ĐẢM BẢO QUYỀN RIÊNG TƯ TRÊN ĐÁM MÂY THÔNG QUA MÃ HOÁ DỰA TRÊN THUỘC TÍNH VÀ TÌM KIẾM AN TOÀN

Phạm Trần Tiến Đạt - 220202017[1]

[1] Trường ĐH Công nghệ Thông tin - ĐHQG TP.HCM

MỤC TIÊU

- Giới thiệu một phương pháp **kiểm soát truy cập** và **tìm kiếm** trên **dữ liệu đã mã hoá** nhằm đảm bảo tính bí mật của dữ liệu trên nền tảng đám mây.
- **Nghiên cứu** các thuật toán mã hoá dựa trên thuộc tính và mã hoá có thể tìm kiếm có hiệu suất tối ưu và so sánh **đánh giá** chúng.
- Triển khai một kịch bản cụ thể bằng cách xây dựng một **ứng dụng mô phỏng** hệ thống quản lý hồ sơ sức khỏe điện tử (EHR).

LÝ DO CHỌN ĐỀ TÀI

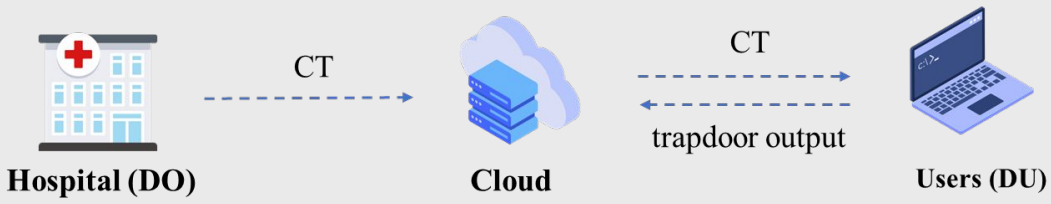
- Ngày nay càng nhiều dữ liệu được lưu trên đám mây và không có gì đảm bảo được **tính bí mật** và **toàn vẹn** của chúng.
- Hệ thống mã hóa đối xứng và bất đối xứng truyền thống thực hiện tốt chức năng mã hóa nhưng lại **không thể kiểm soát tốt việc truy cập dữ liệu**.
- Dữ liệu khi đã mã hoá thì **không thể tìm kiếm được**.
- Dữ liệu cần được xử lý sao cho đảm bảo được quyền riêng tư mà vẫn có thể thực hiện chức năng tìm kiếm.

Mô hình hệ thống

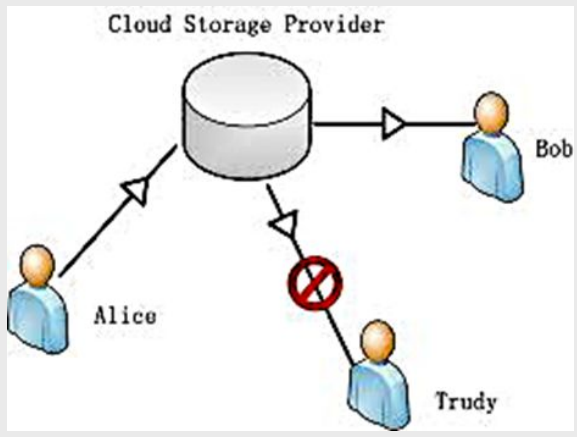
Mô hình hệ thống

Các bên liên quan:

- **Data Owner**: bác sĩ, bệnh nhân, …
- **Data Users**: bác sĩ, nhân viên y tế, người nhà, bệnh nhân, …
- **Untrusted Storage**: cloud, hosting, …
- **Attacker**: dùng máy tính cổ điển



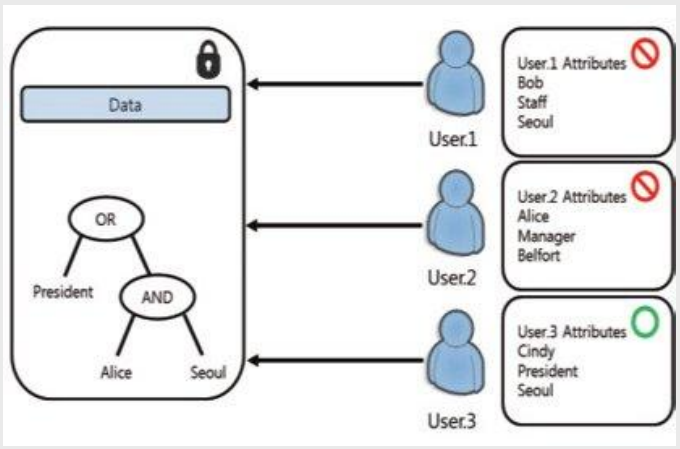
Mô hình kiểm soát truy cập



Mô tả

1. Mã hoá dựa trên thuộc tính

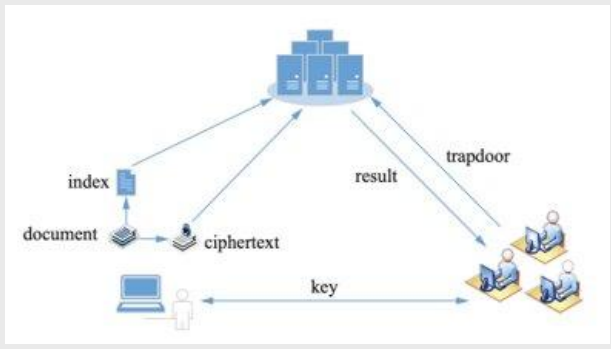
- **Mã hóa dựa trên thuộc tính (ABE)** là một loại mã hóa khóa công khai.
  - **Chính sách** truy cập được thể hiện bằng hàm logic với biến là các thuộc tính.
  - **Thuộc tính** là các chuỗi tùy ý.
- Chỉ khi các thuộc tính **thỏa mãn** chính sách truy cập thì mới có thể giải mã.



- Gồm 2 loại:
  - Mã hóa dựa trên thuộc tính chính sách khóa (**KP-ABE**)
  - Mã hóa dựa trên thuộc tính chính sách bản mã (**CP-ABE**)

2. Mã hoá có thể tìm kiếm

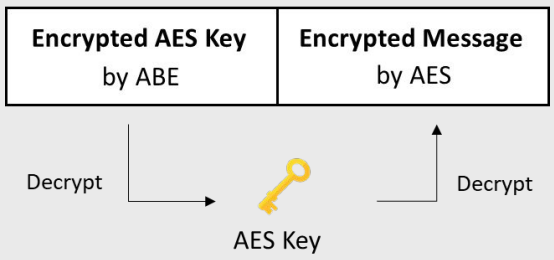
- Cho phép người tìm kiếm trực tiếp trên dữ liệu mã hóa một cách an toàn.
- Mô hình:



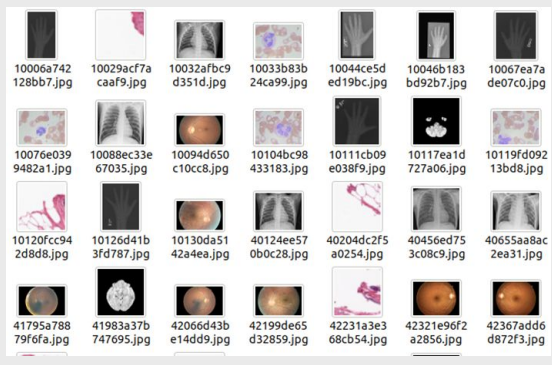
3. Triển khai kịch bản và đánh giá

- Ngữ cảnh: **Hệ thống chăm sóc y tế (EHR)**
- Kịch bản được triển khai trên hệ quản trị CSDL SQL trên đám mây.

- **Kịch bản 1**: Mã hoá dữ liệu theo chính sách truy cập



- **Kịch bản 2**: Thu hồi thuộc tính
  - Khi thuốc tính bị thu hồi thì khoá cũ không thể giải mã dữ liệu.
- **Kịch bản 3**: Tìm kiếm dữ liệu mã hoá (hình ảnh y khoa)



NII

Phạm Trần Tiến Đạt - Trường Đại học Công nghệ Thông tin - ĐHQG TP.HCM
TEL : 0934.993.860 Email : datptt.17@grad.uit.edu.vn