Ngữ cảnh ứng dụng: Dữ liệu được đưa lên cloud từ công ty và các bên liên quan có thể sử dụng dữ liệu nhưng attacker có thể giả danh là một trong các bên liên quan để lấy đi những thông tin nhạy cảm.

Xác định tài sản cần bảo vệ: Thông tin của khách hàng cũng như thông tin của các bên liên quan ví dụ như danh sách hợp đồng.

Các bên liên quan: Ngân hàng, Hành chính, truyền thông, chuỗi cung ứng, vận chuyển.

Mục tiêu bảo mật:

Giải pháp: Phải có cơ chế xác thực các bên liên quan cũng như cấp phát quyền truy cập dữ liệu trên cloud của các bên liên quan.

Cách giải quyết: Sử dụng kiến trúc CP-ABE để lưu dữ liệu trên cloud cũng như cấp phát quyền truy cập dữ liệu cho các bên liên quan.

Lựa chọn ngữ cảnh và kịch bản ứng dụng để triển khai thử nghiệm: Khi các bên liên quan muốn truy cập dữ liệu, giả sử đó là attacker giả danh, phải có cơ chế xác thực bên liên quan.

Thấy k được chỗ nào thì ghi vào notepad

Ngữ cảnh là gì:

Tài sản:

Cách giải quyết:

Khi requests dữ liệu, ý là sử dụng index,ví dụ khi tìm một người trên database, dữ liệu nhập vào là bản rõ nhưng dữ liệu của người đó trên database lại là bản mã, do vậy nếu tìm thì phải tìm index, index là thuộc tính hoặc gì đó.

(ví dụ: khi tìm một bạn học sinh trong lớp được lưu trên database, sẽ tìm danh sách cả lớp trên database, sau đó lấy về và giải mã rồi tìm bạn muốn tìm).

Mã hóa database, dùng AES thì sẽ gặp vấn đề thu hồi khóa.

Bảo vệ secret key bằng phần cứng. Trusted Platform module(phần cứng của apple), TEE(phần mềm của android).

Khóa của AES được tạo ra và cất giữ bởi trusted authority. Khóa public và private của người dùng sẽ được tạo ra bởi trusted authority. Khóa private của người dùng sẽ được người dùng lưu trữ ở local.

Khi người dùng muốn upload data lên database, người dùng sẽ requests đến database để lấy key, người dùng sẽ mã hóa một thông điệp nào đó sử dụng private key của người dùng và public key của nơi nhận để có thể xác thực được cả bên nhận và bên gửi. Nếu hợp lệ thì key AES sẽ được gửi về cho client và giải mã để giải mã dữ liệu được lấy từ database.

Adapter lookback traffic.

=====================================================================================

Ngữ cảnh: nhiều người dùng sàn giao dịch thương mại điện tử muốn lưu lịch sử giao dịch và các thông tin liên quan trên cloud.

Giải pháp: sử dụng identity base( identity base được dùng để mã key và kiểm soát truy cập).

Key được tạo ra từ bên mua và bên bán(key AES để mã hóa dữ liệu). sau đó mã hóa dữ liệu (dữ liệu về hóa đơn thanh toán ), key của AES sẽ được mã hóa bằng khóa private của mình và public của người mà mình muốn cho phép đọc dữ liệu. Sau đó phần đó được gắn vào phần mã hóa dữ liệu và đẩy lên cloud. Trên cloud sẽ gồm nhiều bản mã hóa và mỗi bản mã hóa, key AES sẽ được mà bằng private key của mình và public key của người mà mình muốn cho phép đọc dữ liệu. Public key của người nhận sẽ được xác thực bằng identity base.

Dữ liệu được lưu trữ trên NoSql dưới dạng json.

Tạo bill – thanh toán bill – tất toán.

Shoppee chỉ là một bên trung gian.

Bill được tạo ra bởi người bán hàng.