký.

PHÂN HỆ 2: QUẢN LÝ THÔNG TIN CỦA MỘT BỆNH VIỆN

Một bệnh viện quy mô vừa có những vai trò sau: bộ phận quản lý, bộ phận tiếp tân và điều phối bệnh, bác sĩ điều trị, phòng tài vụ, phòng bán thuốc và bộ phận kế toán.

Bệnh nhân đến bệnh viện sẽ gặp bộ phận tiếp tân và điều phối bệnh để khai bệnh ban đầu gồm tên, năm sinh, địa chỉ liên lạc, số điện thoại, triệu chứng bệnh. Nếu bệnh nhân trước đó đã khám bệnh thì đọc mã khám bệnh thì thông tin bệnh nhân đã có và không cần phải nhập lại. Sau khi hoàn tất giai đoạn tiếp bệnh, nhân viên tiếp tân chỉ định phòng khám và bác sĩ khám. Tại phòng tài vụ, nhân viên phòng tài vụ nhìn thấy thông tin khám bệnh của bệnh nhân mới sẽ thu tiền khám của bệnh nhân và hướng dẫn bệnh nhân đến gặp bác sĩ. Sau khi xem bệnh, bác sĩ chỉ định và ghi nhận vào CSDL liên quan đến bệnh nhân đó là phải dùng thuốc gì, hoặc phải tiếp tục làm những thủ tục xét nghiệm hoặc chẩn đoán hình ảnh nào. Nhân viên phòng tài vụ căn cứ vào đó thu tiền trước khi bệnh nhân được xét nghiệm hoặc chụp hình theo yêu cầu của bác sĩ. Bộ phận tiếp tân và điều phối bệnh dựa vào dữ liệu của hệ thống ghi lại yêu cầu của bác sĩ sẽ ghi lại trên CSDL thông tin điều phối bệnh vào các phòng liên quan và hướng dẫn bệnh nhân vào phòng nào gặp bác sĩ nào. Sau khi hoàn tất các yêu cầu, bệnh nhân mang kết quả về cho bác sĩ khám bệnh ban đầu đọc kết quả và đề nghị dùng thuốc theo toa bác sĩ kê. Nhân viên phòng thuốc căn cứ vào đó bán thuốc cho bệnh nhân.

Chính sách bảo mật trong ứng dụng trên được mô tả như sau:

- Thành viên của bộ phận quản lý được chia ra làm 3 nhóm: nhóm quản lý tài nguyên và nhân sự (phòng ban, bác sĩ, nhân viên, chấm công), nhóm quản lý tài vụ (đơn giá các loại dịch vụ khám bệnh, đơn giá thuốc), và nhóm quản lý chuyên môn. Nhóm quản lý tài nguyên nhân sự chỉ được thêm, xóa, sửa các thông tin trong cách danh mục như: phòng ban, bác sĩ, nhân viên trong từng phòng ban, bác sĩ nào trực phòng nào vào thời gian nào, …và được xem tất cả các thông tin khác kể cả thông tin nhân viên kế toán tạo ra nhưng không được quyền sửa. Nhóm quản lý tài vụ chỉ được nhập mới chỉnh sửa các thông tin liên quan, những thông tin khác được quyền xem tất cả nhưng không được phép sửa. Nhóm quản lý chuyên môn được xem tất cả thông tin trong đó có thông tin điều trị bệnh của các bác sĩ để theo dõi về chuyên môn của bệnh viện và có chiến lược trong tương lai mà không được chỉnh sửa bất cứ thông tin nào.

- Bộ phận tiếp tân và điều phối bệnh được quyền thêm, xóa, sửa, tìm kiếm thông tin bệnh nhân, được điều phối bệnh nhưng không thể xem các thông tin liên quan đến số tiền cho từng thủ tục khám, xét nghiệm hoặc chụp hình hoặc thông tin thuốc điều trị bệnh cho bệnh nhân.
- Nhân viên phòng tài vụ chỉ nhìn thấy các thủ tục mà bác sĩ yêu cầu bệnh nhân phải làm khi điều trị bệnh, thông tin mà bộ phận điều phối bệnh đã điều phối và tính tiền. Nhân viên phòng tài vụ chỉ được cập nhật số tiền phải trả cho từng chi tiết khám trị bệnh của bệnh nhân mà không được chỉnh sửa bất cứ thông tin gì.
- Bác sĩ: chỉ có thể thêm hoặc sửa thông tin liên quan đến việc điều trị bệnh và các loại thuốc phải dùng, liều dùng cho bệnh nhân mà bác sĩ chịu trách nhiệm điều trị. Bác sĩ không được xem hoặc chỉnh sửa thông tin khác của những bệnh nhân do bác sĩ khác điều trị hoặc những thông tin khác trong hệ thống.
- Nhân viên bộ phận bán thuốc: chỉ có thể nhìn thấy toa thuốc mà bác sĩ kê cho từng bệnh nhân để tính tiền thuốc cho bệnh nhân mà không thể xem được bệnh nhân bệnh gì hay bất cứ thông tin gì khác.
- Nhân viên kế toán: tính lương cho các bác sĩ và các nhân viên khác dựa vào lương cơ bản, phụ cấp, số ngày công. Nhân viên kế toán không nhìn thấy bất cứ thông tin gì trong hệ thống liên quan đến quá trình điều trị bệnh cho bệnh nhân của những bộ phận liên quan.

Yêu cầu:

1. Sinh viên tự thiết kế mô hình dữ liệu và tạo dữ liệu thử cho ứng dụng trên. Hãy dùng các cơ chế bảo mật đã học của Oracle để hiện thực các cơ chế bảo mật đề ra.
2. Sinh viên hãy đề ra bối cảnh sử dụng cơ chế mã hóa trong ứng dụng trên, và dùng thư viện hỗ trợ mã dữ liệu của Oracle. Cho biết mục đích, đối tượng cần bảo vệ dữ liệu bằng phương pháp mã hóa, phương pháp quản lý khóa.
3. Sinh viên hãy đề ra bối cảnh sử dụng cơ chế OLS của Oracle. Nhãn gồm đầy đủ 3 thành phần: level, compartment và group. Hãy gán nhãn cho dữ liệu, người dùng và minh họa chính sách bảo mật đã cài đặt.

4. Nếu sinh viên cài đặt thêm các chính sách bảo mật có ứng dụng thực tế trong ứng dụng đã cho sẽ được xem xét điểm.

MỘT SỐ QUY ĐỊNH:

1. Các nhóm đều làm cả hai phân hệ, cùng ứng dụng.
2. Chấm đồ án vào ngày thi theo lịch thi chung của Trường.
3. Cuốn đồ án: trình bày 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. Nhóm trưởng làm bảng phân công công việc và đánh giá hai thành viên trong nhóm (đóng chung trong cuốn đồ án).

   Ghi rõ nhóm đã cài đặt những chính sách bảo mật cụ thể nào, kịch bản gì. Nhóm cố gắng cài đặt tất cả các cơ chế bảo mật đã học.
4. Nộp file: ngoài bản in nộp vào ngày chấm đồ án, sinh viên phải nộp file trên Moodle, gồm file word báo cáo (file cuốn đồ án), source code. Tên file là mã sinh viên của các thành viên trong nhóm, cách nhau bởi dấu '_'.
5. Chia công việc sao cho tất cả các thành viên của nhóm đều phải thực hiện được yêu cầu của đồ án. Sinh viên có thể được yêu cầu phải thực hiện tại chỗ yêu cầu cài đặt một số chính sách bảo mật.
6. Bài giống nhau: tất cả đều 0 điểm.

HẾT.