

**ĐẠI HỌC QUỐC GIA THÀNH PHỐ HỒ CHÍ MINH
TRƯỜNG ĐẠI HỌC KHOA HỌC TỰ NHIÊN
KHOA CÔNG NGHỆ THÔNG TIN**



BÁO CÁO ĐỒ ÁN

AN TOÀN VÀ BẢO MẬT DỮ LIỆU TRONG HỆ THỐNG THÔNG TIN

**ỨNG DỤNG QUẢN LÝ THÔNG TIN
VÀ CÔNG VIỆC CỦA NHÂN VIÊN**

Giảng viên hướng dẫn: TS. Phạm Thị Bạch Huệ
ThS. Lê Vĩ Minh
ThS. Tiết Gia Hồng

Nhóm thực hiện: Nhóm 20H3T-16
Lớp: 20_21

Thành phố Hồ Chí Minh, tháng 6/2023

MỤC LỤC

MỤC LỤC	2
MỤC LỤC HÌNH ẢNH	3
1. TỔNG QUAN	5
1.1. Thông tin chung	5
1.2. Thông tin thành viên	5
1.3. Đánh giá tham gia	5
2. PHÂN CHIA CÔNG VIỆC	6
2.1. Phân hệ 1	6
2.2. Phân hệ 2	7
3. ĐÁNH GIÁ MỨC ĐỘ HOÀN THÀNH	8
4. NỘI DUNG BÁO CÁO	9
4.1. Thông tin đồ án	9
4.2. Phân hệ 1: Hệ thống dành cho người quản trị bảo mật	9
4.2.1. Màn hình đăng nhập	9
4.2.2. Màn hình chính	10
4.2.3. Màn hình chức năng xem danh sách người dùng hệ thống	11
4.2.4. Màn hình cho chức năng xem bảng và view	12
4.2.5. Màn hình cho phép thực hiện việc cấp quyền, thu hồi quyền, và xem quyền hiện có của người dùng	12
4.2.6. Màn hình cho xem quyền hệ thống của người dùng	14
4.2.7. Màn hình cho phép thêm, xóa, chỉnh sửa thông tin user/ role	17
4.3. Phân hệ 2: Hiện thực các chính sách bảo mật	18
4.3.1. Tính năng hệ thống	18
4.3.2. Lược đồ CSDL	29
4.3.3. Các chính sách bảo mật	29
4.3.4. Mã hóa	42
4.3.5. Audit:	46
5. HƯỚNG DẪN SỬ DỤNG	54
6. TÀI LIỆU THAM KHẢO	54

MỤC LỤC HÌNH ẢNH

Hình 1. Giao diện đăng nhập.....	10
Hình 2. Giao diện màn hình chính	10
Hình 3. Giao diện xem danh sách người dùng	11
Hình 4. Giao diện xem bảng và view trong cơ sở dữ liệu	12
Hình 5. Giao diện thực hiện việc cấp quyền	13
Hình 6. Giao diện cấp quyền Role cho User	14
Hình 7. Màn hình kiểm tra quyền user.....	15
Hình 8. Kết quả kiểm tra quyền user.....	15
Hình 9. Giao diện kiểm tra quyền của Role	16
Hình 10. Kết quả kiểm tra quyền Role.....	16
Hình 11. Giao diện thao tác với User/Role	17
Hình 12. Giao diện vai trò Nhân viên xem và sửa thông tin cá nhân.....	19
Hình 13. Giao diện vai trò Nhân viên xem Phòng ban.....	19
Hình 14. Giao diện vai trò Nhân viên xem bảng Đề Án	20
Hình 15. Giao diện vai trò Nhân viên xem phân công của mình	20
Hình 16. Giao diện vai trò Quản lý xem được nhân viên mình quản lý.....	21
Hình 17. Giao diện vai trò Quản lý xem được phân công của mình và nhân viên mình quản lý...22	
Hình 18. Giao diện vai trò Trưởng phòng chỉ xem được nhân viên phòng ban mình quản lý	23
Hình 19. Giao diện vai trò Trưởng phòng thêm, xóa, sửa phân công phòng ban mình quản lý	23
Hình 20. Giao diện vai trò Tài chính xem được toàn bộ quan hệ NHANVIEN	24
Hình 21. Giao diện vai trò Tài chính xem được toàn bộ quan hệ PHANCONG	25
Hình 22. Giao diện vai trò Tài chính sửa lương của Nhân viên.....	25
Hình 23. Giao diện vai trò Tài chính sửa phụ cấp của Nhân viên.....	26
Hình 24. Giao diện vai trò Nhân sự thêm, cập nhật trên quan hệ PHONGBAN	27
Hình 25. Giao diện vai trò Nhân sự thêm, cập nhật trên quan hệ NHANVIEN	27
Hình 26. Giao diện vai trò Trưởng đề án thêm, xóa, sửa trên quan hệ DEAN	28
Hình 27. Lược đồ cơ sở dữ liệu quan hệ được cài đặt.....	29
Hình 28. Giao diện hiển thị các thông báo cho một giám đốc có thể đọc được toàn bộ dữ liệu	37
Hình 29. Giao diện hiển thị các thông báo mà Trưởng phòng sản xuất miền Nam có quyền đọc	38
Hình 30. Giao diện hiển thị các thông báo mà các giám đốc ở miền Bắc có quyền đọc	39
Hình 31. Giao diện phát tán dòng thông báo t1.....	40
Hình 32. Giao diện phát tán dòng thông báo t2	40
Hình 33. Giao diện hiển thị các dòng thông báo mà Nhân viên sản xuất tại miền Nam có thể đọc.....	41

Hình 34. Giao diện hiển thị dòng thông báo được phát tán cho toàn bộ Nhân viên.	42
Hình 35. Giao diện chức năng Standard Audit	51
Hình 36. Giao diện chức năng Fine Gained Audit	51
Hình 37. Giao diện chức năng Trigger Audit	52

1. TỔNG QUAN

1.1. Thông tin chung

- Thông tin nhóm: Nhóm 20H3T-16
- Số lượng thành viên: 4 người

1.2. Thông tin thành viên

STT	MSSV	Họ và tên	Email
1	20120255	Phạm Mai Thiên Bảo	20120255@student.hcmus.edu.vn
2	20120295	Ngô Võ Quang Huy	20120295@student.hcmus.edu.vn
3	20120305	Võ Thị Kiều Khanh	20120305@student.hcmus.edu.vn
4	20120318	Nguyễn Lê Mỹ Linh	20120318@student.hcmus.edu.vn

1.3. Đánh giá tham gia

STT	Họ và tên	Mức độ hoàn thành (%)	Mức độ đóng góp (%)
1	Phạm Mai Thiên Bảo	100	25
2	Ngô Võ Quang Huy	100	25
3	Võ Thị Kiều Khanh	100	25
4	Nguyễn Lê Mỹ Linh	100	25

2. PHÂN CHIA CÔNG VIỆC

2.1. Phân hệ 1

STT	Nội dung công việc	Phụ trách	Đánh giá của nhóm
1	<ul style="list-style-type: none"> Tạo form cho phép tạo mới, xóa, sửa, user hoặc role. Cho phép thu hồi quyền từ người dùng/role. Làm file hướng dẫn chạy 	20120255	10/10
2	<ul style="list-style-type: none"> Tạo form cho phép kiểm tra quyền của các chủ thể vừa dc cấp quyền Tạo form cho phép chỉnh sửa quyền của user/role Quay video demo 	20120295	10/10
3	<ul style="list-style-type: none"> Tạo form chức năng đăng nhập, trang chủ, cấp quyền cho user, cấp quyền cho role, cấp role cho user Tạo giao diện quyền hiện có của 1 user/role Phân chia công việc Tổng hợp code 	20120305	10/10
4	<ul style="list-style-type: none"> Tạo form xem danh sách người dùng cho hệ thống Tạo form xem thông tin về quyền (privileges) của mỗi user/role trên các đối tượng dữ liệu. Xem các bảng và view trong CSDL Làm báo cáo phân hệ 1 	20120318	10/10

2.2. Phân hệ 2

STT	Nội dung công việc	Phụ trách	Đánh giá của nhóm
1	<ul style="list-style-type: none"> Thực hiện CS3 – Trưởng phòng Thực hiện CS4 – Tài chính Làm giao diện CS3 Thực hiện OLS trên Oracle và demo Thực hiện audit b và giao diện audit Làm báo cáo các phần nêu trên 	20120255	10/10
2	<ul style="list-style-type: none"> Thực hiện CS6 – Trưởng đề án Viết script khởi tạo database và thêm dữ liệu mẫu. Làm giao diện CS4 Thực hiện chính sách mã hóa dữ liệu và giải mã Làm giao diện thay đổi mật khẩu Thực hiện audit c và giao diện audit Làm báo cáo các phần đã nêu trên 	20120295	10/10
3	<ul style="list-style-type: none"> Thực hiện CS5 – Nhân sự Làm giao diện CS1 và CS5 Làm giao diện xem Lương và Phụ cấp Thực hiện chính sách mã hóa dữ liệu và giải mã Thực hiện audit d Tổng hợp file script chính sách Tổng hợp và hoàn thiện báo cáo 	20120305	10/10
4	<ul style="list-style-type: none"> Thực hiện CS1 - Nhân viên Thực hiện CS2 - QL trực tiếp Làm giao diện CS2 và CS6 Thực hiện audit a Vẽ CSDL và đặc tả Làm báo cáo các phần đã nêu trên 	20120318	10/10

3. ĐÁNH GIÁ MỨC ĐỘ HOÀN THÀNH

STT	Yêu cầu		Độ hoàn thành (%)	Hạn chế
1	Phân hệ 1	Xem danh sách các đối tượng hiện có trên CSDL (user, role, table, view)	100	0
		Thêm mới đối tượng (table, user, role)	100	0
		Phân quyền/Lấy lại quyền của 1 user/role	100	0
		Xem quyền của 1 chủ thể	100	0
2	Phân hệ 2	Lược đồ CSDL cuối cùng cài đặt	100	0
		Liệt kê các chính sách bảo mật, phân tích và phân loại, đề ra giải pháp và cài đặt	100	0
		Hoàn thiện cài đặt các chính sách bảo mật nêu trong đồ án, gồm cài đặt mức cơ sở dữ liệu và cung cấp giao diện minh họa cho từng vai trò người dùng (DAC, RBAC, VPD, MAC).	100	0
		Mã hóa (chỉ cần cài đặt 1 chính sách, trình bày rõ PP quản lý khóa, trao đổi khóa, thay đổi khóa) và giao diện.	100	0
		Audit cơ bản và FGA (4 chính sách).	100	0

4. NỘI DUNG BÁO CÁO

4.1. Thông tin đề án

Đề án được chia làm 2 phân hệ với những yêu cầu như sau:

- **Phân hệ 1:** Hệ thống dành cho người quản trị bảo mật. Sinh viên hãy xây dựng ứng dụng cho phép các người dùng có quyền quản trị thực hiện công việc.

- **Phân hệ 2:** Hiện thực các chính sách bảo mật. Một công ty A có nhu cầu xây dựng một hệ thống S để quản lý thông tin nhân viên và việc tham gia đề án của nhân viên.

Sinh viên cần mô tả thông tin chặt chẽ, xây dựng ứng dụng Winform theo mô hình Client-Server để phục vụ cho nhu cầu tra cứu và quản lý thông tin trong hệ thống.

Trong bài báo cáo này, nhóm sẽ trình bày về ...

- Ngôn ngữ lập trình:

+ Về *back-end*: Cơ sở dữ liệu Oracle.

+ Về *Front-end*: Winform C#.

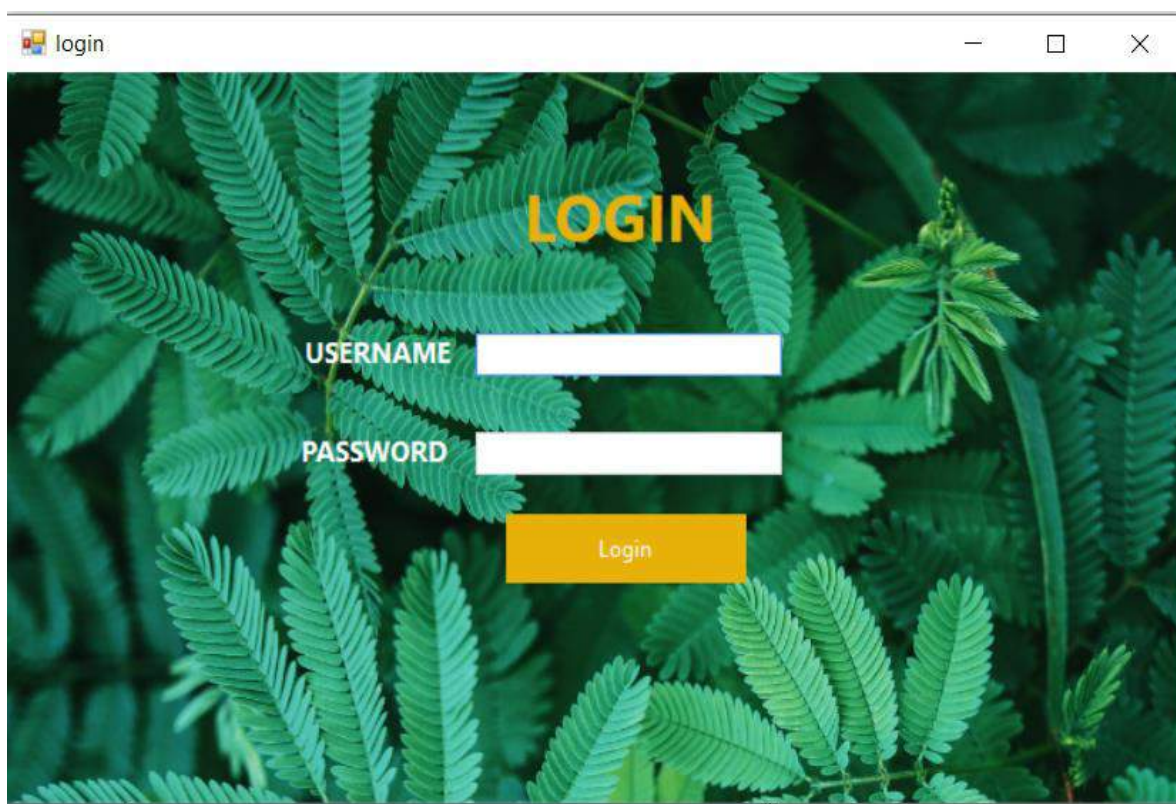
4.2. Phân hệ 1: Hệ thống dành cho người quản trị bảo mật

4.2.1. Màn hình đăng nhập

- Với màn hình giao diện đăng nhập, người dùng cần điền chính xác thông tin tài khoản được cấp cho bản thân. Từ đó, tùy theo vai trò người dùng trong hệ thống mà màn hình sẽ chuyển sang giao diện thích hợp cho người dùng đó.

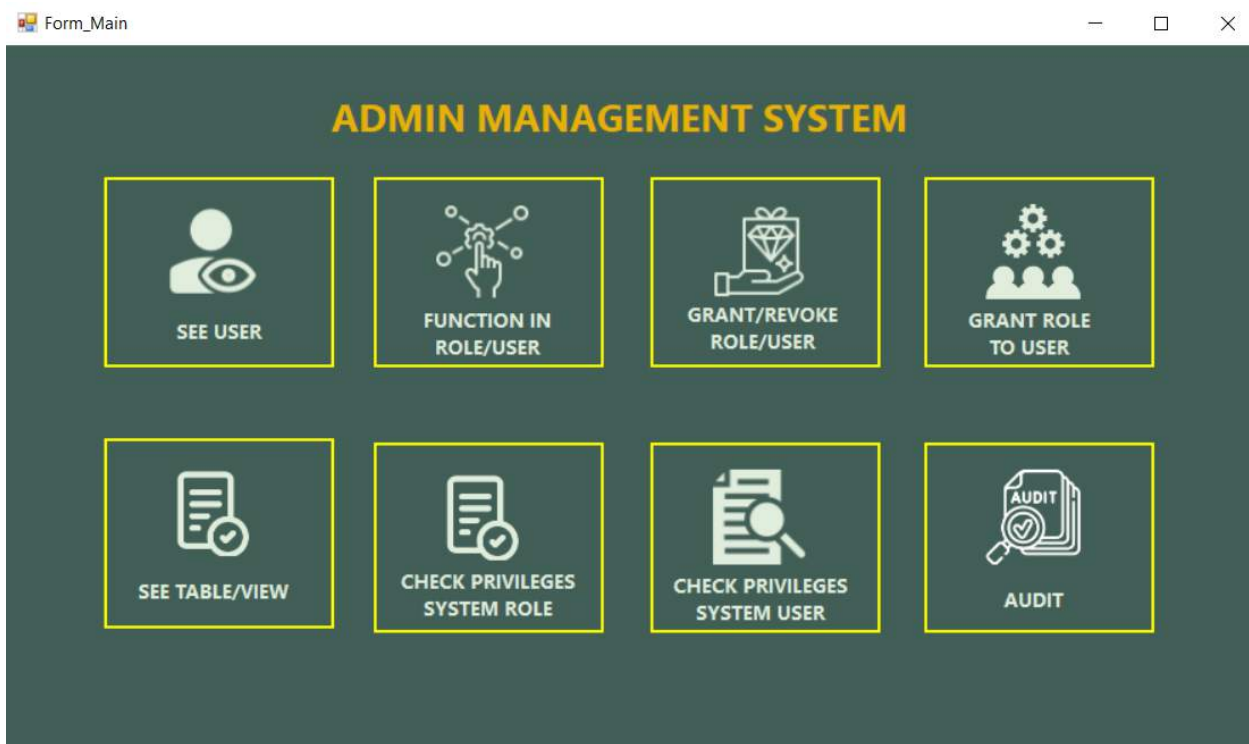
- Cụ thể, trong phân hệ 1 này, người dùng cần có vai trò là DBA trong hệ thống thì mới có thể vào được giao diện dành cho người quản trị bảo mật.

- Và nếu người dùng nhập sai tài khoản, màn hình sẽ xuất thông báo lỗi cho người dùng biết.



Hình 1. Giao diện đăng nhập

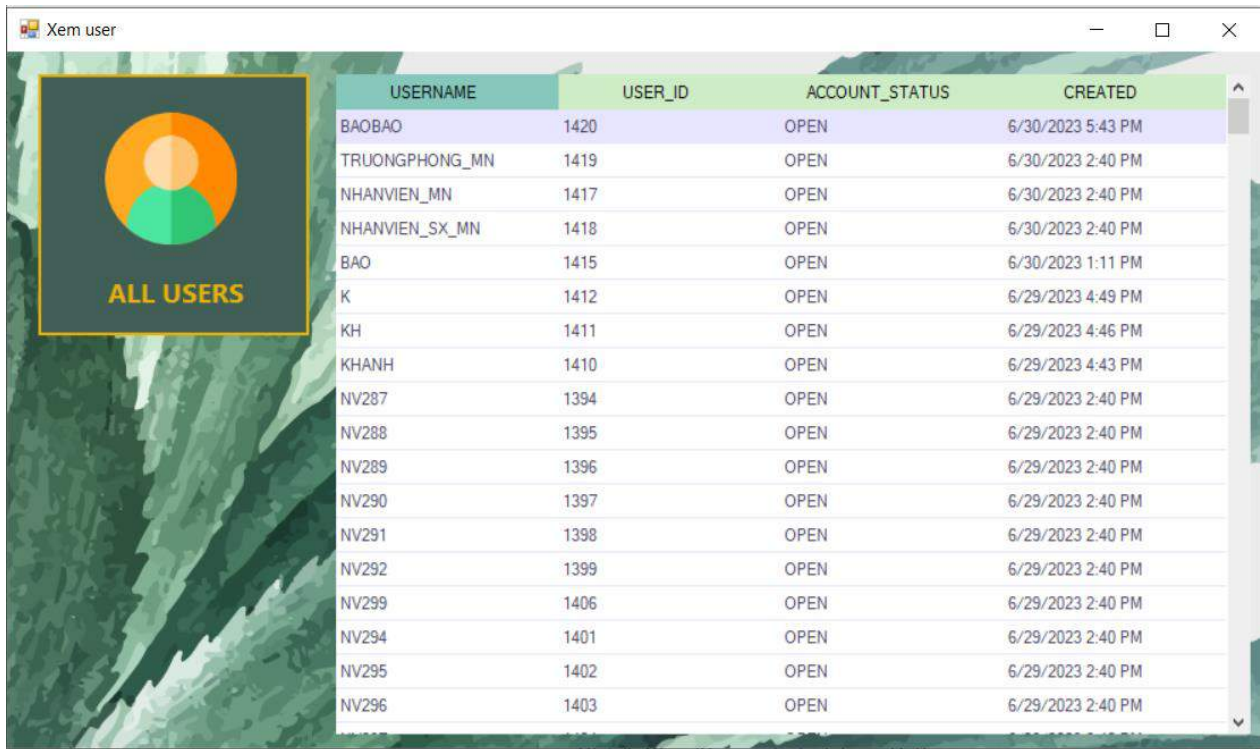
4.2.2. Màn hình chính



Hình 2. Giao diện màn hình chính

Giao diện này thể hiện các chức năng mà người quản trị bảo mật có thể sử dụng để quản lý hệ thống. Tùy vào chức năng mà người quản trị chọn, màn hình sẽ xuất hiện giao diện chức năng đó để người quản trị có thể thao tác.

4.2.3. Màn hình chức năng xem danh sách người dùng hệ thống



USERNAME	USER_ID	ACCOUNT_STATUS	CREATED
BAOBAO	1420	OPEN	6/30/2023 5:43 PM
TRUONGPHONG_MN	1419	OPEN	6/30/2023 2:40 PM
NHANVIEN_MN	1417	OPEN	6/30/2023 2:40 PM
NHANVIEN_SX_MN	1418	OPEN	6/30/2023 2:40 PM
BAO	1415	OPEN	6/30/2023 1:11 PM
K	1412	OPEN	6/29/2023 4:49 PM
KH	1411	OPEN	6/29/2023 4:46 PM
KHANH	1410	OPEN	6/29/2023 4:43 PM
NV287	1394	OPEN	6/29/2023 2:40 PM
NV288	1395	OPEN	6/29/2023 2:40 PM
NV289	1396	OPEN	6/29/2023 2:40 PM
NV290	1397	OPEN	6/29/2023 2:40 PM
NV291	1398	OPEN	6/29/2023 2:40 PM
NV292	1399	OPEN	6/29/2023 2:40 PM
NV299	1406	OPEN	6/29/2023 2:40 PM
NV294	1401	OPEN	6/29/2023 2:40 PM
NV295	1402	OPEN	6/29/2023 2:40 PM
NV296	1403	OPEN	6/29/2023 2:40 PM

Hình 3. Giao diện xem danh sách người dùng

Giao diện này giúp quản trị viên quản lý được các người dùng có trong cơ sở dữ liệu. Thông tin sẽ được sắp xếp giảm dần theo ngày tạo.

4.2.4. Màn hình cho chức năng xem bảng và view

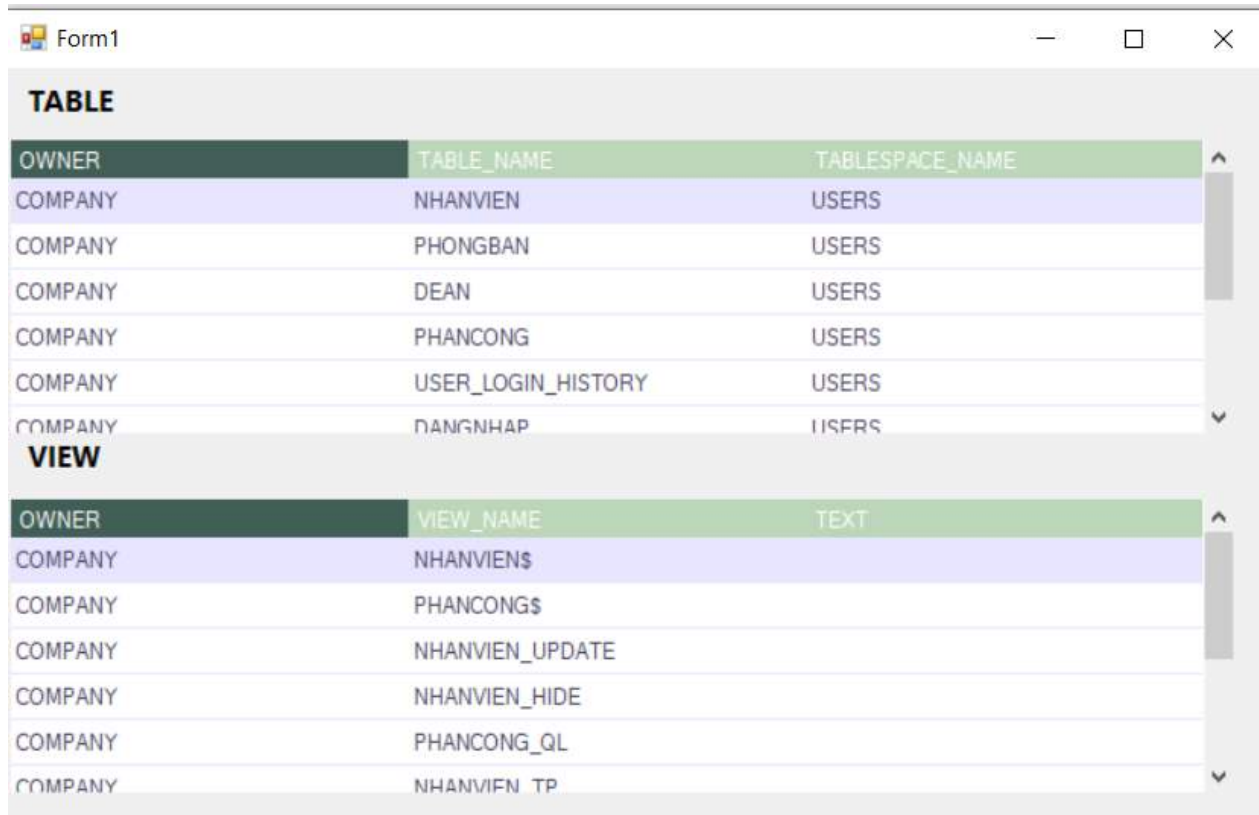


TABLE		
OWNER	TABLE_NAME	TABLESPACE_NAME
COMPANY	NHANVIEN	USERS
COMPANY	PHONGBAN	USERS
COMPANY	DEAN	USERS
COMPANY	PHANCONG	USERS
COMPANY	USER_LOGIN_HISTORY	USERS
COMPANY	DANGNHAP	USERS

VIEW		
OWNER	VIEW_NAME	TEXT
COMPANY	NHANVIENS\$	
COMPANY	PHANCONGS\$	
COMPANY	NHANVIEN_UPDATE	
COMPANY	NHANVIEN_HIDE	
COMPANY	PHANCONG_QL	
COMPANY	NHANVIEN_TP	

Hình 4. Giao diện xem bảng và view trong cơ sở dữ liệu

Giao diện này giúp quản trị viên quản lý được các **table** và **view** có trong cơ sở dữ liệu.

4.2.5. Màn hình cho phép thực hiện việc cấp quyền, thu hồi quyền, và xem quyền hiện có của người dùng

- Việc cấp quyền cho người dùng khi nhấn vào chức năng **“GRANT/REVOKE ROLE/USER”**.

- Với giao diện này, người dùng có thể thực hiện các chức năng như: cấp quyền cho user, cấp quyền cho role, thu hồi quyền cho user, cấp quyền từ role này cho user khác. 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 tính đến mức cột; quyền insert, delete thì không.

Form_grant_userrole

GRANT/REVOKE PRIVILEGES USER OR ROLE

CHOOSE USER: CHECK_USER SUBMIT_USER

CHOOSE ROLE: CHECK_ROLE SUBMIT_ROLE

Table Name	Select	Select (WGO)	Insert	Insert (WGO)	Update	Update (WGO)	Delete	Delete (WGO)
DEAN	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
PHANCONG	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
USER_LOGI...	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
DANGNHAP	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
NHANVIEN...	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
AUD_LUONG	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
ANNOUNCE...	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Hình 5. Giao diện thực hiện việc cấp quyền

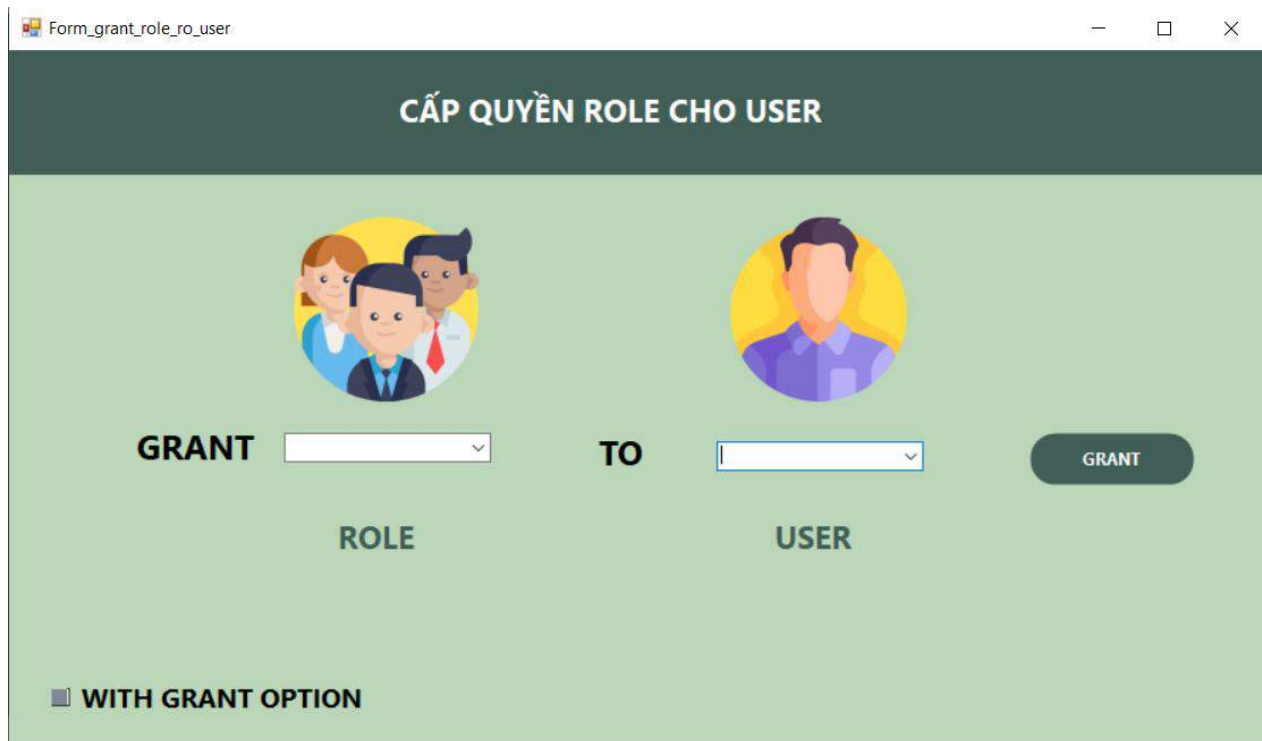
- Trong Role có danh sách các vai trò mà chính DBA đăng nhập vô hệ thống tạo ra.

- Trong User có danh sách các user do chính DBA đăng nhập vô hệ thống tạo ra.

- Chọn **Role** hoặc **User** cần để cấp quyền. Nhấn button “**CHECK_USER**” để kiểm tra quyền của của user và nhấn button “**CHECK_ROLE**” để kiểm tra quyền của role. Các quyền hiện có của Role hoặc user đó sẽ hiện lên trên bảng, từ đó người dùng có thể dựa vào đó để phân quyền.

- Nếu là user thì DBA có quyền chọn tất cả các ô check box có trên màn hình giao diện, DBA cũng có thể thu hồi quyền bằng cách bỏ chọn và nhấn “**SUBMIT_USER**” để thực hiện việc cấp quyền hay thu hồi quyền.

Nếu là role thì các ô check box “**WITH GRANT OPTION**” vẫn có thể chọn nhưng khi nhấn “**SUBMIT_ROLE**” thì các quyền với “**WITH GRANT OPTION**”.



The screenshot shows a web application window titled "Form_grant_role_ro_user". The main heading is "CẤP QUYỀN ROLE CHO USER". The interface includes two circular icons representing a group of people (Role) and a single person (User). Below these icons are two dropdown menus labeled "GRANT" and "TO". Under the "GRANT" dropdown is the label "ROLE", and under the "TO" dropdown is the label "USER". To the right of these dropdowns is a dark green button labeled "GRANT". At the bottom left, there is a checkbox labeled "WITH GRANT OPTION".

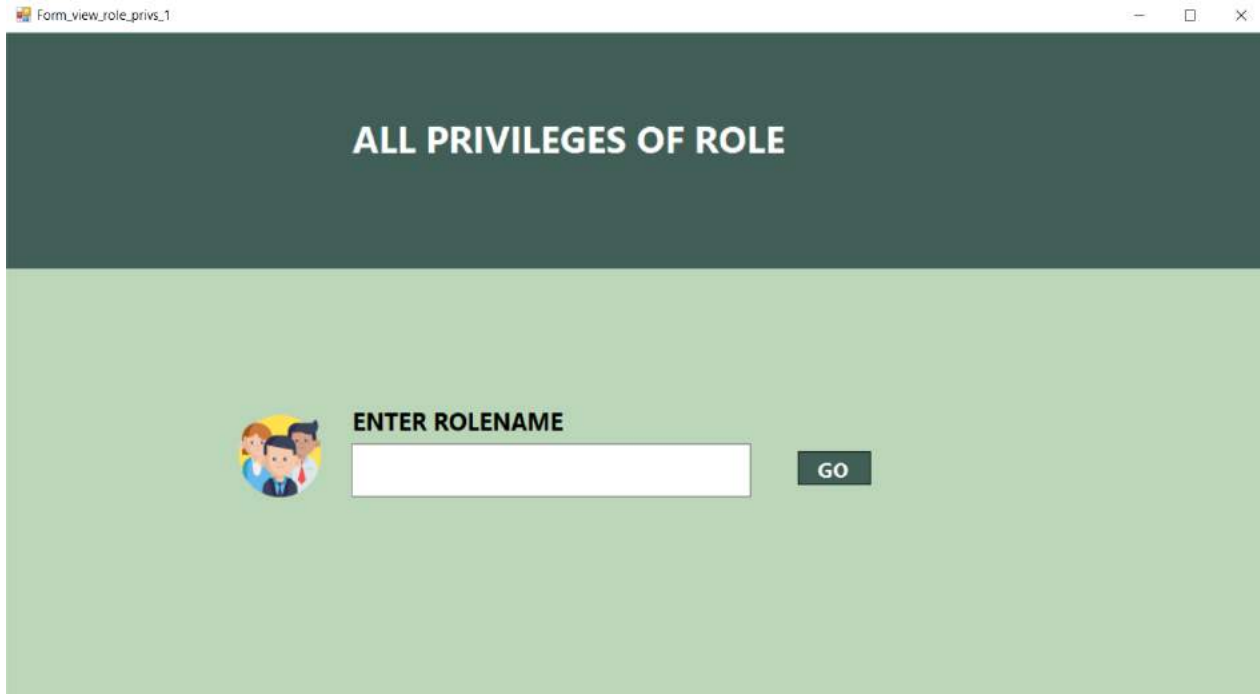
Hình 6. Giao diện cấp quyền Role cho User

- Việc cấp role cho user sẽ được tiến hành khi người dùng chọn **Role** và **User** ở 2 combobox, sau đó nếu muốn thì grant quyền theo “**WITH GRANT OPTION**”. Nhấn “**GRANT**” để hoàn thành việc cấp quyền cho role cho user.

4.2.6. Màn hình cho xem quyền hệ thống của người dùng

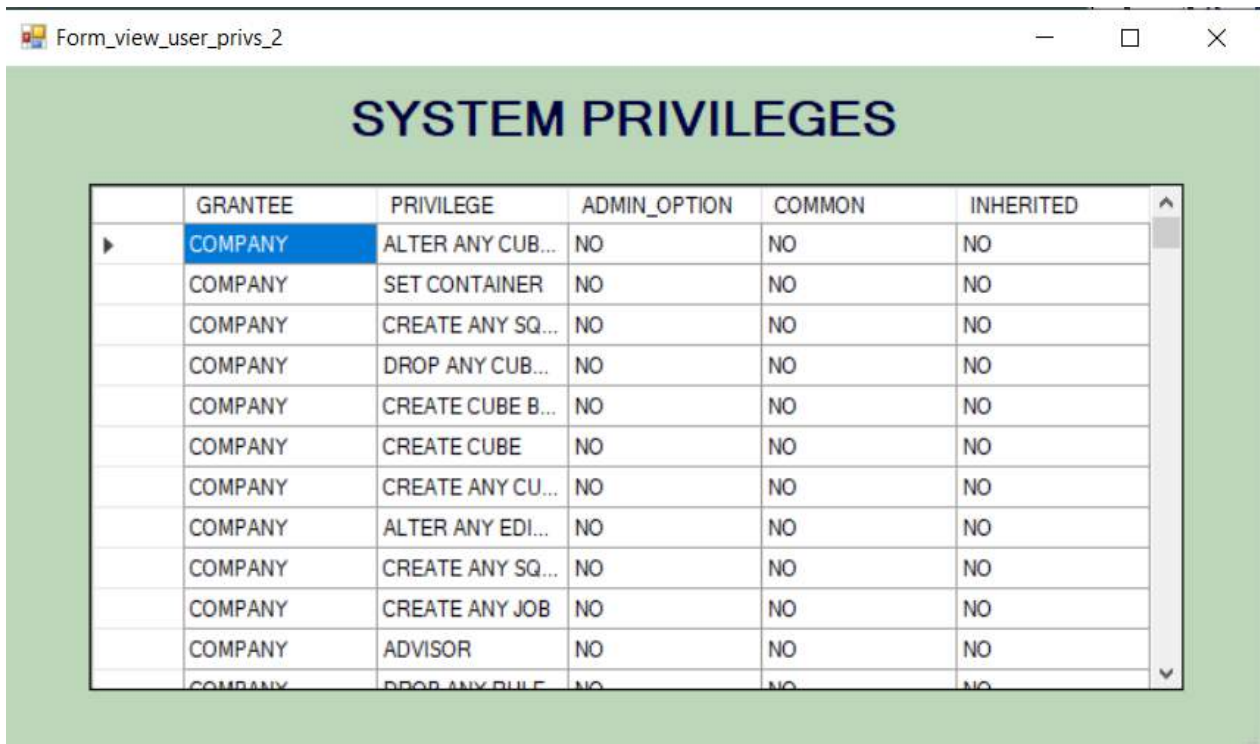
Việc cho phép quản trị viên xem quyền của các chủ thể sẽ giúp cho quản trị viên có thể quản lý được các quyền của từng người dùng trong cơ sở dữ liệu, từ đó có thể đưa ra quyết định cấp quyền cần thiết cho người dùng hoặc có thể thu hồi lại các quyền dư thừa và không hợp lý từ người dùng. Điều này sẽ giúp cho cơ sở dữ liệu sẽ được an toàn hơn.

4.2.6.1. Kiểm tra quyền của user



Hình 7. Màn hình kiểm tra quyền user

Màn hình hiển thị yêu cầu quản trị viên điền username cần kiểm tra

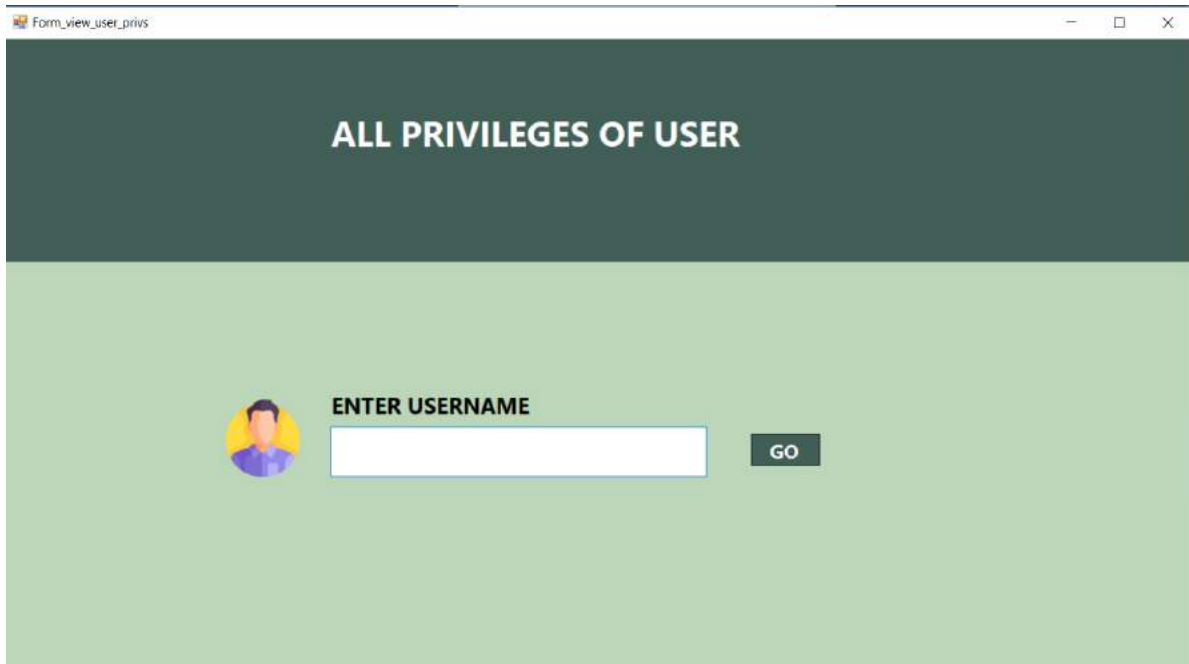


	GRANTEE	PRIVILEGE	ADMIN_OPTION	COMMON	INHERITED
▶	COMPANY	ALTER ANY CUB...	NO	NO	NO
	COMPANY	SET CONTAINER	NO	NO	NO
	COMPANY	CREATE ANY SQ...	NO	NO	NO
	COMPANY	DROP ANY CUB...	NO	NO	NO
	COMPANY	CREATE CUBE B...	NO	NO	NO
	COMPANY	CREATE CUBE	NO	NO	NO
	COMPANY	CREATE ANY CU...	NO	NO	NO
	COMPANY	ALTER ANY EDI...	NO	NO	NO
	COMPANY	CREATE ANY SQ...	NO	NO	NO
	COMPANY	CREATE ANY JOB	NO	NO	NO
	COMPANY	ADVISOR	NO	NO	NO
	COMPANY	DROP ANY DUE	NO	NO	NO

Hình 8. Kết quả kiểm tra quyền user

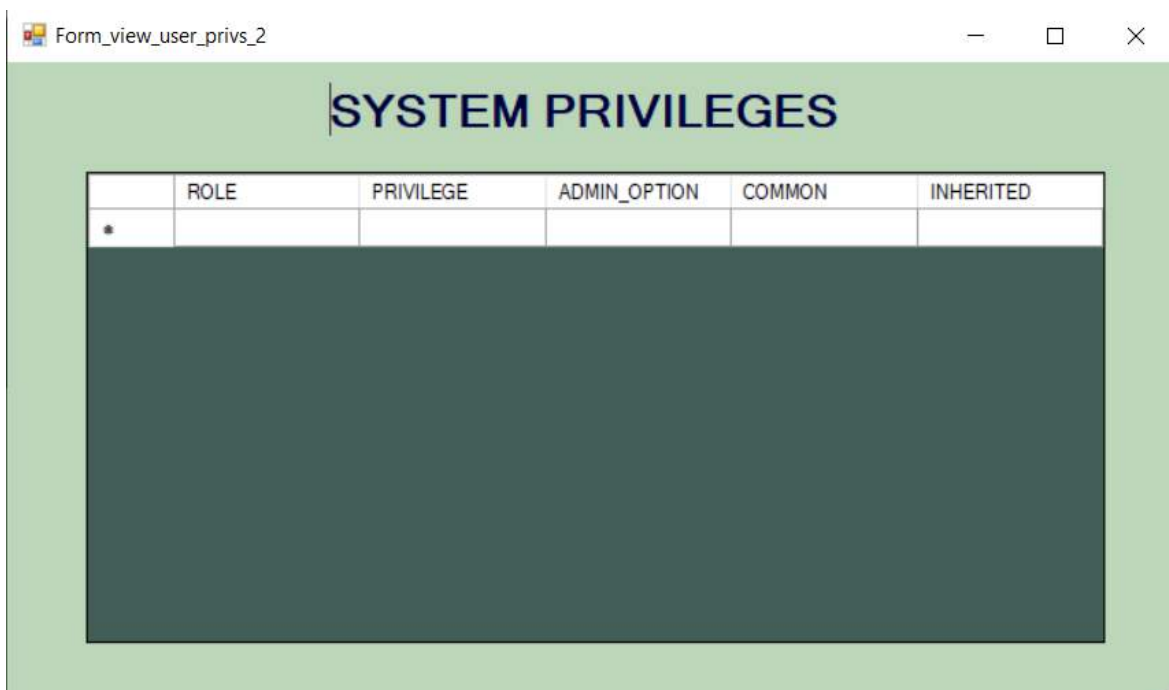
Sau khi nhập đúng username, hệ thống sẽ trả ra kết quả là bảng ‘**SYSTEM PRIVILEGES**’ tương ứng với quyền hệ thống trên các đối tượng trong cơ sở dữ liệu.

4.2.6.2. Kiểm tra quyền của role



Hình 9. Giao diện kiểm tra quyền của Role

- Màn hình yêu cầu quản trị viên điền rolename cần tra cứu.



	ROLE	PRIVILEGE	ADMIN_OPTION	COMMON	INHERITED
*					

Hình 10. Kết quả kiểm tra quyền Role

- Sau khi điền rolename chính xác, hệ thống sẽ trả ra kết quả là hai bảng ‘**SYSTEM PRIVILEGES**’ tương ứng với quyền hệ thống trên các đối tượng trong cơ sở dữ liệu.

4.2.7. Màn hình cho phép thêm, xóa, chỉnh sửa thông tin user/ role.

- Giao diện cung cấp các thông tin về **User** và **Role** đã được tạo trong cơ sở dữ liệu, cho phép người dùng tạo (**CREATE**) một **User** hoặc **Role** mới; xóa (**DROP**), thay đổi (**ALTER**) mật khẩu cho **User** hoặc **Role** đã được tạo trước đó.

The screenshot shows a web application window titled 'Form_thao_tac'. It contains two main tables and a sidebar with operation buttons.

LIST USER Table:

	USERNAME	USER_ID	PASSWORD	ACCOUNT_STATU	Li
▶	SYS	0		OPEN	
	AUDSYS	8		LOCKED	6/
	SYSTEM	9		OPEN	
	SYSBACKUP	2147483617		LOCKED	6/
	SYSDG	2147483618		LOCKED	6/
	SYSKM	2147483619		LOCKED	6/
	SYSRAC	2147483620		OPEN	
	OUTLN	13		LOCKED	6/

LIST ROLE Table:

	ROLE	ROLE_ID	PASSWORD_REQ	AUTHENTICATION	C
▶	CONNECT	2	NO	NONE	YE
	RESOURCE	3	NO	NONE	YE
	DBA	4	NO	NONE	YE
	PDB_DBA	5	NO	NONE	YE
	AUDIT_ADMIN	6	NO	NONE	YE
	AUDIT_VIEWER	7	NO	NONE	YE
	SELECT_CATAL...	10	NO	NONE	YE
	EXECUTE_CAT...	11	NO	NONE	YE
	CAPTURE_ADMIN	12	NO	NONE	YE
	EXP_FULL_DAT...	14	NO	NONE	YE
	IMP_FULL_DAT...	15	NO	NONE	YE

ALL OPERATION Sidebar:

- Name:
- Password:
- CREATE USER
- DELETE USER
- CHANGE PASSWORD USER
- CREATE ROLE
- DELETE ROLE
- CHANGE PASSWOR D ROLE

Hình 11. Giao diện thao tác với User/Role

- Để tạo một **User/Role** mới, người dùng cần nhập đầy đủ thông tin bao gồm tên **User/Role** và mật khẩu cho User/Role đó vào các **textbox Name** và **Password**.

Sau đó người dùng click vào **button “Tạo User”** để tạo **User** mới hoặc **button “Tạo Role để”** tạo **Role** mới.

- Để xóa một **User/Role** đã tồn tại, người dùng cần nhập tên của **User/Role** cần xóa vào **textbox Name** và click vào **button “Xóa User”** để xóa **User** hoặc **button “Xóa Role”** để xóa **Role** đã tồn tại trong cơ sở dữ liệu.

- Để thay đổi thông tin (mật khẩu) của **User/Role** đã tồn tại trước đó, người dùng cần nhập đầy đủ thông tin bao gồm tên **User/Role** đã được tạo trước đó và mật khẩu mới cho **User/Role** đó vào các **textbox Name** và **Password**. Sau đó người dùng click vào **button “Đổi password User”** hoặc **button “Đổi password Role”** để thực hiện thay đổi mật khẩu của **User** hoặc **Role** tương ứng.

4.3. Phân hệ 2: Hiện thực các chính sách bảo mật

4.3.1. Tính năng hệ thống

4.3.1.1. Vai trò “Nhân viên”

Khi người dùng đăng nhập vào hệ thống có vai trò **Nhân viên (NV)**, người dùng đó sẽ được:

- Xem thông tin cá nhân của bản thân và được sửa các thông tin *Ngày sinh*, *Địa chỉ*, *Số điện thoại* của bản thân (Không xem được của người khác đảm bảo tính bảo mật).
- Xem thông tin công việc được phân công của bản thân.
- Xem được danh sách các phòng ban trong công ty và các đề án mà công ty đang thực hiện.
- **Giao diện**

Form1

Welcome, Nhân Viên
ID: NV100

NHAN VIEN
PHONG BAN
DE AN
PHAN CONG
ĐĂNG XUẤT

Thông tin nhân viên

MANV	TENNV	PHAI	NGAYSINH	DIACHI	SDT	VAITRO	MANQL	PHG
NV100	Edra Clev...	0	2/5/2000	Milano	03977231...	NV	NV008	PB04

Cập nhật thông tin

Địa chỉ:

SĐT:

Ngày sinh:

Chức năng

Cập nhật
Tải lại bảng
Xem lương và phụ cấp
Đổi mật khẩu
Thoát

Hình 12. Giao diện vai trò **Nhân viên** xem và sửa thông tin cá nhân

Form1

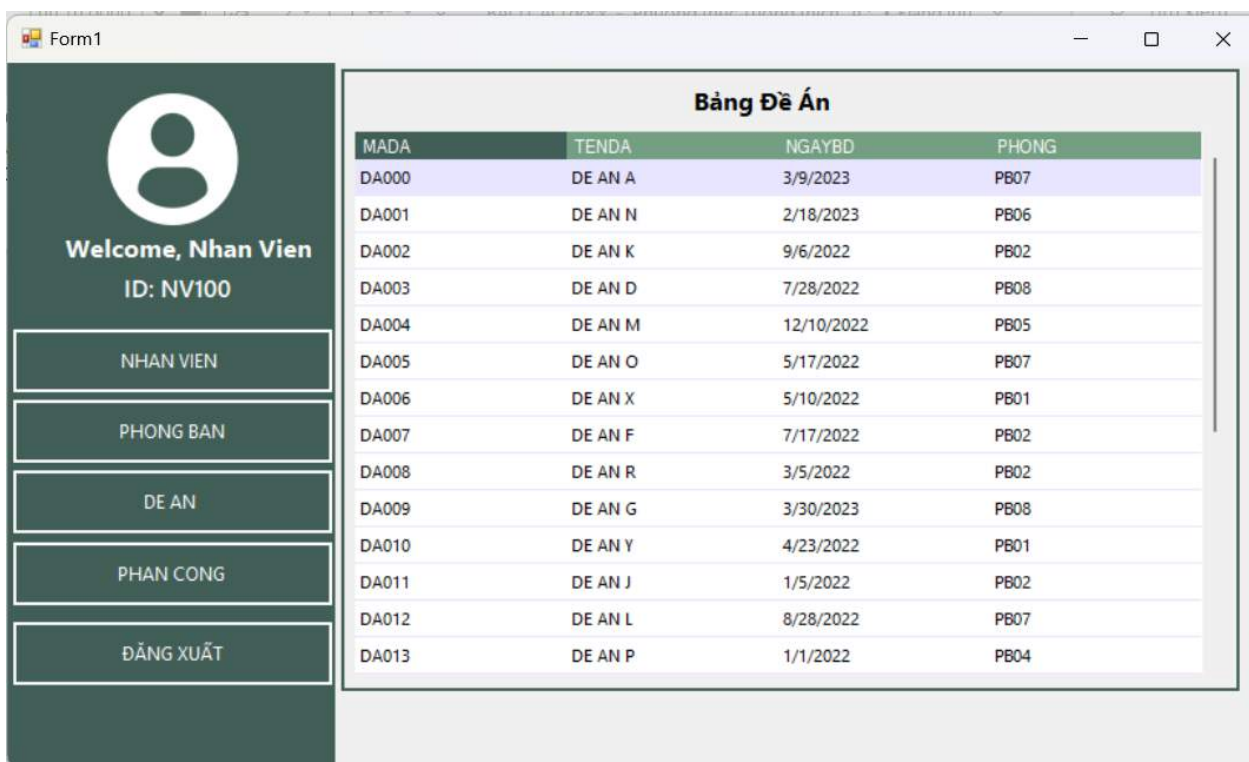
Welcome, Nhân Viên
ID: NV100

NHAN VIEN
PHONG BAN
DE AN
PHAN CONG
ĐĂNG XUẤT

Bảng phòng ban

MAPB	TENPB	TRPHG
PB01	PHONG SAN XUAT	NV038
PB02	PHONG TAI CHINH	NV039
PB03	PHONG NHAN SU	NV040
PB04	PHONG IT	NV041
PB05	PHONG DAO TAO	NV042
PB06	PHONG HANH CHINH	NV043
PB07	PHONG CSKH	NV044
PB08	PHONG MARKETING	NV045

Hình 13. Giao diện vai trò **Nhân viên** xem Phòng ban



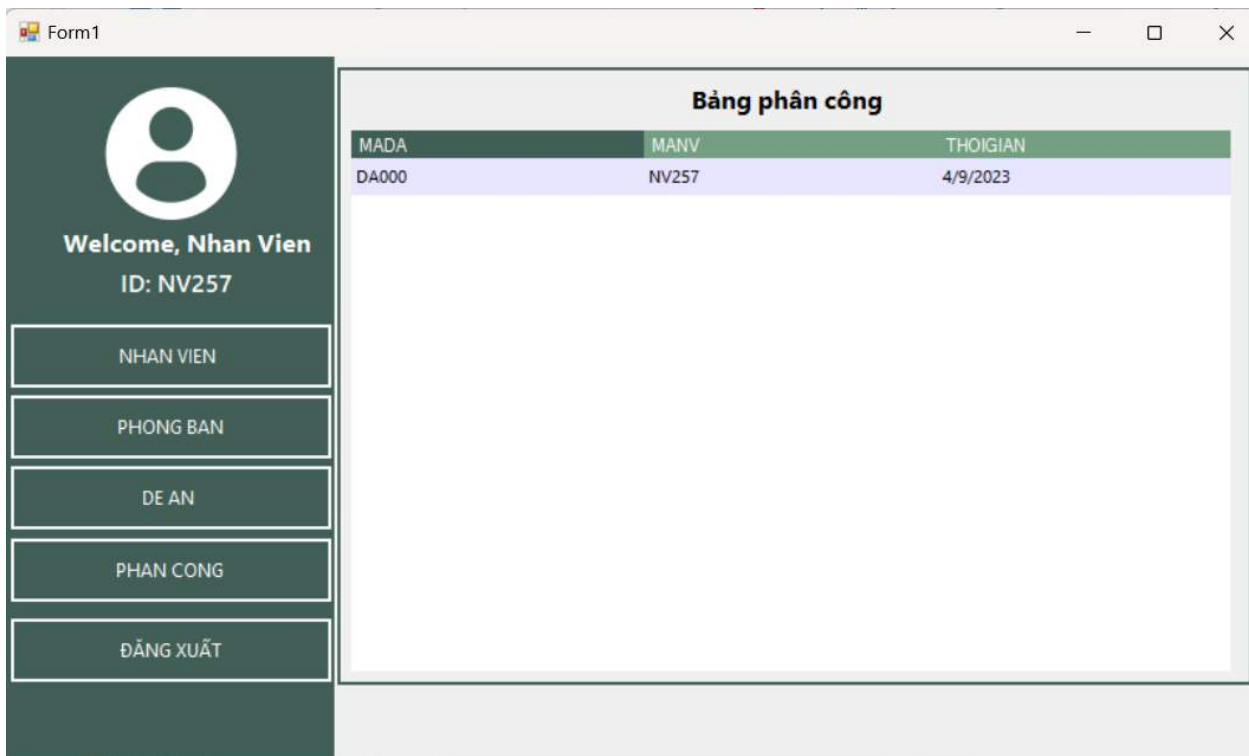
Welcome, Nhan Vien
ID: NV100

NHAN VIEN
PHONG BAN
DE AN
PHAN CONG
ĐĂNG XUẤT

Bảng Đề Án

MADA	TENDA	NGAYBD	PHONG
DA000	DE AN A	3/9/2023	PB07
DA001	DE AN N	2/18/2023	PB06
DA002	DE AN K	9/6/2022	PB02
DA003	DE AN D	7/28/2022	PB08
DA004	DE AN M	12/10/2022	PB05
DA005	DE AN O	5/17/2022	PB07
DA006	DE AN X	5/10/2022	PB01
DA007	DE AN F	7/17/2022	PB02
DA008	DE AN R	3/5/2022	PB02
DA009	DE AN G	3/30/2023	PB08
DA010	DE AN Y	4/23/2022	PB01
DA011	DE AN J	1/5/2022	PB02
DA012	DE AN L	8/28/2022	PB07
DA013	DE AN P	1/1/2022	PB04

Hình 14. Giao diện vai trò *Nhân viên* xem bảng Đề Án



Welcome, Nhan Vien
ID: NV257

NHAN VIEN
PHONG BAN
DE AN
PHAN CONG
ĐĂNG XUẤT

Bảng phân công

MADA	MANV	THOIGIAN
DA000	NV257	4/9/2023

Hình 15. Giao diện vai trò *Nhân viên* xem phân công của mình

4.3.1.2. Vai trò “Quản lý trực tiếp”

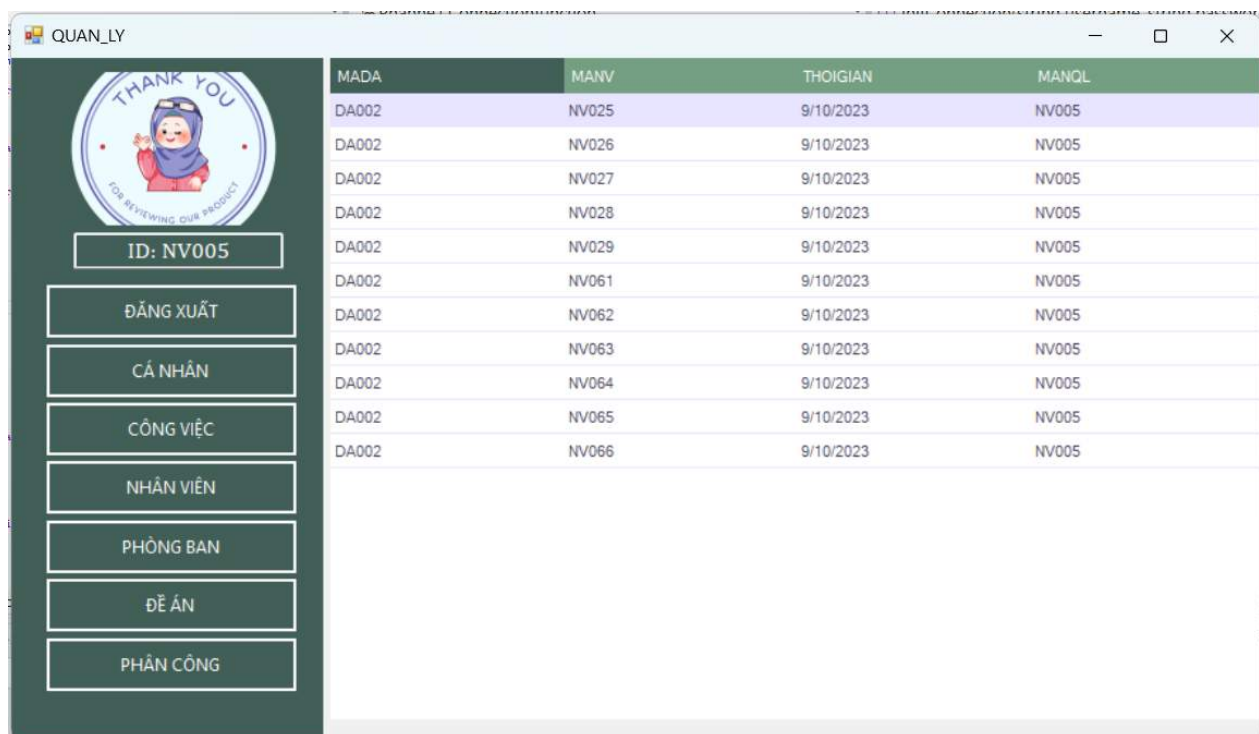
Khi người dùng đăng nhập vào hệ thống có vai trò **Quản lý trực tiếp (QL)**, người dùng đó sẽ được:

- Có các tính năng của vai trò *Nhân viên*.
- Xem được thông tin các nhân viên mà mình quản lý (trừ thông tin *Lương*, *Phụ cấp* của nhân viên đó).
- Xem được thông tin phân công công việc của những nhân viên mà mình quản lý.
- **Giao diện**



MANV	TENNV	PHAI	NGAYSINH	DIACHI	SDT	VAITRO	MANQL	PHG
NV241	Rossana Ri...	0	2/18/2000	Alva	0525508002	NV	NV018	PB06
NV242	Meryl Dotson	0	2/11/1953	Drayton Plai...	0975440109	NV	NV018	PB06
NV243	Clifton Lim	0	7/20/1955	Glen Haven	0913252203	NV	NV018	PB06
NV245	Rosy Halcomb	0	7/13/1986	Dresden	0520984157	NV	NV018	PB06
NV246	Shanae Earle	1	6/11/2000	Rexford	0121366365	NV	NV018	PB06
NV247	Celestina B...	0	9/12/1993	Long Beach	0923407173	NV	NV018	PB06
NV249	Madlyn Truitt	1	8/24/1957	Alvarado	0981535356	NV	NV018	PB06
NV251	Genevive B...	1	11/14/1963	Jupiter	0800164660	NV	NV018	PB06
NV252	Milton Dalton	0	3/9/1988	Zuni	0196576404	NV	NV018	PB06
NV254	Laveta Duran	0	5/25/1961	Satellite Be...	0257386925	NV	NV018	PB06
NV255	Dodie Barone	1	12/22/1954	Peotone	0425439599	NV	NV018	PB06
NV256	Magdalen L...	1	7/21/1984	Sedro Woolley	0200076163	NV	NV018	PB06
NV244	Velvet Castro	0	12/2/1979	Butlerville	0345915827	NV	NV018	PB06
NV248	Jodie Emmo...	1	1/13/1953	Horton	0694170591	NV	NV018	PB06
NV250	Phil King	0	7/6/1967	Peosta	0789362114	NV	NV018	PB06
NV253	Cristopher ...	0	7/28/1993	Blandford	0854835959	NV	NV018	PB06

Hình 16. Giao diện vai trò Quản lý xem được nhân viên mình quản lý

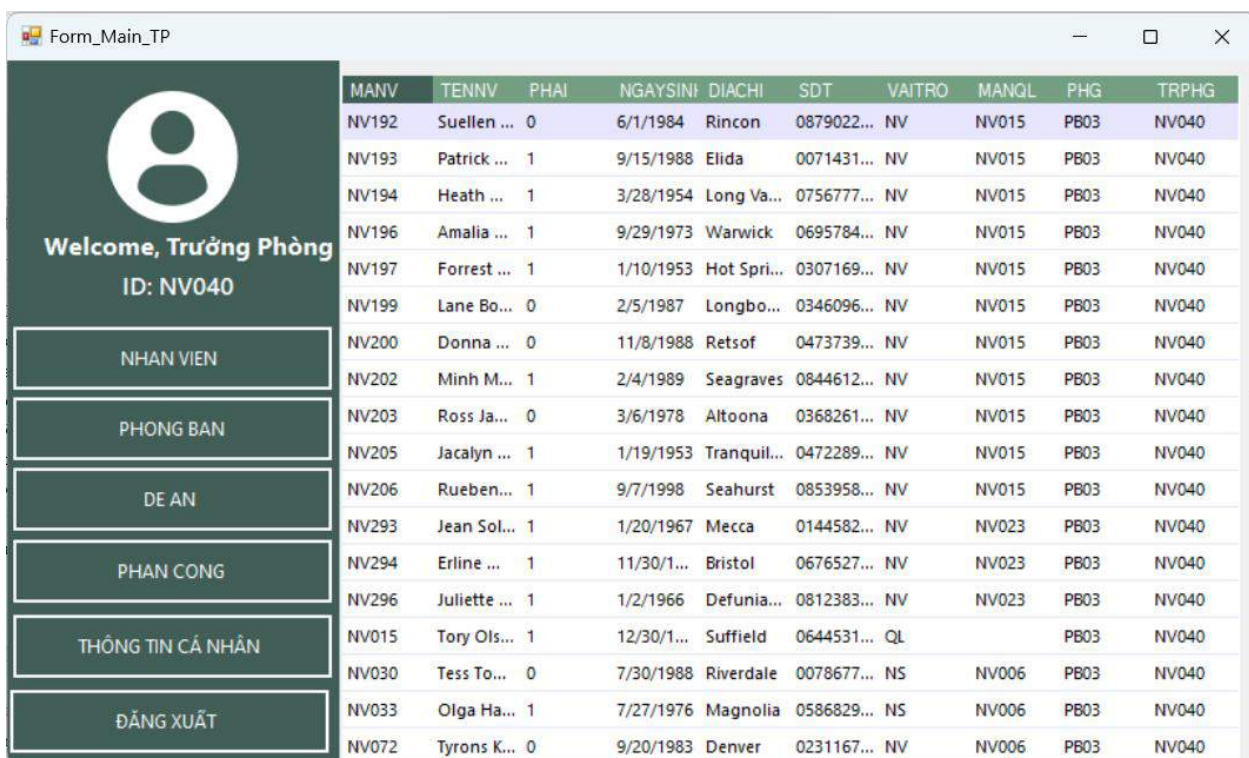


Hình 17. Giao diện vai trò **Quản lý** xem được phân công của mình và nhân viên mình quản lý

4.3.1.3. Vai trò “**Trưởng phòng**”

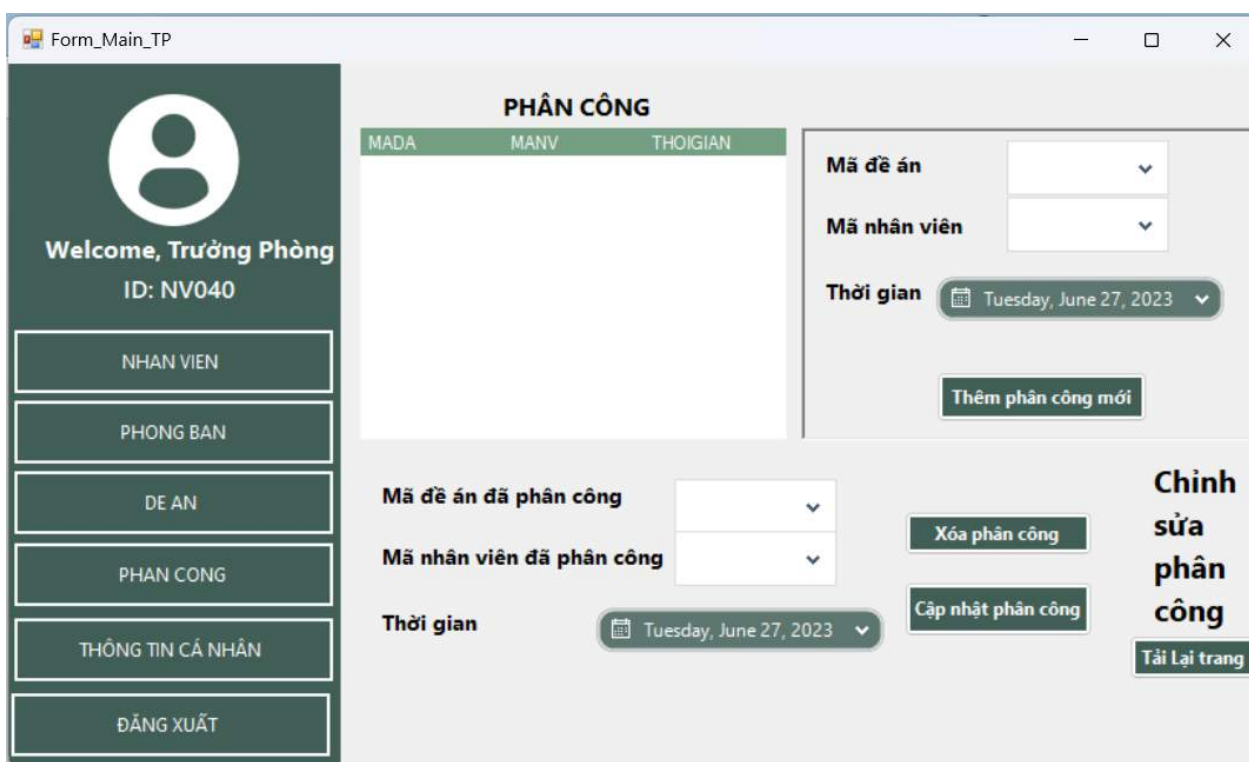
Khi người dùng đăng nhập vào hệ thống có vai trò **Trưởng phòng (TP)**, người dùng đó sẽ được:

- Có các tính năng của vai trò *Nhân viên*.
- Xem được thông tin các nhân viên thuộc phòng ban mình quản lý (trừ thông tin *Lương*, *Phụ cấp* của nhân viên đó).
- Quản lý thông tin phân công công việc (thêm, xóa, cập nhật) của những nhân viên thuộc phòng ban mình quản lý.
- **Giao diện**



MANV	TENNV	PHAI	NGAYSINH	DIACHI	SDT	VAITRO	MANQL	PHG	TRPHG
NV192	Suellen ...	0	6/1/1984	Rincon	0879022...	NV	NV015	PB03	NV040
NV193	Patrick ...	1	9/15/1988	Elida	0071431...	NV	NV015	PB03	NV040
NV194	Heath ...	1	3/28/1954	Long Va...	0756777...	NV	NV015	PB03	NV040
NV196	Amalia ...	1	9/29/1973	Warwick	0695784...	NV	NV015	PB03	NV040
NV197	Forrest ...	1	1/10/1953	Hot Spri...	0307169...	NV	NV015	PB03	NV040
NV199	Lane Bo...	0	2/5/1987	Longbo...	0346096...	NV	NV015	PB03	NV040
NV200	Donna ...	0	11/8/1988	Retsof	0473739...	NV	NV015	PB03	NV040
NV202	Minh M...	1	2/4/1989	Seagraves	0844612...	NV	NV015	PB03	NV040
NV203	Ross Ja...	0	3/6/1978	Altoona	0368261...	NV	NV015	PB03	NV040
NV205	Jacalyn ...	1	1/19/1953	Tranquil...	0472289...	NV	NV015	PB03	NV040
NV206	Rueben...	1	9/7/1998	Seahurst	0853958...	NV	NV015	PB03	NV040
NV293	Jean Sol...	1	1/20/1967	Mecca	0144582...	NV	NV023	PB03	NV040
NV294	Erlene ...	1	11/30/1...	Bristol	0676527...	NV	NV023	PB03	NV040
NV296	Juliette ...	1	1/2/1966	Defunia...	0812383...	NV	NV023	PB03	NV040
NV015	Tory Ols...	1	12/30/1...	Suffield	0644531...	QL		PB03	NV040
NV030	Tess To...	0	7/30/1988	Riverdale	0078677...	NS	NV006	PB03	NV040
NV033	Olga Ha...	1	7/27/1976	Magnolia	0586829...	NS	NV006	PB03	NV040
NV072	Tyrons K...	0	9/20/1983	Denver	0231167...	NV	NV006	PB03	NV040

Hình 18. Giao diện vai trò **Trưởng phòng** chỉ xem được nhân viên phòng ban mình quản lý



PHÂN CÔNG

MADA	MANV	THOIGIAN
------	------	----------

Mã đề án:

Mã nhân viên:

Thời gian:

Thêm phân công mới

Mã đề án đã phân công:

Mã nhân viên đã phân công:

Thời gian:

Xóa phân công

Cập nhật phân công

Tải Lại trang

Hình 19. Giao diện vai trò Trưởng phòng thêm, xóa, sửa phân công phòng ban mình quản lý

4.3.1.4. Vai trò “Tài chính”

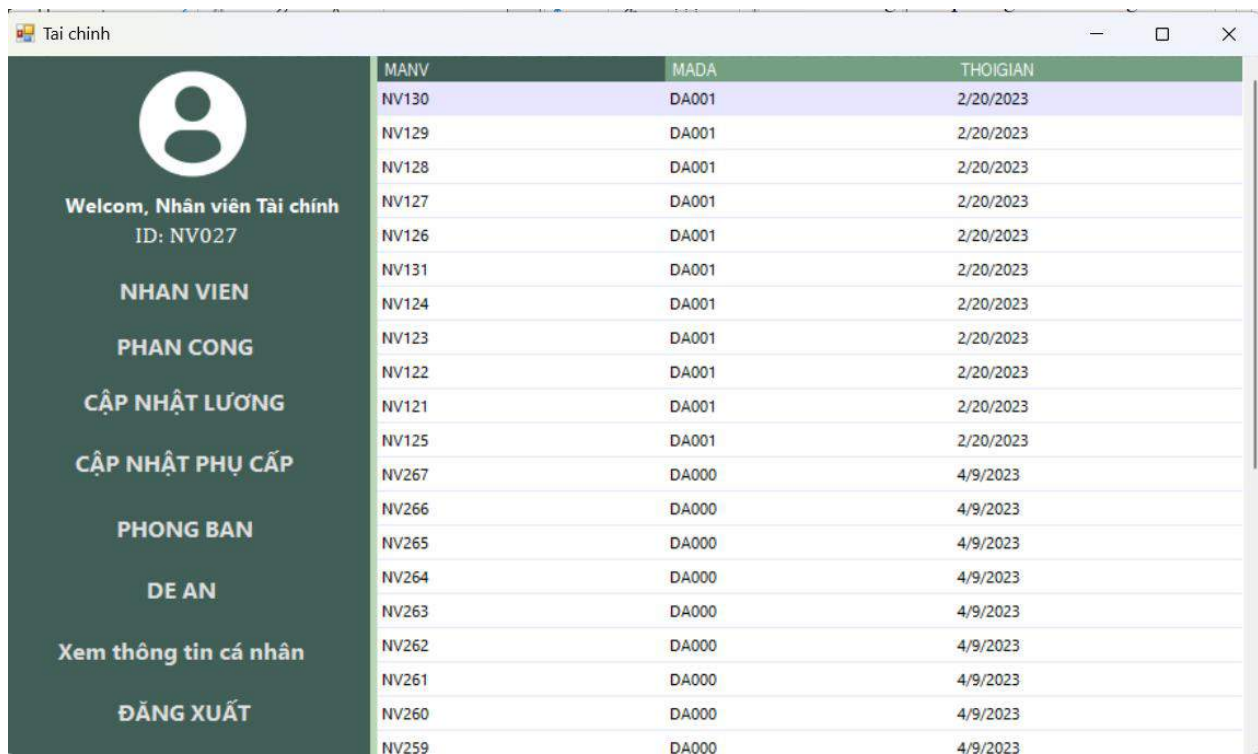
Khi người dùng đăng nhập vào hệ thống có vai trò **Tài chính (TC)**, người dùng đó sẽ được:

- Có các tính năng của vai trò *Nhân viên*.
- Xem được toàn bộ thông tin tất cả nhân viên trong công ty (thừa hành ban giám đốc) và được sửa thông tin *Lương*, *Phụ cấp* của một nhân viên bất kỳ.

- Giao diện

MANV	TENNV	PHAI	NGAYSIN	DIACHI	SDT	LUONG	PHUCAP	VAITRO	MANQL	PHG
NV006	Marco ...	0	5/5/1983	Iowa Pa...	043037...	17258798	711747	QL		PB03
NV007	Tanner ...	1	9/13/19...	Butner	014373...	9184481	1562325	QL		PB01
NV008	Carline...	0	5/18/19...	Zuni	078770...	19999999	1788165	QL		PB04
NV009	Cora P...	0	8/25/19...	Oneida	006703...	19190268	1999999	QL		PB05
NV010	Cleotil...	1	1/7/1953	Suffern	010252...	19999999	1970877	QL		PB06
NV011	Gus Sa...	0	7/21/20...	Alvin	058649...	13926443	500000	QL		PB07
NV012	Alfonz...	0	5/9/1982	Wheatf...	051100...	17369188	500000	QL		PB08
NV013	Addie ...	1	9/8/1953	Butte	008122...	11605877	856203	QL		PB01
NV014	Christi...	0	8/11/19...	Gravette	096750...	15750610	1305936	QL		PB02
NV015	Tory Ol...	1	12/30/1...	Suffield	064453...	16072756	1284967	QL		PB03
NV016	Amiee ...	1	5/26/19...	Maggie...	045958...	7238408	1049453	QL		PB04
NV017	Glynis ...	0	12/11/1...	River R...	076640...	11959632	1215909	QL		PB05
NV018	Joeann...	1	11/8/19...	O'Neill	070950...	17672856	1845247	QL		PB06
NV019	Jeffrey P...	1	4/16/19...	Riverba...	008407...	10608039	2000000	QL		PB07
NV020	Nerissa...	0	1/17/19...	Ipswich	004345...	7604229	1323430	QL		PB08
NV021	Freedda ...	1	9/19/19...	East Pe...	038532...	7000000	555316	QL		PB01
NV022	Stevie ...	0	2/27/19...	Wheatl...	000256...	15916292	1005102	QL		PB02
NV023	Joshua...	0	5/18/19...	Suffolk	058192...	9283801	1350342	QL		PB03
NV024	Federic...	1	1/7/1953	Alviso	087172...	11114296	1750487	QL		PB04
NV025	Emmett...	0	1/22/19...	Magna	007082...	19566604	1684966	TC	NV005	PB02

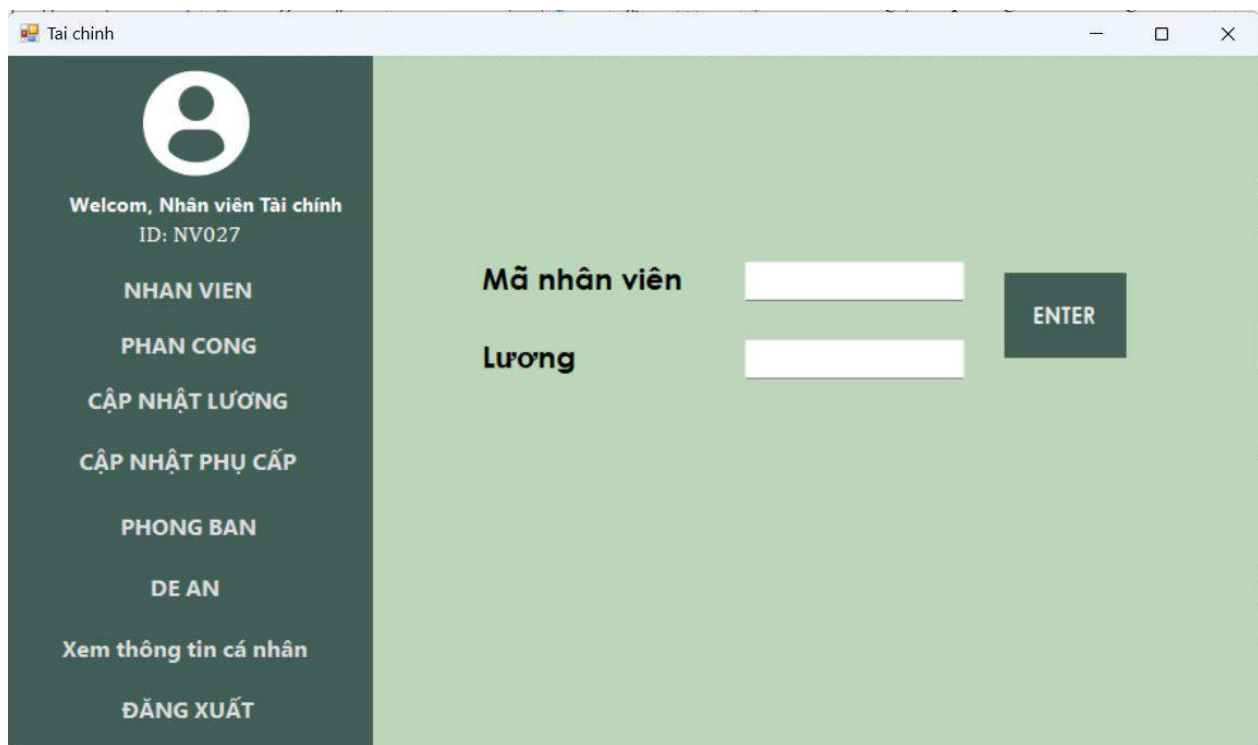
Hình 20. Giao diện vai trò **Tài chính** xem được toàn bộ quan hệ **NHANVIEN**



The screenshot shows a web application window titled 'Tai chinh'. On the left is a dark green sidebar with a user profile icon, the text 'Welcom, Nhân viên Tài chính ID: NV027', and a list of menu items: 'NHAN VIEN', 'PHAN CONG', 'CẬP NHẬT LƯƠNG', 'CẬP NHẬT PHỤ CẤP', 'PHONG BAN', 'DE AN', 'Xem thông tin cá nhân', and 'ĐĂNG XUẤT'. The main area displays a table with three columns: 'MANV', 'MADA', and 'THOIGIAN'.

MANV	MADA	THOIGIAN
NV130	DA001	2/20/2023
NV129	DA001	2/20/2023
NV128	DA001	2/20/2023
NV127	DA001	2/20/2023
NV126	DA001	2/20/2023
NV131	DA001	2/20/2023
NV124	DA001	2/20/2023
NV123	DA001	2/20/2023
NV122	DA001	2/20/2023
NV121	DA001	2/20/2023
NV125	DA001	2/20/2023
NV267	DA000	4/9/2023
NV266	DA000	4/9/2023
NV265	DA000	4/9/2023
NV264	DA000	4/9/2023
NV263	DA000	4/9/2023
NV262	DA000	4/9/2023
NV261	DA000	4/9/2023
NV260	DA000	4/9/2023
NV259	DA000	4/9/2023

Hình 21. Giao diện vai trò **Tài chính** xem được toàn bộ quan hệ **PHANCONG**



The screenshot shows the same 'Tai chinh' web application window. The sidebar menu is identical. The main area has a light green background and contains a form for updating employee salary. It includes labels for 'Mã nhân viên' (Employee ID) and 'Lương' (Salary), each followed by a text input field. To the right of these fields is a dark green button labeled 'ENTER'.

Hình 22. Giao diện vai trò **Tài chính** sửa lương của Nhân viên



Tai chính

Welcom, Nhân viên Tài chính
ID: NV027

NHAN VIEN

PHAN CONG

CẬP NHẬT LƯƠNG

CẬP NHẬT PHỤ CẤP

PHONG BAN

DE AN

Xem thông tin cá nhân

ĐĂNG XUẤT

Mã nhân viên

Phụ cấp

ENTER

Hình 23. Giao diện vai trò Tài chính sửa phụ cấp của Nhân viên

4.3.1.5. Vai trò “Nhân sự”

Khi người dùng đăng nhập vào hệ thống có vai trò **Nhân sự (NS)**, người dùng đó sẽ được:

- Có các tính năng của vai trò *Nhân viên*.
- Quản lý thông tin phòng ban của công ty (Thêm, sửa).
- Quản lý thông tin nhân viên trong công ty (Thêm, sửa nhưng trừ thông tin *Lương*, *Phụ cấp* của nhân viên và cũng không được xem hai thông tin này).
- Giao diện

Welcome, Nhân Sự
ID: NV031

NHAN VIEN
PHONG BAN
DE AN
PHAN CONG
ĐĂNG XUẤT

Bảng phòng ban F5

MAPB	TENPB	TRPHG
PB01	PHONG SAN XUAT	NV038
PB02	PHONG TAI CHINH	NV039
PB03	PHONG NHAN SU	NV040
PB04	PHONG IT	NV041
PB05	PHONG DAO TAO	NV042

Thêm thông tin phòng ban

MaPB: PB09
Tên phòng ban:
Thêm

Cập nhật thông tin phòng ban

Tên phòng ban:
Trưởng phòng:
Cập nhật

Hình 24. Giao diện vai trò *Nhân sự* thêm, cập nhật trên quan hệ **PHONGBAN**

Welcome, Nhân Sự
ID: NV031

NHAN VIEN
PHONG BAN
DE AN
PHAN CONG
ĐĂNG XUẤT

Cập nhật thông tin nhân viên

Tên nhân viên:
Địa chỉ:
Vai trò:
Phái (0-Nam, 1-Nữ):
SDT (Nhập 10 số):
Mã người quản lí:
Ngày sinh: Thursday, June 22, 2023
Phòng:

thi nhân vào dòng có mã nhân viên bạn muốn cập nhật, sau đó sửa thông tin, nhấn cập nhật

Cập nhật

MANV	TENNV	PHAI	NGAYS	DIACHI	SDT	VAITRO	MANQL	PHG
NV000	Vanit...	1	3/7/1...	Sudler...	05807...	BGD		
NV001	Kenni...	1	7/2/1...	Whea...	00225...	BGD		
NV002	Cary B...	0	1/15/...	Butler...	00595...	BGD		
NV003	Kathy...	1	11/22...	Magee...	00707...	BGD		
NV004	Erasm...	0	11/8/...	East P...	07994...	BGD		
NV005	Rodri...	0	2/22/...	Alvara...	01650...	QL		PB02

Chức năng

Thêm
Cập nhật
Load Bảng
Xem thông tin của bản

Hình 25. Giao diện vai trò *Nhân sự* thêm, cập nhật trên quan hệ **NHANVIEN**

4.3.1.6. Vai trò “**Trưởng đề án**”

Khi người dùng đăng nhập vào hệ thống có vai trò **Trưởng đề án (TDA)**, người dùng đó sẽ được:

- Có các tính năng của vai trò *Nhân viên*.
- Quản lý thông tin đề án của công ty (Thêm, xóa, sửa).
- **Giao diện**

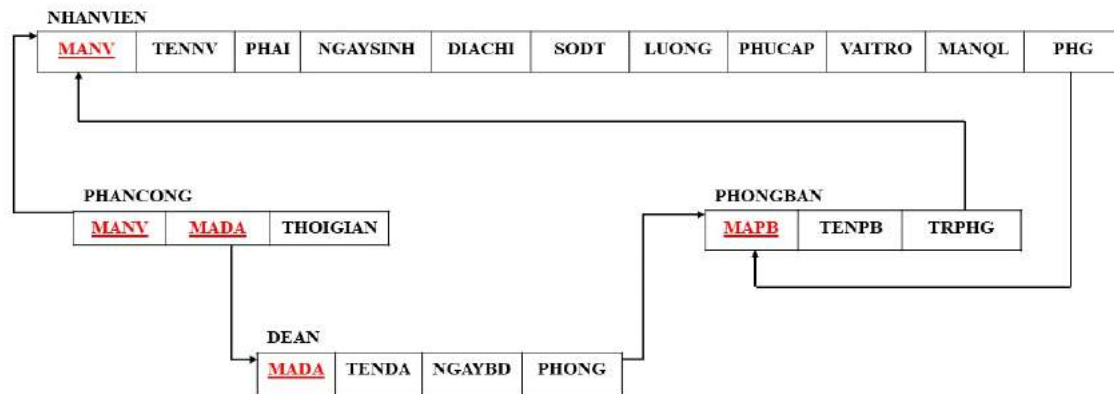
MADA	TENDA	NGÀYBD	PHÒNG
DA000	DE AN A	3/9/2023	PB07
DA001	DE AN N	2/18/2023	PB06
DA002	DE AN K	9/6/2022	PB02
DA003	DE AN D	7/28/2022	PB08
DA004	DE AN M	12/10/2022	PB05
DA005	DE AN O	5/17/2022	PB07
DA006	DE AN X	5/10/2022	PB01
DA007	DE AN F	7/17/2022	PB02
DA008	DE AN R	3/5/2022	PB02
DA009	DE AN G	3/30/2023	PB08
DA010	DE AN Y	4/23/2022	PB01
DA011	DE AN J	1/5/2022	PB02
DA012	DE AN L	8/28/2022	PB07
DA013	DE AN P	1/1/2022	PB04
DA014	DE AN E	10/28/2022	PB08
DA015	DE AN Q	1/15/2023	PB01
DA016	DE AN T	8/22/2022	PB06

Hình 26. Giao diện vai trò **Trưởng đề án** thêm, xóa, sửa trên quan hệ **DEAN**

4.3.1.7. Vai trò “**Ban giám đốc**”

Khi người dùng đăng nhập vào hệ thống có vai trò **Ban giám đốc (BGD)**, người dùng đó sẽ được: Xem tất cả thông tin trong hệ thống nhưng không được thêm, xóa, sửa bất kỳ thông tin nào.

4.3.2. Lược đồ CSDL



Hình 27. Lược đồ cơ sở dữ liệu quan hệ được cài đặt

4.3.3. Các chính sách bảo mật

4.3.3.1. Chính sách DAC

- **DAC** là viết tắt của "**Discretionary Access Control**" (*Kiểm soát truy cập tùy ý*). Trong Oracle Database, DAC đề cập đến hệ thống kiểm soát truy cập dựa trên quyền hạn được xác định bởi người quản trị cơ sở dữ liệu hoặc chủ sở hữu đối tượng. DAC cho phép người quản trị hoặc chủ sở hữu quyết định và kiểm soát quyền truy cập tới các đối tượng cơ sở dữ liệu, chẳng hạn như bảng, chế độ xem, thủ tục lưu trữ và tài khoản người dùng.

- Trong hệ thống DAC của Oracle, người quản trị hoặc chủ sở hữu có thể gán các quyền cụ thể cho người dùng hoặc vai trò. Quyền hạn này có thể bao gồm quyền SELECT, INSERT, UPDATE, DELETE, EXECUTE và nhiều quyền khác. Người dùng hoặc vai trò chỉ có thể thực hiện các hoạt động trên đối tượng nếu được cấp phép.

- Ở phân hệ 2, mỗi người dùng sẽ được cấp một username riêng và mật khẩu riêng để đăng nhập vào cơ sở dữ liệu. Với nhiều số lượng người dùng nhiều hơn 100 người nên nhóm chúng em đã sử dụng phần lớn là RBAC thay cho DAC.

4.3.3.2. Chính sách RBAC

- **RBAC** là viết tắt của "**Role-Based Access Control**" (*Kiểm soát truy cập dựa trên vai trò*). RBAC là một phương pháp quản lý truy cập trong lĩnh vực an ninh thông tin, trong đó quyền hạn truy cập được gán dựa trên vai trò của người dùng.

- Trong hệ thống RBAC, người dùng được gán vào các vai trò khác nhau. Mỗi vai trò sẽ có một tập hợp các quyền hạn tương ứng với các hoạt động mà người dùng trong vai trò đó có thể thực hiện. Thay vì gán quyền truy cập cho từng người dùng cụ thể, quyền hạn được gán cho các vai trò và người dùng được gán vào các vai trò đó.

- Chương trình đã cài đặt chính sách này với từng trường hợp cụ thể, như sau:

- Đối với vai trò '**Nhân viên**', chương trình cài đặt các view để kiểm soát người dùng chỉ được xem thông tin chính mình trong hai bảng **NHANVIEN** và **PHANCONG**. Và chỉ được cập nhật thông tin ngày sinh, địa chỉ và số điện thoại của mình trong bảng **NHANVIEN**.
- Đối với vai trò '**Quản lý**', chương trình cài đặt cái view để người dùng chỉ được phép xem các thuộc tính ngoại trừ **LUONG** và **PHUCAP** của các nhân viên khác.
- Đối với vai trò '**Trưởng phòng**', chương trình cài đặt view để người dùng chỉ *thêm, xoá, cập nhật* trên quan hệ **PHANCONG** của các nhân viên thuộc phòng ban của trưởng phòng đó.
- Đối với vai trò '**Tài chính**', chương trình đã gán quyền xem trên bảng **PHANCONG** và **NHANVIEN**, ngoài ra người dùng còn được gán quyền cập nhật trên hai trường **LUONG** và **PHUCAP** trong quan hệ **NHANVIEN**.
- Đối với vai trò '**Nhân sự**', chương trình đã gán quyền thêm, cập nhật trên quan hệ **PHONGBAN**.

- Đối với vai trò ‘**Trưởng đề án**’, chương trình đã gán quyền thêm, xóa, cập nhật trên quan hệ **DEAN**.

4.3.3.3. Chính sách VPD

- **VPD** là viết tắt của ‘**Virtual Private Database**’. VPD là một tính năng trong cơ sở dữ liệu Oracle cho phép triển khai các quy tắc bảo mật dữ liệu trên cơ sở dữ liệu mà không cần thay đổi ứng dụng hoặc schema hiện có. VPD cho phép kiểm soát quyền truy cập dựa trên các điều kiện động, dựa trên dữ liệu trong cơ sở dữ liệu và thông tin người dùng.

- VPD sử dụng các chức năng quyền (policy function) để xác định các quy tắc truy cập cho dữ liệu. Khi người dùng truy cập vào bất kỳ đối tượng nào trong cơ sở dữ liệu, VPD sẽ kích hoạt các chức năng quyền để xác định quyền truy cập của người dùng dựa trên các quy tắc được xác định trước.

- Chương trình đã cài đặt chính sách này với từng trường hợp cụ thể, như sau:

- Đối với vai trò ‘**Quản lý**’, chương trình đã cài đặt VPD để kiểm soát chỉ cho phép người dùng chỉ được xem thông tin của nhân viên do mình quản lý ngoại trừ hai trường **LUONG** và **PHUCAP**.

- Đối với vai trò ‘**Trưởng phòng**’, chương trình đã cài đặt vpd để giới hạn người dùng chỉ được phép xem các thông tin ngoại trừ **LUONG** và **PHUCAP** của nhân viên thuộc phòng ban của mình.

4.3.3.4. OLS:

4.3.3.4.1. *Gán nhãn cho Giám đốc, Trưởng phòng và Giám đốc miền Bắc*

• **Tạo Level:**

POLICY_NAME	LONG_NAME	SHORT_NAME	LEVEL_NUM
ESBD	GIAM DOC	GD	9000

ESBD	TRUONG PHONG	TP	8000
ESBD	NHAN VIEN	NV	7000

• **Tạo Compartment:**

POLICY_NAME	LONG_NAME	SHORT_NAME	COMP_NUM
ESBD	MUA BAN	MB	100
ESBD	SAN XUAT	SX	200
ESBD	GIA CONG	GC	300

• **Tạo Group:**

POLICY_NAME	LONG_NAME	SHORT_NAME	GROUP_NUM	PARRENT_NAME
ESBD	TAP DOAN S	S	1	NULL
ESBD	MIEN BAC	B	10	1
ESBD	MIEN TRUNG	T	20	1
ESBD	MIEN NAM	N	30	1

• **Tạo Nhãn:**

Quy ước tạo nhãn để dễ dàng quản lý:

- Cấu trúc nhãn: xyzt
 - x: giá trị level quy ước.
 - y: giá trị compartment quy ước.
 - z: giá trị group quy ước.

- t: giá trị dự phòng, mặc định $t = 0$.
- Level:
 - GD: 3
 - TP: 2
 - NV: 1
- Compartment:
 - SX: 1
 - GC: 2
 - MB: 3
 - Các nhãn bao gồm nhiều compartment thì lấy tổng các compartment thành phần làm giá trị quy ước.
- Group:
 - B: 1
 - T: 2
 - N: 3
 - Các nhãn bao gồm nhiều group thì lấy tổng các group thành phần làm giá trị quy ước.

POLICY_NAME	LABEL_TAG	LABEL_VALUE
ESBD	GD	3000
ESBD	TP	2000
ESBD	NV	1000
ESBD	GD:MB,SX,GC:B,T,N	3660
ESBD	NV:SX:N	1130
ESBD	NV:MB,SX,GC:B,T,N	1660
ESBD	TP:SX:N	2130
ESBD	TP:SX:T	2120

ESBD	GD: SX, GC, MB: B	3610
ESBD	TP: MB, SX, GC: B, T, N	2660
ESBD	GD: GC: N	3230

• Gán nhãn cho một số người dùng:

MÔ TẢ NGƯỜI DÙNG	POLICY_NAME	USER_NAME	MAX_READ_LABEL
<i>Giám đốc quản lý toàn bộ công ty</i>	ESBD	GIAMDOC	GD: MB, SX, GC: B, T, N
<i>Giám đốc phụ trách tất cả các lĩnh vực ở miền Bắc</i>	ESBD	GIAMDOCMB	GD: MB, SX, GC: B
Trưởng phòng quản lý tất cả các chi nhánh.	ESBD	TRUONGPHONG	TP: MB, SX, GC: B, T, N
<i>Trưởng phòng phụ trách lĩnh vực sản xuất ở miền Nam</i>	ESBD	TPSXMN	TP: SX: N
Trưởng phòng phụ trách lĩnh vực sản xuất ở miền Trung	ESBD	TPSXMT	TP: SX: T
Nhân viên bình thường, không làm trong bất kì các lĩnh vực nào.	ESBD	NHANVIEN	NV
Giám đốc phụ trách lĩnh vực gia công ở miền Nam	ESBD	GIAMDOC_GC_MN	GD: GC: N

4.3.3.4.2. *Cách thức phát tán dòng thông báo t1 đến tất cả các Trưởng phòng không phân biệt lĩnh vực*

❖ **REMOVE** chính sách OLS hiện tại (**ESBD**) trên bảng **ANNOUNCEMENTS**.

❖ Áp dụng lại chính sách '**ESBD**' lên bảng **ANNOUNCEMENTS** với **TABLE_OPTIONS** => '**NO_CONTROL**'.

❖ Thêm dòng dữ liệu (thông báo t1) vào bảng **ANNOUNCEMENTS**.

❖ Thiết lập giá trị **ROW_LABEL** của dòng dữ liệu bằng cách sử dụng phương thức: **CHAR_TO_LABEL** ('**ESBD**', '**TP**').

❖ Áp dụng lại chính sách '**ESBD**' lên bảng **ANNOUNCEMENTS** một lần nữa với **TABLE_OPTIONS** => '**READ_CONTROL, CHECK_CONTROL**'.

4.3.3.4.3. *Cách thức phát tán dòng thông báo t2 đến tất cả các Trưởng phòng sản xuất miền Trung*

❖ **REMOVE** chính sách OLS hiện tại (**ESBD**) trên bảng **ANNOUNCEMENTS**.

❖ Áp dụng lại chính sách '**ESBD**' lên bảng **ANNOUNCEMENTS** với **TABLE_OPTIONS** => '**NO_CONTROL**'.

❖ Thêm dòng dữ liệu (thông báo t2) vào bảng **ANNOUNCEMENTS**.

❖ Thiết lập giá trị **ROW_LABEL** của dòng dữ liệu bằng cách sử dụng phương thức: **CHAR_TO_LABEL** ('**ESBD**', '**TP: SX:T**').

❖ Áp dụng lại chính sách '**ESBD**' lên bảng **ANNOUNCEMENTS** một lần nữa với **TABLE_OPTIONS** => '**READ_CONTROL, CHECK_CONTROL**'.

4.3.3.4.4. *Một số cách thức phát tán dòng dữ liệu khác*

4.3.3.4.4.1. Phát tán dòng thông báo đến tất cả các nhân viên không phân biệt lĩnh vực, vị trí:

❖ **REMOVE** chính sách OLS hiện tại (**ESBD**) trên bảng **ANNOUNCEMENTS**.

❖ Áp dụng lại chính sách ‘ESBD’ lên bảng ANNOUNCEMENTS với TABLE_OPTIONS => ‘NO_CONTROL’.

❖ Thêm dòng dữ liệu vào bảng ANNOUNCEMENTS.

❖ Thiết lập giá trị ROW_LABEL của dòng dữ liệu bằng cách sử dụng phương thức: CHAR_TO_LABEL (‘ESBD’, ‘NV’).

❖ Áp dụng lại chính sách ‘ESBD’ lên bảng ANNOUNCEMENTS một lần nữa với TABLE_OPTIONS => ‘READ_CONTROL, CHECK_CONTROL’.

4.3.3.4.4.2. Phát tán dòng thông báo đến các giám đốc gia công miền Nam

❖ REMOVE chính sách OLS hiện tại (ESBD) trên bảng ANNOUNCEMENTS.

❖ Áp dụng lại chính sách ‘ESBD’ lên bảng ANNOUNCEMENTS với TABLE_OPTIONS => ‘NO_CONTROL’.

❖ Thêm dòng dữ liệu vào bảng ANNOUNCEMENTS.

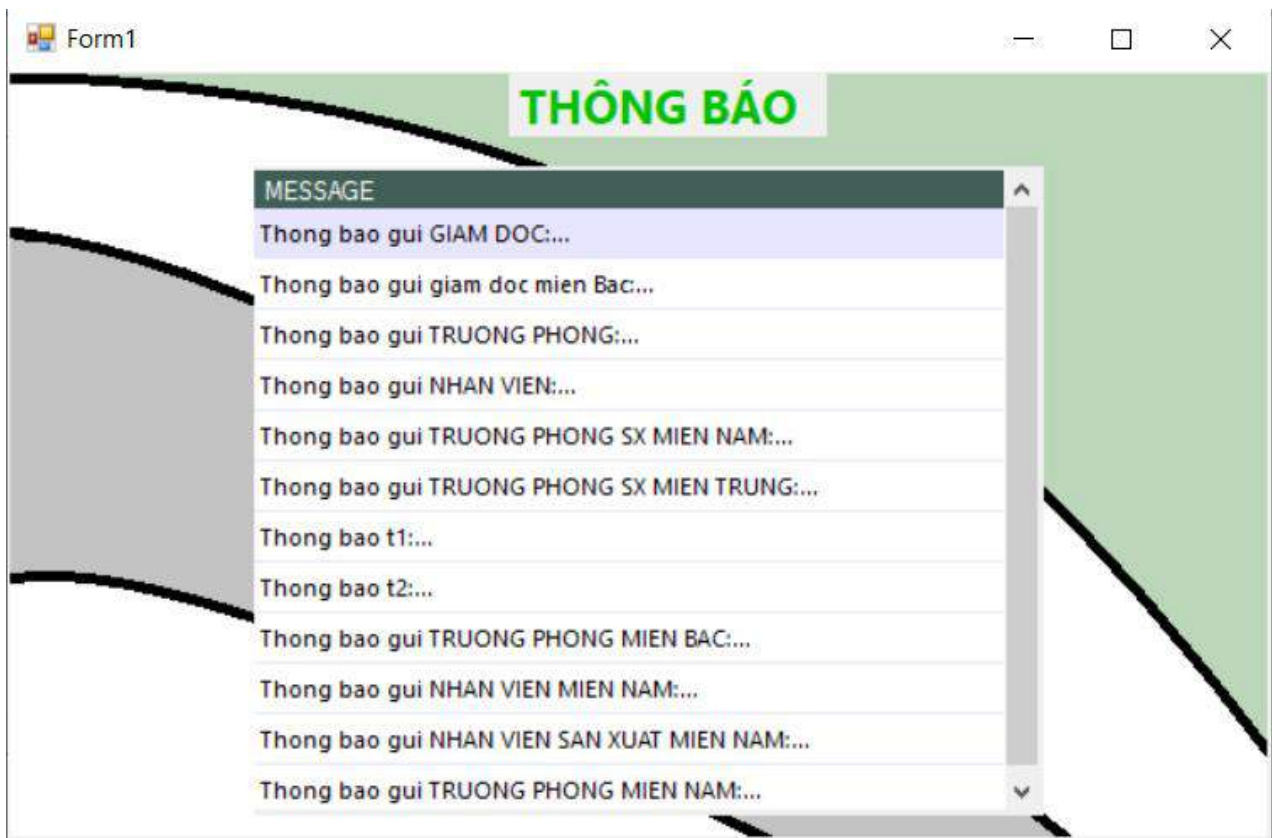
❖ Thiết lập giá trị ROW_LABEL của dòng dữ liệu bằng cách sử dụng phương thức: CHAR_TO_LABEL (‘ESBD’, ‘GD:GC:N’).

❖ Áp dụng lại chính sách ‘ESBD’ lên bảng ANNOUNCEMENTS một lần nữa với TABLE_OPTIONS => ‘READ_CONTROL. CHECK_CONTROL’.

4.3.3.4.5. *Giao diện chức năng OLS*

4.3.3.4.5.1. Một giám đốc có thể đọc được toàn bộ dữ liệu

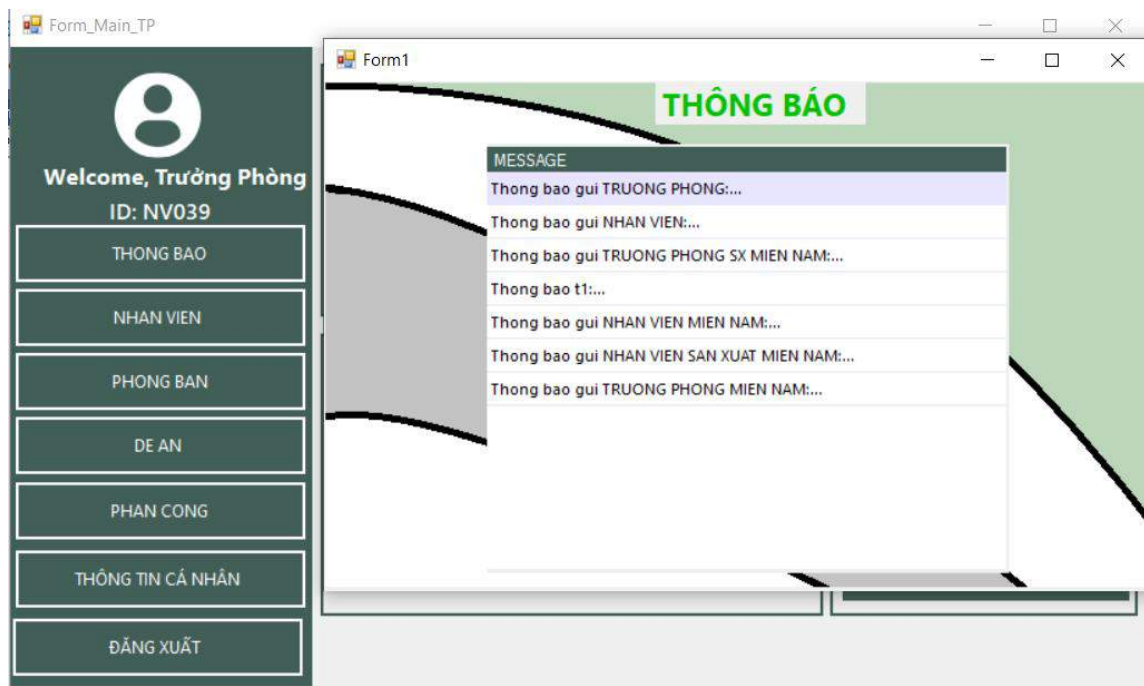
Nhóm chúng em đã gán nhãn cho người dùng là “NV000” với nhãn là ‘GD:MB,SX,GC:B,T,N’ để cho người dùng này có vai trò giám đốc có thể đọc được toàn bộ thông báo.



Hình 28. Giao diện hiển thị các thông báo cho một giám đốc có thể đọc được toàn bộ dữ liệu

4.3.3.4.5.2. Người dùng có vai trò trưởng phòng sản xuất Miền Nam

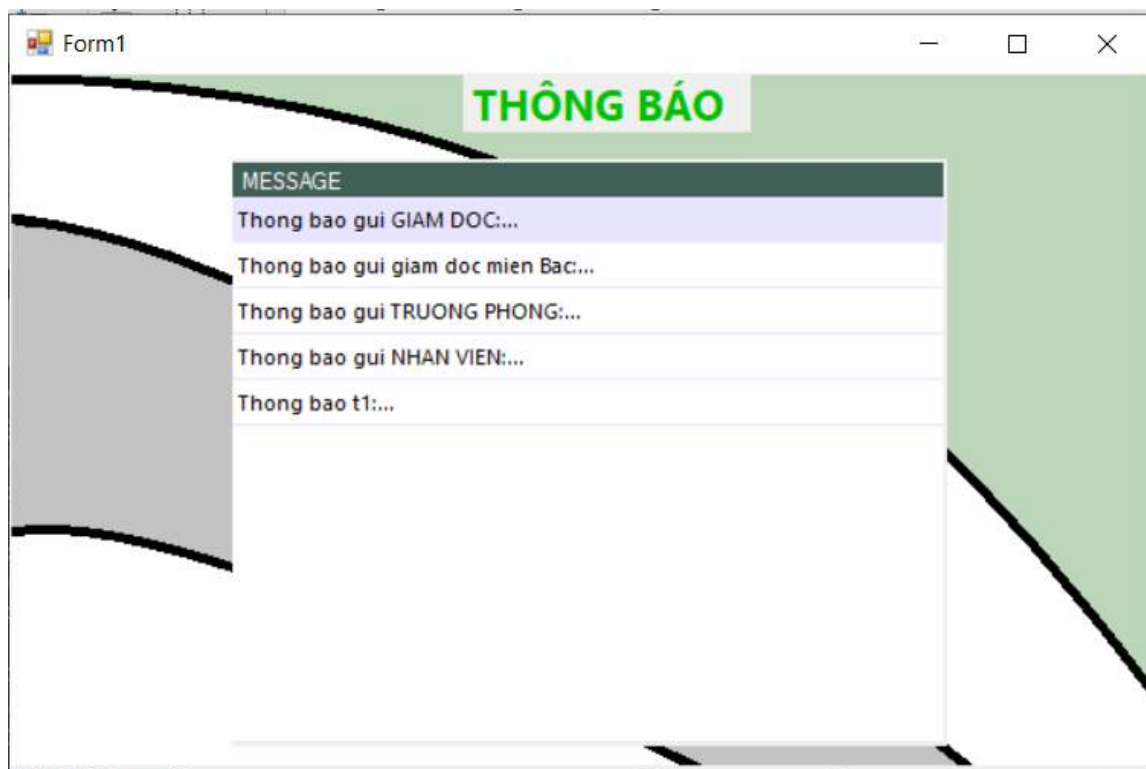
- Gán nhãn cho người dùng “NV039” với nhãn 'TP: SX: N' để cho người dùng này có vai trò Trưởng phòng sản xuất miền Nam.



Hình 29. Giao diện hiển thị các thông báo mà *Trưởng phòng sản xuất miền Nam* có quyền đọc

4.3.3.4.5.3. Người dùng với vai trò giám đốc phụ trách bất kì lĩnh vực nào ở miền bắc

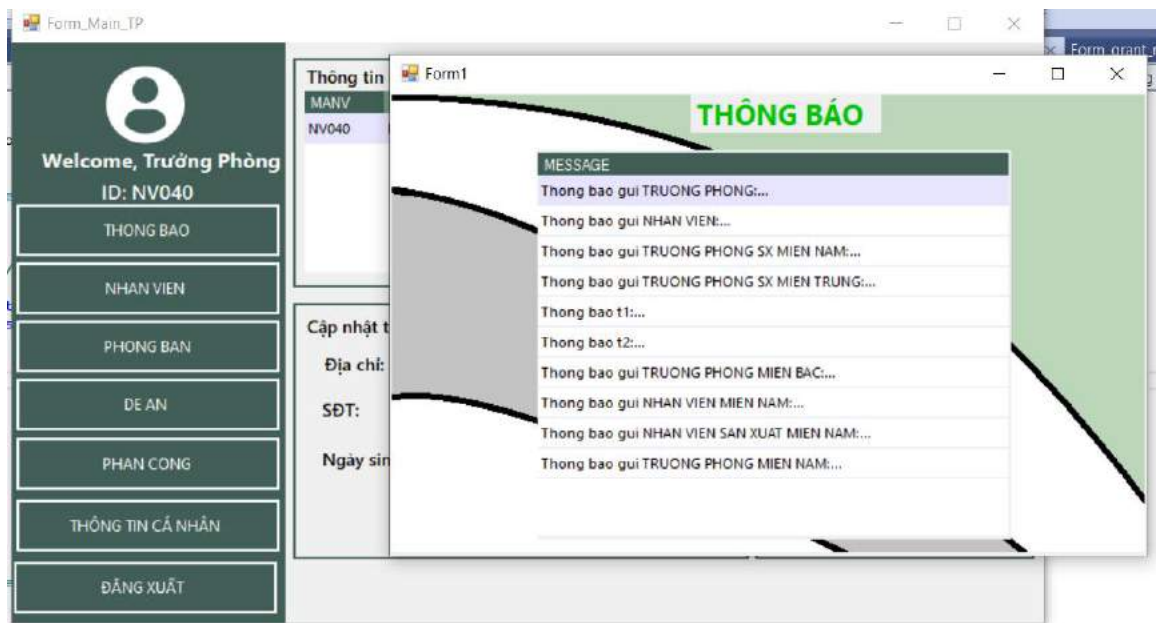
- Gán nhãn '**GD:MB,SX,GC:B**' cho người dùng “**NV001**” để cho người dùng này trở thành Giám đốc miền Bắc.



Hình 30. Giao diện hiển thị các thông báo mà các *giám đốc ở miền Bắc* có quyền đọc

4.3.3.4.5.4. Cách thức phát tán dòng thông báo t1 đến tất cả trưởng phòng phụ trách tất cả các lĩnh vực không phân biệt chi nhánh.

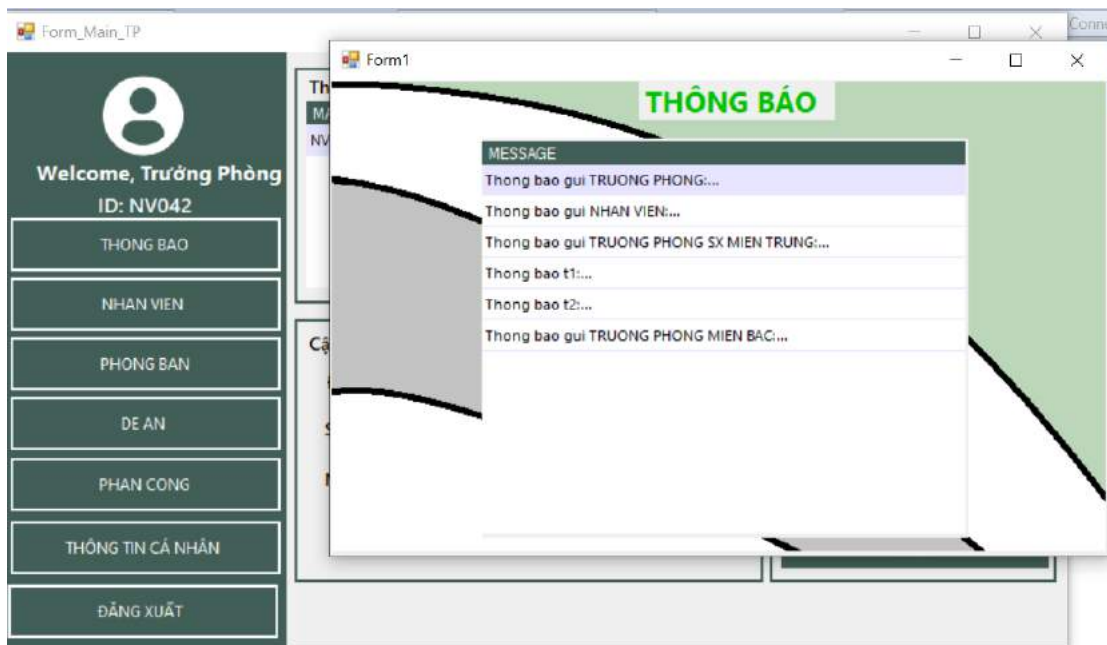
- Khi thêm vào bảng, thông báo t1 sẽ được gán nhãn '**TP**' để cho các người dùng là trưởng phòng xem được thông báo này.



Hình 31. Giao diện phát tán dòng thông báo t1

4.3.3.4.5.5. Cách thức phát tán dòng thông báo t2 đến trưởng phòng phụ trách lĩnh vực sản xuất ở miền Trung.

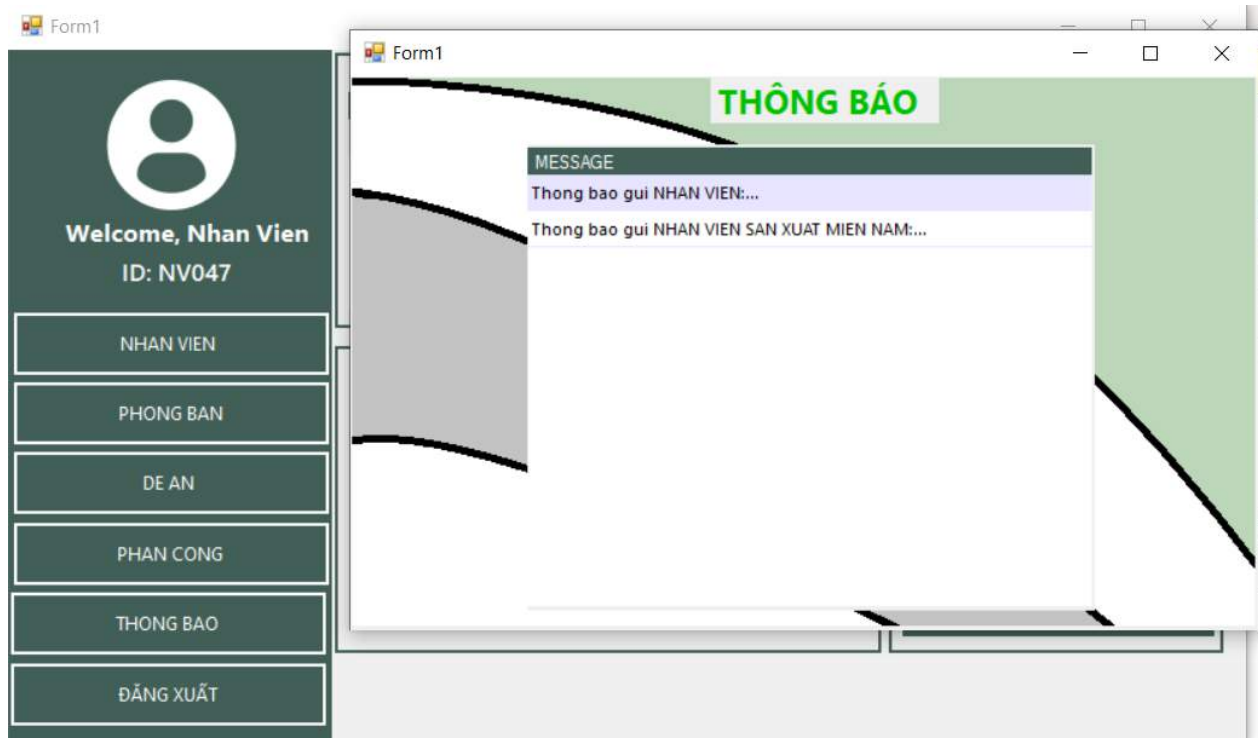
- Gán cho “NV042” và thông báo t2 cùng một nhãn ‘**TP:SX:T**’ để cho người dùng này trở thành Trưởng phòng phụ trách lĩnh vực sản xuất ở miền Trung và xem được thông báo t2.



Hình 32. Giao diện phát tán dòng thông báo t2

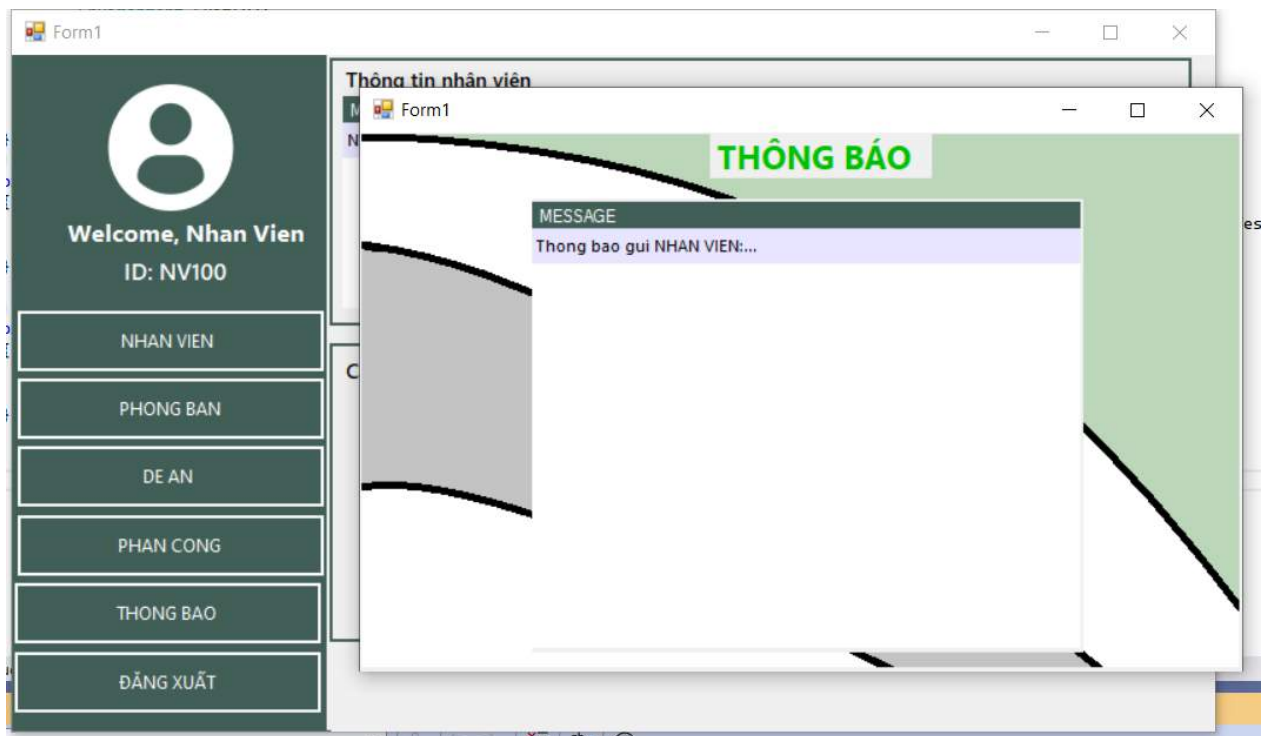
4.3.3.4.5.6. Một số kịch bản phụ

- Gán nhãn ‘NV: SX: N’ cho ‘NV047’, giả sử rằng đây là một Nhân viên sản xuất Miền Nam. Nhân viên này chỉ đọc được các thông báo gửi đến toàn bộ các nhân viên, các nhân viên sản xuất và các nhân viên có cùng nhãn với nhân viên này.



Hình 33. Giao diện hiển thị các dòng thông báo mà Nhân viên sản xuất tại miền Nam có thể đọc

- Gán nhãn một thông báo với nhãn ‘NV’, đây sẽ là thông báo chứa thông tin có mức độ nhạy cảm thấp nhất, thông báo này sẽ được đọc bởi tất cả các người dùng được gán nhãn và cấp quyền truy cập vào bảng thông báo.



Hình 34. Giao diện hiển thị dòng thông báo được phát tán cho toàn bộ Nhân viên.

4.3.4. Mã hóa

4.3.4.1. User vai trò gì thực hiện mã hóa?

User có vai trò là quản trị hệ thống hoặc quản trị cơ sở dữ liệu sẽ thực hiện mã hóa dữ liệu. Những người dùng này có quyền truy cập và sửa đổi cấu trúc dữ liệu và mã hóa.

4.3.4.2. Mã hóa dữ liệu ở mức nào?

Nhóm thực hiện mã hóa mức cơ sở dữ liệu (Database Level). Những lí do mà nhóm chọn mức mã hóa này:

- **Tính toàn vẹn của dữ liệu:** Mã hóa dữ liệu ở mức cơ sở dữ liệu đảm bảo tính toàn vẹn của dữ liệu. Dữ liệu được mã hóa trước khi lưu trữ, điều này đảm bảo rằng dữ liệu chỉ có thể được giải mã bởi những người có quyền truy cập.
- **Bảo mật toàn diện:** Mã hóa dữ liệu ở mức cơ sở dữ liệu bảo vệ thông tin nhạy cảm khỏi sự truy cập trái phép. Ngay cả khi dữ liệu bị lộ, thông tin sẽ

không thể đọc được nếu không có khóa mã hóa phù hợp.

- **Tính linh hoạt:** Mã hóa dữ liệu ở mức cơ sở dữ liệu giúp đảm bảo tính riêng tư của thông tin mà không yêu cầu thay đổi cấu trúc lưu trữ dữ liệu. Các ứng dụng hoặc giao diện người dùng có thể tiếp tục hoạt động như bình thường, chỉ thay đổi ở mức cơ sở dữ liệu.
- **Chống được các kiểu tấn công:** đánh cắp thiết bị lưu trữ, tấn công mức cơ sở dữ liệu (ví dụ SQL injection), người quản trị truy cập dữ liệu bất hợp pháp
- Được đảm nhận thông qua việc dùng thủ tục hoặc trigger

Ở đây chúng em đã sử dụng cấp độ mã hóa cơ sở dữ liệu là **Column/Attribute level (cấp độ cột/thuộc tính)** cụ thể là mã hóa các thông tin trong cột **LUONG** và **PHUCAP**.

4.3.4.3. Có cần thay đổi gì về cấu trúc lưu trữ dữ liệu hay không?

Trong đề xuất giải pháp mã hóa dữ liệu ở mức cơ sở dữ liệu, không cần thay đổi cấu trúc lưu trữ dữ liệu. Dữ liệu vẫn được lưu trữ dưới dạng thông thường trong cơ sở dữ liệu, nhưng trước khi lưu trữ, thông tin liên quan đến trường **LUONG** và **PHUCAP** sẽ được mã hóa.

Việc mã hóa dữ liệu không yêu cầu thay đổi cấu trúc lưu trữ dữ liệu vì quá trình mã hóa và giải mã được thực hiện trên dữ liệu gốc trước khi lưu vào cơ sở dữ liệu. Khi cần truy xuất dữ liệu, quá trình giải mã sẽ được thực hiện để trả về dữ liệu ban đầu cho ứng dụng hoặc giao diện người dùng.

Điều này giúp bảo vệ tính riêng tư của thông tin nhân viên liên quan đến trường **LUONG** và **PHUCAP** mà không ảnh hưởng đến cấu trúc lưu trữ dữ liệu hiện có. Hệ thống và ứng dụng có thể tiếp tục hoạt động như bình thường mà không cần thay đổi cách lưu trữ dữ liệu.

4.3.4.4. Cơ chế quản lý khóa

Cơ chế mã hóa được áp dụng như sau:

- ❖ Thiết lập khoá

- Việc tạo khóa sẽ dựa trên mật khẩu người dùng.
- Nhóm chúng em đã sử dụng hàm **PBKDF2** (*Password-Based Key Derivation Function 2*) để tạo ra một khóa từ mật khẩu với muối.
- Với tham số đầu vào là mật khẩu ban đầu trong dạng VARCHAR2, muối, số lần lặp để gia tăng độ phức tạp thuật toán và một biến để yêu cầu độ dài khóa đầu ra mong muốn.
- Trong hàm có sử dụng thuật toán **HMAC-SHA1**(*HMAC-Secure Hash Algorithm 1*).
- Sau khi chạy hàm thì sẽ trả về kết quả cuối cùng, khóa đầu ra của hàm cũng với độ dài tương ứng bằng cách sử dụng hàm **UTL_RAW.SUBSTR**.
- Mã hóa hai cột **LUONG** và **PHUCAP**
- Viết 1 thủ tục gọi là "**encrypt_EACH_NHANVIEN**" sử dụng 1 package mã hóa dữ liệu trên Oracle là **DBMS_CRYPTO**. Trong package đó, nhóm em sử dụng một số phương pháp để hỗ trợ mã hóa dữ liệu:
 - **DBMS_CRYPTO.ENCRYPT_AES128**: Chọn thuật toán mã hóa AES với khóa 128 bit. Độ dài khóa 128-bit đảm bảo tính bảo mật cao đối với việc mã hóa dữ liệu. Việc sử dụng **DBMS_CRYPTO.ENCRYPT_AES128** trong thủ tục "**encrypt_EACH_NHANVIEN**" cho phép mã hóa dữ liệu lương và phụ cấp của nhân viên với một thuật toán mã hóa mạnh mẽ và bảo mật, đồng thời đảm bảo tính hiệu suất và tương thích với hệ thống Oracle Database.
 - **DBMS_CRYPTO.CHAIN_CBC**: Chế độ **Cipher Block Chaining (CBC)** được sử dụng để mã hóa. Trong chế độ này, mỗi khối dữ liệu được mã hóa được kết hợp với khối trước đó trước khi tiến hành mã hóa.
 - **DBMS_CRYPTO.PAD_PKCS5**: Chuẩn **PKCS5** được sử dụng để thực hiện padding cho dữ liệu. **Padding** là quá trình thêm các bytes đệm vào dữ liệu để đảm bảo độ dài của dữ liệu là bội số của kích thước khối mã hóa.
 - **key**: Đây là khóa được sử dụng để mã hóa dữ liệu. Trong trường hợp này, khóa (v_key) đã được tạo trước đó bằng cách sử dụng hàm **pbkdf2**.

▪ **iv**: Đây là vector khởi tạo (**Initialization Vector - IV**), được sử dụng trong quá trình mã hóa CBC. Trong trường hợp này, vector khởi tạo (**v_iv**) đã được tạo ngẫu nhiên.

❖ Phân phối khoá

- Mỗi người dùng sau khi được tạo tài khoản thì sẽ được cấp mật khẩu ban đầu là username của mình và mật khẩu này cũng sẽ được dùng để làm khoá cho việc mã hoá hai trường '**LUONG**' và '**PHUCAP**'.

- Sau khi đăng nhập lần đầu tiên, ứng dụng sẽ yêu cầu người dùng đổi mật khẩu trước khi sử dụng ứng dụng.

- Đối với chức năng '**Xem LUONG và PHUCAP**' thì người dùng phải nhập đúng mật khẩu của mình mới được xem.

❖ Lưu trữ khoá

- Nhóm chúng em đã tạo ra một bảng **DANGNHAP** để *lưu trữ khóa tạo ra và vector khởi tạo iv*. Bằng cách lưu trữ khóa trên bảng đăng nhập, chúng em thể quản lý khóa một cách cụ thể cho từng người dùng và có thể áp dụng các chính sách bảo mật khác nhau cho khóa.

- Việc lưu trữ khóa trên bảng đăng nhập cũng có thể giúp quản lý và kiểm soát quyền truy cập vào khóa. Chỉ các người dùng được phép truy cập vào bảng đăng nhập mới có thể lấy được khóa. Điều này giúp đảm bảo rằng chỉ những người dùng có quyền truy cập hợp lệ mới có thể sử dụng khóa để giải mã dữ liệu.

❖ Phục hồi khóa

- **PBKDF2** được sử dụng để tạo khóa từ mật khẩu người dùng. Điều này đảm bảo rằng khóa mã hóa sẽ được tạo ra từ mật khẩu của người dùng một cách an toàn và không thể dễ dàng phục hồi. **PBKDF2** sử dụng một số lượng lặp lại và giá trị muối (salt) để tăng cường tính bảo mật. Quá trình tính toán **PBKDF2** là một hàm một chiều, nghĩa là không thể dễ dàng đảo ngược để phục hồi mật khẩu ban đầu từ khóa.

- Trong trường hợp người dùng quên mật khẩu của họ, không có cách trực tiếp để phục hồi khóa để giải mã cột Lương và Phụ Cấp. Thay vào đó, phương pháp phổ biến là yêu cầu người dùng tạo một mật khẩu mới và sử dụng nó để tạo khóa mới thông qua **PBKDF2**. Sau đó, bạn có thể sử dụng khóa mới này để giải mã và truy cập vào dữ liệu cột Lương và Phụ Cấp.

- Trong quá trình này, mật khẩu ban đầu sẽ không được phục hồi, và bạn sẽ cần thông báo cho người dùng về việc thay đổi mật khẩu và cập nhật dữ liệu mật khẩu mới. Điều này đảm bảo tính bảo mật và không cho phép ai khác truy cập vào dữ liệu bằng mật khẩu đã quên.

⇒ Tóm lại, trong trường hợp sử dụng PBKDF2 để tạo khóa AES-128 từ mật khẩu người dùng, việc phục hồi khóa khi người dùng quên mật khẩu không khả thi. Thay vào đó, việc thay đổi mật khẩu và tạo khóa mới thông qua PBKDF2 là cách tiếp cận thông thường.

❖ Thay đổi khoá

- Ứng dụng sẽ bắt buộc người dùng đăng nhập đầu tiên đổi mật khẩu trước khi tiếp tục sử dụng ứng dụng.
- Sau khi mật khẩu được đổi, mật khẩu sẽ được mã hoá bằng hàm **PBKDF2** và cập nhật lại trên quan hệ **DANGNHAP**.
- Tiếp theo, hai cột **LUONG** và **PHUCAP** trên quan hệ **NHANVIEN** của người dùng đó sẽ được mã hoá bằng mật khẩu mới và cập nhật lại trên quan hệ **NHANVIEN**.

4.3.5. Audit:

4.3.5.1. Những người đã cập nhật trường THOIGIAN trong quan hệ PHANCONG.

❖ Phương thức sử dụng: FGA Audit.

❖ Cách thức cụ thể:

- Sử dụng gói **DBMS_FGA**.

• Gọi thủ tục **ADD_POLICY** và truyền các tham số để áp dụng chính sách audit lên bảng **PHANCONG** theo yêu cầu:

OBJECT_SCHEMA	COMPANY
OBJECT_NAME	PHANCONG
POLICY_NAME	A_AUDIT
AUDIT_COLUMN	THOIGIAN
STATEMENT_TYPES	UPDATE
ENABLE	TRUE

⇒ Chính sách sẽ ghi lại các hoạt động **UPDATE** trên cột **THOIGIAN** của bảng **PHANCONG** khi người dùng truy cập vào hệ thống và thực hiện việc sửa đổi thông tin cột **THOIGIAN**.

4.3.5.2. Những người đã đọc trên trường **LUONG** và **PHUCAP** của người khác:

❖ Phương thức sử dụng: FGA Audit.

❖ Cách thức cụ thể:

• Sử dụng gói **DBMS_FGA**.

• Gọi thủ tục **ADD_POLICY** và truyền các tham số để áp dụng chính sách audit lên bảng **NHANVIEN** theo yêu cầu:

OBJECT_SCHEMA	COMPANY
OBJECT_NAME	NHANVIEN
POLICY_NAME	B_AUDIT
AUDIT_COLUMN	LUONG, PHUCAP

AUDIT_CONDITION	NHANVIEN.MANV != SYS_CONTEXT ("USERENV", "SESSION_USER")
STATEMENT_TYPES	SELECT
ENABLE	TRUE

⇒ Chính sách sẽ ghi lại các hoạt động **SELECT** trên cột **LUONG** và **PHUCAP** của bảng **NHANVIEN** khi mà người dùng truy cập có **USERNAME** khác với **MANV** trong bảng **NHANVIEN** mà người đó đang cố gắng **SELECT**.

4.3.5.3. Những người không thuộc vai trò “Tài chính” nhưng cập nhật thành công thuộc tính ‘LUONG’ và ‘PHUCAP’

- ❖ Phương thức sử dụng: Trigger Audit
- ❖ Cách thức cụ thể:

- Tạo bảng ‘**aud_LUONG**’: Bảng này được tạo để lưu trữ các bản ghi kiểm tra. Nó bao gồm các cột để lưu trữ thông tin như tên người dùng, loại hành động (insert, update, delete), **NHANVIEN** bị ảnh hưởng, tên cột, Call Stack, ID Client, giá trị cũ, giá trị mới và ngày thực hiện hành động.

- Thủ tục ‘**audit_LUONG**’: Thủ tục này được sử dụng để chèn các bản ghi kiểm tra vào bảng ‘**aud_LUONG**’. Nó nhận các tham số như tên người dùng, loại hành động, **NHANVIEN**, tên cột, giá trị cũ và giá trị mới. Thủ tục sử dụng hàm **DBMS_UTILITY.format_call_stack** để lấy **Call Stack** và **SYS_CONTEXT('userenv', 'client_identifier')** để lấy **ID Client**.

- Thủ tục ‘**show_aud_LUONG_PHUCAP**’: Thủ tục này được sử dụng để hiển thị các bản ghi kiểm tra từ bảng ‘**aud_LUONG**’. Nó truy xuất các bản ghi từ bảng theo thứ tự giảm dần của ngày hành động và xuất thông tin liên quan bằng cách sử dụng gói ‘**DBMS_OUTPUT**’.

- Trigger ‘**update_LUONG_trig**’: Trigger này được kích hoạt trước khi thực hiện cập nhật trên cột ‘**LUONG**’ của bảng ‘**NHANVIEN**’. Nó kiểm tra xem người dùng có vai trò 'TC' (như được chỉ định trong bảng ‘**DBA_ROLE_PRIVS**’)

hoặc người dùng 'COMPANY' hay không. Nếu điều kiện được đáp ứng, thủ tục 'audit_LUONG' được gọi với các tham số cần thiết để chèn một bản ghi kiểm tra cho việc cập nhật.

- Trigger 'update_PHUCAP_trig': Trigger này tương tự như trigger trước, nhưng được kích hoạt trước khi thực hiện cập nhật trên cột 'PHUCAP' của bảng 'NHANVIEN'. Nó cũng gọi thủ tục 'audit_LUONG' để chèn một bản ghi kiểm tra.

4.3.5.4. Kiểm tra nhật kí hệ thống

- Kiểm tra nhật kí hệ thống bằng các sử dụng view **UNIFIED_AUDIT_TRAIL**.

- Khi mà **unified auditing** được kích hoạt trên Oracle thì những bản ghi kiểm tra sẽ được ghi vào view này.

- Nhóm chúng em đã sử dụng chính sách FGA để thực hiện việc khi vết. Để có thể truy cập được view này thì người dùng đã được cấp role **AUDIT_ADMIN** và **AUDIT_VIEWER**.

- **SELECT * FROM UNIFIED_AUDIT_TRAIL WHERE AUDIT_TYPE = 'FineGrainedAudit'** để có thể lọc ra các bản ghi sử dụng chính sách FGA.

4.3.5.5. Giao diện

4.3.4.4.1. Màn hình sử dụng *Standard Audit*:

Ở chức năng này, giao diện sẽ hiển thị chi tiết để kiểm tra nhật ký hệ thống, cụ thể sẽ có các thông tin đáng quan tâm như sau:

- **SESSIONID**: ID phiên của người dùng trong cơ sở dữ liệu.
- **OS_USERNAME**: Tên người dùng trên hệ thống điều hành.
- **USERHOST**: Tên máy tính của người dùng.
- **INSTANCE_ID**: ID của phiên cơ sở dữ liệu.
- **DBID**: ID của cơ sở dữ liệu.
- **AUTHENTICATION_TYPE**: Loại xác thực (ví dụ: PASSWORD, EXTERNAL, KERBEROS)

- **DBUSERNAME:** Tên người dùng trên cơ sở dữ liệu
- **CLIENT_PROGRAM_NAME:** Tên chương trình sử dụng kết nối đến cơ sở dữ liệu.
- **ENTRY_ID:** ID của mục nhập trong bảng UNIFIED_AUDIT_TRAIL.
- **STATEMENT_ID:** ID của câu lệnh SQL được thực thi.
- **EVENT_TIMESTAMP:** Thời điểm xảy ra sự kiện trong múi giờ địa phương.
- **EVENT_TIMESTAMP_UTC:** Thời điểm xảy ra sự kiện trong múi giờ UTC.
- **ACTION_NAME:** Tên hoạt động được thực hiện (ví dụ: SELECT, INSERT, UPDATE, DELETE)
- **OS_PROCESS:** ID quá trình hệ thống.
- **SCN:** Số bảo đảm cho thời điểm truy cập.
- **EXECUTION_ID:** ID của phiên thực thi.
- **OBJECT_SCHEMA:** Tên schema của đối tượng được truy cập.
- **OBJECT_NAME:** Tên của đối tượng được truy cập.
- **SQL_TEXT:** Câu lệnh SQL được thực thi.
- **CURRENT_USER:** Người dùng hiện tại trên cơ sở dữ liệu.
- **ADDITIONAL_INFO:** Thông tin bổ sung về sự kiện.
- **UNIFIED_AUDIT_POLICIES:** Tên chính sách kiểm tra toàn diện được áp dụng.
- **FGA_POLICY_NAME:** Tên chính sách ghi lại truy cập bảo vệ dữ liệu (Fine-Grained Auditing Policy) nếu có.

Form_audit

Chức năng
GIÁM SÁT

Standard Audit

Fine Grained Audit

Audit use Trigger

Mô tả: Xem lịch sử chỉnh sửa trên LUONG và PHUCAP mà người dùng không thuộc vai trò TÀI CHÍNH

SESSIONID	OS_USERNAME	USERHOST	INSTANCE_ID	DBID	AUTHENTIC.
3293474538	X	DESKTOP-2HQ1...	1	600195586	(TYPE=(DATA
3802874571	X	DESKTOP-2HQ1...	1	600195586	(TYPE=(DATA
3802874571	X	DESKTOP-2HQ1...	1	600195586	(TYPE=(DATA
3802874571	X	DESKTOP-2HQ1...	1	600195586	(TYPE=(DATA
3802874571	X	DESKTOP-2HQ1...	1	600195586	(TYPE=(DATA
3529054876	X	DESKTOP-2HQ1...	1	600195586	(TYPE=(DATA
3529054876	X	DESKTOP-2HQ1...	1	600195586	(TYPE=(DATA
3529054876	X	DESKTOP-2HQ1...	1	600195586	(TYPE=(DATA
3529054876	X	DESKTOP-2HQ1...	1	600195586	(TYPE=(DATA
3529054876	X	DESKTOP-2HQ1...	1	600195586	(TYPE=(DATA
3529054876	X	DESKTOP-2HQ1...	1	600195586	(TYPE=(DATA
3529054876	X	DESKTOP-2HQ1...	1	600195586	(TYPE=(DATA
3529054876	X	DESKTOP-2HQ1...	1	600195586	(TYPE=(DATA
3529054876	X	DESKTOP-2HQ1...	1	600195586	(TYPE=(DATA
3529054876	X	DESKTOP-2HQ1...	1	600195586	(TYPE=(DATA
3529054876	X	DESKTOP-2HQ1...	1	600195586	(TYPE=(DATA
1500327072	DESKTOP-2HQ1...	WORKGROUP\...	1	2069361546	(TYPE=(OS));(
1500327072	DESKTOP-2HQ1...	WORKGROUP\...	1	2069361546	(TYPE=(OS));(
1500327072	DESKTOP-2HQ1...	WORKGROUP\...	1	2069361546	(TYPE=(OS));(

Hình 35. Giao diện chức năng Standard Audit

4.3.4.4.2. Màn hình sử dụng **Fine Grained Audit**:

Form_audit

Chức năng
GIÁM SÁT

Standard Audit

Fine Grained Audit

Audit use Trigger

Mô tả: Xem lịch sử chỉnh sửa trên LUONG và PHUCAP mà người dùng không thuộc vai trò TÀI CHÍNH

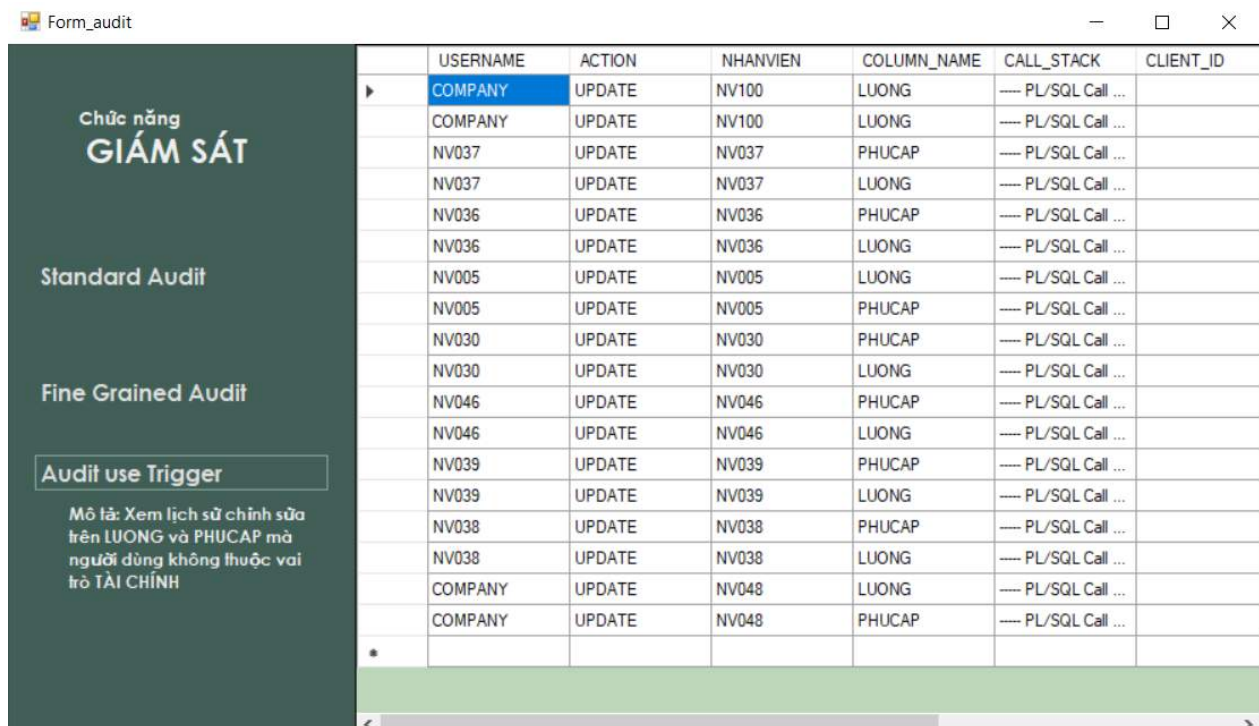
SESSIONID	OS_USERNAME	USERHOST	INSTANCE_ID	DBID	AUTHENTIC.
2045608424	X	DESKTOP-2HQ1...	1	600195586	(TYPE=(DATA
542112253	X	DESKTOP-2HQ1...	1	600195586	(TYPE=(DATA
542112253	X	DESKTOP-2HQ1...	1	600195586	(TYPE=(DATA
188847763	X	DESKTOP-2HQ1...	1	600195586	(TYPE=(DATA
188847763	X	DESKTOP-2HQ1...	1	600195586	(TYPE=(DATA
188847763	X	DESKTOP-2HQ1...	1	600195586	(TYPE=(DATA
188847763	X	DESKTOP-2HQ1...	1	600195586	(TYPE=(DATA
188847763	X	DESKTOP-2HQ1...	1	600195586	(TYPE=(DATA
188847763	X	DESKTOP-2HQ1...	1	600195586	(TYPE=(DATA
2901032147	X	DESKTOP-2HQ1...	1	600195586	(TYPE=(DATA
2901032147	X	DESKTOP-2HQ1...	1	600195586	(TYPE=(DATA
2901032147	X	DESKTOP-2HQ1...	1	600195586	(TYPE=(DATA
3054617014	X	DESKTOP-2HQ1...	1	600195586	(TYPE=(DATA
3054617014	X	DESKTOP-2HQ1...	1	600195586	(TYPE=(DATA
3054617014	X	DESKTOP-2HQ1...	1	600195586	(TYPE=(DATA
1376581206	X	DESKTOP-2HQ1...	1	600195586	(TYPE=(DATA
218148349	X	DESKTOP-2HQ1...	1	600195586	(TYPE=(DATA
3286113404	X	DESKTOP-2HQ1...	1	600195586	(TYPE=(DATA
1259578873	X	DESKTOP-2HQ1...	1	600195586	(TYPE=(DATA
218148349	X	DESKTOP-2HQ1...	1	600195586	(TYPE=(DATA
218148349	X	DESKTOP-2HQ1...	1	600195586	(TYPE=(DATA

Hình 36. Giao diện chức năng Fine Grained Audit

Với chức năng này, màn hình sẽ hiển thị chi tiết các thông tin tương tự chức năng Standard Audit. Tuy nhiên, màn hình chỉ hiển thị thông tin ghi vết các hoạt động bằng chính sách FGA (Fine-Grained Auditing Policy) được yêu cầu cài đặt trong đồ án:

- Những người đã cập nhật trường THOIGIAN trong quan hệ PHANCONG.
- Những người đã đọc trên trường LUONG và PHUCAP của người khác.

4.3.4.4.3. Màn hình sử dụng Trigger Audit



USERNAME	ACTION	NHANVIEN	COLUMN_NAME	CALL_STACK	CLIENT_ID
COMPANY	UPDATE	NV100	LUONG	----- PL/SQL Call ...	
COMPANY	UPDATE	NV100	LUONG	----- PL/SQL Call ...	
NV037	UPDATE	NV037	PHUCAP	----- PL/SQL Call ...	
NV037	UPDATE	NV037	LUONG	----- PL/SQL Call ...	
NV036	UPDATE	NV036	PHUCAP	----- PL/SQL Call ...	
NV036	UPDATE	NV036	LUONG	----- PL/SQL Call ...	
NV005	UPDATE	NV005	LUONG	----- PL/SQL Call ...	
NV005	UPDATE	NV005	PHUCAP	----- PL/SQL Call ...	
NV030	UPDATE	NV030	PHUCAP	----- PL/SQL Call ...	
NV030	UPDATE	NV030	LUONG	----- PL/SQL Call ...	
NV046	UPDATE	NV046	PHUCAP	----- PL/SQL Call ...	
NV046	UPDATE	NV046	LUONG	----- PL/SQL Call ...	
NV039	UPDATE	NV039	PHUCAP	----- PL/SQL Call ...	
NV039	UPDATE	NV039	LUONG	----- PL/SQL Call ...	
NV038	UPDATE	NV038	PHUCAP	----- PL/SQL Call ...	
NV038	UPDATE	NV038	LUONG	----- PL/SQL Call ...	
COMPANY	UPDATE	NV048	LUONG	----- PL/SQL Call ...	
COMPANY	UPDATE	NV048	PHUCAP	----- PL/SQL Call ...	

Hình 37. Giao diện chức năng *Trigger Audit*

Trong chức năng này, màn hình sẽ hiển thị thông tin ghi vết của hoạt động: Một người không thuộc vai trò “Tài chính” nhưng đã cập nhật thành công trên trường LUONG và PHUCAP.

Cụ thể, sẽ có các thông tin đáng quan tâm như:

- **username:** Tên người dùng thực hiện hoạt động này trên cơ sở dữ liệu.
- **action:** Hành động được thực hiện trên bảng LUONG, ví dụ như "INSERT", "UPDATE", hoặc "DELETE" (ở đây là “UPDATE”).
- **nhanvien:** Mã nhân viên liên quan đến hoạt động này.

- **column_name**: Tên cột được thay đổi trong hoạt động "UPDATE".
- **call_stack**: Chuỗi gọi hàm được lưu trữ khi thực hiện hoạt động trên cơ sở dữ liệu.
- **client_id**: ID của khách hàng thực hiện hoạt động này.
- **old_value**: Giá trị cũ của cột được thay đổi trong hoạt động "UPDATE".
- **new_value**: Giá trị mới của cột được thay đổi trong hoạt động "UPDATE".
- **action_date**: Ngày giờ thực hiện hành động trên cơ sở dữ liệu.

5. HƯỚNG DẪN SỬ DỤNG

- Hướng dẫn sử dụng được trình bày cụ thể trong file “**23H3T-16-PH1-PH2-Guide.pdf**”.

- Demo sử dụng được trình bày trong file “**23H3T-16-PH1-PH2-demo.pdf**”.

6. TÀI LIỆU THAM KHẢO

1. github.com. 2023. *GitHub* - *hduylam31/ATBM-trong-HTTP: Đồ án thực hành môn an toàn và bảo mật dữ liệu trong hệ thống thông tin*. [ONLINE] Available at: <https://github.com/hduylam31/ATBM-trong-HTTP/tree/main>. [Accessed 29 June 2023].
2. github.com. 2023. *GitHub* - *tuanhbui/ATBM: sc*. [ONLINE] Available at: <https://github.com/tuanhbui/ATBM>. [Accessed 29 June 2023].
3. docs.oracle.com. 2023. *Oracle Database Database Concepts, 21c*. [ONLINE] Available at: [Database Concepts \(oracle.com\)](https://docs.oracle.com/en/database/oracle/oracle-database/21/c/). [Accessed 29 June 2023].