Trường Đại học Khoa học Tự nhiên

Khoa Công nghệ thông tin

NĂM HỌC 2021 – 2022, 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.

PHÂN HỆ 2: Sở y tế tỉnh/ thành phố X cần gom dữ liệu về kho dữ liệu D (cấp sở), gồm hồ sơ bệnh án (và một số dữ liệu liên quan) từ các cơ sở y tế trong tỉnh/ thành phố và quản lý chuyên môn về việc khám chữa bệnh của các cơ sở y tế thông qua một hệ thống thông tin quản lý S.

HSBA (<u>MÃHSBA</u>, MÃBN, NGÀY, CHẨNĐOÁN, MÃBS, MÃKHOA, MÃCSYT, KẾTLUẬN): mỗi hồ sơ bệnh án (HSBA) có một mã duy nhất (MÃHSBA), liên quan đến một bệnh nhân (MÃBN), được lập vào một ngày (NGÀY), có chẩn đoán (CHẨNĐOÁN) của bác sĩ điều trị (MÃBS), được tiếp nhận khám và điều trị tại khoa (MÃKHOA), của cơ sở y tế (có mã là MÃCSYT), với kết luận của bác sĩ (KẾTLUẬN).

HSBA_DV (<u>MÃHSBA, MÃDV, NGÀY</u>, MÃKTV, KẾTQUẢ): ghi nhận lại các dịch vụ (thông qua MÃDV) đã sử dụng theo chỉ định của bác sĩ điều trị (ví dụ các loại xét nghiệm, chụp hình, …), người thực hiện dịch vụ (MÃKTV) và kết quả (KẾTQUẢ).

BỆNHNHÂN (MÃBN, MÃCSYT, TÊNBN, CMND, NGÀYSINH, SỐNHÀ, TÊNĐƯỜNG, QUẬNHUYỆN, TỈNHTP, TIỀNSỬBỆNH, TIỀNSỬBỆNHGĐ, DỊỨNGTHUỐC): mỗi bệnh nhân được cơ sở y tế có mã là MÃCSYT cấp mã duy nhất (MÃBN), có tên (TÊNBN), ngày sinh (NGÀYSINH), địa chỉ (SỐNHÀ, TÊNĐƯỜNG, QUẬNHUYỆN), và tiền sử bệnh của bệnh nhân (TIỀNSỬBỆNH) và gia đình (TIỀNSỬBỆNHGĐ), cũng như tình trạng dị ứng thuốc (nếu có, DỊỨNGTHUỐC).

CSYT (MÃCSYT, TÊNCSYT, ĐCCSYT, SĐTCSYT): ghi nhận thông tin về các cơ sở y tế thuộc tỉnh/ thành phố gồm mã, tên, địa chỉ, số điện thoại.

NHÂNVIÊN (MÃNV, HỌTÊN, PHÁI, NGÀYSINH, CMND, QUÊQUÁN, SỐĐT, CSYT, VAITRÒ, CHUYÊNKHOA)

Quan hệ NHÂNVIÊN chứa dữ liệu về các nhân viên trực thuộc cơ sở y tế hoặc thuộc sở y tế có vai trò trong hệ thống S. Mỗi nhân viên có mã (MÃNV) do đơn vị quản lý trực tiếp cấp, giả sử các mã này không trùng nhau trong phạm vi toàn tỉnh/ thành phố. Ngoài ra cũng cần ghi lại thông tin họ tên (HỌTÊN), phái (PHÁI), ngày sinh (NGÀYSINH), số chứng minh nhân dân (CMND), quê quán, số điện thoại, thuộc cơ sở y tế nào (CSYT). Thuộc tính VAITRÒ nhận một trong các giá trị sau: "Thanh tra", "Cơ sở y tế", "Y sĩ/ bác sĩ", "Nghiên cứu".

Với các nhân viên có vai trò "Y sĩ/ bác sĩ" hoặc "Nghiên cứu" thì cần lưu thêm thông tin về chuyên khoa (CHUYÊNKHOA) mà người đó được cấp bằng cấp chuyên môn.

Cơ sở dữ liệu được cài đặt trên **Oracle**. Hệ thống dùng chính sách đóng (người dùng *u* cần được cấp quyền *p* trên đối tượng dữ liệu *o* mới có thể thực hiện *p* trên *o*). DBA trong hệ thống S thực hiện việc cấp quyền cho nhân sự trong toàn hệ thống theo mô tả như sau:

TC#1: Ngoài DBA, tất cả người dùng trong hệ thống S gồm những nhân viên trong quan hệ NHÂNVIÊN và cả những bệnh nhân trong quan hệ BỆNHNHÂN. DBA tạo tài khoản cho tất cả những người dùng này. DBA không tự định nghĩa bảng (table) dùng để quản lý tài khoản người dùng mà sử dụng thông tin tài khoản do Hệ quản trị CSDL Oracle quản lý. Bằng cách nào DBA có thể kết nối một tên tài khoản với 1 dòng dữ liệu là người dùng tương ứng (trong quan hệ NHÂNVIÊN và BỆNHNHÂN) mà không phải truy cập dữ liệu từ nhiều hơn 1 bảng, đồng thời phải ép thỏa các chính sách bảo mật liên quan đến những người dùng này. DBA phụ trách thêm, cập nhật dữ liệu trong bảng CSYT và thêm dữ liệu trong NHÂNVIÊN, gồm những nhân viên thuộc các cơ sở y tế hoặc thuộc sở y tế có vai trò trong hệ thống S.

TC#2: Có 5 nhân viên thuộc sở y tế với vai trò "Thanh tra". Các nhân viên giữ vai trò thanh tra có thể đọc dữ liệu trên tất cả các quan hệ được mô tả để kết xuất báo cáo định kỳ, mà không có quyền thêm, xóa, sửa trên bất cứ quan hệ nào.

TC#3: Mỗi cơ sở y tế được cấp duy nhất 01 tài khoản trên hệ thống S để thao tác trên kho dữ liệu D. Có 50 nhân viên thuộc 50 cơ sở y tế trong tỉnh/ thành phố được cử để sử dụng tài khoản được cấp. Các nhân viên thuộc cơ sở y tế có quyền thêm hoặc xóa dữ liệu phát sinh từ chính cơ sở y tế mà nhân viên này trực thuộc, trong tháng hiện tại từ ngày 5 đến 27 dương lịch hàng tháng, liên quan các nghiệp vụ:

a. Thêm, xóa dòng trên hồ sơ bệnh án (HSBA)

b. Thêm, xóa dòng dịch vụ (HSBA_DV) liên quan 1 hồ sơ bệnh án.

TC#4: Có 500 nhân viên giữ vai trò "Y sĩ/ bác sĩ" trực tiếp khám chữa bệnh cho bệnh nhân ở các cơ sở y tế thuộc tỉnh/ thành phố. Y sĩ/ Bác sĩ có quyền xem hồ sơ bệnh án (HSBA) mà họ đã chữa trị và kết quả về các dịch vụ đã sử dụng (HSBA_DV) và thông tin bệnh nhân (BỆNHNHÂN) khi nhập thông tin mã bệnh nhân hoặc số CMND.

TC#5: Có 50 nhân viên ở vai trò "Nghiên cứu" ở mỗi cơ sở y tế, chỉ có thể xem các hồ sơ bệnh án (bảng HSBA và HSBA_DV) được điều trị tại cùng cơ sơ y tế (với nhân viên nghiên cứu đó), tại khoa giống chuyên khoa ghi trên bằng cấp của nhân viên nghiên cứu đó.

TC#6: Hệ thống hiện tại có khoảng 10000 bệnh nhân. Trên hệ thống S, trừ những người giữ vai trò thanh tra (và DBA), mỗi nhân viên hoặc bệnh nhân đăng nhập chỉ có thể xem thông tin của chính mình, (trên bảng NHÂN VIÊN nếu là nhân viên, trên bảng BỆNH NHÂN nếu là bệnh nhân), và có thể chỉnh sửa các trường (trừ trường mã) liên quan đến chính người đó.

TC#7: Dựa vào chuyên môn, kỹ thuật của đơn vị mà Sở y tế tỉnh/ thành phố X chia các cơ sở y tế trực thuộc thành 3 tuyến:

+ *"Điều trị ngoại trú"*: các cơ sở khám chữa bệnh ban đầu, điều trị ngoại trú.
+ *"Điều trị nội trú"*: các bệnh viện với các kỹ thuật chuyên khoa cơ bản và nâng cao.
+ *"Điều trị chuyên sâu"*: các bệnh viện đa khoa và chuyên khoa thực hiện được các kỹ thuật chuyên sâu.

Ngoài ra, tùy vào vị trí địa lý của cơ sở y tế mà Sở y tế tỉnh/ thành phố X chia ra làm 3 vùng: *trung tâm, cận trung tâm, ngoại thành*. Có sự phân chia vai trò người dùng theo 03 cấp bậc: **Giám đốc sở**, **Giám đốc cơ sở y tế** và **Y/ Bác sĩ**. Sở cần gửi những dòng

trong quan hệ THÔNGBÁO, gồm các trường NỘIDUNG, NGÀYGIỜ và ĐỊAĐIỂM về những cuộc họp khẩn đến các vai trò liên quan ở các cơ sở y tế. Dùng OLS (Oracle Label Security). Hãy thiết lập hệ thống nhãn và thiết lập 5 loại người dùng khác nhau. Cho minh họa cách phát tán dữ liệu.

Sinh viên có thể mô tả bổ sung cho hệ thống dễ hiểu hơn. Sinh viên cũng có điều chỉnh mô hình dữ liệu để phục vụ tốt cho các quy trình xử lý.

Yêu cầu:

1. Hãy dùng các cơ chế bảo mật đã học của Oracle để hiện thực các chính sách bảo mật đặt ra ở các TC#i, $1 \leq i \leq 6$.

Ở tiêu chí TC#7, 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 cho các kịch bản đã nêu, và các kịch bản khác (nếu có thể).

2. Sinh viên hãy đề xuất bối cảnh vận 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 dữ liệu cần bảo vệ dữ liệu bằng phương pháp mã hóa, phương pháp quản lý khóa.
3. Sinh viên hãy thực hiện chức năng ghi nhật ký hệ thống (audit, chỉ yêu cầu thực hiện mức HQT CSDL Oracle):
   - Kích hoạt việc ghi nhật ký toàn hệ thống.
   - 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.
   - Thực hiện Fine-grained Audit một số tình huống và cho kịch bản minh họa.
   - Kiểm tra dữ liệu nhật ký hệ thống.
4. 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.

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.