**Báo cáo ngày 30/12/2024**

* Các vấn đề được đặc ra ở tuần trước:

1. Tổng thể của CP-ABE
2. Chi tiết thành phần
3. Ứng dụng
4. Hạn chế
5. Làm sao để áp dụng thư viện RELIC vào CP-ABE

* Giải quyết

1. Tổng thể CP-ABE:

* Mã hóa dựa trên thuộc tính là kỹ thuật mã hóa cho phép kiểm soát truy cập dữ liệu dựa trên các thuộc tính của người dùng và dữ liệu. Thay vì mã hóa dữ liệu cho một người dùng cụ thể, ABE cho phép mã hóa dữ liệu dựa trên chính sách truy cập, trong đó quy định các thuộc tính cần thiết để giải mã. Có 2 loại chính: CP-ABE và KP-ABE
* CP-ABE (Ciphertext-Policy Attribute-Based Encryption): Trong CP-ABE, chính sách truy cập được nhúng vào bản mã, khóa bí mật của người dùng được liên kết với các thuộc tính. Người dùng có thể giải mã bản mã nếu các thuộc tính của họ thỏa mãn chính sách truy cập. CP-ABE thường được sử dụng trong các ứng dụng như chia sẻ dữ liệu trên đám mây, nơi người gửi dữ liệu muốn kiểm soát ai có thể truy cập dữ liệu của họ

1. Chi tiết thành phần:

* Key word:
  + Thuộc tính (Attributes): Các đặc điểm hoặc vai trò của người dùng hoặc dữ liệu.
  + Chính sách truy cập (Access Policy): Các quy tắc xác định ai có quyền truy cập dữ liệu, được biểu diễn bằng các biểu thức logic kết hợp các thuộc tính.
  + Khóa công khai (Public Key): được sử dụng để mã hóa dữ liệu
  + Khóa bí mật (Secret Key): được cấp cho người dùng và được liên kết với các thuộc tính của họ, dùng để giải mã dữ liệu
  + Bản mã (Ciphertext): dữ liệu được mã hóa bằng CP-ABE, chứa chính sách truy cập
  + Cơ quan cấp thuộc tính (Attribute Authority - AA): tổ chức chịu trách nhiệm quản lý và cấp các thuộc tính cho người dùng
* Cơ chế hoạt động:
  + Setup: Hệ thống được khởi tạo bằng cách tạo ra khóa công khai (PK) và Master Key.
  + KeyGen: Cơ quan cấp thuộc tính tạo khóa bí mật cho người dùng dựa trên các thuộc tính của họ và Master Key.
  + Encrypt: Người dùng mã hóa dữ liệu bằng khóa công khai và chỉ định chính sách truy cập, tạo ra bản mã.
  + Decrypt: Người dùng có thể giải mã bản mã nếu các thuộc tính của họ thỏa mãn chính sách truy cập trong bản mã. Nếu không, việc giải mã thất bại.

1. Ứng dụng:

* Bảo mật dữ liệu y tế: bảo vệ thông tin bệnh nhân bằng cách chỉ cho bác sĩ và nhân viên y tế có đủ thẩm quyền truy cập, Internet of Medical Things (IoMT) bảo mật các dữ liệu y tế được thu thập bởi các thiết bị IoMT
* Chia sẻ dữ liệu trên đám mây: cho phép người dùng kiểm soát ai có thể truy cập dữ liệu của họ trên đám mây
* Quản lý quyền truy cập trong tổ chức: cho phép các tổ chức kiểm soát truy cập dữ liệu dựa trên vai trò, vị trí và các thuộc tính khác của nhân viên
* Hệ thống truyền hình trả tiền: đảm bảo chỉ những người dùng đã trả tiền mới có thể xem các kênh
* Chia sẻ tập tin: kiểm soát ai có thể truy cập các tập tin chia sẻ
* Quản lý khóa nhóm: kiểm soát quyền truy cập vào các tin nhắn đa phương tiện an toàn

1. Ưu điểm, hạn chế:

* Ưu điểm:
  + Kiểm soát truy cập chi tiết: CP-ABE cho phép kiểm soát truy cập dữ liệu một cách linh hoạt và chi tiết dựa trên các thuộc tính của người dùng. Thay vì mã hóa cho một người dùng cụ thể, dữ liệu được mã hóa dựa trên chính sách truy cập.
  + Tính linh hoạt: hệ thống hỗ trợ các chính sách truy cập phức tạp, có thể bao gồm các cổng AND, OR và các cấu trúc ngưỡng (threshold). Các chính sách này có thể kết hợp nhiều thuộc tính khác nhau.
  + Bảo mật dữ liệu: dữ liệu được mã hóa và chỉ những người dùng có thuộc tính phù hợp với chính sách truy cập mới có thể giải mã. Điều này đảm bảo tính bảo mật của dữ liệu ngay cả khi máy chủ lưu trữ bị xâm nhập.
  + Không cần biết trước danh sách người nhận: người gửi có thể mã hóa dữ liệu mà không cần biết chính xác danh sách người nhận, chỉ cần xác định chính sách truy cập dưa trên thuộc tính.
  + Chống tấn công thông đồng: hệ thống được thiết kế để chống lại các cuộc tấn công thông đồng, trong đó nhiều người dùng kết hợp khóa của họ để truy cập dữ liệu trái phép
* Hạn chế:
  + Quản lý khóa tập trung (Trong một số triển khai): Một số triển khai CP-ABE có thể tập trung vào một cơ quan quản lý khóa, gây rủi ro nếu cơ quan này bị tấn công *(Authority sở hữu một khóa bí mật của hệ thống (master secret key) để tạo khóa bí mật cho từng người dùng, hệ thống như vậy gọi là hệ thống tập trung hóa. Hệ thống tập trung hóa có hai điểm yếu. Điểm yếu đầu tiên cũng là quan trọng nhất là do authority là người tạo khóa, do đó authority biết tất cả khóa bí mật của người dùng trong hệ thống. Điều này dẫn đến nguy cơ mất an toàn đối với người dùng khi authority gian dối hoặc bị tấn công lấy mất master secret key. Điểm yếu thứ hai là do chỉ có một authority tạo khóa cho người dùng, nên nếu authority bị quá tải hay bị tấn công hệ thống sẽ không thể tạo khóa cho người dùng. Tuy nhiên do số lượng người dùng mới tham gia vào hệ thống là ít và không thường xuyên đối với đa số ứng dụng, do vậy điểm yếu thứ hai thường không được coi trọng bằng điểm yếu đầu tiên. Một hệ thống có tính chất phi tập trung hóa là hệ thống giải quyết tốt được ít nhất điểm yếu đầu tiên.)* Điều này có thể được giảm thiểu bằng cách sử dụng các hệ thống phi tập trung hóa*. (Mã hóa dựa trên thuộc tính là hướng nghiên cứu được các nhà nghiên cứu quan tâm, có rất nhiều các hệ mã hóa dựa trên thuộc tính với các tính chất khác nhau [1-9] đã được công bố. Trong đó hệ mã của hai tác giả Riepel-Wee đề xuất năm 2022 [6] (được công bố 135 TẠP CHÍ KHOA HỌC TRƯỜNG ĐẠI HỌC HỒNG ĐỨC - SỐ 67.2023 tại một trong những hội nghị lớn nhất của ngành an toàn bảo mật thông tin ACM CCS) được xem là quan trọng nhất. Trong bài báo này đóng góp của chúng tôi là cải tiến hệ mã này bằng cách bổ sung thêm tính chất phi tập trung hóa cho hệ mã này. Đồng thời chúng tôi cũng đưa ra sự so sánh hệ mã đề xuất với các hệ mã dựa trên thuộc tính có hỗ trợ tính chất phi tập trung hóa khác).*
  + Độ phức tạp tính toán: các thuật toán mã hóa và giải mã có thể phức tạp, đặc biệt khi chính sách truy cập phức tạp. Điều này có thể làm chậm quá trình mã hóa và giải mã. Tuy nhiên, các nghiên cứu đã chỉ ra rằng có thể giảm độ phức tạp tính toán bằng cách sử dụng các sensitive attributes thay vì kiểm tra toàn bộ các thuộc tính của đối tượng (object) và chủ thể (subject), hệ thống chỉ cần kiểm tra những thuộc tính thực sự ảnh hưởng đến quyết định truy cập. Điều này giúp giảm bớt lượng thông tin cần xử lý.
  + Kích thước bản mã: kích thước bản mã có thể tăng lên khi chính sách truy cập phức tạp hoặc số lượng thuộc tính lớn. điều này có thể ảnh hưởng đến hiệu suất trong các hệ thống có băng thông hạn chế. Tuy nhiên, có các phương pháp tối ưu hóa để giảm kích thước bản mã như cấu trúc phân cấp các thuộc tính (hierarchy of attributes) cấu trúc này giúp giảm số lượng các phần tử nhóm cần thiết để biểu diễn các thuộc tính, làm hệ thống nhẹ hơn. Hierarchy of attributes là cách tổ chức các thuộc tính trong một hệ thống theo một cấu trúc phân cấp, trong đó các thuộc tính được sắp xếp theo thứ bậc từ tổng quát đến chi tiết hoặc từ cấp cao đến cấp thấp.
  + Khó khắn trong việc kiểm soát toàn bộ hành vi của kẻ tấn công: đòi hỏi việc sử dụng các kỹ thuật machine learning để bảo vệ các hệ thống đám mây
  + Khó khăn trong việc chứng minh an toàn tuyệt đối
  + Quản lý thuộc tính phức tạp: việc quản lý và cấp phát thuộc tính cho người dùng có thể phức tạp, đặc biệt trong các hệ thống lớn với nhiều thuộc tính
  + Vấn đề thu hồi khóa: việc thu hồi khóa của người dùng có thể khó khăn và tốn kém nếu không được thiết kế cẩn thận

1. Làm sao để áp dụng thư viện RELIC vào CP-ABE

* Xác định các thành phần CP-ABE có thể được thay thế bằng RELIC:
  + Phép ghép cặp song tuyến tính (Bilinear Pairing): Các thư viện như PBC thường được dùng cho các phép ghép cặp song tuyến tính. RELIC cũng cung cấp các hàm tương tự và có thể thay thế PBC trong các thuật toán CP-ABE.
  + Các phép toán trên nhóm elliptic: Các phép toán này là cần thiết cho CP-ABE. RELIC có thể cung cấp các hàm để thực hiện các phép toán này trên các đường cong elliptic.
* Ví dụ về việc tích hợp: Trong lược đồ CP-ABE được mô tả trong một tài liệu, các tác giả sử dụng thư viện PBC. Có thể thay thế các hàm liên quan đến phép ghép cặp song tuyến tính và các phép toán trên nhóm trong PBC bằng các hàm tương ứng của RELIC. Tuy nhiên vẫn cần cân nhắc về tính tương thích