**Tên Đề Tài:**

- Tên: Bảo mật và Kiểm soát Quyền truy cập Cơ sở Dữ liệu –

Database Confidentiality and Access Control in Cloud-native DBMS

- Thuật toán sử dụng: AES và CP-ABE

**Ngữ Cảnh:**

Một doanh nghiệp vừa và nhỏ có rất nhiều dữ liệu riêng tư của nhân sự nội bộ và các đối tác bên ngoài. Họ muốn lưu trữ những thông tin trên vào cơ sở dữ liệu của mình lên Cloud. Để đảm bảo an toàn cho những dữ liệu này, họ cần mã hóa và kiểm soát quyền truy cập, chỉ cho phép những người được ủy quyền mới có thể sử dụng.

Các bên liên quan gồm:

- Key Management Center (KMC): Trung tâm quản lý khoá chịu trách nhiệm cung cấp các khóa và quyền truy cập cho các bên khác.

- Admins: Chủ sở hữu dữ liệu, phía thực hiện mã hóa dữ liệu trong cơ sở dữ liệu bằng AES trước khi đưa lên cloud

- Users: Người dùng dữ liệu trong cơ sở dữ liệu. Vì dữ liệu được lưu trữ trên cloud đã được mã hóa, Users muốn truy cập và giải mã dữ liệu cần phải có quyền truy cập do bên KMC cung cấp.

- Threats: Tập hợp các mối đe dọa cho doanh nghiệp – là bên tìm cách gây hại, tấn công vào hệ thống nhằm mục đích đánh cắp, phá hoại dữ liệu, gây mất uy tín cho doanh nghiệp.

**Mục Tiêu:**

Trong thời đại công nghệ 4.0 hiện nay, Việt Nam chúng ta đang trong quá trình phát triển và hội nhập quốc tế. Do đó, số hoá các dữ liệu cá nhân/tập thể là một nhu cầu cấp thiết hơn bao giờ hết.

Việc lưu trữ và truy xuất các thông tin nhạy cảm trong một hoặc nhiều cơ sở dữ liệu đòi hỏi ta phải có một cơ chế bảo mật đáng tin cậy, kiểm soát chặt chẽ sự truy cập vào dữ liệu, điều đó phải đảm bảo được tính bảo mật, sự toàn vẹn của dữ liệu và tính sẵn sàng của thông tin.

Các sự kiện rò rỉ thông tin và dữ liệu tại nước ta nói riêng và thế giới nói chung trong những năm gần đây là con số không hề nhỏ. Đặc biệt, trong các doanh nghiệp, hậu quả của việc mất mát hoặc lộ thông tin có thể gây ra những tổn thất nghiêm trọng, không chỉ về mặt tài chính mà còn ảnh hưởng đến uy tín và danh tiếng của doanh nghiệp.

**Kịch Bản Triển Khai:**

- Key Management Center (KMC) là bên xác thực cho Admins và Users trước khi cho phép vào hệ thống

- Admins tiến hành đăng nhập vào hệ thống bằng cách cung cấp ID và password để xác thực, sau khi xác thực thành công, admins thao tác để:

+ Chọn dữ liệu cần mã hóa.

+ Cấp quyền truy cập (quyền truy cập được yêu cầu để Users giải mã được một số cột trong database còn một số cột khác thì không)

- Users ở một máy khác sẽ tiến hành đăng nhập hệ thống bằng cách cung cấp ID và password, sau khi xác thực thành công Users tiến hành tải dữ liệu trên Cloud về và tiến hành giải mã để lấy key AES. Các thao tác như: kiểm tra đã có secret key hay chưa, gửi yêu cầu đến TA, giải mã lấy key -> sẽ được thực hiện, đối với những key mà Users không có quyền truy cập sẽ hiện kết quả là “Permission denied” trong file key đã được giải mã; sau khi có key AES, user sử dụng key này để giải mã dữ liệu trong cột tương ứng.