NGHIÊN CỨU PHƯƠNG PHÁP ĐIỀU KHIỂN TRUY CẬP DỰA VAI TRÒ TRONG VIỆC ĐẢM BẢO AN TOÀN CHO CÁC ỨNG DỤNG DỰA THÀNH PHẦN

Học viên: Nguyễn Thị Thu Phương
Đơn vị công tác: Ngân hàng No&PTNT VN
Email: phuongntt.itca@gmail.com

GVHD: Nguyễn Việt Hà
Đơn vị công tác: Trường Đại học Công nghệ-ĐHQGHN
Email: hanv@vnu.edu.vn

Từ khóa: CBSE, RBAC, EJB

1. GIỚI THIỆU BÀI TOÁN

Trong công nghệ thành phần phần mềm, các hệ thống thông tin được phát triển bởi các thành phần. Việc tái sử dụng các thành phần mang lại nhiều lợi ích như giảm độ phức tạp, thời gian, và chi phí phát triển hệ thống. Tuy nhiên, việc sử dụng các thành phần trong việc phát triển các hệ thống thông tin cũng gặp nhiều khó khăn, đặc biệt là các vấn đề về an ninh.

Trong luận văn này, chúng tôi nghiên cứu tăng cường an ninh cho hệ thống dựa thành phần bằng cách sử dụng phương pháp điều khiển truy cập dựa vai trò (Role-Based Access Control - RBAC). RBAC là một công nghệ mở và rất phong phú, có phạm vi từ rất đơn giản đến phức tạp, tinh vi. RBAC là một phương pháp quan trọng cho việc quản lý định danh người dùng và đang được chấp nhận rộng rãi.

2. NỘI DUNG LUẬN VĂN

Có nhiều mô hình thành phần phần mềm, trong luận văn nghiên cứu mô hình Enterprise JavaBean (EJB). Kiến trúc EJB là kiến trúc thành phần dành cho việc phát triển và triển khai các ứng dụng phân tán hướng thành phần. Việc cài đặt EJB tập trung vào lô gic nghiệp vụ. Công nghệ EJB là một phần của J2EE, nó cung cấp một tập API và các dịch vụ khác. Ưu điểm của EJB là khả năng sử dụng lại cao, viết một lần chạy mọi nơi (Write Once Run Anywhere - WORA), có tính khả chuyển, linh hoạt. Thành phần EJB đã được biên dịch có thể triển khai trên bất kỳ máy chủ EJB nào (J2EE, JBoss, WebLogic Enterprise).

An ninh cho các ứng dụng EJB bao gồm ba phần: mã hóa, chứng thực và cấp phép. Luận văn tập trung nghiên cứu cơ chế cấp phép. Sự cấp phép của EJB dựa trên công nghệ RBAC. Có hai cách thiết lập RBAC bao gồm điều khiển truy cập chương trình và điều khiển truy cập khai báo. Với phương pháp điều khiển truy cập chương trình, việc kiểm tra quyền truy cập được nhúng bên trong mã của các thành phần EJB. Ưu điểm của phương pháp này là cung cấp cho người phát triển khả năng xác định các chính sách mịn. Trong phương pháp điều khiển truy cập khai báo, việc điều khiển truy cập được thiết đặt độc lập với mã chương trình. Gọi là phương pháp khai báo vì trong đó ta mô tả các vai trò an ninh và các quyền bằng cách sử dụng mô tả XML chuẩn hơn là nhúng cả phần an ninh vào trong các thành phần nghiệp vụ. Điều này tách riêng vấn đề an ninh khỏi các mã lệnh mức nghiệp vụ vì an ninh có xu hướng trở thành một chức năng độc lập hơn là một khía cạnh vốn có lô gic nghiệp vụ. Một tập tin (được đặt tên là ejb-jar.xml) được dùng để xác định các chính sách điều khiển truy cập khai báo. Ưu điểm của phương pháp này là đơn giản, linh hoạt. Điều khiển truy cập khai báo là linh động hơn khi so sánh với điều khiển truy cập chương trình. Trong bối cảnh công nghệ dựa thành phần, điều khiển truy cập khai báo được ưa thích hơn.

Từ các vấn đề lý thuyết được nghiên cứu, chúng tôi ứng dụng vào hệ thống quản trị - báo cáo thanh toán hóa đơn. Hiện tại, việc kiểm soát người dùng có quyền truy cập vào các thành phần EJB hay không được viết bằng mã lệnh đặt trong các file JSP và phương pháp này có nhiều hạn chế như phức tạp (người phát triển ứng dụng vừa phải viết các chức năng ngiệp vụ, vừa phải viết các chính sách điều khiển truy cập), không linh hoạt (nếu cần thay đổi chính sách truy cập, cần sửa đổi hầu hết các thành phần trong hệ thống như các file JSP, các thành phần EJB, v.v...), không có tính mở (nếu cần phát triển một ứng dụng phía client có thể dùng chung các thành phần EJB thì bắt buộc phải viết lại toàn bộ các chính sách điều khiển truy cập). Để khắc phục các nhược điểm này, luận văn đã nghiên cứu để áp dụng phương pháp điều khiển truy cập khai báo vào hệ thống.

3. KẾT LUẬN

Việc áp dụng phương pháp điều khiển truy cập khai báo cho hệ thống quản trị - báo cáo đã khắc phục được các hạn chế về mặt an ninh của hệ thống. Việc tách riêng vấn đề an ninh khỏi các chức nghiệp vụ tạo thuận lợi cho cả người phát triển và người quản trị hệ thống. Người phát triển chỉ cần tập trung viết các chức năng nghiệp vụ, còn người quản trị hệ thống dễ dàng hơn trong việc bảo trì các chính sách điều khiển truy cập. Hơn nữa, phương pháp này cũng tạo điều kiện cho việc phát triển mở rộng hệ thống.

Đối với phương pháp điều khiển truy cập khai báo, các phương thức bean trong một ứng dụng EJB thường tương tác với nhau để thực hiện một số chức năng. Nếu ta cho phép một vai trò thực hiện một phương thức thì chúng ta phải cho phép vai trò này thực hiện bất kỳ phương thức nào được gọi bởi phương thức đó. Dùng phương pháp điều khiển truy cập dựa phương thức để xác định các chính sách điều khiển truy cập chỉ tốt khi hệ thống ứng dụng có số lượng bean nhỏ và không có nhiều tương tác giữa các bean (do số các phần tử <*method-permission*> và số các phần tử <*method*> sẽ tăng nhanh theo số lượng các thành phần EJB và số lượng vai trò trong hệ thống). Do đó, trong các hệ thống quy mô lớn, phương pháp dựa phương thức dễ bị lỗi và rất khó cho việc bảo trì chính sách an ninh. Hướng nghiên cứu tiếp theo của đề tài là khắc phục hạn chế trên.