**ĐẠI HỌC QUỐC GIA THÀNH PHỐ HỒ CHÍ MINH**

**TRƯỜNG ĐẠI HỌC CÔNG NGHỆ THÔNG TIN**

**KHOA MẠNG MÁY TÍNH VÀ TRUYỀN THÔNG**

****

**BÁO CÁO ĐỒ ÁN**

**ĐỀ TÀI**

**USING CP-ABE FOR SECURE SHARING OF PERSONAL HEALTH RECORDS**

**NHÓM THỰC HIỆN**

**NGUYỄN KHẮC HẬU – 22520410**

**HUỲNH MINH HIỂN – 22520415**

**NGÔ TRUNG HIẾU – 22520437**

**GIẢNG VIÊN HƯỚNG DẪN**

**TS. NGUYỄN NGỌC TỰ**

**MỤC LỤC**

[I. Ngữ cảnh hệ thống 1](#_Toc169336485)

[**1. Các thành phần trong hệ thống 1**](#_Toc169336486)

[**2. Vai trò của các thành phần trong hệ thống 1**](#_Toc169336487)

[**3. Tương tác giữa các thành phần trong hệ thống 2**](#_Toc169336488)

[II. Tài sản, các rủi ro và các yêu cầu về bảo mật 2](#_Toc169336489)

[**1. Tài sản 2**](#_Toc169336490)

[**2. Rủi ro 2**](#_Toc169336491)

[**3. Các yêu cầu về bảo mật 3**](#_Toc169336492)

[III. Chi tiết giải pháp 4](#_Toc169336493)

[**1. Kiến trúc hệ thống 4**](#_Toc169336494)

[**2. Chi tiết giải pháp 5**](#_Toc169336495)

[**a. Khởi tạo người dùng mới 5**](#_Toc169336496)

[**b. Xác thực người dùng khi đăng nhập 5**](#_Toc169336497)

[**c. Triển khai hệ thống 5**](#_Toc169336498)

[IV. Chi tiết demo 7](#_Toc169336499)

[**1. Platforms 7**](#_Toc169336500)

[**2. Thư viện sử dụng 7**](#_Toc169336501)

[**3. Demo 8**](#_Toc169336502)

[**Link video demo: 16**](#_Toc169336503)

[TÀI LIỆU THAM KHẢO 17](#_Toc169336504)

[NHẬN XÉT CỦA GIẢNG VIÊN 18](#_Toc169336505)

**DANH MỤC HÌNH**

[Hình 1: Ngữ cảnh hệ thống 1](#_Toc169338662)

[Hình 2: Kiến trúc hệ thống 4](#_Toc169338663)

[Hình 3: Quá trình thu hồi thuộc tính và cập nhật ciphertext 4](#_Toc169338664)

[Hình 4: Giao diện đăng ký 8](#_Toc169338665)

[Hình 5: Dữ liệu người dùng trên database 8](#_Toc169338666)

[Hình 6: Giao diện đăng nhập 9](#_Toc169338667)

[Hình 7: Giao diện của Data-owner 9](#_Toc169338668)

[Hình 8: Giao diện thêm PHR của Data-owner 10](#_Toc169338669)

[Hình 9: Dữ liệu PHR lưu trên database 10](#_Toc169338670)

[Hình 10: Giao diện cập nhật PHR của Data-owner 11](#_Toc169338671)

[Hình 11: Giao diện thu hồi thuộc tính của Data-owner 12](#_Toc169338672)

[Hình 12: Giao diện cập nhật policy của Data-owner 12](#_Toc169338673)

[Hình 13: Giao diện của Data-users 13](#_Toc169338674)

[Hình 14: Giao diện xem thành công dữ liệu PHR của Data-users 14](#_Toc169338675)

[Hình 15: Dữ liệu PHR đã được giải mã 15](#_Toc169338676)

[Hình 16: Dữ liệu PHR đã được giải mã 15](#_Toc169338677)

[Hình 17: Thuộc tính của Data-users không thỏa policy 16](#_Toc169338678)

# **I. Ngữ cảnh hệ thống**

**A diagram of a cloud computing system

Description automatically generated**

Hình 1: Ngữ cảnh hệ thống

## **1. Các thành phần trong hệ thống**

**-** **Data-owner:** người tạo ra dữ liệu trong PHR như nhân viên bệnh viện, bác sĩ,…

**-** **Data-users:** người có nhu cầu truy cập vào PHR của Data-owner như bệnh nhân, bác sĩ điều trị, nhân viên bệnh viện, người nhà bệnh nhân, …

**- Trusted authority (TA):** Khởi tạo hệ thống và nhận các tham số hệ thống cần thiết.

**- Cloud – semitrusted:** bán tín cậy, là nơi lưu trữ dữ liệu, không có quyền thay đổi dữ liệu.

## **2. Vai trò của các thành phần trong hệ thống**

- **Data-owner:** người tạo ra dữ liệu, chỉnh sửa, cập nhật dữ liệu. Data-owner sẽ định nghĩa Access Policy liên quan đến quyền truy cập vào dữ liệu PHR, mã hóa dữ liệu PHR sau đó gửi lên cloud.

- **Data-users:** người truy vấn các bản ciphertext PHR được lưu trên cloud.

- **TA:** sẽ lưu master key và public key tương ứng với từng bản PHR được mã hóa; tạo secret key từ danh sách thuộc tính và gửi cho người dùng.

- **Cloud:** là nơi bán tin cậy, lưu dữ liệu PHR sau khi đã mã hóa được Data-owner gửi lên.

## **3. Tương tác giữa các thành phần trong hệ thống**

- Data-owner sẽ tạo ra master key và public key để mã hóa PHR, các key này sẽ được gửi đến TA để lưu trữ.

- Data-owner sau khi mã hóa PHR sẽ gửi dữ liệu đã mã hóa đến Cloud để lưu trữ.

- Data-users khi có yêu cầu dữ liệu của PHR, Cloud sẽ gửi bản dữ liệu mã hóa cho Data-users.

- Data-users sẽ gửi yêu cầu secret key đến TA kèm theo danh sách thuộc tính của bản thân.

- TA sẽ tạo ra secret key từ danh sách thuộc tính và các public key, master key đã lưu và gửi lại cho Data-users.

# **II. Tài sản, các rủi ro và các yêu cầu về bảo mật**

## **1. Tài sản**

- Bản Personal Health Records (PHR) chứa các thông tin của bệnh nhân.

## **2. Rủi ro**

- Một số hệ thống y tế không có cơ chế kiểm soát truy cập, khiến cho dữ liệu liên quan tới hồ sơ, bệnh án của bệnh nhân có thể được truy cập bởi bất cứ cá nhân nào, gây rò rỉ thông tin, không an toàn. Ngoài ra, không có cơ chế mã hóa mạnh mẽ đã làm cho hệ thống có khả năng bị tấn công và mất mát dữ liệu

- Một số hệ thống khác sử dụng các cơ chế kiểm soát truy cập truyền thống, chẳng hạn như kiểm soát truy cập dựa trên vai trò (RBAC). RBAC là một cách đơn giản và hiệu quả để kiểm soát truy cập dữ liệu, nhưng nó có thể khó triển khai các chính sách kiểm soát truy cập chi tiết.

- Khi quyền truy cập của người dùng cần phải bị thu hồi như khi bác sĩ hay y tá không còn làm trong bệnh viện, hệ thống không có cơ chế thu hồi thuộc tính hiệu quả, dẫn đến người dùng vẫn có thể truy cập dữ liệu mà họ không còn thẩm quyền.

- Hệ thống không có cơ chế ngăn chặn việc chia sẻ thuộc tính, dẫn đến việc người dùng có thể chia sẻ thông tin hoặc thuộc tính của họ với người khác, trong khi người đó không được cấp quyền nhưng vẫn có thể truy cập vào PHR.

## **3. Các yêu cầu về bảo mật**

**- Tính bảo mật:** Dữ liệu PHR phải được giữ bí mật với những bên không được cấp quyền.

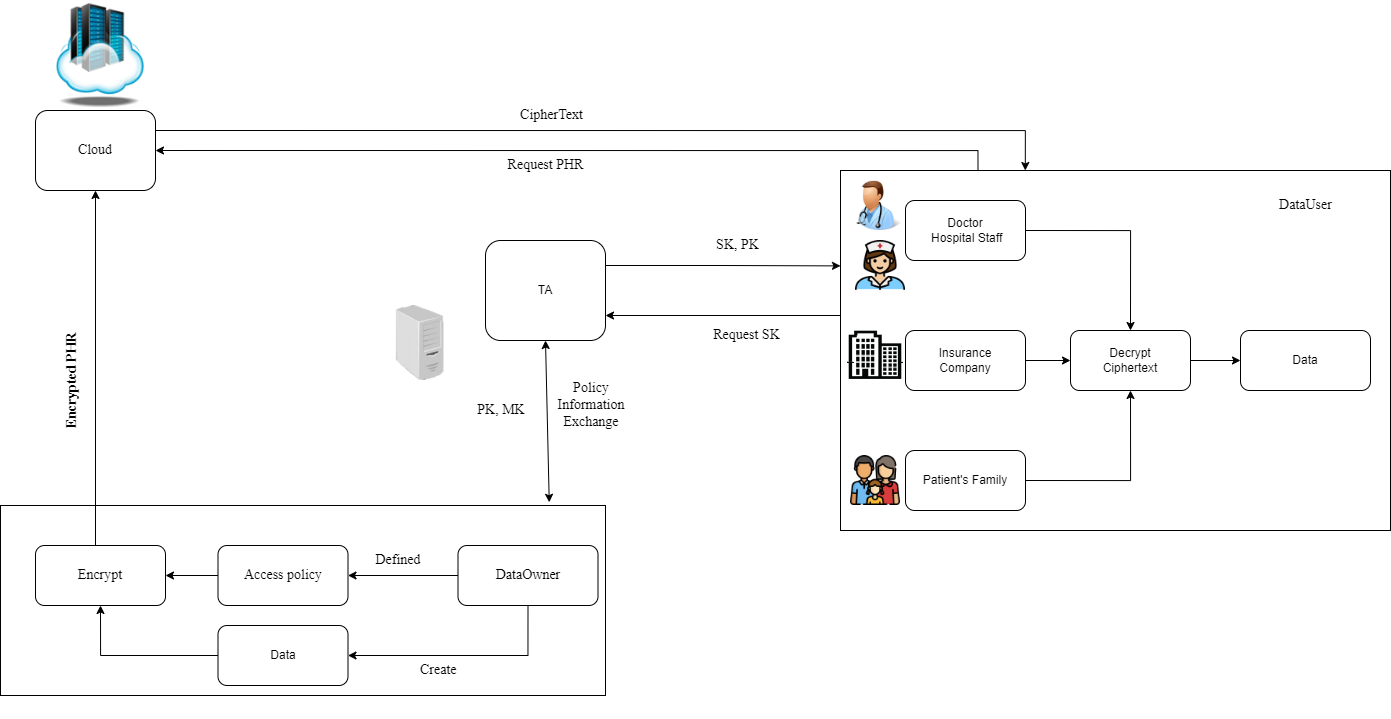
**- Kiểm soát truy cập:** Chủ sở hữu PHR sẽ có toàn quyền kiểm soát outsourced health data cho phép họ xác định ai có thể truy cập đến dữ liệu đó.

**- Tính thu hồi:** Thu hồi thuộc tính của người dùng khi không còn hiệu lực.

**- Ngăn chặn việc chia sẻ thuộc tính:** Nhiều người dùng sẽ không thể chia sẻ thuộc tính của họ với nhau và giải mã dữ liệu PHR.

# **III. Chi tiết giải pháp**

## **1. Kiến trúc hệ thống**



Hình 2: Kiến trúc hệ thống

Ảnh có chứa văn bản, biểu đồ, ảnh chụp màn hình, Kế hoạch

Mô tả được tạo tự động

Hình 3: Quá trình thu hồi thuộc tính và cập nhật ciphertext

## **2. Chi tiết giải pháp**

### **a. Khởi tạo người dùng mới**

- Nhân viên bệnh viên, bác sĩ sẽ được cấp tài khoản ngay từ khi bắt đầu. Người dùng phải đăng ký mới có thể xem PHR.

- Khi đăng ký thành công, thông tin người dùng sẽ được lưu vào cloud MongoDB.

- Nhằm đảm bảo tính bảo mật cho mật khẩu và ngăn không cho người quản lý database hoặc attacker nhìn thấy, mật khẩu sẽ được băm sử dụng thuật toán SHA256 trước khi cho vào database.

### **b. Xác thực người dùng khi đăng nhập**

- Khi đăng nhập, người dùng sẽ nhập tài khoản email và mật khẩu.

- Mật khẩu của người dùng sẽ được băm bằng thuật toán SHA256 và so sánh với mật khẩu trên database, nếu như cả hai bằng nhau, sẽ trả về ID của người dùng. Sử dụng ID đã có và lấy dữ liệu của người dùng trên database và so sánh các thuộc tính đó với các thuộc tính chung. Nếu như thỏa mãn các thuộc tính đó, người dùng đăng nhập thành công.

### **c. Triển khai hệ thống**

- Sau khi đăng nhập thành công, DataOwner sẽ được chuyển hướng đến giao diện dành cho dataowner và họ có thể thêm dữ liệu PHR, cập nhật dữ liệu PHR, thu hồi thuộc tính của người dùng, cập nhật lại Access Policy của dữ liệu PHR. Đối với user và staff, họ sẽ chuyển hướng đến giao diện dành cho user và staff, user và staff có quyền xem PHR.

- Data-owner có các quyền cụ thể sau:

+ **Thêm mới PHR:** Data-owner cần chọn tệp dữ liệu PHR (dạng JSON) và có thể chọn hình ảnh (.PNG). Dữ liệu PHR sẽ được mã hóa theo thuật toán mã hóa AES\_GCM\_256 và tạo policy chứa thuộc tính của những người dùng có quyền truy cập PHR. Key dùng cho AES\_GCM\_256 được mã hóa bằng CP-ABE dựa vào policy đã được định nghĩa. Sau đó dữ liệu được mã hóa sẽ được lưu trữ ở cloud. Public key và Master Key sẽ gửi đến TA để lưu trữ.

+ **Cập nhật PHR:** Data-owner có thể cập nhật lại tệp dữ liệu PHR (dạng JSON). Ngoài ra khi cập nhật lại PHR, policy cũng sẽ được cập nhật và sẽ mã hóa lại dữ liệu PHR và hình ảnh với policy mới.

+ **Thu hồi thuộc tính:** Khi người dùng không còn quyền truy cập vào dữ liệu PHR của bệnh nhân, họ sẽ bị thu hồi thuộc tính trong policy. Điều này đồng nghĩa, Data-owner sẽ cập nhật policy mới không có thuộc tính của người dùng bị thu hồi. Sau đó, sử dụng policy mới để mã hóa lại dữ liệu PHR và hình ảnh.

+ **Cập nhật policy:** Nếu như người nhà bệnh nhân hoặc các nhân viên không phải bác sĩ phụ trách của bệnh nhân nhưng được cấp quyền truy cập vào PHR của bệnh nhân, cần cập nhật lại policy và thêm các thuộc tính của người nhà bệnh nhân hoặc nhân viên bệnh viện vào policy. Mã hóa dữ liệu PHR và hình ảnh bằng policy mới.

- Data-users có quyền xem những dữ liệu PHR nếu thuộc tính của họ thỏa policy. Nhập ID của bệnh nhân và nếu thỏa policy, dữ liệu PHR mã hóa sẽ được tải về máy, sau đó Data-users sẽ sử dụng public key và secret key nhận từ TA sau khi request (request kèm theo thuộc tính của người dùng đến TA bằng giao thức TCP và TLSv1.3) để giải mã dữ liệu PHR mã hóa thành bản rõ có dạng JSON.

- Đối với TA (Trusted Authority), giao tiếp với client bằng giao thức TCP và TLSv1.3, server được xác thực bằng certificate tạo bằng ECDSA, sẽ có 2 luồng được tạo ra: 1 luồng giao tiếp với data-owner, 1 luồng là giao tiếp với Data-users. TA có nhiệm vụ lưu master key và public key của các PHR tương ứng. Khi nhận được các request về secret key kèm tập thuộc tính của người dùng, TA sẽ tạo và gửi secret key kèm public key đã lưu lại cho người dùng.

# **IV. Chi tiết demo**

## **1. Platforms**

- Ubuntu 22.04

- Ngôn ngữ lập trình: Python

- IDE: Visual Studio Code

- Database: MongoDB

## **2. Thư viện sử dụng**

- Tkinter sử dụng để tạo giao diện sử dụng.

- Charm-Crypto, PyCryptodome, PBC để mã hóa AES\_GCM\_256 và CP-ABE.

- Hashlib: SHA256, SHAKE\_256.

- Cryptography để tạo chứng chỉ Certificate xác thực server.

- Thư viện ssl, socket dùng để tạo kết nối TCP và TLSv1.3 giao tiếp giữa server và client.

## **3. Demo**

Đây giao diện đăng ký

A screen shot of a login form

Description automatically generated

Hình 4: Giao diện đăng ký

Ảnh có chứa văn bản, ảnh chụp màn hình, phần mềm, số

Mô tả được tạo tự động

Hình 5: Dữ liệu người dùng trên database

Đây là giao diện đăng nhập

A screenshot of a login form

Description automatically generated

Hình 6: Giao diện đăng nhập

Sau khi đăng nhập thành công, Data-owner sẽ được chuyển hướng đến giao diện dành cho Data-owner.

Ảnh có chứa văn bản, ảnh chụp màn hình, phần mềm, Phông chữ

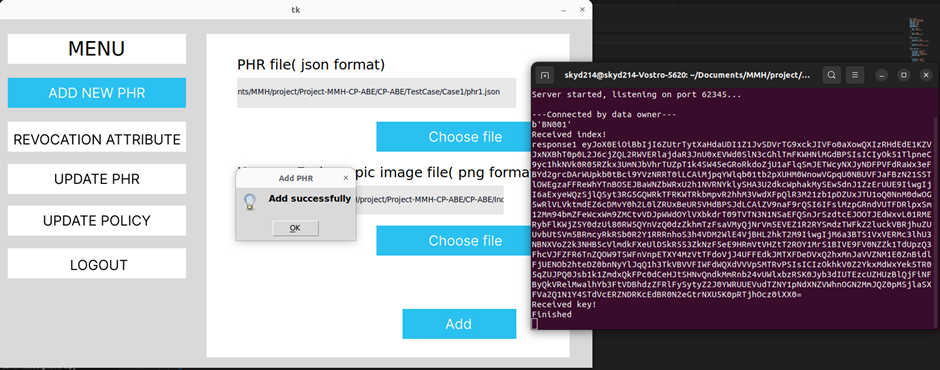
Mô tả được tạo tự động

Hình 7: Giao diện của Data-owner

Để thêm mới một dữ liệu PHR, Data-owner nhập đường dẫn các file dữ liệu và bấm nút Add.

Public key và Master Key sẽ được gửi đến server.

Kết nối giữa Data-owner và TA là kết nối với giao thức TCP và TLSv1.3 bằng certificate được tạo bằng ECDSA.



Hình 8: Giao diện thêm PHR của Data-owner

TA nhận và tạo 2 file chứa masterkey và public key và lưu trữ ở thư mục của server.

Dữ liệu PHR và hình ảnh (nếu có) dựa trên policy với các thuộc tính của Data-owner, bệnh nhân và bác sĩ phụ trách khám cho bệnh nhân.

Dữ liệu đã mã hóa được tải lên cloud.

Ảnh có chứa văn bản, ảnh chụp màn hình, phần mềm, Biểu tượng máy tính

Mô tả được tạo tự động

Hình 9: Dữ liệu PHR lưu trên database

Cập nhật nội dung PHR: Data-owner cần nhập ID của bệnh nhân và đường dẫn đến file dữ liệu đã chỉnh sửa.

Ảnh có chứa văn bản, ảnh chụp màn hình, phần mềm, Biểu tượng máy tính

Mô tả được tạo tự động

Hình 10: Giao diện cập nhật PHR của Data-owner

Data-owner tạo public key và master key mới gửi đến TA, TA sẽ cập nhật lại publickey và masterkey đã lưu.

Data-owner mã hóa lại dữ liệu PHR và hình ảnh lấy về từ database dựa trên policy mới.

Dữ liệu đã mã hóa được tải lên cloud.

Ảnh có chứa văn bản, ảnh chụp màn hình, phần mềm, Biểu tượng máy tính

Mô tả được tạo tự động

Hình 11: Giao diện thu hồi thuộc tính của Data-owner

Nhập ID bệnh nhân để truy cập vào dữ liệu PHR của bệnh nhân có ID đó, nhập IDUser là những ID bị thu hồi quyền truy cập vào PHR.

Data-owner tạo public key và master key mới gửi đến TA, TA sẽ lưu public key và master key đó vào file.

Data-owner mã hóa lại dữ liệu PHR và hình ảnh lấy về từ database dựa trên policy mới.

Dữ liệu đã mã hóa được tải lên cloud.

A screenshot of a computer

Description automatically generated

Hình 12: Giao diện cập nhật policy của Data-owner

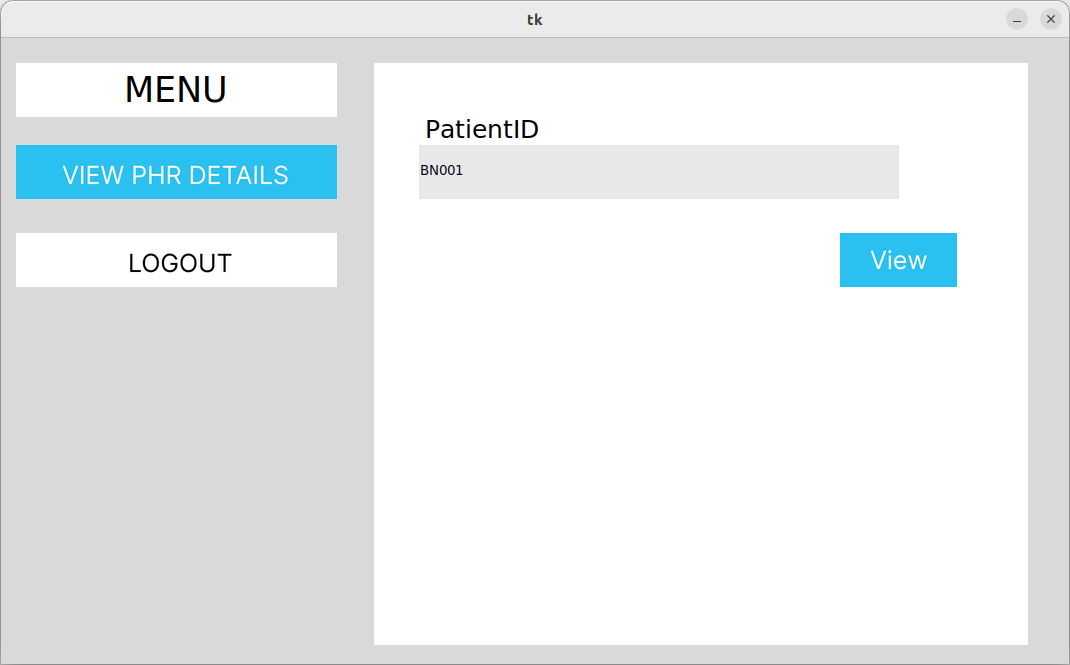
Nhập ID bệnh nhân để truy cập vào dữ liệu PHR của bệnh nhân có ID đó, nhập IDUser là những ID được cấp quyền truy cập vào PHR.

Data-owner tạo public key và master key mới gửi đến TA, TA sẽ lưu public key và master key đó vào file.

Data-owner mã hóa lại dữ liệu PHR và hình ảnh lấy về từ database dựa trên policy mới.

Dữ liệu đã mã hóa được tải lên cloud.

Sau khi đăng nhập thành công, Data-users sẽ được chuyển hướng đến giao diện này.



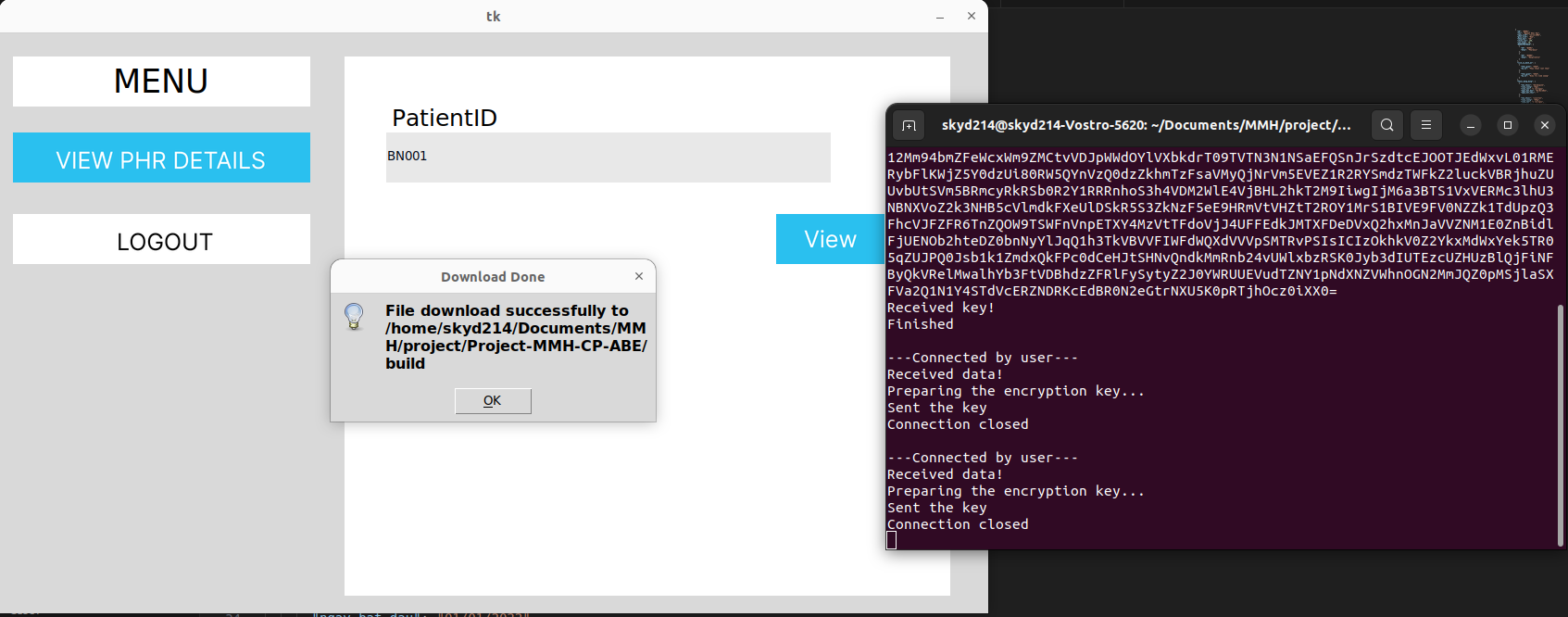
Hình 13: Giao diện của Data-users

Truy vấn dữ liệu PHR: Data-users nhập ID bệnh nhân và ấn nút View.

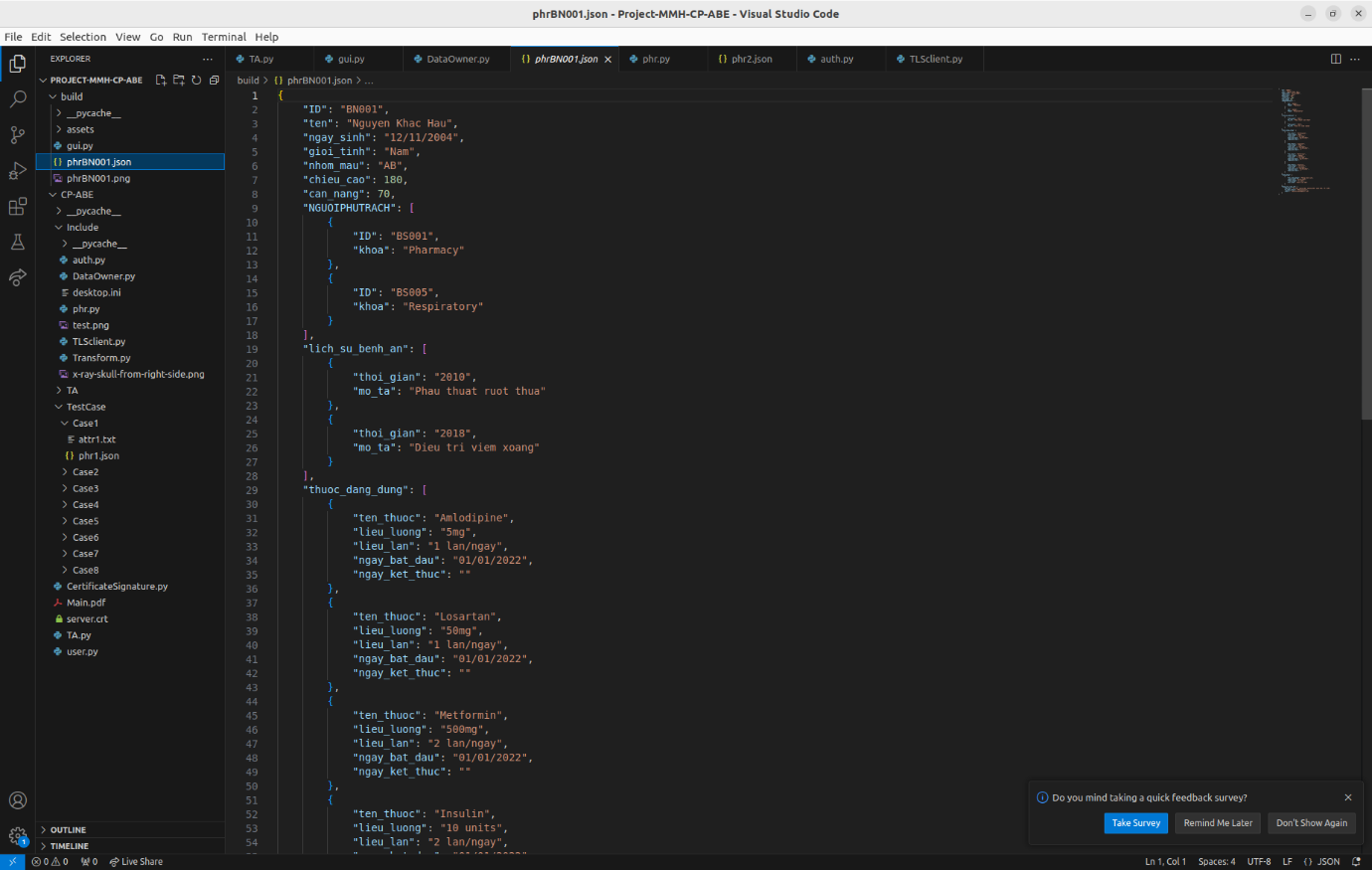
Data-users gửi yêu cầu ciphertext đến cloud, yêu cầu về secret key đến TA.

Ciphertext sẽ được lưu vào file tạm để làm đầu vào cho việc giải mã.

Việc giải mã sẽ được thực hiện sau khi nhận được secret key và public key từ TA.



Hình 14: Giao diện xem thành công dữ liệu PHR của Data-users



Hình 15: Dữ liệu PHR đã được giải mã

Ảnh có chứa phim x quang, Hình ảnh y khoa, X quang học, Chụp x quang y tế

Mô tả được tạo tự động

Hình 16: Dữ liệu PHR đã được giải mã

Nếu secret key của Data-users không thỏa policy thì việc giải mã sẽ thất bại.

Ảnh có chứa văn bản, ảnh chụp màn hình, phần mềm, Biểu tượng máy tính

Mô tả được tạo tự động

Hình 17: Thuộc tính của Data-users không thỏa policy

## **Link video demo:**

<https://drive.google.com/file/d/10199pkijh6BwgA9s8GXRqDGmmgCpLash/view?usp=sharing>

# **TÀI LIỆU THAM KHẢO**

[1] Edemacu, K., Jang, B., & Kim, J. W. (2020). Efficient and expressive access control with revocation for privacy of PHR based on OBDD access structure. IEEE Access, 8, 18546-18557.

[2] Bethencourt, J., Sahai, A., & Waters, B. (2007, May). Ciphertext-policy attribute-based encryption. In 2007 IEEE symposium on security and privacy (SP'07) (pp. 321-334). IEEE.

[3] <https://github.com/JHUISI/charm/blob/dev/charm/schemes/abenc/ac17.py>

# **NHẬN XÉT CỦA GIẢNG VIÊN**

………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………