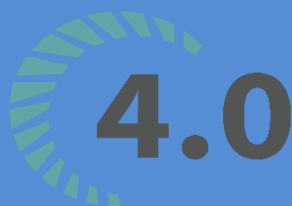


BỘ MÔN HỆ THỐNG THÔNG TIN – KHOA CÔNG NGHỆ THÔNG TIN
ĐẠI HỌC KHOA HỌC TỰ NHIÊN THÀNH PHỐ HỒ CHÍ MINH, ĐẠI HỌC QUỐC GIA TP HCM

MÔN AN TOÀN BẢO MẬT HỆ THỐNG THÔNG TIN






Sinh viên thực hiện: 19127372 – Đặng Nguyễn Duy
19127460 – Nguyễn Nhật Linh
19127635 – Hồ Nguyễn Lê Vy

ĐỒ ÁN MÔN HỌC – AN TOÀN BẢO MẬT HỆ THỐNG THÔNG TIN
HỌC KỲ II – NĂM HỌC 2021 – 2022



BẢNG THÔNG TIN CHI TIẾT NHÓM

| | | | |
|------------------------|---|--|---|
| Mã nhóm: | 05 | | |
| Số lượng: | 3 | | |
| Link GitHub | https://github.com/honguyenlevy/QuanLyBenhVien | | |
| Link video demo | https://youtu.be/Nps6FfzPVxA | | |
| MSSV | Họ tên | Email | Hình ảnh |
| 19127372 | Đặng Nguyễn Duy | 19127372@student.hcmus.edu.vn |  |
| 19127460 | Nguyễn Nhật Linh | 19127460@student.hcmus.edu.vn |  |
| 19127635 | Hồ Nguyễn Lê Vy | 19127635@student.hcmus.edu.vn |  |

MỤC LỤC

| | |
|--|----|
| MỤC LỤC | 3 |
| PHẦN 1: XÁC THỰC VÀ ỦY QUYỀN | 5 |
| I. XÁC THỰC (AUTHENTICATION) | 5 |
| 1. Giới thiệu | 5 |
| 2. Các nhân tố xác thực của authentication | 5 |
| 3. Phân loại..... | 7 |
| 4. Authentication sẽ được thực hiện ra sao?..... | 8 |
| II. ỦY QUYỀN (AUTHORIZATION)..... | 8 |
| III. AUTHENTICATION VS AUTHORIZATION..... | 9 |
| PHẦN 2: ĐIỀU KHIỂN TRUY CẬP..... | 10 |
| I. GIỚI THIỆU | 10 |
| II. TẠI SAO CẦN KIỂM SOÁT QUYỀN TRUY CẬP..... | 10 |
| III. ACCESS CONTROL HOẠT ĐỘNG NHƯ THẾ NÀO..... | 11 |
| IV. CÁC LOẠI ACCESS CONTROL..... | 12 |
| 1. Mandatory Access Control (MAC) | 12 |
| 2. Discretionary Access Control (DAC) | 14 |
| 3. Role – based Access Control..... | 17 |



| | |
|---|----|
| 4. Rule – base Access Control | 20 |
| 5. Attributed – Based Access Control..... | 22 |
| PHẦN 3: PRIVILEGES TRONG ORACLE | 26 |
| I. USER VÀ SCHEMA | 26 |
| 1. User..... | 26 |
| 2. Schema..... | 26 |
| II. SYSTEM PRIVILEGES | 26 |
| III. OBJECT PRIVILEGES | 28 |
| IV. ROLE | 29 |
| PHẦN 4: DEMO GIAO DIỆN VÀ ĐÁNH GIÁ..... | 31 |
| I. GIAO DIỆN..... | 31 |
| II. ĐÁNH GIÁ..... | 36 |
| TÀI LIỆU THAM KHẢO..... | 37 |

PHẦN 1: XÁC THỰC VÀ ỦY QUYỀN

I. XÁC THỰC (AUTHENTICATION)

1. Giới thiệu

- Authentication (tạm dịch: xác thực) là quá trình kiểm tra danh tính một tài khoản đang vào hệ thống hiện tại thông qua một hệ thống xác thực. Đây là bước ban đầu của mọi hệ thống có yếu tố người dùng.
- Nếu không có bước xác thực này, hệ thống sẽ không biết được người đang truy cập vào hệ thống là ai để có các phản hồi phù hợp.
- Quá trình này rất thông dụng trong hầu hết các CMS liên quan đến quản lý, tương tác người dùng thông qua form đăng ký (login form) và nó được xác thực dựa trên tên người dùng và mật khẩu (password-based authentication).

2. Các nhân tố xác thực của authentication

2.1. Mật khẩu (Password & Pin)

- Mật khẩu là một trong những phương pháp đơn giản và dễ triển khai nhất.
- Khi người dùng truy cập, mỗi hệ thống sẽ lưu lại mật khẩu ở dạng đã được mã hóa một chiều (MD5, SHA1, tự chế...). Tính năng này sẽ đảm bảo mật khẩu có bị hack cũng không thể khôi phục thành chuỗi gốc.
- Phương pháp này còn có nhiều biến thể như thiết kế dạng Swipe Pattern PIN (trong các điện thoại android) hoặc mật khẩu dùng một lần (dùng cho các chức năng quan trọng).

2.2. Khóa (*Public-key cryptography*)

- Phương pháp này dựa trên thuật toán mã hóa khóa công cộng (public key) và khóa cá nhân (private key).
- Để đăng nhập vào hệ thống, ta chỉ cần có khóa cá nhân (private key) trên máy và đăng nhập vào hệ thống (nếu đã khai báo với khóa công cộng của chúng ta) mà không cần phải nhớ thông tin gì về đăng nhập như phương pháp mật khẩu.
- Các hệ thống quản trị server thường áp dụng cách này.

2.3. Sinh học (*Biometrics*)

- Dùng như dấu vân tay, tròng mắt hoặc khuôn mặt là phương pháp dựa trên các yếu tố đặc trưng của con người để xác thực.
- Ưu điểm của phương pháp này là “ID” và “mật khẩu” luôn đi cùng nhau nên không cần lo lắng bị quên hay lạc mất. Mỗi khi cần đăng nhập vào hệ thống, ta đều chủ động sử dụng dễ dàng mà không gặp bất cứ khó khăn gì.
- Dù có nhiều phương pháp để xác thực một tài khoản, tuy nhiên cũng không tránh khỏi rủi ro khi triển khai như mất mật khẩu, mất khóa cá nhân, bị đánh cắp vân tay...
- Áp dụng trên website, phương thức mật khẩu có vẻ là dễ triển khai và có nhiều lợi thế hơn vì thường thao tác trên màn hình và độ chính xác cao.
- Chúng ta có thể cải tiến hệ thống bảo mật hơn như theo dõi thói quen đăng nhập, địa điểm, IP, trình duyệt, mật khẩu một lần...

3. Phân loại

3.1. HTTP Basic Authentication

- HTTP Basic Authentication là một kỹ thuật xác thực nhằm bảo mật cho ứng dụng web trên giao thức http, yêu cầu người dùng cung cấp tên truy cập và mật khẩu khi sử dụng ứng dụng.
- Web server thu thập thông tin và danh tính người dùng (username & password) qua một hộp thoại trên Browser.
- Khi muốn bảo mật một tài nguyên, ta có thể sử dụng nhiều cách nhưng có một cách khác đơn giản để bảo vệ là dùng HTTP Authentication.

3.2. Multi-factor Authentication (MFA)

- Xác thực đa nhân tố (viết tắt: MFA) là một hệ thống bảo mật yêu cầu nhiều phương thức xác thực từ các danh mục thông tin đăng nhập độc lập để xác minh danh tính của người dùng cho thông tin đăng nhập hoặc giao dịch khác.
- Xác thực multi-factor kết hợp hai hoặc nhiều thông tin độc lập:
 - Password: mật khẩu.
 - Security token: mã thông báo bảo mật.
 - Biometric verification: xác minh sinh trắc học.
- Tạo một lớp bảo vệ – tường thành vững chắc gây khó khăn cho một người không được phép truy cập vào một mục tiêu cụ thể, như: vị trí thực tế, thiết bị máy tính, mạng hoặc cơ sở dữ liệu là mục tiêu của MFA.

- Nếu một yếu tố xác thực bị xâm phạm, kẻ tấn công vẫn phải vượt qua ít nhất một rào cản nữa để vi có thể xâm nhập trái phép thành công vào mục tiêu.

4. Authentication sẽ được thực hiện ra sao?

Để có được các dấu hiệu nhận dạng, thì buộc phải có sự thống nhất giữa người dùng và ứng dụng để có thể thực hiện được quá trình nhận dạng.

Mỗi một quá trình Authentication sẽ bao gồm 3 phần là:

- Phát sinh ra các dấu hiệu: Đây là lúc chúng ta quyết định xem nên lựa chọn và sử dụng dấu hiệu gì và dùng cách nào để tạo ra dấu hiệu đó. Mỗi một quá trình Authentication sẽ có sự xuất hiện của nhiều dấu hiệu như: password/username, user token, api key, ... Mỗi một dấu hiệu này đều sẽ có cách sinh ra khác nhau bởi quy ước sử dụng khác biệt.
- Lưu trữ cho các dấu hiệu: Đây là một trong những bước quyết định xem bạn nên lưu trữ dấu hiệu này ở đâu. Bạn nên lưu ở cả client và server hay thông qua vị trí nào của bản tin HTTP.
- Kiểm tra các dấu hiệu: Đây là điều mà ứng dụng của chúng ta để kiểm tra lại các tích hợp lệ của dấu hiệu, từ đó đối chiếu xem lại các dấu hiệu này của của người dùng nào, ...

II. ỦY QUYỀN (AUTHORIZATION)

- Authorization xảy ra sau khi hệ thống của được authentication (xác thực) thành công, cuối cùng cho phép toàn quyền truy cập các tài nguyên như thông tin, file, cơ sở dữ liệu, quỹ, địa điểm, hầu hết mọi thứ. Nói một cách đơn giản, authorization xác định khả năng của người dùng để truy cập hệ thống và ở mức độ nào. Khi danh tính của

người dùng được hệ thống xác minh sau khi xác thực thành công, họ sẽ được phép truy cập tài nguyên của hệ thống.

- Authorization là quá trình để xác định xem người dùng được xác thực có quyền truy cập vào các tài nguyên cụ thể hay không. Nó xác minh quyền để cấp cho người dùng quyền truy cập vào các tài nguyên như thông tin, cơ sở dữ liệu, file, v.v. Authorization thường được đưa ra sau khi xác thực xác nhận các đặc quyền của người dùng để thực hiện. Nói một cách đơn giản hơn, nó giống như cho phép ai đó chính thức làm điều gì đó hoặc bất cứ điều gì.
- Ví dụ, quy trình xác minh và xác nhận ID nhân viên và mật khẩu trong một tổ chức được gọi là authentication, nhưng xác định nhân viên nào có quyền truy cập vào tầng nào được gọi là authorization.

III. AUTHENTICATION VS AUTHORIZATION

| Authentication | Authorization |
|---|---|
| Authentication xác nhận danh tính của bạn để cấp quyền truy cập vào hệ thống. | Authorization xác định xem bạn có được phép truy cập tài nguyên không. |
| Đây là quá trình xác nhận thông tin đăng nhập để có quyền truy cập của người dùng. | Đó là quá trình xác minh xem có cho phép truy cập hay không. |
| Nó quyết định liệu người dùng có phải là những gì anh ta tuyên bố hay không. | Nó xác định những gì người dùng có thể và không thể truy cập. |
| Authentication thường yêu cầu tên người dùng và mật khẩu. | Các yếu tố xác thực cần thiết để authorization có thể khác nhau, tùy thuộc vào mức độ bảo mật. |
| Authentication là bước đầu tiên của authorization vì vậy luôn luôn đến trước. | Authorization được thực hiện sau khi authentication thành công. |
| Ví dụ, sinh viên của một trường đại học cụ thể được yêu cầu tự xác thực trước khi truy cập vào liên kết sinh viên của trang web chính thức của trường đại học. Điều này được gọi là authentication. | Ví dụ, authorization xác định chính xác thông tin nào sinh viên được phép truy cập trên trang web của trường đại học sau khi authentication thành công. |

PHẦN 2: ĐIỀU KHIỂN TRUY CẬP

I. GIỚI THIỆU

- Access Control là một kỹ thuật bảo mật quy định ai hoặc những gì có thể xem hoặc sử dụng tài nguyên trong môi trường máy tính. Đây là một khái niệm cơ bản trong bảo mật nhằm giảm thiểu rủi ro cho doanh nghiệp hoặc tổ chức.
- Có hai loại Access Control: vật lý và logic. Access Control vật lý giới hạn quyền truy cập vào khuôn viên, tòa nhà, phòng và tài sản CNTT vật lý. Access Control logic giới hạn kết nối với mạng máy tính, tệp hệ thống và dữ liệu.
- Access Control cơ sở dữ liệu là một phương pháp chỉ cho phép truy cập vào dữ liệu nhạy cảm của công ty đối với những người (người dùng cơ sở dữ liệu) được phép truy cập vào dữ liệu đó và hạn chế quyền truy cập của những người không được phép. Nó bao gồm hai thành phần chính: xác thực và ủy quyền.

II. TẠI SAO CẦN KIỂM SOÁT QUYỀN TRUY CẬP

- Mục tiêu của kiểm soát truy cập là giảm thiểu rủi ro bảo mật của việc truy cập trái phép vào các hệ thống vật lý và logic. Kiểm soát truy cập là một thành phần cơ bản của các chương trình tuân thủ bảo mật nhằm đảm bảo công nghệ bảo mật và các chính sách kiểm soát truy cập được áp dụng để bảo vệ thông tin bí mật, chẳng hạn như dữ liệu khách hàng. Hầu hết các tổ chức có cơ sở hạ tầng và thủ tục hạn chế quyền truy cập vào mạng, hệ thống máy tính, ứng dụng, tệp và dữ liệu nhạy cảm, chẳng hạn như thông tin nhận dạng cá nhân (PII) và tài sản trí tuệ.

- Hệ thống kiểm soát truy cập rất phức tạp và có thể khó quản lý trong môi trường CNTT động liên quan đến các hệ thống tại chỗ và dịch vụ đám mây. Sau một số vi phạm cấp cao, các nhà cung cấp công nghệ đã chuyển từ hệ thống đăng nhập một lần (SSO) sang quản lý truy cập thống nhất, cung cấp các biện pháp kiểm soát truy cập cho môi trường tại chỗ và đám mây.

III. ACCESS CONTROL HOẠT ĐỘNG NHƯ THẾ NÀO

Hệ thống kiểm soát truy cập cơ sở dữ liệu hoạt động trên ba mặt: người dùng, quản trị viên và cơ sở hạ tầng.

- **User:** Khi một nhân viên muốn truy cập vào dữ liệu bị hạn chế, họ phải cung cấp thông tin xác thực của họ. Yêu cầu mở khóa được thực hiện tại đầu đọc thẻ, thiết bị này sẽ gửi thông tin đến Access Control Unit, sau đó cho phép người dùng mở khóa.
- **Administrator:** Hệ thống kiểm soát truy cập có trang tổng quan hoặc cổng thông tin quản lý ở phía quản trị. Quản trị viên văn phòng, người quản lý CNTT và giám đốc bảo mật có thể sử dụng cổng kiểm soát để chỉ định ai có quyền truy cập vào cơ sở và trong những điều kiện nào.
- **System Infrastructure:** Cơ sở hạ tầng của hệ thống kiểm soát truy cập bao gồm khóa điện, đầu đọc thẻ, trạng thái cửa để giám sát giao thông và yêu cầu thoát thiết bị, tất cả đều báo cáo cho bảng điều khiển và máy chủ.

IV. CÁC LOẠI ACCESS CONTROL

1. Mandatory Access Control (MAC)

1.1. Giới thiệu

- Mandatory Access Control (MAC) là một mô hình kiểm soát truy cập trong đó hệ điều hành cung cấp cho người dùng quyền truy cập dựa trên mức độ bảo mật của dữ liệu và người dùng. Trong mô hình này, quyền truy cập được cấp trên cơ sở cần biết: người dùng phải chứng minh nhu cầu thông tin trước khi đạt được quyền truy cập.
- MAC được coi là an toàn nhất trong tất cả các mô hình kiểm soát truy cập. Các quy tắc truy cập được xác định theo cách thủ công bởi quản trị viên hệ thống và được thực thi nghiêm ngặt bởi hệ điều hành hoặc nhân bảo mật. Người dùng thông thường không thể thay đổi các thuộc tính bảo mật ngay cả đối với dữ liệu họ đã tạo.
- Với MAC, quá trình “giành” quyền truy cập như sau
 - Người quản trị cấu hình các chính sách truy cập và xác định các thuộc tính bảo mật: mức độ bảo mật, khoảng trống để truy cập các dự án và các loại tài nguyên khác nhau.
 - Người quản trị chỉ định mỗi chủ thể (người dùng hoặc tài nguyên truy cập dữ liệu) và đối tượng (tệp, cơ sở dữ liệu, công, v.v.) một tập hợp các thuộc tính.
 - Khi một chủ thể cố gắng truy cập một đối tượng, hệ điều hành sẽ kiểm tra các thuộc tính bảo mật của đối tượng và quyết định xem có thể cấp quyền truy cập hay không.

1.2. Ưu, nhược điểm của MAC

| Ưu điểm | Nhược điểm |
|---|--|
| Mức độ bảo vệ dữ liệu cao - Quản trị viên xác định quyền truy cập vào các đối tượng và người dùng không thể chỉnh sửa quyền truy cập đó. | Khả năng bảo trì - Việc cấu hình thủ công các cấp độ bảo mật yêu cầu sự quan tâm thường xuyên của các quản trị viên. |
| Granular - Quản trị viên đặt quyền truy cập của người dùng và các tham số truy cập đối tượng theo cách thủ công. | Khả năng mở rộng - MAC không tự động mở rộng quy mô. |
| Miễn nhiễm với các cuộc tấn công Trojan Horse - Người dùng không thể giải mật dữ liệu hoặc chia sẻ quyền truy cập vào dữ liệu đã phân loại. | Không thân thiện với người dùng - Người dùng phải yêu cầu quyền truy cập vào từng phần dữ liệu mới; họ không thể định cấu hình các thông số truy cập cho dữ liệu của riêng mình. |

1.3. Khi nào nên sử dụng MAC

- MAC được chính phủ Hoa Kỳ sử dụng để bảo mật thông tin đã phân loại và hỗ trợ các ứng dụng và chính sách bảo mật đa cấp. Mô hình kiểm soát truy cập này hầu hết được sử dụng bởi các tổ chức chính phủ, quân đội và các cơ quan thực thi pháp luật. Sẽ là hợp lý khi sử dụng MAC trong các tổ chức coi trọng bảo mật dữ liệu hơn tính linh hoạt trong hoạt động và chi phí. Việc triển khai MAC trong một tổ chức tư nhân là rất hiếm vì sự phức tạp và không linh hoạt của một hệ thống như vậy.
- Mô hình MAC thuần túy cung cấp mức độ bảo mật cao và chi tiết. Mặt khác, rất khó để thiết lập và duy trì. Đó là lý do tại sao người ta thường kết hợp MAC với các mô hình kiểm soát truy cập khác.

- Ví dụ: kết hợp nó với mô hình dựa trên vai trò sẽ tăng tốc cấu hình hồ sơ người dùng. Thay vì xác định quyền truy cập cho từng người dùng, quản trị viên có thể tạo vai trò người dùng. Mỗi tổ chức có những người dùng có vai trò và quyền truy cập tương tự: nhân viên có cùng vị trí công việc, nhà cung cấp bên thứ ba, v.v. Quản trị viên có thể định cấu hình vai trò cho các nhóm này thay vì định cấu hình hồ sơ người dùng riêng lẻ từ đầu.
- Một sự kết hợp phổ biến khác là MAC và mô hình kiểm soát truy cập tùy ý (DAC). MAC có thể được sử dụng để bảo mật dữ liệu nhạy cảm, trong khi DAC cho phép đồng nghiệp chia sẻ thông tin trong hệ thống tệp công ty.

2. Discretionary Access Control (DAC)

2.1. Giới thiệu

- Discretionary Access Control (DAC) là một mô hình kiểm soát truy cập dựa trên danh tính cung cấp cho người dùng một lượng kiểm soát nhất định đối với dữ liệu của họ. Chủ sở hữu dữ liệu (hoặc bất kỳ người dùng nào được ủy quyền kiểm soát dữ liệu) có thể xác định quyền truy cập cho người dùng hoặc nhóm người dùng cụ thể.
- Quyền truy cập cho từng phần dữ liệu được lưu trữ trong danh sách kiểm soát truy cập (ACL). Danh sách này có thể được tạo tự động khi người dùng cấp quyền truy cập cho ai đó hoặc có thể được tạo bởi quản trị viên. ACL bao gồm những người dùng và nhóm có thể truy cập dữ liệu và các cấp độ truy cập

mà họ có thể có. Một ACL cũng có thể được thực thi bởi quản trị viên hệ thống. Trong trường hợp này, ACL hoạt động như một chính sách bảo mật và người dùng thông thường không thể chỉnh sửa hoặc ghi đè nó

– Việc “giành” quyền truy cập trong mô hình DAC hoạt động như sau:

- Người dùng 1 tạo một tệp và trở thành chủ sở hữu của nó hoặc có được quyền truy cập vào một tệp hiện có.
- Người dùng 2 yêu cầu quyền truy cập vào tệp này.
- Người dùng 1 cấp quyền truy cập theo quyết định của riêng họ. Tuy nhiên, người dùng 1 không thể cấp quyền truy cập vượt quá quyền của họ. Ví dụ: nếu người dùng 1 chỉ có thể đọc một tài liệu, thì họ không thể cho phép người dùng 2 chỉnh sửa tài liệu đó.
- Nếu không có mâu thuẫn nào giữa ACL do quản trị viên tạo và quyết định của người dùng 1, thì quyền truy cập sẽ được cấp.

2.2. Ưu, nhược điểm của DAC

| Ưu điểm | Nhược điểm |
|---|---|
| Thân thiện với người dùng - Người dùng có thể quản lý dữ liệu của mình và nhanh chóng truy cập dữ liệu của những người dùng khác. | Mức độ bảo vệ dữ liệu thấp - DAC không thể đảm bảo tính bảo mật đáng tin cậy vì người dùng có thể chia sẻ dữ liệu của họ theo cách họ muốn. |
| Linh hoạt - Người dùng có thể định cấu hình các thông số truy cập dữ liệu mà không cần quản trị viên. | Ít người biết đến - Không có quản lý truy cập tập trung, vì vậy để tìm ra các thông số truy cập, bạn phải kiểm tra từng ACL. |

| Ưu điểm | Nhược điểm |
|--|------------|
| Dễ bảo trì - Thêm đối tượng mới và người dùng không mất nhiều thời gian cho quản trị viên. | |
| Granular - Người dùng có thể cấu hình các thông số truy cập cho từng phần dữ liệu. | |

2.3. Khi nào nên sử dụng DAC

- DAC rất linh hoạt và giảm tải cho quản trị viên hệ thống vì người dùng có thể tự quản lý quyền truy cập. Mặt khác, nó không cung cấp mức độ bảo mật cao vì một số lý do:
 - Nếu người dùng 1 chia sẻ quyền truy cập với người dùng 2, không có gì đảm bảo rằng người dùng 2 cần quyền truy cập này để làm việc hoặc sẽ không đánh cắp hoặc làm hỏng dữ liệu hoặc cấp quyền truy cập cho người dùng độc hại.
 - Không thể kiểm soát các luồng thông tin bên trong mạng.
 - Không thể thực thi các nguyên tắc về đặc quyền ít nhất, cần biết và tách bạch các nhiệm vụ.
- Do những hạn chế này, DAC không thể được sử dụng bởi các tổ chức làm việc với dữ liệu cực kỳ nhạy cảm (y tế, tài chính, quân sự, v.v.).
- Đồng thời, DAC là một lựa chọn tốt cho các doanh nghiệp nhỏ với số lượng nhân viên CNTT và ngân sách an ninh mạng hạn chế. Nó cho phép chia sẻ thông tin và đảm bảo hoạt động

trơn tru của doanh nghiệp. Cách tiếp cận này, khi được áp dụng trong một tổ chức có từ 10 đến 20 nhân viên, thiếu sự phức tạp và những thách thức giám sát liên quan đến việc sử dụng DAC trong các tổ chức có hàng trăm hoặc hàng nghìn nhân viên.

3. Role – based Access Control

3.1. Giới thiệu

- Trong an ninh đối với các hệ thống máy tính, Role-Based Access Control (viết tắt là RBAC) là một trong số các phương pháp điều khiển và đảm bảo quyền sử dụng cho người dùng. Đây là một phương pháp có thể thay thế Discretionary Access Control - DAC và Mandatory Access Control - MAC.
- Điều khiển truy cập trên cơ sở vai trò (RBAC) khác với hình thức MAC và DAC truyền thống. MAC và DAC trước đây là hai mô hình duy nhất được phổ biến trong điều khiển truy cập. Nếu một hệ thống không dùng MAC thì người ta chỉ có thể cho rằng hệ thống đó dùng DAC, hoặc ngược lại, mà thôi. Song cuộc nghiên cứu trong những năm 1990 đã chứng minh rằng RBAC không phải là MAC hoặc DAC.
- Trong nội bộ một tổ chức, các vai trò (roles) được kiến tạo để đảm nhận các chức năng công việc khác nhau. Mỗi vai trò được gắn liền với một số quyền hạn cho phép nó thao tác một số hoạt động cụ thể (permissions). Các thành viên trong lực lượng cán bộ công nhân viên (hoặc những người dùng trong hệ thống) được phân phối một vai trò riêng, và thông qua việc

phân phối vai trò này mà họ tiếp thu được một số những quyền hạn cho phép họ thi hành những chức năng cụ thể trong hệ thống.

- Vì người dùng không được cấp phép một cách trực tiếp, song chỉ tiếp thu được những quyền hạn thông qua vai trò của họ (hoặc các vai trò), việc quản lý quyền hạn của người dùng trở thành một việc đơn giản, và người ta chỉ cần chỉ định những vai trò thích hợp cho người dùng mà thôi. Việc chỉ định vai trò này đơn giản hóa những công việc thông thường như việc cho thêm một người dùng vào trong hệ thống, hay đổi ban công tác (department) của người dùng.

3.2. Một số quy ước

Khi định nghĩa một mô hình RBAC, những quy ước sau đây là những quy ước hữu dụng và cần phải cân nhắc:

- $U = (\text{User})$ Người dùng = Một người hoặc một tác nhân tự động.
- $R = (\text{Role})$ Vai trò = Chức năng công việc / Danh hiệu dùng định nghĩa một cấp bậc quyền thế.
- $P = \text{Quyền được cấp}$ = Sự phê chuẩn một hình thức truy cập tài nguyên.
- $S = (\text{Session})$ Phiên giao dịch = Một xếp đặt liên kết giữa U , R và P
- $UA = (\text{User Assignment})$ Chỉ định người dùng.
- $PA = (\text{Permission Assignment})$ Cấp phép

- RH = (Role Hierarchy) Sắp xếp trật tự một phần nào theo thứ tự cấp bậc của vai trò.
- Một người dùng có thể có nhiều vai trò.
- Một vai trò có thể có thể có nhiều người dùng.
- Một vai trò có thể có nhiều phép được cấp cho nó.
- Một phép được cấp có thể được chỉ định cho nhiều vai trò.

3.3. Ưu điểm của RBAC

Quản lý và kiểm tra truy cập mạng là điều cần thiết để bảo mật thông tin. Quyền truy cập có thể và nên được cấp trên cơ sở cần biết. Với hàng trăm hoặc hàng nghìn nhân viên, bảo mật được duy trì dễ dàng hơn bằng cách hạn chế quyền truy cập không cần thiết vào thông tin nhạy cảm dựa trên vai trò thiết lập của mỗi người dùng trong tổ chức. Các lợi thế khác bao gồm:

- **Giảm bớt công việc hành chính và hỗ trợ CNTT.** Với RBAC, ta có thể giảm nhu cầu về thủ tục giấy tờ và thay đổi mật khẩu khi nhân viên được thuê hoặc thay đổi vai trò của họ. Thay vào đó, có thể sử dụng RBAC để thêm và chuyển đổi các vai trò một cách nhanh chóng và triển khai chúng trên toàn cầu trên các hệ điều hành, nền tảng và ứng dụng. Nó cũng làm giảm khả năng xảy ra lỗi khi chỉ định quyền của người dùng. Việc giảm thời gian dành cho các công việc hành chính chỉ là một trong số những lợi ích kinh tế của RBAC. RBAC cũng giúp tích hợp người dùng bên thứ ba vào mạng dễ dàng hơn bằng cách cấp cho họ các vai trò được xác định trước.

- **Tối đa hóa hiệu quả hoạt động.** RBAC đưa ra một cách tiếp cận hợp lý và hợp lý về mặt định nghĩa. Thay vì cố gắng quản lý kiểm soát truy cập cấp thấp hơn, tất cả các vai trò có thể phù hợp với cơ cấu tổ chức của doanh nghiệp và người dùng có thể thực hiện công việc của họ một cách hiệu quả và tự chủ hơn.
- **Cải thiện sự tuân thủ.** Tất cả các tổ chức đều phải tuân theo các quy định của liên bang, tiểu bang và địa phương. Với hệ thống RBAC, các công ty có thể dễ dàng đáp ứng các yêu cầu luật định và quy định về quyền riêng tư và bảo mật vì các bộ phận CNTT và giám đốc điều hành có khả năng quản lý cách dữ liệu được truy cập và sử dụng. Điều này đặc biệt quan trọng đối với các tổ chức tài chính và chăm sóc sức khỏe, những tổ chức quản lý nhiều dữ liệu nhạy cảm như dữ liệu PHI và PCI.

4. Rule – base Access Control

4.1. Khái niệm

Rule – base Access Control quản lý quyền truy cập vào các khu vực, thiết bị hoặc cơ sở dữ liệu theo một bộ quy tắc định trước hoặc quyền truy cập bất kể vai trò hoặc vị trí của họ trong tổ chức.

4.2. Rule – base Access Control hoạt động như thế nào

- Trong kiểm soát truy cập dựa trên quy tắc, quản trị viên sẽ đặt hệ thống bảo mật để cho phép mục nhập dựa trên các tiêu chí đặt trước. Ví dụ: trong cài đặt kiểm soát truy cập dựa trên quy

tắc, quản trị viên có thể đặt giờ truy cập cho ngày làm việc thông thường. Trong trường hợp này, một người không thể vào tòa nhà của bạn ngoài khung giờ từ 9 giờ sáng đến 5 giờ chiều.

- Các bước trong kiểm soát truy cập dựa trên quy tắc là:
 - Các quy tắc truy cập được tạo bởi quản trị viên hệ thống.
 - Các quy tắc được tích hợp trong toàn bộ hệ thống kiểm soát truy cập.
 - Một người trưng bày thông tin xác thực truy cập của họ, chẳng hạn như keyfob hoặc điện thoại di động.
 - Cơ chế kiểm soát kiểm tra thông tin xác thực của họ dựa trên các quy tắc truy cập.
 - Người được cấp hoặc từ chối quyền truy cập.

4.3. Lợi ích của Role – based Access Control

- Chi tiết và tính linh hoạt là động lực chính để các doanh nghiệp áp dụng Role – based Access Control
- Đối với các tổ chức lớn hơn, có thể có giá trị trong việc có các chính sách kiểm soát truy cập linh hoạt. Quản trị viên hệ thống chỉ có thể hạn chế quyền truy cập vào các bộ phận của tòa nhà trong những ngày nhất định trong tuần.
- Tính linh hoạt của quyền truy cập là một lợi ích chính cho việc áp dụng Role – based Access Control

5. Attributed – Based Access Control

5.1. Giới thiệu

- Attributed – Based Access Control (ABAC) là một mô hình ủy quyền đánh giá các thuộc tính (hoặc đặc điểm), thay vì vai trò, để xác định quyền truy cập. Mục đích của ABAC là bảo vệ các đối tượng như dữ liệu, thiết bị mạng và tài nguyên CNTT khỏi hành động và người dùng trái phép – những đối tượng không có đặc điểm "được chấp thuận" như được xác định bởi chính sách bảo mật của tổ chức.
- ABAC như một hình thức kiểm soát truy cập logic đã trở nên nổi bật trong thập kỷ qua, đã phát triển từ danh sách kiểm soát truy cập đơn giản và kiểm soát truy cập dựa trên vai trò (RBAC). Là một phần của sáng kiến giúp các tổ chức liên bang cải thiện kiến trúc kiểm soát truy cập của họ, Hội đồng Giám đốc Thông tin Liên bang đã tán thành ABAC vào năm 2011. Họ đã đề xuất ABAC là mô hình áp dụng cho các tổ chức chia sẻ thông tin một cách an toàn.

5.2. Thành phần chính của ABAC

Với ABAC, các chính sách truy cập của một tổ chức thực thi các quyết định truy cập dựa trên các thuộc tính của chủ thể, tài nguyên, hành động và môi trường liên quan đến một sự kiện truy cập.

– Subject

Chủ thể là người dùng yêu cầu quyền truy cập vào một tài nguyên để thực hiện một hành động. Các thuộc tính chủ đề trong hồ sơ người dùng bao gồm ID, vai trò công việc, thành viên nhóm, thành viên phòng ban và tổ chức, cấp quản lý, giải pháp bảo mật và các tiêu chí nhận dạng khác. Hệ thống ABAC thường lấy dữ liệu này từ hệ thống nhân sự hoặc thư mục, hoặc

thu thập thông tin này từ mã thông báo xác thực được sử dụng trong quá trình đăng nhập.

– **Resources**

Tài nguyên là nội dung hoặc đối tượng (chẳng hạn như tệp, ứng dụng, máy chủ hoặc thậm chí là API) mà chủ thể muốn truy cập. Các thuộc tính tài nguyên là tất cả các đặc điểm nhận dạng, như ngày tạo tệp, chủ sở hữu, tên và loại tệp cũng như độ nhạy của dữ liệu. Ví dụ: khi cố gắng truy cập vào tài khoản ngân hàng trực tuyến của bạn, tài nguyên liên quan sẽ là “tài khoản ngân hàng = <số tài khoản chính xác>”

– **Action**

Hành động là những gì người dùng đang cố gắng thực hiện với tài nguyên. Các thuộc tính hành động phổ biến bao gồm “đọc”, “viết”, “chỉnh sửa”, “sao chép” và “xóa”. Trong một số trường hợp, nhiều thuộc tính có thể mô tả một hành động. Để tiếp tục với ví dụ về ngân hàng trực tuyến, yêu cầu chuyển khoản có thể có các đặc điểm “loại hành động = chuyển khoản” và “số tiền = 200 đô la”.

– **Environment**

Môi trường là bối cảnh rộng hơn của mỗi yêu cầu truy cập. Tất cả các thuộc tính môi trường đều nói lên các yếu tố ngữ cảnh như thời gian và vị trí của nỗ lực truy cập, thiết bị của đối tượng, giao thức liên lạc và cường độ mã hóa. Thông tin theo ngữ cảnh cũng có thể bao gồm các tín hiệu rủi ro mà tổ chức đã thiết lập, chẳng hạn như cường độ xác thực và các mẫu hành vi bình thường của chủ thể.

5.3. Ưu điểm của ABAC

– **Hoạch định chính sách chi tiết nhưng linh hoạt**

- Lợi ích chính của ABAC là tính linh hoạt của nó. Về cơ bản, giới hạn cho việc hoạch định chính sách nằm ở những thuộc tính nào phải được tính đến và các điều kiện mà ngôn ngữ tính toán có thể diễn đạt. ABAC cho phép phạm vi rộng lớn nhất của các đối tượng truy cập vào lượng tài

nguyên lớn nhất mà không yêu cầu quản trị viên chỉ định mối quan hệ giữa từng chủ thể và đối tượng. Lấy các bước sau làm ví dụ:

- ✓ Khi một chủ thể tham gia vào một tổ chức, họ sẽ được chỉ định một tập hợp các thuộc tính của chủ thể (ví dụ: John Doe là chuyên gia tư vấn cho khoa X quang).
- ✓ Một đối tượng, khi được tạo, sẽ được gán các thuộc tính của nó (ví dụ: một thư mục chứa các tệp xét nghiệm hình ảnh tim cho bệnh nhân tim).
- ✓ Sau đó, quản trị viên hoặc chủ sở hữu đối tượng tạo quy tắc kiểm soát truy cập (ví dụ: “Tất cả các chuyên gia tư vấn cho khoa X quang có thể xem và chia sẻ các tệp xét nghiệm hình ảnh tim cho bệnh nhân tim”).
- Quản trị viên có thể sửa đổi thêm các thuộc tính này và các quy tắc kiểm soát truy cập để phù hợp với nhu cầu của tổ chức. Ví dụ: khi xác định các chính sách truy cập mới cho các chủ thể bên ngoài như nhà thầu và nhà cung cấp, họ có thể làm như vậy mà không cần thay đổi từng mối quan hệ chủ thể-đối tượng theo cách thủ công. ABAC cho phép nhiều tình huống truy cập khác nhau mà không cần giám sát hành chính.
- **Khả năng tương thích với người dùng mới**
 - Với ABAC, quản trị viên và chủ sở hữu đối tượng có thể tạo các chính sách cho phép các đối tượng mới truy cập tài nguyên. Miễn là các đối tượng mới được chỉ định các thuộc tính cần thiết để truy cập các đối tượng (ví dụ: tất cả

các chuyên gia tư vấn cho khoa X quang đều được chỉ định các thuộc tính đó), thì không cần phải sửa đổi các quy tắc hoặc thuộc tính đối tượng hiện có.

- Mô hình ABAC cho phép các tổ chức nhanh nhẹn khi giới thiệu nhân viên mới và tạo điều kiện cho các đối tác bên ngoài.

– **Bảo mật nghiêm ngặt và quyền riêng tư**

- Thông qua việc sử dụng các thuộc tính, ABAC cho phép các nhà hoạch định chính sách kiểm soát nhiều biến số tình huống, đảm bảo quyền truy cập trên cơ sở chi tiết. Ví dụ, trong mô hình RBAC, các nhóm nhân sự có thể luôn có quyền truy cập vào thông tin nhạy cảm của nhân viên, chẳng hạn như dữ liệu bảng lương và thông tin nhận dạng cá nhân. Với ABAC, quản trị viên có thể thực hiện các hạn chế truy cập thông minh phù hợp với ngữ cảnh — ví dụ: nhân viên nhân sự chỉ có thể có quyền truy cập vào thông tin này vào những thời điểm nhất định hoặc chỉ dành cho nhân viên trong văn phòng chi nhánh có liên quan.
- Do đó, ABAC cho phép các tổ chức thu hẹp hiệu quả các lỗ hổng bảo mật và tôn trọng quyền riêng tư của nhân viên, đồng thời tuân thủ hiệu quả các yêu cầu tuân thủ quy định.

PHẦN 3: PRIVILEGES TRONG ORACLE

I. USER VÀ SCHEMA

1. User

- Mỗi cơ sở dữ liệu Oracle có một danh sách những người dùng cơ sở dữ liệu hợp lệ.
- Để truy cập cơ sở dữ liệu, người dùng phải kết nối với cá thể cơ sở dữ liệu bằng cách sử dụng tên người dùng hợp lệ được xác định trong cơ sở dữ liệu.
- Người dùng đã được cấp đặc quyền hệ thống CREATE USER có thể tạo tài khoản người dùng.
- Bởi vì đặc quyền hệ thống CREATE USER là một đặc quyền mạnh mẽ, quản trị viên cơ sở dữ liệu hoặc quản trị viên bảo mật thường là người dùng duy nhất có đặc quyền hệ thống này.

2. Schema

- Một schema là một tập hợp các đối tượng cơ sở dữ liệu.
- Một schema thuộc sở hữu của người dùng cơ sở dữ liệu và có cùng tên với người dùng đó.
- Đối tượng schema là cấu trúc logic do người dùng tạo ra.
- Mọi đối tượng trong cơ sở dữ liệu thuộc về một schema và có một tên duy nhất trong schema đó

II. SYSTEM PRIVILEGES

- System Privileges là quyền thực hiện một hành động cụ thể hoặc thực hiện một hành động trên bất kỳ đối tượng nào thuộc một loại cụ thể. Các đối tượng bao gồm tables, views, materialized views,

synonyms, indexes, sequences, cache groups, replication schemes and PL/SQL functions, procedures và packages. Chỉ quản trị viên phiên bản hoặc người dùng có đặc quyền ADMIN mới có thể cấp hoặc thu hồi các đặc quyền hệ thống.

– Ví dụ

| Loại | Ví dụ |
|---------|--|
| INDEX | CREATE ANY INDEX ALTER ANY INDEX DROP ANY INDEX |
| TABLE | CREATE TABLE CREATE ANY TABLE ALTER ANY TABLE DROP ANY TABLE SELECT ANY TABLE UPDATE ANY TABLE DELETE ANY TABLE |
| SESSION | CREATE SESSION ALTER SESSION RETRICTED SESSION |

| Loại | Ví dụ |
|------------|---|
| TABLESPACE | CREATE TABLESPACE ALTER TABLESPACE DROP TABLESPACE |
| USER | CREATE USER DROP USER |

III. OBJECT PRIVILEGES

- Object Privileges là quyền thực hiện một hành động cụ thể trên một đối tượng hoặc truy cập đối tượng của người dùng khác. Các đối tượng bao gồm bảng, khung nhìn, khung nhìn cụ thể hóa, chỉ mục, từ đồng nghĩa, chuỗi, nhóm bộ đệm, lược đồ sao chép và các hàm, thủ tục và gói PL / SQL.
- Chủ sở hữu của một đối tượng có tất cả các đặc quyền đối tượng cho đối tượng đó và không thể thu hồi những đặc quyền đó. Chủ sở hữu của đối tượng có thể cấp đặc quyền đối tượng cho đối tượng đó cho những người dùng cơ sở dữ liệu khác. Người dùng có đặc quyền QUẢN TRỊ có thể cấp và thu hồi các đặc quyền đối tượng từ những người dùng không sở hữu đối tượng được cấp đặc quyền.
- Ví dụ

| Privilege | Object type | Description |
|------------|--|--|
| DELETE | Table | Enables a user to delete from a table. |
| EXECUTE | PL/SQL package, procedure or function | Enables a user to execute a PL/SQL package, procedure or function directly. |
| FLUSH | Cache group | Enables a user to flush a cache group. |
| INDEX | Table or materialized view | Enables a user to create an index on a table or materialized view. |
| INSERT | Table or synonym | Enables a user to insert into a table or into the table through a synonym. |
| LOAD | Cache group | Enables a user to load a cache group. |
| REFERENCES | Table or materialized view | <p>Enables a user to create a foreign key dependency on a table or materialized view.</p> <p>The REFERENCES privilege on a parent table implicitly grants SELECT privilege on the parent table.</p> |
| REFRESH | Cache group | Enables a user to refresh a cache group. |
| SELECT | Table, sequence, view, materialized view, or synonym | <p>Enables a user to select from a table, sequence, view, materialized view, or synonym.</p> <p>The SELECT privilege enables a user to perform all operations on a sequence.</p> <p>A user can be granted the SELECT privilege on a synonym or a view without being explicitly granted the SELECT privilege on the originating table.</p> |
| UNLOAD | Cache group | Enables a user to unload a cache group. |
| UPDATE | Table | Enables a user to update a table. |

IV. ROLE

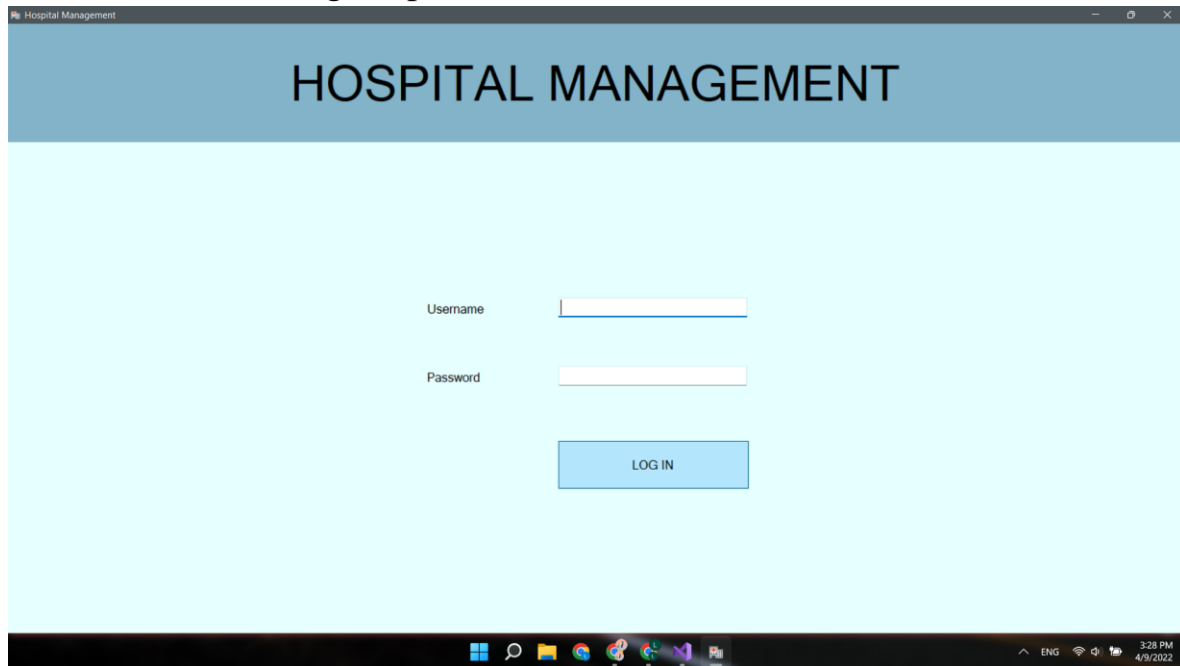
- User Privileges là quyền thực thi một loại câu lệnh SQL cụ thể hoặc quyền truy cập đối tượng của người dùng khác. Các loại đặc quyền được xác định bởi Oracle.
- Mặt khác, các ROLE được tạo bởi người dùng (thường là quản trị viên) và được sử dụng để nhóm các đặc quyền lại với nhau hoặc các vai trò khác. Chúng là một phương tiện tạo điều kiện thuận lợi cho việc cấp nhiều đặc quyền hoặc vai trò cho người dùng.

- ROLE nhóm một số đặc quyền và vai trò để chúng có thể được cấp và thu hồi từ người dùng đồng thời. Một ROLE phải được bật cho người dùng trước khi người dùng có thể sử dụng ROLE đó.
- Oracle cung cấp một số ROLE được xác định trước để trợ giúp trong việc quản trị cơ sở dữ liệu. Các ROLE này được tự động xác định cho cơ sở dữ liệu Oracle khi chạy các tập lệnh tiêu chuẩn là một phần của quá trình tạo cơ sở dữ liệu. Chúng ta có thể cấp các đặc quyền và vai trò cũng như thu hồi các đặc quyền và vai trò từ những ROLE được xác định trước này theo cách giống như cách ta làm với bất kỳ vai trò nào chúng ta xác định.

PHẦN 4: DEMO GIAO DIỆN VÀ ĐÁNH GIÁ

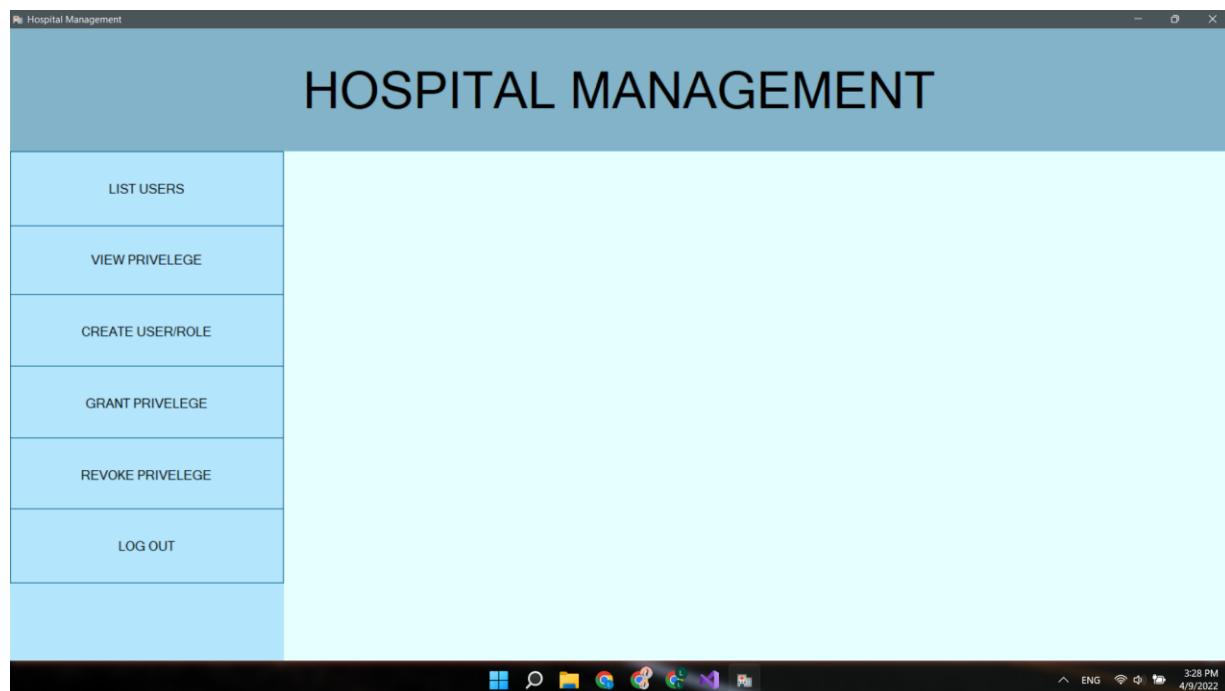
I. GIAO DIỆN

– Màn hình đăng nhập



The screenshot shows a web application window titled "Hospital Management". The main heading "HOSPITAL MANAGEMENT" is centered at the top. Below it, there are two input fields: "Username" and "Password". A blue "LOG IN" button is positioned below the password field. The background is a light blue gradient. The Windows taskbar at the bottom shows the time as 3:28 PM on 4/9/2022.

– Màn hình chính



The screenshot shows the main menu of the "Hospital Management" application. The heading "HOSPITAL MANAGEMENT" is at the top. On the left side, there is a vertical list of menu items: "LIST USERS", "VIEW PRIVELEGE", "CREATE USER/ROLE", "GRANT PRIVELEGE", "REVOKE PRIVELEGE", and "LOG OUT". The background is a light blue gradient. The Windows taskbar at the bottom shows the time as 3:28 PM on 4/9/2022.

– Xem danh sách User

Hospital Management

HOSPITAL MANAGEMENT

| LIST USERS | USERNAME | ACCOUNT_STATUS | DEFAULT_TABLESPACE | CREATED | AUTHENTICATION_TYPE |
|------------|-------------------|----------------|--------------------|-------------------|---------------------|
| | SYS | OPEN | SYSTEM | 9/28/2021 4:32 AM | PASSWORD |
| | SYSTEM | OPEN | SYSTEM | 9/28/2021 4:32 AM | PASSWORD |
| | X\$NULL | LOCKED | SYSTEM | 9/28/2021 4:39 AM | NONE |
| | OJMSYS | LOCKED | SYSTEM | 9/28/2021 6:44 AM | NONE |
| | LBACSYS | LOCKED | SYSTEM | 9/28/2021 7:38 AM | NONE |
| | OUTLN | LOCKED | SYSTEM | 9/28/2021 4:32 AM | NONE |
| | DBSNMP | LOCKED | SYSAUX | 9/28/2021 5:06 AM | NONE |
| | APPQOSSYS | LOCKED | SYSAUX | 9/28/2021 5:07 AM | NONE |
| | GGSYS | LOCKED | SYSAUX | 9/28/2021 5:07 AM | NONE |
| | ANONYMOUS | LOCKED | SYSAUX | 9/28/2021 5:18 AM | NONE |
| | DBSFUSER | LOCKED | SYSAUX | 9/28/2021 4:39 AM | NONE |
| | CTXSYS | LOCKED | SYSAUX | 9/28/2021 6:58 AM | NONE |
| | DVSYS | LOCKED | SYSAUX | 9/28/2021 7:40 AM | NONE |
| | DVF | LOCKED | SYSAUX | 9/28/2021 7:40 AM | NONE |
| | AUDSYS | LOCKED | SYSAUX | 9/28/2021 4:32 AM | NONE |
| | GSMADMIN_INTERNAL | LOCKED | SYSAUX | 9/28/2021 4:39 AM | NONE |
| | OLAPSYS | LOCKED | SYSAUX | 9/28/2021 7:10 AM | NONE |
| | MDSYS | LOCKED | SYSAUX | 9/28/2021 7:13 AM | NONE |
| | XDB | LOCKED | SYSAUX | 9/28/2021 5:18 AM | NONE |
| | WMSYS | LOCKED | SYSAUX | 9/28/2021 6:35 AM | NONE |
| | GSMCATUSER | LOCKED | USERS | 9/28/2021 5:07 AM | NONE |
| | LINH123 | OPEN | USERS | 4/9/2022 2:26 PM | PASSWORD |
| | MDDATA | LOCKED | USERS | 9/28/2021 7:13 AM | NONE |
| | BACSI | OPEN | USERS | 4/9/2022 3:02 PM | PASSWORD |
| | SYSBACKUP | LOCKED | USERS | 9/28/2021 4:32 AM | NONE |

– Xem danh sách quyền

Hospital Management

HOSPITAL MANAGEMENT

| LIST USERS | Column | | | | |
|----------------|------------|-------|---------------|-----------|-----------|
| VIEW PRIVELEGE | GRANTEE | OWNER | TABLE_NAME | PRIVILEGE | GRANTABLE |
| | LINH | QTV | HSBA | SELECT | YES |
| | TAM | QTV | HSBA | SELECT | NO |
| | TAM | QTV | DOCGIA | SELECT | YES |
| | TAM | QTV | DOCGIA | UPDATE | YES |
| | TAM | QTV | PHIEUMUONSACH | SELECT | YES |
| | TAM | QTV | PHIEUMUONSACH | INSERT | YES |
| | TAM | QTV | PHIEUMUONSACH | UPDATE | YES |
| | DOCGIA6 | QTV | THUVIEN | DELETE | YES |
| | THUTHU8 | QTV | PHIEUMUONSACH | INSERT | NO |
| | R_GIAOVU | QTV | BENHNHAN | SELECT | NO |
| | R_GIAOVU | QTV | BENHNHAN | INSERT | NO |
| | LINH | QTV | BENHNHAN | UPDATE | YES |
| | GIAOVIEI | QTV | DOCGIA | UPDATE | NO |
| | LINH | QTV | CSYT | SELECT | YES |
| | TAMLINH | QTV | HSBA | UPDATE | YES |
| | TAMLINH | QTV | HSBA_DV | UPDATE | YES |
| | ROLE_BACSI | QTV | CSYT | UPDATE | NO |
| | TAMLINH | QTV | CSYT | SELECT | NO |
| | TAM | QTV | BENHNHAN | DELETE | YES |
| | TAM | QTV | HSBA | DELETE | YES |
| | QUANLI7 | QTV | BENHNHAN | SELECT | YES |
| | LINH | QTV | HSBA | INSERT | NO |
| | LINH | QTV | HSBA | DELETE | NO |

– Xem danh sách quyền theo cột

Hospital Management

HOSPITAL MANAGEMENT

LIST USERS

VIEW PRIVELEGE

CREATE USER/ROLE

GRANT PRIVELEGE

REVOKE PRIVELEGE

LOG OUT

Column

| GRANTEE | TABLE_NAME | COLUMN_NAME | PRIVILEGE | GRANTABLE |
|-------------------|--------------------|-------------|-----------|-----------|
| QUANLI7 | BENHNHAN | TINHTP | INSERT | YES |
| LINH | HSBA | MAHSBA | INSERT | NO |
| R_GIAOVU | SACH | MASACH | INSERT | NO |
| R_GIAOVU | HSBA_DV | NGAY | INSERT | NO |
| TAM | BENHNHAN | MABN | INSERT | YES |
| TAM | BENHNHAN | TIENSUBENH | INSERT | YES |
| TAM | BENHNHAN | QUANHUYEN | INSERT | YES |
| TAMLINH | HSBA_DV | MAHSBA | INSERT | YES |
| GIAOVUEN | DOCGIA | CMND | INSERT | NO |
| LINH123 | BENHNHAN | MABN | INSERT | YES |
| BACSI | HSBA | MABS | INSERT | YES |
| LINH | HSBA | MAHSBA | UPDATE | NO |
| IMP_FULL_DATABASE | KETS_CLIENT_CONFIG | FIELD_3 | UPDATE | NO |
| IMP_FULL_DATABASE | KETS_CLIENT_CONFIG | FIELD_2 | UPDATE | NO |
| IMP_FULL_DATABASE | KETS_CLIENT_CONFIG | FIELD_1 | UPDATE | NO |

Windows taskbar: 3:29 PM 4/9/2022

– Tạo User

Hospital Management

HOSPITAL MANAGEMENT

LIST USERS

VIEW PRIVELEGE

CREATE USER/ROLE

GRANT PRIVELEGE

REVOKE PRIVELEGE

LOG OUT

CREATE USER/ROLE

DELETE USER/ROLE

ALTER USER/ROLE

Username

Role ☐

Password

Confirm Password

CREATE

Windows taskbar: 3:29 PM 4/9/2022

– Xóa User

HOSPITAL MANAGEMENT

LIST USERS | CREATE USER/ROLE | **DELETE USER/ROLE** | ALTER USER/ROLE

VIEW PRIVELEGE | ☐ Role | Selected User/Role | DROP

| USERNAME | ACCOUNT_STATUS | DEFAULT_TABLESPACE | CREATED | AUTHENTICATION_TYP | LAST_LOGIN |
|----------|----------------|--------------------|--------------------|--------------------|-------------------|
| LINH123 | OPEN | USERS | 4/9/2022 2:26 PM | PASSWORD | |
| BACSI | OPEN | USERS | 4/9/2022 3:02 PM | PASSWORD | |
| 19127544 | OPEN | USERS | 3/22/2022 7:36 PM | PASSWORD | |
| LINH | OPEN | USERS | 3/29/2022 7:36 PM | PASSWORD | 4/9/2022 8:45 AM |
| TAMLINH | OPEN | USERS | 4/1/2022 9:30 AM | PASSWORD | |
| 19127468 | OPEN | USERS | 3/22/2022 7:36 PM | PASSWORD | |
| 1001 | OPEN | USERS | 3/22/2022 7:36 PM | PASSWORD | |
| 19127635 | OPEN | USERS | 3/22/2022 7:36 PM | PASSWORD | |
| GIAOVU | OPEN | USERS | 3/22/2022 7:36 PM | PASSWORD | |
| 19127460 | OPEN | USERS | 3/22/2022 7:36 PM | PASSWORD | 3/22/2022 7:37 PM |
| 1000 | OPEN | USERS | 3/22/2022 7:36 PM | PASSWORD | 3/22/2022 7:39 PM |
| TAM | OPEN | USERS | 3/30/2022 10:34 PM | PASSWORD | |
| 19127372 | OPEN | USERS | 3/22/2022 7:36 PM | PASSWORD | |

– Revoke Privileges của User

HOSPITAL MANAGEMENT

LIST USERS | **REVOKE PRIVELEGE FROM USER** | REVOKE PRIVELEGE FROM ROLE | REVOKE ROLE FROM USER

VIEW PRIVELEGE | User | Load Privilege

CREATE USER/ROLE | Privilege | Object | Revoke

GRANT PRIVELEGE

REVOKE PRIVELEGE

LOG OUT

– Revoke Privileges của Role

Hospital Management

HOSPITAL MANAGEMENT

LIST USERS
REVOKE PRIVELEGE FROM USER
REVOKE PRIVELEGE FROM ROLE
REVOKE ROLE FROM USER

VIEW PRIVELEGE
Role:
Load

CREATE USER/ROLE
Privilege: Object:
Revoke

GRANT PRIVELEGE

| GRANTEE | TABLE_NAME | PRIVILEGE | GRANTABLE | TYPE |
|----------|------------------|-----------|-----------|-----------|
| R_GIAOVU | BENHNHAN | SELECT | NO | TABLE |
| R_GIAOVU | BENHNHAN | INSERT | NO | TABLE |
| R_GIAOVU | SACH | SELECT | NO | TABLE |
| R_GIAOVU | SACH | UPDATE | NO | TABLE |
| R_GIAOVU | SACH | DELETE | NO | TABLE |
| R_GIAOVU | NHANVIEN | SELECT | NO | TABLE |
| R_GIAOVU | SINHVIEN | SELECT | NO | TABLE |
| R_GIAOVU | MONHOC | SELECT | NO | TABLE |
| R_GIAOVU | HIEUCHINH_DANGKY | EXECUTE | NO | PROCEDURE |
| R_GIAOVU | THEM_SINHVIEN | EXECUTE | NO | PROCEDURE |
| R_GIAOVU | THEM_MONHOC | EXECUTE | NO | PROCEDURE |
| R_GIAOVU | DANGKY | SELECT | NO | TABLE |
| R_GIAOVU | THEM_DANGKY | EXECUTE | NO | PROCEDURE |

REVOKE PRIVELEGE

LOG OUT

ENG 3:29 PM 4/9/2022

– Revoke Role từ User

Hospital Management

HOSPITAL MANAGEMENT

LIST USERS
REVOKE PRIVELEGE FROM USER
REVOKE PRIVELEGE FROM ROLE
REVOKE ROLE FROM USER

VIEW PRIVELEGE
User:
Load

CREATE USER/ROLE
Role:
Revoke

GRANT PRIVELEGE

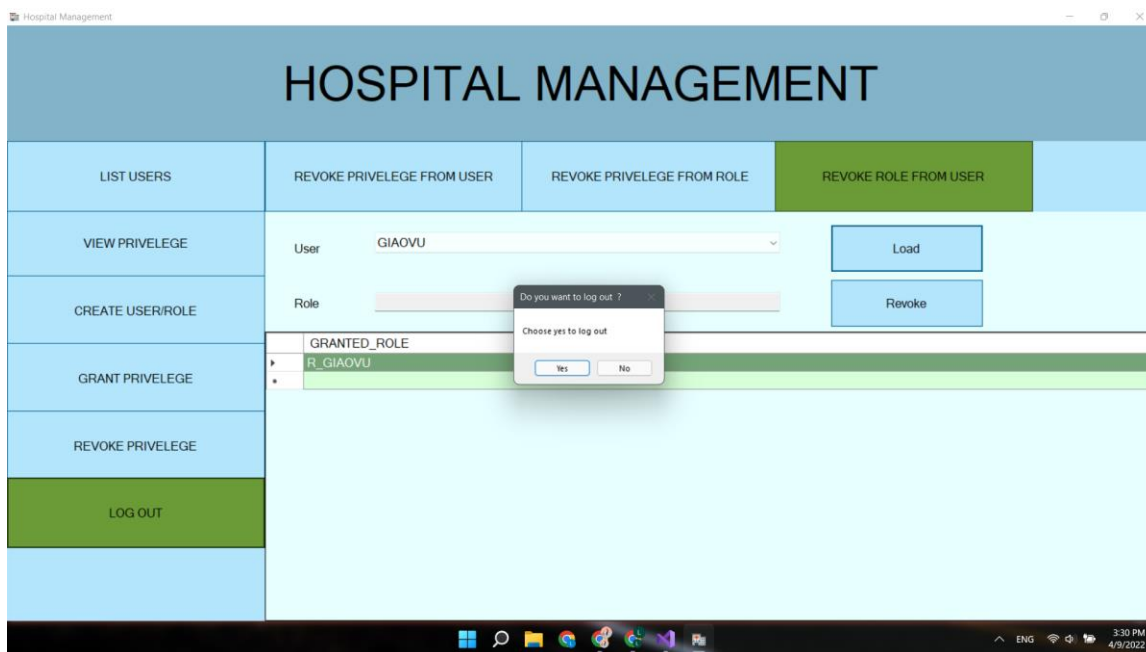
| GRANTED_ROLE |
|--------------|
| R_GIAOVU |

REVOKE PRIVELEGE

LOG OUT

ENG 3:30 PM 4/9/2022

– Log out



II. ĐÁNH GIÁ

| Yêu cầu | Mức độ hoàn thành | Ghi chú |
|--|-------------------|--|
| Xem danh sách người dùng. | 100% | |
| Thông tin về quyền của user/role | 100% | |
| Tạo mới, xóa, sửa user/role | 100% | |
| Cho phép thực hiện cấp quyền cho user, cho role, cấp role cho user | 80% | Chưa thực hiện được cấp quyền select đến mức cột |
| Thu hồi quyền | 100% | |
| Kiểm tra quyền | 100% | |

TÀI LIỆU THAM KHẢO

<https://wiki.tino.org/authentication-la-gi/>

<https://itnavi.com.vn/blog/authentication-la-gi>

<https://viblo.asia/p/phan-biet-su-khac-nhau-giua-authentication-va-authorization-Eb85oad4Z2G>

<https://ladigi.vn/dieu-khien-truy-cap-bat-buoc-la-gi-chi-tiet-ve-dieu-khien-truy-cap-bat-buoc-moi-nhat-2021>

<https://www.ekransystem.com/en/blog/mac-vs-dac>

https://vi.wikipedia.org/wiki/%C4%90i%E1%BB%81u_khi%E1%BB%83n_truy_c%E1%BA%ADp_tr%C3%AAn_c%C6%A1_s%E1%BB%9F_vai_tr%C3%B2

<https://digitalguardian.com/blog/what-role-based-access-control-rbac-examples-benefits-and-more>

<https://www.okta.com/blog/2020/09/attribute-based-access-control-abac/>