Journal of educational equipment: Applied research, Volume 1, Issue 298 (October 2023)
ISSN 1859 - 0810

Quản lý khóa phân cấp trên đám mây nhằm chia sẻ hệ thống bảo mật dữ liệu thuê ngoài

Mai Trung Đông*

**TS. Học Viện Hành chính Quốc gia*

Received: 5/9/2023; Accepted: 8/9/2023; Published: 19/9/2023

Abstract: *As society develops, the need to store and use data is increasing, meeting data on the cloud is not enough, so we need more data to be shared outside. A cloud outsourcing data sharing technology based on linear geometric level key management is proposed to solve the full sharing of existing cloud outsourcing data and complex hierarchical structure and access groups. Hierarchical Key Management technical diagram and principles are explained, and three rules are designed. The article will design and analyze in detail the system construction algorithm, key derivation algorithm and dynamic key management. The algorithm is tested experimentally, and the verification results show that the solution is safe and relatively effective.*

Keywords: *Cloud computing; Share data*

1. Mở đầu

Với sự phát triển nhanh chóng của điện toán đám mây, dịch vụ lưu trữ đám mây ngày càng được nhiều người dùng sử dụng. Do người quản lý dữ liệu ở dạng lưu trữ này, tức là nhà cung cấp dịch vụ đám mây, không hoàn toàn đáng tin cậy [1], nên cần phải thiết lập một Cơ chế tương ứng để đảm bảo tính riêng tư của dữ liệu thuê ngoài.

Nói chung, dữ liệu gia công phần mềm đám mây của CSHDL sẽ được chia sẻ bởi nhiều người và có các yêu cầu chi tiết về quyền chia sẻ [2], vì vậy việc chia sẻ bảo mật dữ liệu gia công phần mềm đám mây cũng rất quan trọng. Thông thường, việc chia sẻ dữ liệu thuê ngoài có thể được coi là một vấn đề kiểm soát truy cập phân cấp, vì vậy bài báo này nghiên cứu và thiết kế một công nghệ chia sẻ dữ liệu thuê ngoài trên đám mây dựa trên QLKPC HHTT.

2. Nội dung nghiên cứu

2.1.Quản lý khóa phân cấp (QLKPC)

Sử dụng tập hợp có thứ tự (V, ≤) để biểu diễn khung phân cấp trong kiểm soát truy cập phân cấp, trong đó V = {V_1, V_2, ..., V_n} là tập hợp các nhóm người dùng, V_i là một người dùng hoặc nhiều Một nhóm truy cập bao gồm những người dùng có cùng quyền truy cập thường được gọi là một lớp.

Mối quan hệ nhị phân "≤" là mối quan hệ thứ bậc của các phần tử trong tập V, chẳng hạn $V_i \leq V_j$ có nghĩa là người dùng thuộc lớp V_j có thể truy cập tài nguyên dữ liệu tương ứng với lớp V_i, tức là cấp độ truy cập của lớp V_j là cao hơn so với lớp V_i. Bất kỳ (V, ≤) nào cũng có thể biểu diễn dưới dạng đồ thị có hướng G = (V, E) [3], nếu V_i, $V_j \in V$ và $V_i \leq V_j$ thì trong G có đồ thị từ V_j The cạnh hướng tới V_i. Để thuận tiện cho việc biểu diễn, hãy xác định hai tập hợp: Anc (V_i, G) và Des (V_i, G), nếu tồn tại một đường đi từ V_i đến V_j trong G thì $V_i \in$ Anc(V_j , G) Và $V_j \in$ Des (V_i, G), thể hiện rằng các quyền truy cập tương ứng với một nhóm truy cập trong cấu trúc phân cấp cao hơn và thấp hơn so với các tập nhóm truy cập khác, vì vậy chúng được gọi là cụm cấp cao và cấp thấp của V_i tương ứng.

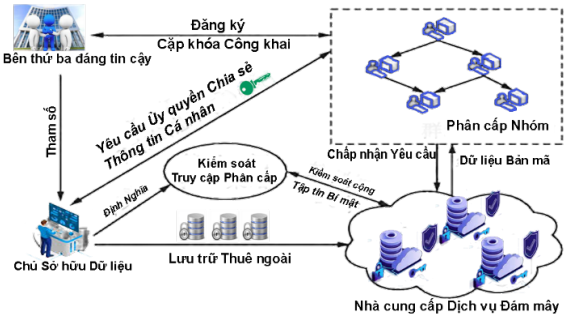
Đặt Γ biểu diễn tập đồ thị truy cập tương ứng với hệ thống truy cập phân cấp và sơ đồ QLKPC bao gồm hai thuật toán như sau:

1) Thuật toán thiết lập hệ thống [4]. Bản chất của nó là xác suất, đầu vào là tham số bảo mật κ và một cấu trúc phân cấp tương ứng với đồ thị truy cập G = (V, E) ∈ Γ, đầu ra là tham số công khai của hệ thống pub và mỗi lớp $V_i \in V$ tương ứng với (p_i, k_i), trong đó p_i và ki lần lượt là thông tin riêng tư và khóa mã hóa đối xứng của lớp V_i.

2) Thuật toán dẫn xuất khóa Der (pub, V_i, V_j, p_i, k_i) [5]. Bản chất của nó là xác định, đầu vào là tham số công khai của hệ thống pub, hai lớp V_i và V_j và (p_i, k_i) tương ứng với lớp V_i, nếu đầu ra $V_j \leq V_i$ thì xuất mã hóa đối xứng tương ứng với lớp V phím j.

2.2. Lược đồ QLKPC hình học tuyến tính (HHTT)

Khung của sơ đồ QLKPC sử dụng HHTT được hiển thị trong Hình 2.1.



***Hình 2.1**: Khung chia sẻ bảo mật dữ liệu dùng chung được thuê ngoài trên nền tảng đám mây dựa trên QLKPC*

Theo đó, lược đồ bao gồm các bên thứ ba đáng tin cậy, chủ sở hữu dữ liệu, người dùng và nhà cung cấp dịch vụ đám mây. Khi sử dụng QLKPC để giải quyết việc chia sẻ an toàn dữ liệu thuê ngoài trên đám mây, CSHDL đóng vai trò là trung tâm ủy quyền trong sơ đồ, mã hóa dữ liệu được chia sẻ và truyền bản mã được mã hóa đến máy chủ của nhà cung cấp dịch vụ đám mây. Ngoài ra, CSHDL xác định cấu trúc phân cấp của nhóm chia sẻ, đồng thời hoàn thành yêu cầu chia sẻ của người dùng đối với dữ liệu được thuê ngoài. Tất cả người dùng có thể gửi yêu cầu truy cập tới nhà cung cấp dịch vụ đám mây và chỉ những người dùng có được thông tin cá nhân và khóa mã hóa đối xứng mới có thể giải mã bản mã tương ứng với quyền được chia sẻ của họ.

Hàm giả ngẫu nhiên F [6] được định nghĩa là: K × D→RG. Trong đó, K là tập khóa của F, D và RG là miền và khoảng của F. Đối với k∈K, $F_k(x) = F(k, x)$ đại diện cho một thể hiện của F, đặt Rand = { g | g : D→RG} là tập hợp tất cả các hàm từ D đến RG và hF là đối số thời gian đa thức . Đối với một chức năng g trong Rand hoặc F: D → RG, đối thủ hF có quyền truy cập vào lời tiên tri.

Đặt nhóm truy cập V_i, $V_j \in V$ thì khóa gián tiếp từ V_i đến V_j là

(1)

Trong công thức: $k_{i,l}$ và $k_{j,j}$ lần lượt là các khóa mã hóa đối xứng tương ứng với các nhóm truy cập V_i và V_j;

$w_{i,1}$ và $w_{i,2}$ lần lượt là thông tin riêng của nhóm khách V_i thông qua hàm giả ngẫu nhiên F.

Quy tắc xây dựng đề án như sau:

1) Đối với bất kỳ nhóm truy cập V_i nào, tích bên trong giữa vectơ riêng X_i và vectơ công khai A_i bằng khóa mã hóa đối xứng tương ứng của nó [7-8], cụ thể là ;

2) Nếu V_i, $V_j \in V$ và $V_i \in Anc(V_j, G)$, thì tích bên trong của vectơ riêng X_i của nhóm truy cập V_i và vectơ công khai A_i của nó bằng với khóa gián tiếp $k_{i,j}$[9], cụ thể là ;

Nếu V_i, $V_j \in V$ và $V_i \in Anc(V_j, G)$, thì tích trong của vectơ riêng X_i của nhóm truy cập V_i và vectơ công khai Ai của nó bằng 0[10], cụ thể là ;

2.3 Xây dựng hệ thống thuật toán Gen(l_κ, G)

Các bước xây dựng thuật toán Gen(l_κ, G) như sau:

1) Chọn ngẫu nhiên các vectơ khác 0 $Y_i = (y_{i,1}, y_{i,2})$ và $Z_i = (z_{i,1}, z_{i,2})$ cho lớp V_i là thông tin riêng của nó.

2) Ánh xạ tất cả các vectơ riêng Y_i sang một vectơ mới W_i thông qua hàm giả ngẫu nhiên F, quy trình cụ thể là:

ⓐ Chọn ngẫu nhiên một tham số công khai r trong trường hữu hạn, sau đó tính $w_{i,1} = Fy_{i,1}(r)$ và $w_{i,2} = Fy_{i,2}(r)$, i = 1, 2,..., n;

ⓑ Nếu wi,2 = 0, chọn lại thông số r, sau đó quay lại bước ⓐ để vận hành lại

Chuyển đổi Zi thành vectơ n chiều X_i, khi i = 1, 2, đặt $x_{i,1} = z_{i,1}$, $x_{i,2} = z_{i,2}$, $x_{i,3} = x_{i,4}$, ..., $x_{i,n} = 0$; Khi i = 3, 4, ..., n, cho xi, 1 = $z_{i,1}$, xi, 2 = $z_{i,2}$, cho j≠1 đều có $x_{i,j}$ = 0 thì véc tơ X có thể được thể hiện như

3) Kiểm tra xem X_1, X_2, ..., Xn có độc lập tuyến tính hay không, nếu không độc lập tuyến tính thì chuyển sang bước 4); ngược lại thì quay lại bước 1).

4) Chọn khóa mã hóa đối xứng cho mỗi lớp và tính ma trận công khai A, các bước tính như sau:

ⓐ Đối với mỗi lớp Vi trong G, chọn ngẫu nhiên khóa mã hóa đối xứng $k_{i,i}$ của nó trong trường hữu hạn và sử dụng công thức (1) để tính khóa trung gian $k_{i,j}$;

ⓑ Lập hệ phương trình tuyến tính về ma trận công khai A theo công thức (1), đặt Kj = ($k_{j,1}$, $k_{j,2}$, ..., $k_{j,n}$) và K = [K_1, K_2, .. ., K_n] T , thì X × A = K;

ⓒ Giải hệ phương trình ở bước ⓑ để được $A = X^{-1} \times K$.

5) Gửi ((Y_i, Z_i), $k_{i,i}$) tới từng người dùng trong V_i thông qua kênh bảo mật và gửi F, r và A tới nhà cung cấp dịch vụ đám mây.

Xây dựng thuật toán dẫn xuất Der (pub, V_i, V_j, p_i, k_i) Nếu người dùng trong V_i muốn lấy dữ liệu dùng chung tương ứng với nhóm truy cập cấp thấp V_j, và $V_i \in Anc(V_j, G)$, thì khóa mã hóa đối xứng tương ứng với V_j có thể được lấy thông qua hai bước sau:

1) Áp dụng các quy tắc 2) Tính khóa trung gian $k_{i,j}$;

2) Sau khi giải phương trình $k_{j,j} = w_{i,1} k_{i,i} + w_{i,2} k_{i,j}$, người dùng trong nhóm truy cập V_j có thể nhận được các khóa mã hóa đối xứng tương ứng của họ.

2.4 Quản lý khóa động

Chèn nút mới: Đối với V_i, $V_j \in V$ và $V_i < Vj$, để chèn một nút mới V_t, nghĩa là $Vi < Vt < V_j$, trước tiên hãy chọn ngẫu nhiên hai vectơ khác 0 mới Y_t và Z_t và một $k_{t,t}$ tương ứng được sử dụng làm thông tin riêng tư tương ứng với nhóm V_t và khóa mã hóa đối xứng. Nếu có người dùng trong nhóm truy cập V_t, hãy sử dụng kênh bảo mật để truyền (Y_t, Z_t), $k_{t,t}$) cho người dùng, sau đó chọn lại mã hóa đối xứng cho tất cả các nhóm truy cập có quyền truy cập thấp hơn than V_t Cuối cùng, theo thuật toán xây dựng hệ thống vận hành lại để thu được ma trận công khai A. Sau đó hoàn thành việc mã hóa lại dữ liệu liên quan và đồng thời gửi đến nhà cung cấp dịch vụ đám mây.

xóa một nút: Nếu cấu trúc phân cấp chứa n + 1 nhóm và CSHDL muốn xóa một nhóm khỏi nhóm đó và đặt nhóm truy cập đã xóa thành V_l, thì cần cập nhật tất cả các nhóm truy cập có quyền truy cập thấp hơn V_l khóa mã hóa đối xứng mới của nó và tính toán lại theo các bước của thuật toán xây dựng hệ thống để thu được ma trận công khai A. Quá trình mã hóa lại dữ liệu liên quan sau đó được hoàn tất và đồng thời được truyền tới nhà cung cấp dịch vụ đám mây.

2.5. Phân tích thực nghiệm

Đặt kích thước của một phần tử trong trường hữu hạn và số nhóm truy cập trong hệ thống lần lượt là L và n, và số phần tử trung bình trong tập lớp cấp thấp tương ứng với mỗi nhóm truy cập là c.

Mỗi nhóm truy cập cần lưu thông tin riêng Y_i và Z_i của mình, vì hai vectơ này chứa hai phần tử nên chi phí lưu trữ của người dùng trong mỗi nhóm truy cập là 4L và CSHDL phải lưu thông tin riêng tương ứng với tất cả các nhóm truy cập, vì vậy chi phí lưu trữ của nó bằng 4nL.

Gọi H là chi phí tính toán của hàm giả ngẫu nhiên F và a, m và v lần lượt là chi phí tính toán của phép toán cộng, nhân và nghịch đảo trên trường hữu hạn. Để có được khóa mã hóa đối xứng tương ứng của nhóm truy cập, mỗi thành viên trong nhóm cần thực hiện hai phép nhân và một phép cộng trên trường hữu hạn; Để có được khóa mã hóa đối xứng tương ứng với nhóm có quyền truy cập thấp, người dùng ở lớp cấp cao cần tính F 2 lần, đồng thời thực hiện 4 lần nhân 2 lần cộng, như vậy tổng phép tính tốn bằng 2H + (4c + 2)m + (2c + 1) a.

CSHDL cần tính giá trị hàm giả ngẫu nhiên F của Y_i tương ứng của mỗi nhóm và chi phí tính toán là 2nH; sau đó cần tính khóa trung gian $k_{i,j}$ và 2cn lần nhân và n lần nghịch đảo phép toán cần hoàn thành; ma trận công khai A cũng phải được tính toán, để hoàn thành không quá $3n^2 + 2n + 6$ lần phép nhân và n lần phép nghịch đảo, do đó tổng chi phí tính toán của CSHDL trong quá trình khóa hệ thống cách dựng bằng 2nH + ($3n^2$ +(2c + 2)n + 6)m + ($3n^2$ + (c + 2) n + 2)a + 2nv.

Đặt L = 160, chọn nền tảng vận hành của CSHDLvà nhà cung cấp dịch vụ đám mây là máy trạm Dell T5610 và nền tảng vận hành của người dùng là máy trạm HP XW4600. Chi phí thời gian để CSHDLhoàn thành việc xây dựng khóa hệ thống, dẫn xuất khóa và quản lý khóa được thể hiện tương ứng.

Thời gian của khóa mã hóa đối xứng tương ứng với bất kỳ nhóm truy cập cấp thấp nào là 0,0019 ms. Với tiền đề xác định tập nhóm truy cập cấp thấp, khi c = 5 và c = 10, thời gian để người dùng lấy được khóa mã hóa đối xứng tương ứng với tất cả các nhóm truy cập cấp thấp lần lượt là 0,0508 ms và 0,0689 ms. Khi người dùng trong bất kỳ nhóm truy cập nào lấy được khóa, trước tiên hãy kiểm tra xem giá trị của khóa trung gian có bằng 0 hay không, sau đó tính toán chi phí thời gian của khóa mã hóa đối xứng tương ứng với tất cả các nhóm truy cập cấp thấp.

3. Kết luận

Sơ đồ chia sẻ bảo mật dữ liệu gia công phần mềm đám mây QLKPC dựa trên HHTT được thiết kế và ba quy tắc bao gồm thuật toán xây dựng hệ thống, thuật toán dẫn xuất khóa và quản lý khóa động được xây dựng. CSHDL tiết lộ một véc-tơ cho từng nhóm truy cập và sản phẩm bên trong của véc-tơ riêng và véc-tơ công khai của mỗi nhóm truy cập được sử dụng làm khóa mã hóa đối xứng. Sử dụng các khóa gián tiếp, người dùng trong các nhóm truy cập cấp cao có thể lấy các khóa mã hóa đối xứng của các nhóm truy cập cấp thấp. Trong quá trình giải quản lý khóa chia sẻ quyền động, CSHDL chỉ cần cập nhật ma trận công khai trong hệ thống. Theo phân tích kết quả thử nghiệm, chương trình này an toàn và tương đối hiệu quả.

Tài liệu tham khảo

[1] ZHAO Ming-hao. Applied cryptography for security and privacy protection of outsourcing big data service [D]. Jinan: Shandong University, 2017.

[2] Hur J. Improving security and efficiency in attributebased data sharing [J] IEEE Transactions on know -ledge and data engineering, 2013, 25 (10): 2271-2282.

[3] PEI Xin. Study on key technologies of data security model design and analysis in cloud storage [D] Shanghai: East China University of Science and Technology, 2016.