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

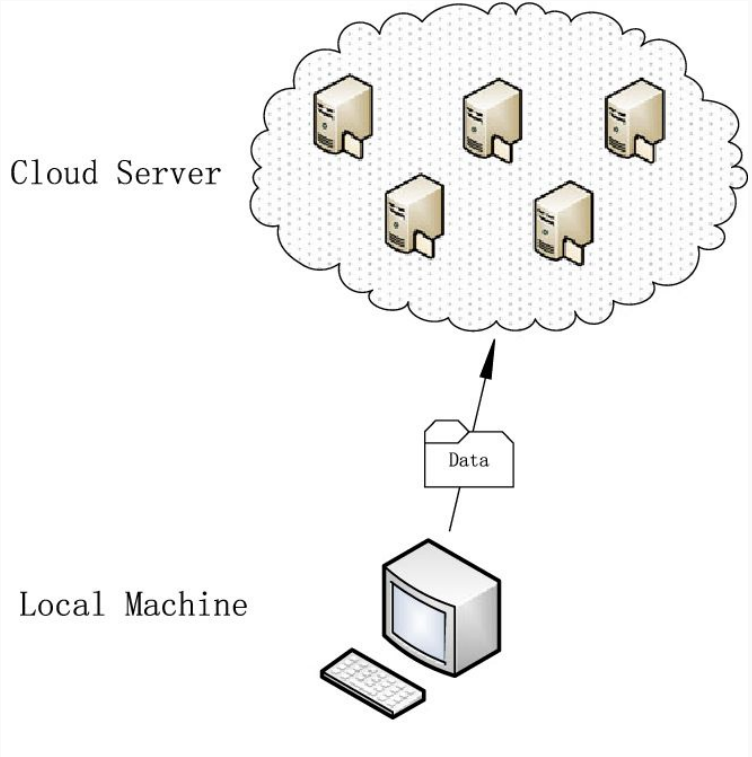
Tóm tắt

- **Lớp**: CS2205.CH1702
- **Link Github**: https://github.com/phamtrantienda t/CS2205.APR2023
- **Link YouTube video**:

  https://youtu.be/y3vP1IO00MU

Giới thiệu

- Do nhu cầu lưu trữ ngày càng lớn, càng có nhiều dữ liệu được lưu trên đám mây kể cả dữ liệu nhạy cảm.
- Không có gì đảm bảo được tính bí mật và toàn vẹn của dữ liệu khi lưu trữ trên những nền tảng này.

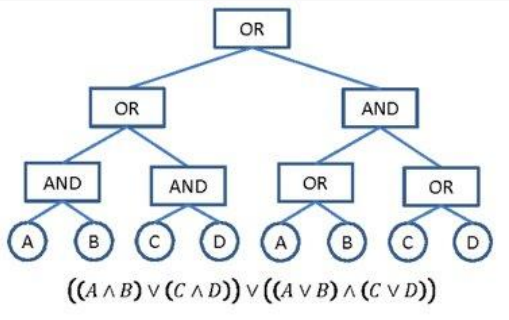


Giới thiệu

- Các hệ thống mã hoá đối xứng và bất đối xứng truyền thống thực hiện tốt chức năng mã hoá nhưng không thể kiểm soát việc truy cập dữ liệu của người dùng.
- Đề xuất **mã hoá dựa trên thuộc tính** (Attribute-Based Encryption)
- Dữ liệu đã mã hoá thì không thể tìm kiếm được.
- Đề xuất **mã hoá có thể tìm kiếm** (Searchable Encryption).

Mục tiêu

- Nghiên cứu các thuật toán mã hoá dựa trên thuộc tính và thuật toán tìm kiếm trên dữ liệu mã.
- Chạy thực nghiệm và so sánh một số thuật toán tối ưu.
- Kết hợp hai loại mã hoá nhằm xây dựng một kịch bản bảo vệ dữ liệu cho bệnh nhân trong ngữ cảnh **healthcare system**.



Nội dung

- Nghiên cứu cách hoạt động, các giải thuật của một số lược đồ cải tiến theo hướng tăng tính hiệu quả và các tính năng bảo mật.
- Triển khai đánh giá trên môi trường hệ quản trị cơ sở dữ liệu SQL/NoSQL trên môi trường đám mây.
- Đánh giá tính hiệu quả bằng cách chạy thực nghiệm.
- Lựa chọn kịch bản triển khai ứng dụng, phân tích cơ sở dữ liệu, lập trình các thuật toán bằng thư viện OpenABE.

Phương pháp

- Đọc tài liệu, các bài báo nghiên cứu uy tín.
- Đánh giá kết quả dựa trên phương pháp triển khai các thực nghiệm.
- Triển khai ứng dụng nhằm xem xét tính hiệu quả trong thực tế.

Kết quả dự kiến

- Phân tích được một số lược đồ, giải thích trình bày được các thuật toán, đánh giá tính hiệu quả.
- Lập trình các thuật toán và xây dựng được một ứng dụng có giao diện để tái hiện ngữ cảnh bảo vệ dữ liệu cho bệnh nhân.
- Đánh giá được tính khả thi trong thực tế.

Tài liệu tham khảo

- Mazhar Ali, Samee U. Khan, & Athanasios V. Vasilakos (2015). Security in cloud computing: Opportunities and challenges. Inf. Sci., 305, 357–383.
- Luo Sheng (2021). User Privacy Protection Scheme Based on Verifiable Outsourcing Attribute-Based Encryption. Secur. Commun. Networks, 2021, 6617669:1–6617669:11.
- Seny Kamara, & Kristin E. Lauter (2010). Cryptographic Cloud Storage. In Financial Cryptography and Data Security, FC 2010 Workshops, RLCPS, WECSR, and WLC 2010, Tenerife, Canary Islands, Spain, January 25-28, 2010, Revised Selected Papers (pp. 136–149). Springer.
- John Bethencourt, Amit Sahai, & Brent Waters (2007). Ciphertext-Policy Attribute-Based Encryption. In 2007 IEEE Symposium on Security and Privacy (S&P 2007), 20-23 May 2007, Oakland, California, USA (pp. 321–334). IEEE Computer Society.
- K. Sowjanya, Mou Dasgupta, & Sangram Ray (2021). A lightweight key management scheme for key-escrow-free ECC-based CP-ABE for IoT healthcare systems. J. Syst. Archit., 117, 102108.
- Christoph Bösch, Pieter H. Hartel, Willem Jonker, & Andreas Peter (2015). A Survey of Provably Secure Searchable Encryption. ACM Comput. Surv., 47(2), 18:1–18:51.
- Shujie Cui, Xiangfu Song, Muhammad Rizwan Asghar, Steven D. Galbraith, & Giovanni Russello (2021). Privacy-preserving Dynamic Symmetric Searchable Encryption with Controllable Leakage. ACM Trans. Priv. Secur., 24(3), 18:1–18:35.
- Yanyu Huang, Siyi Lv, Zheli Liu, Xiangfu Song, Jin Li, Yali Yuan, & Changyu Dong (2021). Cetus: an efficient symmetric searchable encryption against file-injection attack with SGX. Sci. China Inf. Sci., 64(8).