Tạp Chí Tin Học và Điều Khiển Học
Tập IX(1993), Số 2, 22-27

Về Một Phương Pháp Điều Khiển Truy Nhập Trong Cơ Sở Dữ Liệu

Đào Thị Hồng Hạnh
Bộ Giáo Dục và Đào Tạo

I. Mở đầu

Ta dùng thuật ngữ an toàn để nói sự bảo vệ dữ liệu trong cơ sở dữ liệu chống lại sự truy nhập, sửa đổi mà không được phép. Đây là mối quan tâm to lớn hiện nay trong lĩnh vực này. Ở đây chúng ta không xem xét những khía cạnh đạo đức và xã hội của vấn đề. Thay vào đó chúng ta sẽ xét một biện pháp bảo vệ thông qua điều khiển truy nhập.

Điều khiển truy nhập đảm bảo rằng mọi truy nhập trựctiếp tới đối tượng phải hợp pháp. Khái niệm điều khiển truy nhập đồng nhất với khái niệm quyền sở hữu (ownship) nghĩa là người quản trị hệ thống có thể phân phối và hủy các quyền trên các đối tượng của họ. Trong hệ thống bảo vệ cơ sở dữ liệu các đối tượng được hiểu là các file dữ liệu và thành phần của chúng.

Hiệu quả của điều khiển truy nhập dựa trên ba tiên đề:

- Thứ nhất là nhận biết chính xác người xử dụng, có một số phương pháp giải quyết yêu cầu này: sử dụng mật khẩu (password) có thể là một xâu gồm kí tự và chữ số. Độ bảo mật của phương pháp này thụ thuộc độ dài của xâu và sự ngẫu nhiên của sự xuất hiện từng phần tử xấu. Phương pháp dùng hàm một chiều có tính chất tồn tại hàm ngược nhưng thuật toán để xác định hàm ngược có độ phức tạp tính toán cao. Hệ thống bảo vệ đưa ra một số ngẫu nhiên x, người xử dụng đưa vào giá trị y. Nếu $y = f(x)$, f là hàm một chiều cài đặt trong hệ thốngthì người xử dụng được phép vào làm việc.

- Thứ hai là các thông tin xác định quyền truy nhập của người xử dụngphải được bảo vệ đối với những thay đổi không được phép.

- Thứ ba là nhận biết chính xác quyền xử dụng của từng người được phép vào làm việc. Mô hình ma trận truy nhập cung cấp cho ta một khung nhìn mô tả điều khiển truy nhập. Mô hình

này đã được Graham và Denning nghiên cứu [5], sau đó được Harrison, Ruzzo và Ullman phát triển [6]. Mô hình này được xây dựng như sau:

Gọi S là tập các người xử dụng, gọi F là tập các file; A là ma trận truy nhậpmà các dòng tương ứng với người xử dụng, các cột tương ứng với các file và $A[s, f]$ liệt kê các quyền của người xử dụng s đối với file f.

Quyền truy nhập đối với file có thể bao gồm: không có quyền gì, quyền thực hiện (execute), quyền đọc (read), ghi (write) và có mọi quyền (own).

Trong những năm gần đây một số tác giả đã đề xuất các phương pháp điều khiển ma trận truy nhập để hệ thống nhận biết được các quyền $A[s, f]$ trong ma trận đó: phương pháp liệt kê các khả năng (capability - list method), phương pháp liệt kê truy nhập (access - list method) trong [2]. Hai phương pháp này đòi hỏi bộ nhớ lớn để lưu trữ các quyền và tốn thời gian tìm kiếm để cập nhật thông tin. Để khắc phục nhược điểm trên, bài báo này đề cập một phương pháp điều khiển truy nhập dùng khóa đơn cho hệ thống bảo vệ thông tin. Mỗi người xử dụng được cấp một khóa số nguyên, nhờ đó hệ thống nhận biết các quyền của họ. Cấu trúc của bài báo như sau:

Phần 2 trình bày sơ đồ điều khiển truy nhập dùng khóa đơn. Phần 3 đề xuất một áp dụngcủa phương pháp này cho mô hình cơ sởdữ liệu quan hệ. Phần 4 đưa ra đánh giá độ phức tạp thời gian của khóa. Phần 5 đưa ra khái niệm khóa nhóm để giải quyết giá trị khóa bị tràn. Phần 6 là phần kết luận.

2. Sơ đồ điều khiển truy nhập dùng khóa đơn

Giả sử hệ thống bảo vệ điều khiển quyền truy nhập của m người sử dụng đối với n file dữ liệu.

Mỗi người sử dụng được xác định bởi một số nguyên dương i, mỗi file được xác định bởi một số nguyên dương j, mỗi phần tử a_{ij} của ma trận là số nguyên dương không âm có thể được mã như sau:

- $a_{ij} = 0$ - không có quyền gì,
- $a_{ij} = 1$ - quyền thựchiện (ví dụ in),
- $a_{ij} = 2$ - quyền đọc,
- $a_{ij} = 3$ - quyền ghi,
- $a_{ij} = 4$ - có mọi quyền.

Ví dụ một ma trận truy nhập cho 4 người sử dụng đối với 5 file

User i	file $j = 1$	2	3	4	5
1	2	0	1	1	3
2	1	3	1	2	0
3	3	0	2	0	1
4	1	1	0	2	0

Định lí sau cho ta câu trả lời cách tính khóa K_i cho mỗi người sử dụng và cách tính giá trị a_{ij}.

Định lý 2.1 [1] *Cho $A_{m\times n}$ là một ma trận điều khiển truy nhập, t là tổng số các quyền truy nhập file, a_{ij} là phần tử (i,j) của ma trận. Khi đó tồn tại một số nguyên K_i gọi là khóa của người sử dụng i sao cho*

$$a_{ij} = [K_i/(t+1)^{j-1}] mod(t+1),\ 1 \le i \le m,\ 1 \le j \le n. \tag{1}$$

Khóa K_i được tính như sau:

$$K_i = \sum_{q=1}^{n} a_{iq}(t+1)^{q-1}. \tag{2}$$

Từ đó suy ra sơ đồ điều khiển truy nhập dùng khóa đơn giản như sau: Hệ thống bảo vệ cấp cho người sử dụng i một khóa K_i. Khi người sử dụng nêu yêu cầu truy nhập t tới file j, hệ thống sẽ tính toán a_{ij} từ đó chấp nhận hay từ chối.

Ví dụ ta tính khóa K_1 cho người sử dụng thứ nhất trong ma trận trên

$$K_1 = \sum_{q=1}^{5} a_{1q}5^{q-1},\ K_1 = 2027.$$

Tương tự ta tính được $K_2 = 291,\ K_3 = 653,\ k_4 = 256.$

Ta tính quyền truy nhập của người sử dụng có số hiệu 3 trên file có số hiệu 4 tức là tính A_{34} như sau

$$a_{34} = [K_3/(4+1)^{4-1}] mod(4+1) = [653/5^3] = 0.$$

3. Áp dụng điều khiển truy nhập khóa đơn cho mô hình cơ sở dữ liệu quan hệ

Giả sử hệ thống điều khiển quyền truy nhập của m người sử dụng trên n file dữ liệu, mỗi file có k trường. Phần này chúng tôi đưa ra cách điều khiển truy nhập của người sử dụng i đối với trường t của file j.

Ta lập ma trận điều khiển truy nhập $B = (b^i_{jt})$, các dòng ứng với các file, các cột ứng với các trường, b^i_{jt} cho biết quyền của người sử dụng i trên file j đối với trường t. Cách mã b^i_{jt} có thể giống như với a_{ij} ở trên đồng thời có thể bổ xung thêm các quyền sửa, xóa đối với từng trường t.

Định lý dưới đây có thể dùng làm cơ sở cho việc điều khiển truy nhập ma trận $B = (b^i_{jt}$.

Định lý 3.1 *Cho (b^i_{jt}) là ma trận điều khiển truy nhập của người sử dụng i trên file j đối với trường t của cơ sở dữ liệu quan hệ. trong đó $1 \le i \le m,\ 1 \le j \le n,\ 1 \le t \le k$. Gọi h là tổng số quyền, b^i_{jt} là phần tử (j,t) của ma trận. Khi đó tồn tại số nguyên F^i_j được gọi là khóa của người sử dụng i trên file j sao cho*

$$b^i_{jt} = [F^i_j/(h+1)^{t-1}] mod(h+1). \tag{3}$$

Trong đó $1 \le i \le m,\ 1 \le j \le n,\ 1 \le t \le k$. Như vậy mỗi người sử dụng i muốn truy nhập vào file j thì phải đưa khóa F^i_j và hệ thống bảo vệ sẽ chấp nhận hay từ chối yêu cầu truy nhập trường t của họ.

Chứng minh. Ta đặt

$$F_j^i = \sum_{t=1}^{k} b_{jt}^i (h+1)^{t-1} \tag{4}$$

khi đó F_j^i được khai triển như sau

$$F_j^i = b_{ji}^i + b_{j2}^i(h+1) + ... + b_{jk}^i(h+1)^{k-1}.$$

Ta xét

$$[F_j^i/(h+1)^{i-1}] mod(h+1) =$$

$$b_{j1}^i(h+1)^{1-t} + ... + b_{jt-1}^i(h+1)^{-1} + b_{jt}^i + b_{jt+1}^i(h+1) + ... + b_{jk}^i(h+1)^{k-1}] mod(h+1).$$

Đặt

$$C = b_{j1}^i(h+1)^{1-t} + ... + b_{jt-1}^i(h+1)^{-1},$$

$$U = b_{jt+1}^i(h+1) + ... + b_{jk}^i(h+1)^{k-t}.$$

Do h là tổng số quyền truy nhập tới trường, ta có

$$h \geq b_{jt}^i \quad \text{với } 1 \leq i \leq m,\ 1 \leq j \leq n,\ 1 \leq t \leq k.$$

Vì vậy

$$C \leq h/(h+1)^{t-1} + h/(h+1)^{t-2} + ...h/(h+1),\ C \leq 1 - (\frac{1}{h+1})^{t-1}.$$

Suy ra

$$0 \leq C \leq 1 \quad 1 \leq t \leq k$$

Mặt khác

$$U = (h+1)(b_{jt+1}^i + b_{jt+2}^i(h+1) + ... + b_{jk}^i(h+1)^{k-t-1}$$

$$U = (h+1)M, \quad \text{với } M \text{ là một số nguyên nào đó.}$$

Từ đó chúng ta có

$$[F_j^i/(h+1)^{t-1}] mod(h+1) = [C + b_{jt}^i + U] mod(h+1)$$

$$= [C + b_{jt}^i + (h+1)M] mod(h+1) = b_{jt}^i (dpcm).$$

Nhận xét: -Nếu làm việc trên máy 32 bit thì khóa sẽ tràn nếu h=4 và k > 14. Thật vậy, do $b_{jt}^i \leq h$ với mọi j,t nên từ (4) ta có

$$F_j^i \leq (h+1)^k - 1$$

- F_j^i là khóa nhỏ nhất biểu diễn véc tơ dòng thứ j vì véc tơ dòng được xem như biểu trong cơ sở $h+1$.

4. Độ phức tạp thời gian tính toán khóa

Kí hiệu $T(X)$ là số phép nhân để tính X. Knuth [4] chứng minh rằng $T(a^b) \leq 2[log_2 b]$.

Do

$$F_j^i = \sum_{t=1}^{k} (h+1)^{t-1} \times b_{jt}^i$$

nên

$$T(F_j) = \sum_{i=1}^{k} b_{jt}^i T((h+1)^{t-1})$$

$$= \sum_{t=1}^{k} T(h+1)^{t-1}) + O(k)$$

$$\leq k.2[log_2(k-1)] + O(k)$$

$$\leq O(klog_2 k).$$

Để tăng độ bảo mật của khóa ta sử dụng phép biến đổi t trong lớp hàm một chiều T nêu trên để mã khóa, do đó ma trận truy nhập được bảo vệ.

Để truy nhập file j, ta cấp cho người sử dụng i khóa $L_j^i = t[F_j^i]$ trong đó F_j^i được chỉ ra ở (2).

Ví dụ hàm một chiều t trong [2] như sau:

Ta chọn p và q là hai số nguyên tố ngẫu nhiên lớn, $n = pq$, e là số nguyên thuộc khoảng $(1, n-1)$, $l_i = t[k_i] = (k_i)^e mod n$, phép biến đổi ngược được tính: $k_i = p(l_i) = (l_i)^d mod n$, trong đó $ed = 1\ mod\ phi(n)$, $phi(n)$ là hàm Ơ- le, $phi(n) = (p-1)(q-1)$.

Để bảo vệ dữ liệu, trước khi ghi vào cơ sở dữ liệu ta sử dụng các phép mã hóa có độ bảo mật cao. Gọi L là bản rõ, M là bản mã, K_m là khóa biến bản rõ thành bản mã: $M = K_m(R)$. Khi hệ thống bảo vệ cho phép đọc thì hệ thống sẽ giải mã nhờ khóa giải mã G_m biến bản mã thành bản rõ: $R = G_m(M)$. Các khóa K_m, G_m có thể dụng hàm một chiều nêu trên để mã và giải mã dữ liệu.

5. Khái niệm khóa nhóm

Để giải quyết giá trị khóa bị tràn ta dùng phương pháp khóa nhóm như sau:

Giả sử F_j^i có thể biểu diễn với giá trị cực đại $k = 14$. Để hệ thống điều khiển truy nhập các file có số trường $k > 14$ ta nhóm 14 trường thành nhóm con $j1$, giả sử k trường nhóm thành g nhóm trường. Gọi S_{j1} là số trường của nhóm trường $j1$, trường $(j1,t)$ kí hiệu trường thứ t của nhóm $j1$ với $1 \leq j1 \leq g$, $1 \leq t \leq S_{j1}$, $\sum_{j1=1}^{g} S_{j1} = k$.

Kí hiệu $b_j^i(j1,t)$ cho biết quyền của người sử dụng i đối với trường $(j1,t)$ của file j. Gọi K_{jj1}^i là giá trị khóa của người sử dụng i đối với nhóm trường thứ $j1$ của file j. Khi đó khóa K_{jj1}^i và quyền truy nhập $b_j^i(j1,t)$ được tính như sau

$$K_{jj1}^i = \sum_{q=1}^{S_{j1}} b_j^i(j1,t)(h+1)^{q-1}$$

$$b^i_j(j1,t) = [K^i_{jj1}/(h+1)^{t-1}] mod(h+1)$$

6. Kết luận

Bài báo đã đưa ra phương pháp cài đặt điều khiện truy nhập cho mô hình bảo vệ thông tin các file đồng thời chỉ ra áp dụng cho mô hình cơ sở dữ liệu quan hệ. ưa ra biện ph'ap bảo vệ khóa và dữ liệu bằng cách sử dụng hàm một chiều và mã hóa dữ liệu.

Tài liệu tham khảo

1. Jin Ke Jan *A single - key access control scheme in information protection systems,* Information Sciences **51** (1990), 1-13.
2. Denning D.E. & Peter J., *Data secutity,* Computing Surveys **v. 11** (1979, n° 3.
3. Wu M.L., *Access control with single - key - lock,* IEEE Trans. Software Ergng. SE - 10(2) (1984), 185-191.
4. Knuth D.E., The Art of computer Programming vol. 2, Add. Wesley, Reading, Mass 1981, 441-462.
5. Graham G.G. & Denning P.J. *Protection - principles and practice,* in Proc. Spring J1, Computer Conf. vol. 40, AFIPS Press, Montvale, N. J. (1972).
6. Harrison M.A; Ruzzo W.L. & Ullman J.D. *Protection in Operating Systems,* Comm. ACM **v.** 19(8) (1976), 461-471.

Abstract

On a Method of Access Control in Database

A new access control sheme for information protection system is proposed. It assigns every legal user just on interger key in such a way that employing a simple formula to the key of the user subject and the ID number of the resuorce object yields the corresponding access right in the protection system.

In the article also has given a concept of access control and grouped key. The described method is applied to relational database for implementing a single key that achieves access control in it.