- Tên đề tài: Searchable Encryption for Distributed Systems

- Các bài báo liên quan

1. Privacy-Preserving Multi-Keyword Searchable Encryption for Distributed Systems

DOI Bookmark: 10.1109/TPDS.2020.3027003

2. Multiserver searchable data crypt: searchable data encryption scheme for secure distributed cloud storage

DOI: 10.1007/s12652-020-02621-8

3. Forward Secure Searchable Symmetric Encryption

DOI: 10.23919/ICITST.2017.8356345

- Ngữ cảnh và ý tưởng demo:

**Ngữ cảnh:**

Ngày nay, nhu cầu về lưu trữ dữ liệu người dùng ngày càng cao, đòi hỏi chủ sở hữu dữ liệu phải sử dụng dịch vụ đám mây để lưu trữ các dữ liệu của người dùng. Tuy nhiên phải đối mặt với nguy cơ bị tấn công, mất cắp thông tin rất cao. Do vậy, giải pháp đặt ra là cần mã hóa dữ liệu trước khi lưu trữ, nhưng điều này sẽ gây ra khó khăn cho việc tìm kiếm và truy xuất thông tin tin. => Cần mô hình mã hoá để vừa tránh bị lộ dữ liệu vừa thuận tiện cho việc tìm kiếm, truy xuất thông tin mà phải tiết kiệm thời gian. Điều này có nghĩa là người dùng có khả năng truy vấn/tìm kiếm các tệp được mã hóa của mình ở phía máy chủ mà không cần giải mã chúng.

**Ý tưởng Demo:**

Kịch bản chủ yếu bao gồm bốn thực thể: chủ sở hữu dữ liệu, người dùng dữ liệu, nhà cung cấp dịch vụ đám mây và trình tạo khóa.

Ban đầu, chủ sở hữu dữ liệu sẽ mã hoá các file và liên kết nó với các index và gửi cả 2 lên cloud server. Tiếp theo người dùng sẽ tạo 1 trapdoor để có thể tìm kiếm dựa trên keyword, trapdoor này sau đó sẽ được gửi lên cloud server, server sẽ sử dụng trapdoor và từ khoá để tìm các file liên quan và trả về cho người dùng mà không cần phải giải mã tất cả các file.

Okie chưa? ukm