Hệ thống bảo mật cơ sở dữ liệu linh hoạt sử dụng nhiều chính sách kiểm soát truy cập\*

Min-A Jeong1, Jung-Ja Kim1 và Yonggwan Won2

1 Viện Nghiên cứu Công nghệ Điện tử Viễn thông, Đại học Quốc gia Chonnam

300 Yongbong-dong Buk-gu Kwangju, Hàn Quốc

grace.chonnam.ac.kr 2019

2 Khoa Kỹ thuật Máy tính, Đại học Quốc gia Chonnam

300 Yongbong-dong Buk-gu Kbangju, Hàn Quốc [Ekoun@chnam.ac.kr](mailto:ykwon@chonnam.ac.kr)

**Trừu tượng.** Do các yêu cầu khác nhau đối với việc kiểm soát truy cập người dùng vào cơ sở dữ liệu lớn trong bệnh viện và ngân hàng, bảo mật cơ sở dữ liệu đã được nhấn mạnh. Có nhiều mô hình bảo mật cho các hệ thống cơ sở dữ liệu sử dụng nhiều phương pháp kiểm soát truy cập dựa trên chính sách. Tuy nhiên, chúng không đủ chức năng để đáp ứng các yêu cầu đối với các loại kiểm soát truy cập phức tạp và khác nhau. Trong bài báo này, chúng tôi đề xuất một hệ thống bảo mật cơ sở dữ liệu có thể kiểm soát riêng quyền truy cập của người dùng vào các nhóm dữ liệu có kích thước khác nhau và phù hợp với tình huống đặc quyền truy cập của người dùng đối với dữ liệu tùy ý được thay đổi thường xuyên. (Các) nhóm dữ liệu có kích thước khác nhau ***d*** được xác định bởi (các) tên bảng, (các) thuộc tính và/hoặc (các) khóa bản ghi và đặc quyền truy cập được xác định bởi các cấp độ bảo mật, vai trò và chính sách. Hệ thống đề xuất hoạt động theo hai giai đoạn. Giai đoạn đầu tiên bao gồm mô hình MAC (Kiểm soát truy cập bắt buộc) được sửa đổi và mô hình RBAC (Kiểm soát truy cập dựa trên vai trò). Người dùng có thể truy cập bất kỳ dữ liệu nào có mức độ bảo mật thấp hơn hoặc bằng nhau và có thể truy cập được bởi các vai trò mà người dùng được chỉ định. Tất cả các loại chế độ truy cập được kiểm soát trong giai đoạn này. Trong giai đoạn thứ hai, một mô hình DAC (Kiểm soát truy cập tùy ý) được sửa đổi được áp dụng để kiểm soát lại *chế độ 'đọc*' bằng cách lọc ra dữ liệu không thể truy cập từ kết quả thu được ở giai đoạn đầu tiên. Với mục đích này, chúng tôi cũng đã xác định các nhóm người dùng ***s*** có thể được đặc trưng bởi mức độ bảo mật, vai trò hoặc bất kỳ phân vùng nào của người dùng. Các chính sách được thể hiện dưới dạng (***các***) khối, ***d, r***) cũng được xác định và sử dụng để kiểm soát quyền truy cập vào bất kỳ dữ liệu hoặc (các) nhóm dữ liệu nào không được phép ở *chế độ 'đọc*'. Với hệ thống bảo mật được đề xuất này, quyền truy cập 'đọc' phức tạp hơn vào các kích thước dữ liệu khác nhau cho người dùng cá nhân có thể được kiểm soát linh hoạt, trong khi chế độ truy cập khác có thể được kiểm soát như bình thường. Một ví dụ triển khai cho một hệ thống cơ sở dữ liệu quản lý mẫu bệnh phẩm và thông tin lâm sàng được trình bày.

\* Nghiên cứu này được hỗ trợ bởi một khoản tài trợ của Dự án R & D Viễn thông Di động Quốc tế 2000, Bộ Thông tin & Truyền thông, Hàn Quốc.

V. Maet al. (Eds.): DEXA 2003, LNCS 2736, pp. 876–885, 2003.

© Springer-Verlag, Berlin, Heidelberg, 2003;

Một hệ thống bảo mật cơ sở dữ liệu linh hoạt sử dụng nhiều chính sách kiểm soát truy cập 877

**1 Giới thiệu**

Bảo mật cơ sở dữ liệu trở nên quan trọng hơn khi quy mô cơ sở dữ liệu cho các tổ chức công cộng và tư nhân đang phát triển và các chương trình truy cập người dùng khác nhau được yêu cầu. Gần đây, hầu hết các hệ thống quản lý cơ sở dữ liệu quan hệ (RDBMS) chỉ cung cấp một số kỹ thuật bảo mật hạn chế, thường sử dụng kiểm soát truy cập dựa trên chính sách [1].

Các chính sách kiểm soát truy cập phổ biến nhất hiện đang được sử dụng là Kiểm soát truy cập bắt buộc (MAC), Kiểm soát truy cập tùy ý (DAC), Kiểm soát truy cập dựa trên vai trò (RBAC). Chính sách MAC chỉ định mức độ bảo mật cho dữ liệu và người dùng, và do đó có thể kiểm soát luồng thông tin bất thường. Tuy nhiên, chính sách MAC thiếu tính linh hoạt để đáp ứng các điều kiện cho kiểm soát truy cập phức tạp [2]. Mặc dù chính sách DAC có thể kiểm soát truy cập linh hoạt hơn là chính sách MAC, nhưng nó không thể kiểm soát luồng thông tin bất hợp pháp đến người dùng trái phép [3]. Chính sách RBAC chỉ định người dùng cho các vai trò áp dụng và người dùng có thể truy cập dữ liệu theo quyền truy cập được gán cho từng vai trò. Do đó, chính sách RBAC có thể cung cấp các phương pháp quản lý bảo mật đơn giản và cũng ngăn chặn quyền truy cập bị lạm dụng bằng cách chỉ cho phép đặc quyền tối thiểu cho người dùng [4][5].

Đối với các đặc điểm của từng chính sách kiểm soát truy cập ở trên, một số mô hình bảo mật sử dụng một hoặc hai chính sách đã được đề xuất cho hệ thống cơ sở dữ liệu. Một số mô hình sử dụng chính sách MAC là mô hình Ma trận truy cập, mô hình Task-Grant, mô hình Action-Entity, Wood, v.v. [6]. Mô hình Jojodia-sandhu và mô hình Smith-Winslett áp dụng chính sách DAC [7][8][9]. Mô hình Sea View là một gợi ý để kết hợp cả hai chính sách[10]. Ngoài ra, có những nghiên cứu đề cập đến các kỹ thuật RBAC cung cấp quản lý an ninh đơn giản của Sandhu-Bhamidipati và Ferraiolo [11][12].

Các mô hình bảo mật đó mở rộng mô hình cơ sở dữ liệu quan hệ tiêu chuẩn và có một nhược điểm là việc sửa đổi hoặc thay thế không dễ dàng khi các yêu cầu bảo mật thường xuyên thay đổi. Đó là, chúng không phù hợp với các tình huống khi quyền truy cập của người dùng vào dữ liệu thay đổi bất cứ lúc nào và cũng gặp khó khăn trong việc thực hiện kiểm soát truy cập khác nhau cho mỗi người dùng vào cùng một dữ liệu. Ví dụ: nếu hai người dùng có cùng quyền truy cập trên cùng một thuộc tính nhưng có quyền truy cập khác nhau ngay trên các bộ khác nhau trong bảng cơ sở dữ liệu thông tin y tế, không dễ để kiểm soát quyền truy cập cá nhân bằng các mô hình bảo mật hiện có. Trong một số trường hợp, người dùng có quyền truy cập vào dữ liệu bệnh nhân cụ thể thường được yêu cầu cấp quyền truy cập cho một số người dùng không có. Do đó, một kiểm soát truy cập đặc biệt là cần thiết cho mỗi nhóm dữ liệu có kích thước khác nhau, được hình thành bởi sự kết hợp của các bộ và thuộc tính khác nhau.

Trong bài báo này, chúng tôi đề xuất một hệ thống kiểm soát truy cập dành riêng cho người dùng đối với các nhóm dữ liệu của

kích cỡ khác nhau. Hệ thống đề xuất hoạt động theo hai giai đoạn. Giai đoạn đầu tiên bao gồm một mô hình MAC sửa đổi và mô hình RBAC. Người dùng có thể truy cập bất kỳ dữ liệu nào có mức độ bảo mật thấp hơn hoặc bằng nhau và có thể truy cập được bởi các vai trò mà người dùng được chỉ định. Tất cả các loại chế độ truy cập được kiểm soát trong giai đoạn này. Trong giai đoạn thứ hai, một mô hình DAC đã sửa đổi được áp dụng để kiểm soát lại *chế độ 'đọc*' bằng cách lọc ra dữ liệu không thể truy cập từ kết quả thu được ở giai đoạn đầu tiên. Đối với các quy trình này, các nhóm người dùng và nhóm dữ liệu trước tiên được xác định và sau đó quy tắc truy cập được thiết lập trên cơ sở các nhóm người dùng và dữ liệu được xác định. Hệ thống không mở rộng mô hình quan hệ tiêu chuẩn nhưng cho phép xử lý kiểm soát truy cập phức tạp bằng cách cung cấp các quy tắc truy cập khác nhau cho từng người dùng hoặc nhóm người dùng.