Tạp chí Tin học và Điều khiển học, T.21, S.3 (2005), 230–243

PHÂN CẤP VAI TRONG MÔ HÌNH KIỂM SOÁT TRUY NHẬP DỰA TRÊN VAI VỚI RÀNG BUỘC THỜI GIAN

LÊ THANH[1], NGUYỄN VĂN NGỌC[2], NGUYỄN THÚC HẢI[3]

[1] *Trường ĐH Sư phạm Thể dục Thể thao Hà Tây*
[2] *Cục B12, Tổng cục 5, Bộ Công An*
[3] *Khoa CNTT, Trường Đại học Bách khoa Hà Nội*

Abstract. The role-based access control models are interested by many researchers analysing and modeling theoretically as well as designing the security infrastructure for an organization' s resource management system. Generalized Temporal Role Based Access Control model (GTRBAC) that captures an comprehensive set of temporal constraints need for access control has recently been proposed. Its language structures allow one to specify various temporal constraints on role, user-role assignments and permission-role assignments. Here, we present the different types of role hierarchies for temporal constraint role-based access control model based on the permission-inheritance and role-activation semantics. Thereby we construct a set of inference rules among various role hierarchical relations and demonstrate its correctness.

Tóm tắt. Các mô hình kiểm soát truy nhập dựa trên vai đang là mối quan tâm của nhiều nhà nghiên cứu trong việc phân tích và lập mô hình về mặt lý thuyết cũng như trong việc thiết kế cơ sở hạ tầng an ninh, an toàn cho hệ thống quản lý tài nguyên của một tổ chức. Mô hình kiểm soát truy nhập dựa trên vai theo thời gian tổng quát (GTRBAC) với một tập toàn diện các ràng buộc thời gian cần cho kiểm soát truy nhập đã được đề xuất mới đây. Các cấu trúc ngôn ngữ của mô hình này cho phép người ta đặc tả các ràng buộc thời gian trên các vai, trong việc gán người dùng cho vai và gán giấy phép cho vai. Ở đây chúng tôi trình bày các phân cấp vai của mô hình kiểm soát truy nhập dựa trên vai với ràng buộc thời gian căn cứ theo ngữ nghĩa kế thừa giấy phép và ngữ nghĩa kích hoạt vai. Từ đó xây dựng và chứng minh tính đúng đắn của một tập luật suy diễn trong các quan hệ phân cấp vai.

1. MỞ ĐẦU

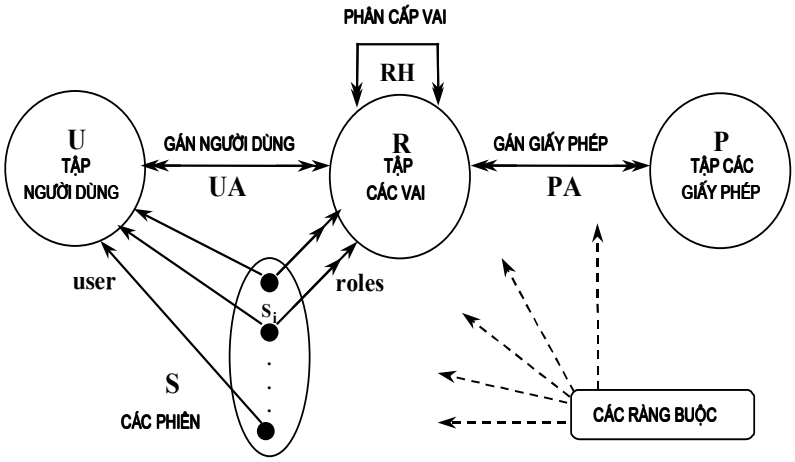
Kiểm soát truy nhập dựa trên vai (Role-Based Access Control - RBAC) đã nổi lên như một lựa chọn đầy hứa hẹn thay thế các mô hình kiểm soát truy nhập tùy ý và kiểm soát truy nhập bắt buộc truyền thống ([6, 7]) nhưng chúng có một số hạn chế về đặc tính kế thừa. Một số đặc tính có lợi như chính sách trung tính, trợ giúp đặc quyền ít nhất, quản lý kiểm soát truy nhập hiệu quả được kết hợp với các mô hình RBAC ([6]). Một trong những mặt quan trọng của kiểm soát truy nhập đó là kiểm soát các ràng buộc về thời gian truy nhập để hạn chế việc sử dụng tài nguyên. Đề cập về các yêu cầu kiểm soát truy nhập dựa trên thời gian, Bertino và cộng sự đề xuất một mô hình RBAC theo thời gian (Temporal RBAC - TRBAC), mà mới đây đã được Joshi và cộng sự tổng quát hoá [3]. Tầm quan trọng của các phân cấp

vai và việc sử dụng chúng trong các mô hình RBAC đã được chú ý đến trong một số công trình. Ở đây chúng tôi chú trọng các vấn đề có được giấy phép và kích hoạt vai khi nhiều kiểu phân cấp cùng tồn tại bên trong một phân cấp vai. Bài báo được tổ chức như sau. Mục 2 nêu vắn tắt các mô hình kiểm soát truy nhập dựa trên vai: RBAC, TRBAC, GTRBAC. Mục 3 trình bày các kiểu phân cấp vai của mô hình kiểm soát truy nhập dựa trên vai với ràng buộc thời gian. Mục 4 trình bày các luật suy diễn đối với các quan hệ phân cấp được suy diễn giữa các vai và chứng minh tính đúng đắn của tập luận này. Mục 5 trình bày một số kết luận.

2. CÁC MÔ HÌNH KIỂM SOÁT TRUY NHẬP DỰA TRÊN VAI

2.1. Mô hình kiểm soát truy nhập dựa trên vai (RBAC)

Kiểm soát truy nhập dựa trên vai RBAC có thể được cấu hình để thực thi kiểm soát truy nhập tùy ý hoặc để thực thi kiểm soát truy nhập bắt buộc [7]. Một họ chung các mô hình RBAC (gọi là RBAC96) được Ravi Sandhu và cộng sự định nghĩa [6]. Trong [5] chúng tôi đã khái quát về mô hình RBAC. Hình 2.1 minh họa mô hình tổng quát nhất trong họ này. Một người dùng (user) là một con người hoặc một tác tử tự trị (autonomous agent), một *vai* là một chức năng công việc hoặc một tiêu đề công việc bên trong một tổ chức với một số ngữ nghĩa được kết hợp đối với việc cấp quyền và trách nhiệm được gán cho một thành viên của vai. Một giấy phép là một sự phê chuẩn của một hình thức truy nhập cụ thể tới một hoặc nhiều đối tượng trong hệ thống hoặc một số đặc quyền để thực hiện các hoạt động đặc biệt. Các vai được tổ chức theo thứ tự bộ phận $\geqslant$ sao cho nếu $x \geqslant y$ thì vai x kế thừa các giấy phép của vai y. Các thành viên của x rõ ràng là các thành viên của y, nhưng ngược lại không đúng. Trong các trường hợp như thế, chúng ta nói x là cấp trên của y đối với quan hệ $\geqslant$. Mỗi phiên liên hệ một người dùng với một số vai mà họ được gán vào. Một người dùng thiết lập một phiên và kích hoạt một số tập con các vai mà người dùng này là thành viên của chúng (trực tiếp hay gián tiếp thông qua phân cấp vai). Mô hình RBAC96 có các thành phần sau:



Hình 2.1. Mô hình RBAC96

Định nghĩa 2.1. Mô hình RBAC [5] gồm có các thành phần sau:

- Các tập U, R, P và S tương ứng biểu diễn tập hợp người dùng, tập hợp các vai, tập hợp các giấy phép và tập hợp các phiên;
- $UA \subseteq U \times R$, quan hệ gán người dùng cho vai (User-role Assignment).
- $PA \subseteq P \times R$, quan hệ gán giấy phép cho vai (Permission-role Assignment).
- $RH \subseteq R \times R$, quan hệ phân cấp vai thứ tự bộ phận (Role Hierarchy).
  (vai x là cấp trên của vai y thì được viết là $x \geqslant y$)
- Hàm $user : S \to U$, ánh xạ mỗi phiên s_i tới một người dùng u_i (không thay đổi trong suốt phiên làm việc): $u_i = user(s_i)$.
- Hàm $roles : S \to 2^R$, ánh xạ mỗi phiên s_i tới một tập vai:
  $roles(s_i) \subseteq \{r | (\exists r' \geqslant r)(user(s_i), r') \in UA\}$ (có thể thay đổi cùng với thời gian).
- Phiên s_i có tập các giấy phép là $\bigcup_{r \in roles(s_i)} \{p | (\exists r'', r \geqslant r'') \in [(p, r'') \in PA]\}$.
- Có một tập hợp các ràng buộc tác động lên giá trị của các thành phần khác nhau được liệt kê ở trên (cụ thể là các quan hệ PA, UA, RH và các hàm $user$, hàm $roles$ cũng như các phiên làm việc S) và cho kết quả là được phép hay bị cấm.

Một người dùng khi đăng nhập vào hệ thống sẽ thiết lập một phiên và trong suốt phiên đó có thể yêu cầu kích hoạt một số tập con vai mà người dùng này được cấp quyền thực hiện. Một yêu cầu kích hoạt chỉ được phép nếu vai tương ứng có khả năng vào thời gian yêu cầu và người dùng được quyền kích hoạt vai đó vào thời gian này. Nếu yêu cầu kích hoạt được thoả mãn, người dùng sẽ có được tất cả các giấy phép được kết hợp với vai mà anh ta đã kích hoạt. Một số hàm được xác định trên các tập hợp U, R, P và S. Các quan hệ UA (user-role assignment) và PA (permission-role assignment) tương ứng là các phép gán người dùng cho vai và gán giấy phép cho vai. Một người dùng có thể là thành viên của một số vai và một vai có thể có một số thành viên. Hơn nữa, một vai có thể có một số giấy phép và cùng một giấy phép có thể được kết hợp với một số vai. Hàm $user$ ánh xạ mỗi một phiên tới một người dùng đơn, trong khi hàm $roles$ thiết lập một sự gắn kết giữa một phiên và một tập vai (nghĩa là các vai được người dùng tương ứng kích hoạt trong phiên này). Một sự phân cấp được xác định trên tập R, được kí hiệu là $\geqslant$. Nếu $r_1 \geqslant r_2$ với $r_1, r_2 \in R$ thì r_1 kế thừa các giấy phép của r_2. Trong trường hợp như thế, r_1 là vai cấp trên và r_2 là vai cấp dưới.

2.2. Mô hình kiểm soát truy nhập dựa trên vai theo thời gian (TRBAC)

Bertino và cộng sự [1] đã đề xuất mô hình RBAC theo thời gian (Temporal Role Based Access Control: TRBAC) đề cập đến một số vấn đề thời gian liên quan đến RBAC. TRBAC là một mở rộng của mô hình RBAC. Các đặc tính chủ yếu mà nó cung cấp bao gồm việc tạo khả năng, làm mất khả năng của các vai theo chu kỳ và các phụ thuộc thời gian giữa chúng được biểu diễn bằng các luật kích hoạt vai (trigger) được thực hiện tự động dựa trên việc tạo khả năng và/hoặc làm mất khả năng của các vai. Tính ưu tiên được kết hợp với cả

các trigger và việc tạo khả năng/làm mất khả năng của các vai theo chu kỳ để quản lý các đụng độ có khả năng xảy ra khi việc tạo khả năng/làm mất khả năng đồng thời của một vai được yêu cầu. Trong các trường hợp như vậy, sự kết hợp tính ưu tiên và luật *sự từ chối được sử dụng trước (denials-take-precedence)* được dùng để giải quyết các đụng độ. Hơn nữa TRBAC cho phép một nhà quản trị phát hành các yêu cầu run-time để tạo khả năng và làm mất khả năng một vai và kiểm soát hạn chế một người dùng kích hoạt vai. Tuy nhiên mô hình TRBAC không có khả năng kiểm soát một số ràng buộc thời gian hữu ích, cụ thể là:

1. TRBAC không bao gồm các ràng buộc thời gian trên các phép gán người dùng cho vai và trên các phép gán giấy phép cho vai. Do vậy mô hình này thừa nhận rằng các vai chỉ là tạm thời, tức là chúng có khả năng/không có khả năng trong các khoảng thời gian khác nhau.

2. TRBAC chỉ quản lý các ràng buộc thời gian trong việc tạo khả năng cho vai và không bao gồm bất kỳ một ràng buộc nào trong việc kích hoạt hiện thời các vai do người dùng thực hiện. Do vậy, TRBAC không sử dụng các khái niệm tách biệt việc tạo khả năng cho vai và việc kích hoạt vai. Do điều này, TRBAC không thể quản lý một số ràng buộc liên quan tới việc kích hoạt một vai như là các ràng buộc về thời gian kích hoạt tối đa được phép đối với một người dùng, số tối đa các kích hoạt một vai mà cùng một người dùng thực hiện trong một khoảng thời gian cụ thể.v.v... Mặc dù TRBAC có khả năng nhất định trong việc hạn chế người dùng kích hoạt một vai, nhưng nó chỉ được quản lý như là một yêu cầu run-time mà một nhà quản trị tạo ra.

3. Vì TRBAC không xét các ràng buộc độ dài thời gian và các ràng buộc trong việc kích hoạt hiện thời các vai, nên nó không bao gồm khái niệm về việc tạo khả năng/làm mất khả năng của các ràng buộc.

2.3. Mô hình kiểm soát truy nhập dựa trên vai theo thời gian tổng quát

Mô hình TRBAC tổng quát (Generalized Temporal Role Based Access Control-GTRBAC) [3] là một mở rộng của mô hình TRBAC [1] . Nó tích hợp một tập các cấu trúc ngôn ngữ để đặc tả các ràng buộc thời gian khác nhau trên các vai, bao gồm các ràng buộc thời gian trong việc kích hoạt vai cũng như về thời gian có khả năng của các vai , trong việc gán người dùng cho vai và trong việc gán giấy phép cho vai. Mô hình này đưa ra các khái niệm tách biệt về trạng thái có khả năng và trạng thái bị kích hoạt của vai và cung cấp các ràng buộc và biểu thức sự kiện được kết hợp với hai trạng thái này. Một vai có khả năng chỉ ra rằng một người dùng có thể kích hoạt nó, trái lại một vai bị kích hoạt chỉ ra rằng ít nhất một chủ thể đã kích hoạt vai này trong một phiên. Các ràng buộc thời gian trong GTRBAC cho phép đặc tả các ràng buộc và các sự kiện như sau:

1. *Các ràng buộc thời gian trong việc tạo khả năng/làm mất khả năng của vai*: Các ràng buộc này cho phép người ta đặc tả các khoảng thời gian hoặc độ dài thời gian mà trong đó một vai là có khả năng, việc gán người dùng cho vai hoặc việc gán giấy phép cho vai là hợp lệ.

2. *Các ràng buộc thời gian trong việc gán người dùng cho vai và gán giấy phép cho vai*: Các cấu trúc này được dùng để biểu diễn hoặc một khoảng thời gian cụ thể hoặc một độ dài

thời gian mà trong đó một người dùng hoặc một giấy phép được gán cho vai.

3. *Các ràng buộc kích hoạt*: Các ràng buộc này được dùng để đặc tả các hạn chế đối với một người dùng khi họ kích hoạt một vai. Các ràng buộc này có thể đặc tả độ dài thời gian mà trong đó một người dùng được phép kích hoạt một vai hoặc có thể hạn chế số người dùng được phép đồng thời kích hoạt một vai cụ thể.

4. *Các sự kiện run-time*: Một tập các sự kiện run-time cho phép một nhà quản trị khởi tạo động các sự kiện GTRBAC hoặc các ràng buộc độ dài thời gian có khả năng của vai hoặc các ràng buộc kích hoạt vai. Một tập các sự kiện run-time khác cho phép người dùng tạo ra các yêu cầu kích hoạt tới hệ thống.

5. *Các biểu thức tạo khả năng cho ràng buộc*: GTRBAC bao gồm các sự kiện tạo khả năng hoặc làm mất khả năng các ràng buộc độ dài thời gian và các ràng buộc kích hoạt vai. Các ràng buộc thời gian có thể áp đặt trong việc tạo khả năng cho vai, trong việc gán người dùng cho vai hoặc trong việc gán giấy phép cho vai.

6. *Trigger*: Các trigger cho phép người ta biểu diễn sự phụ thuộc trong các sự kiện GTRBAC cũng như lấy lại được các sự kiện quá khứ và xác định các sự kiện tương lai dựa trên các sự kiện hiện tại.

3. PHÂN CẤP VAI VỚI RÀNG BUỘC THỜI GIAN

3.1. Các vị từ trạng thái

Trong [2], Joshi và cộng sự đã định nghĩa ba loại phân cấp: phân cấp kế thừa giấy phép, phân cấp kế thừa kích hoạt và phân cấp kế thừa tổng quát. Sau đây là một số vị từ trạng thái được dùng trong các định nghĩa hình thức được nói trong Mục 3.2 và 3.3. Trong đó U, R, P, S tương ứng biểu diễn tập hợp người dùng, tập hợp các vai, tập hợp các giấy phép và tập hợp các phiên như ở mô hình RBAC96, T là tập các thời điểm $(0, \infty); u \in U, r \in R, p \in P, s \in S, t \in T$.

$enabled(r, t)$: r có khả năng tại thời điểm t.

$u\_assigned(u, r, t)$: u được gán vào r tại thời điểm t.

$p\_assigned(p, r, t)$: p được gán vào r tại thời điểm t.

$can\_activate(u, r, t)$: u có thể kích hoạt r tại thời điểm t.

$can\_acquire(u, p, t)$: u có thể có được p tại thời điểm t.

$r\_can\_acquire(u, p, r, t)$: u có thể có được p thông qua r tại thời điểm t.

$can\_be\_acquired(p, r, t)$: p có thể có được thông qua r tại thời điểm t.

$active(u, r, t)$: r ở trạng thái kích hoạt trong phiên của u tại thời điểm t.

$s\_active(u, r, s, t)$: r ở trạng thái kích hoạt trong phiên s của u tại thời điểm t.

$acquires(u, p, t)$: u có được p tại thời điểm t.

$r\_acquires(u, p, r, t)$: u có được p thông qua r tại thời điểm t.

$s\_acquires(u, p, s, t)$: u có được p trong phiên s tại thời điểm t.

$rs\_acquires(u, p, r, s, t)$: u có được p thông qua r trong phiên s tại thời điểm t.

Hệ tiên đề sau đây thể hiện các quan hệ chủ yếu giữa các vị từ nêu trên, làm cơ sở để nhận biết chính xác sự có được giấy phép và sự kích hoạt vai có khả năng hoặc đang xảy ra trong một hệ thống RBAC.

Hệ tiên đề. $\forall r \in R, \forall u \in U, \forall p \in P, \forall s \in S$ *và* $\forall t \in T$, *các phép kéo theo sau là đúng:*

1. $p\_assigned(p, r, t) \rightarrow can\_be\_acquired(p, r, t)$.
2. $u\_assigned(u, r, t) \rightarrow can\_activate(u, r, t)$.
3. $can\_activate(u, r, t) \wedge can\_be\_acquired(p, r, t) \rightarrow can\_acquire(u, p, t)$.
4. $s\_active(u, r, s, t) \wedge can\_be\_acquired(p, r, t) \rightarrow s\_acquires(u, p, s, t)$.

Về mặt ngữ nghĩa, việc dùng một phân cấp vai là mở rộng khả năng lấy được giấy phép và kích hoạt vai dựa trên việc gán rõ vai như ta sẽ thấy trong các mục sau. Các định nghĩa trong Mục 3.2 dưới đây đưa ra ngữ nghĩa hình thức của các kiểu phân cấp vai phụ thuộc thời gian, trong đó không xem xét thời gian có khả năng của các vai có quan hệ phân cấp và vì thế được gọi là sự phân cấp không hạn chế. Các dạng phân cấp hạn chế sẽ được đưa ra ở Mục 3.3.

3.2. Sự phân cấp vai theo thời gian không hạn chế

Trong các định nghĩa từ mục này trở đi, với $x, y \in R, \tau \subseteq T, \langle f \rangle$ là một quan hệ phân cấp vai, nếu xảy ra $x\langle f \rangle y$ trong khoảng thời gian τ thì x được gọi là vai cấp trên của y và ngược lại y được gọi là vai cấp dưới của x đối với quan hệ phân cấp $\langle f \rangle$ trong khoảng thời gian τ. Chúng tôi phát biểu lại các định nghĩa do Joshi nêu trong [2] về sự phân cấp vai theo thời gian không hạn chế, được xác định trong khoảng thời gian $\tau \subseteq T$.

Định nghĩa 3.2.1. Cho $x, y \in R, \tau \subseteq T$, ta nói x có quan hệ phân cấp kế thừa giấy phép không hạn chế trên y trong khoảng thời gian τ và viết $(x \geqslant_\tau y)$ nếu thoả mãn điều kiện sau: $\forall p \in P, \forall t \in \tau, can\_be\_acquired(p, y, t) \rightarrow can\_be\_acquired(p, x, t)$.

Định nghĩa 3.2.2. Cho $x, y \in R, \tau \subseteq T$, ta nói x có quan hệ phân cấp kế thừa kích hoạt không hạn chế trên y trong khoảng thời gian τ và viết $(x > y)$ nếu thoả mãn điều kiện sau: $\forall u \in U, \forall t \in \tau, can\_activate(u, x, t) \rightarrow can\_activate(u, y, t)$.

Định nghĩa 3.2.3. Cho $x, y \in R, \tau \subseteq T$. Ta nói x có quan hệ phân cấp kế thừa tổng quát không hạn chế trên y trong khoảng thời gian τ và viết $(x \geqslant_\tau y)$, nếu đồng thời xảy ra $(x \geqslant_\tau y)$ và $(x >_\tau y)$.

Trên một tập hợp vai đã cho, có thể có các quan hệ kế thừa khác nhau. Do đó chúng ta đòi hỏi rằng một quan hệ cấp trên-cấp dưới giữa hai vai trong một kiểu phân cấp thì không bị đảo ngược trong các kiểu phân cấp khác. Cụ thể trong một tập vai R, nếu tồn tại đồng thời phân cấp kế thừa giấy phép và phân cấp kế thừa kích hoạt không hạn chế thì ta đòi hỏi phải thoả mãn các điều kiện:

$$\forall x, y \in R : (x \geqslant_\tau y) \wedge \neg(y >_\tau x) \text{ và } (x >_\tau y) \wedge \neg(y \geqslant_\tau x) \text{ đều đúng} \qquad (c1)$$

Dưới đây chúng tôi sẽ làm rõ tính nhất quán giữa các kiểu phân cấp vai đã được Joshi nêu trong [2] và sau đó chứng minh tính bắc cầu của các quan hệ phân cấp không hạn chế.

Tính chất 3.2.1. *Trên tập vai R có các kiểu phân cấp* $\{\geqslant_\tau, >_\tau, \geqslant_\tau\}$ *thoả mãn điều kiện (c1). Xét* $\langle f \rangle, \langle f' \rangle \in \{\geqslant_\tau, >_\tau, \geqslant_\tau\}$ *mà* $\langle f \rangle \neq \langle f' \rangle$. *Cho* $x, y \in R$ *sao cho* $x\langle f \rangle y$, *thế thì điều kiện* $\neg(y\langle f' \rangle x)$ *là đúng.*

Chứng minh. Xét cặp bất kỳ $\langle f \rangle, \langle f' \rangle \in \{\geqslant_\tau, >_\tau, \geqslant_\tau\}$ và $\langle f \rangle \neq \langle f' \rangle$. Cho $x, y \in R$ sao cho $x\langle f \rangle y$. Giả sử ngược lại ta có: $y\langle f' \rangle x$. Ta xét các trường hợp sau:

* Nếu $\langle f \rangle$ là quan hệ $\geqslant_\tau$ thì xảy ra 2 khả năng:

- Hoặc $\langle f' \rangle$ là quan hệ $\geqslant_\tau$ thì ta có: $x \geqslant_\tau y$ và $y \geqslant_\tau x$, nên $x \geqslant_\tau y$ và $y \geqslant_\tau x$ đều đúng (mâu thuẫn).

- Hoặc $\langle f' \rangle$ là quan hệ $>_\tau$ thì ta có: $x \geqslant_\tau y$ và $y >_\tau x$, nên $x >_\tau y$ và $y >_\tau x$ đều đúng (mâu thuẫn).

* Nếu $\langle f \rangle$ là quan hệ $>_\tau$ thì xảy ra 2 khả năng:

- Hoặc $\langle f' \rangle$ là quan hệ $\geqslant_\tau$ thì ta có : $x >_\tau y$ và $y \geqslant_\tau x$, nên $x >_\tau y$ và $y >_\tau x$ đều đúng (mâu thuẫn).

- Hoặc $\langle f' \rangle$ là quan hệ $\geqslant_\tau$ thì ta có : $x >_\tau y$ và $y \geqslant_\tau x$ đều đúng (trái với điều kiện c1).

* Nếu $\langle f \rangle$ là quan hệ $\geqslant_\tau$ thì xảy ra 2 khả năng:

- Hoặc $\langle f' \rangle$ là quan hệ $\geqslant_\tau$ thì ta có : $x \geqslant_\tau y$ và $y \geqslant_\tau x$, nên $x \geqslant_\tau y$ và $y \geqslant_\tau x$ đều đúng (mâu thuẫn).

- Hoặc $\langle f' \rangle$ là quan hệ $>_\tau$ thì ta có : $x \geqslant_\tau y$ và $y >_\tau x$ đều đúng (trái với điều kiện c1). ■

Định lý 3.2.1. *Các quan hệ phân cấp không hạn chế kế thừa giấy phép và kế thừa kích hoạt đều có tính bắc cầu.*

Chứng minh

(i) Xét quan hệ phân cấp kế thừa giấy phép không hạn chế trên tập vai R. Giả sử với $x, y, z \in R$ và trong khoảng $\tau \subseteq T$ xảy ra $x \geqslant_\tau y,\ y \geqslant_\tau z$. Theo định nghĩa quan hệ $\geqslant_\tau$, ta có:

$$\forall p \in P, \forall t \in \tau, can\_be\_acquired(p, y, t) \rightarrow can\_be\_acquired(p, x, t)$$

$$\forall p \in P, \forall t \in \tau, can\_be\_acquired(p, z, t) \rightarrow can\_be\_acquired(p, y, t)$$

Suy ra: $\forall p \in P, \forall t \in \tau, can\_be\_acquired(p, z, t) \rightarrow can\_be\_acquired(p, x, t)$ Thế thì $x \geqslant_\tau z$. Vậy quan hệ phân cấp kế thừa giấy phép không hạn chế có tính bắc cầu.

(ii) Xét quan hệ phân cấp kế thừa kích hoạt không hạn chế trên tập vai R. Giả sử với $x, y, z \in R$ và trong khoảng $\tau \subseteq T$ xảy ra $x >_\tau y,\ y >_\tau z$. Theo định nghĩa quan hệ $>_\tau$, ta có:

$$\forall u \in U, \forall t \in \tau, can\_activate(u, x, t) \rightarrow can\_activate(u, y, t)$$

$$\forall u \in U, \forall t \in \tau, can\_activate(u, y, t) \rightarrow can\_activate(u, z, t)$$

Suy ra: $\forall u \in U, \forall t \in \tau, can\_activate(u, x, t) \rightarrow can\_activate(u, z, t)$ thế thì $x >_\tau z$. Vậy quan hệ phân cấp kế thừa kích hoạt không hạn chế có tính bắc cầu. ■

Hệ quả 3.2.1. *Quan hệ phân cấp kế thừa tổng quát không hạn chế có tính bắc cầu.*

Chứng minh. Vì quan hệ phân cấp kế thừa tổng quát không hạn chế bao gồm cả hai mặt: kế thừa giấy phép không hạn chế và kế thừa kích hoạt không hạn chế, nên hệ quả được suy ra từ chứng minh Định lý 3.2.1 và định nghĩa quan hệ phân cấp kế thừa tổng quát không hạn chế. ■

3.3. Sự phân cấp vai theo thời gian hạn chế

Sự phân cấp không hạn chế bỏ qua mối quan hệ giữa các thời gian có khả năng của các vai quan hệ phân cấp. Trong mục này, khi xét thời gian có khả năng của các vai, chúng tôi

phát biểu lại các định nghĩa về sự phân cấp vai theo thời gian hạn chế do Joshi nêu trong [2], được xác định trong khoảng thời gian $\tau \subseteq T$.

Định nghĩa 3.3.1. Cho $x, y \in R, \tau \subseteq T$. Ta nói x có quan hệ kế thừa giấy phép hạn chế yếu trên y trong khoảng thời gian τ và viết $(x \geqslant_{w,\tau} y)$, nếu x có khả năng trong τ và thoả mãn điều kiện sau: $\forall p \in P, \forall t \in \tau, can\_be\_acquired(p, y, t) \rightarrow can\_be\_acquired(p, x, t)$.

Định nghĩa 3.3.2. Cho $x, y \in R, \tau \subseteq T$. Ta nói x có quan hệ kế thừa giấy phép hạn chế mạnh trên y trong khoảng thời gian τ và viết $(x \geqslant_{s,\tau} y)$, nếu cả x và y đều có khả năng trong τ và thoả mãn điều kiện sau: $\forall p \in P, \forall t \in \tau, can\_be\_acquired(p, y, t) \rightarrow can\_be\_acquired(p, x, t)$.

Định nghĩa 3.3.3. Cho $x, y \in R, \tau \subseteq T$. Ta nói x có quan hệ kế thừa kích hoạt hạn chế yếu trên y trong khoảng thời gian τ và viết $(x >_{w,\tau} y)$, nếu y có khả năng trong τ và thoả mãn điều kiện sau: $\forall u \in U, \forall t \in \tau, can\_activate(u, x, t) \rightarrow can\_activate(u, y, t)$.

Định nghĩa 3.3.4. Cho $x, y \in R, \tau \subseteq T$. Ta nói x có quan hệ kế thừa kích hoạt hạn chế mạnh trên y trong khoảng thời gian τ và viết $(x >_{s,\tau} y)$, nếu cả x và y đều có khả năng trong τ và thoả mãn điều kiện sau: $\forall u \in U, \forall t \in \tau, can\_activate(u, x, t) \rightarrow can\_activate(u, y, t)$.

Định nghĩa 3.3.5. Cho $x, y \in R, \tau \subseteq T$. Ta nói x có quan hệ kế thừa tổng quát hạn chế yếu trên y trong khoảng thời gian τ, và viết $(x \geqslant_{w,\tau} y)$ nếu đồng thời xảy ra $(x \geqslant_{w,\tau} y)$ và $(x >_{w,\tau} y)$.

Định nghĩa 3.3.6. Cho $x, y \in R, \tau \subseteq T$. Ta nói x có quan hệ kế thừa tổng quát hạn chế mạnh trên y trong khoảng thời gian τ, và viết $(x \geqslant_{s,\tau} y)$, nếu đồng thời xảy ra $(x \geqslant_{s,\tau} y)$ và $(x >_{s,\tau} y)$.

Một ví dụ để minh họa là: trong khoảng τ_1 vai cấp dưới có khả năng nhưng vai cấp trên không có khả năng hoặc trong khoảng τ_2 vai cấp trên có khả năng nhưng vai cấp dưới lại không có khả năng. Trong phân cấp hạn chế mạnh, sự kế thừa không được phép trong các khoảng thời gian này, nhưng trong phân cấp hạn chế yếu, sự kế thừa có thể được phép.

Xuất phát từ các định nghĩa trên chúng tôi chứng minh tính bắc cầu của các quan hệ phân cấp kế thừa giấy phép, kế thừa kích hoạt và kế thừa tổng quát ở các dạng hạn chế yếu và hạn chế mạnh thông qua Định lý 3.3.1 và Hệ quả 3.3.1.

Định lý 3.3.1. *Các quan hệ phân cấp kế thừa giấy phép và kế thừa kích hoạt ở các dạng hạn chế yếu và hạn chế mạnh đều có tính bắc cầu.*

Chứng minh:
(i) Xét quan hệ phân cấp kế thừa giấy phép hạn chế yếu trên tập vai R. Giả sử với $x, y, z \in R$ và trong khoảng $\tau \subseteq T$ xảy ra: $x \geqslant_{w,\tau} y,\ y \geqslant_{w,\tau} z$. Theo định nghĩa của quan hệ $\geqslant_{w,\tau}$, thì x và y có khả năng trong τ và xảy ra:

$$\forall p \in P, \forall t \in \tau, can\_be\_acquired(p, y, t) \rightarrow can\_be\_acquired(p, x, t)$$

$$\forall p \in P, \forall t \in \tau, can\_be\_acquired(p, z, t) \rightarrow can\_be\_acquired(p, y, t)$$

Do đó x có khả năng trong τ và xảy ra: $\forall p \in P, \forall t \in \tau, can\_be\_acquired(p, z, t) \rightarrow can\_be\_acquired(p, x, t)$. Suy ra: $x \geqslant_{w,\tau} z$. Vậy phân cấp kế thừa giấy phép hạn chế yếu có tính bắc cầu.

(ii) Xét quan hệ phân cấp kế thừa giấy phép hạn chế mạnh trên tập vai R. Giả sử với $x, y, z \in R$ và trong khoảng $\tau \in T$ xảy ra: $x \geqslant_{s,\tau} y,\ y \geqslant_{s,\tau} z$. Theo định nghĩa của quan hệ $\geqslant_{s,\tau}$, thì cả ba vai x, y, z đều có khả năng trong τ và xảy ra:

$$\forall p \in P, \forall t \in \tau, can\_be\_acquired(p, y, t) \rightarrow can\_be\_acquired(p, x, t)$$

$$\forall p \in P, \forall t \in \tau, can\_be\_acquired(p, z, t) \rightarrow can\_be\_acquired(p, y, t)$$

Do đó x, z có khả năng trong τ và xảy ra: $\forall p \in P, \forall t \in \tau, can\_be\_acquired(p, z, t) \rightarrow can\_be\_acquired(p, x, t)$. Suy ra: $x \geqslant_{s,\tau} z$. Vậy phân cấp kế thừa giấy phép hạn chế mạnh có tính bắc cầu.

(iii) Xét quan hệ phân cấp kế thừa kích hoạt hạn chế yếu trên tập vai R. Giả sử với $x, y, z \in R$ và trong khoảng $\tau \in T$ xảy ra: $x >_{w,\tau} y, y >_{w,\tau} z$. Theo định nghĩa của quan hệ $>_{w,\tau}$, thì y, z có khả năng trong τ và xảy ra:

$$\forall u \in U, \forall t \in \tau, can\_activate(u, x, t) \rightarrow can\_activate(u, y, t)$$

$$\forall u \in U, \forall t \in \tau, can\_activate(u, y, t) \rightarrow can\_activate(u, z, t)$$

Thế thì z có khả năng trong τ và xảy ra: $\forall u \in U, \forall t \in \tau, can\_activate(u, x, t) \rightarrow can\_activate(u, z, t)$. Suy ra: $x >_{\cdot w,\tau} z$. Vậy phân cấp kế thừa kích hoạt hạn chế yếu có tính bắc cầu.

(iv) Xét quan hệ phân cấp kế thừa kích hoạt hạn chế mạnh trên tập vai R. Giả sử với $x, y, z \in R$ và trong khoảng $\tau \subseteq T$ xảy ra: $x >_{s,\tau} y, y >_{s,\tau} z$. Theo định nghĩa của quan hệ $>_{s,\tau}$, thì cả ba vai x, y, z đều có khả năng trong τ và xảy ra:

$$\forall u \in U, \forall t \in \tau, can\_activate(u, x, t) \rightarrow can\_activate(u, y, t)$$

$$\forall u \in U, \forall t \in \tau, can\_activate(u, y, t) \rightarrow can\_activate(u, z, t)$$

Thế thì x, z đều có khả năng trong τ và xảy ra: $\forall u \in U, \forall t \in \tau, can\_activate(u, x, t) \rightarrow can\_activate(u, z, t)$. Suy ra: $x >_{s,\tau} z$. Vậy phân cấp kế thừa kích hoạt hạn chế mạnh có tính bắc cầu.

Hệ quả 3.3.1. *Các quan hệ phân cấp kế thừa tổng quát ở các dạng hạn chế yếu và hạn chế mạnh đều có tính bắc cầu.*

Chứng minh. Ta thấy quan hệ phân cấp kế thừa tổng quát hạn chế yếu bao gồm cả hai mặt: kế thừa giấy phép hạn chế yếu và kế thừa kích hoạt hạn chế yếu; Quan hệ phân cấp kế thừa tổng quát hạn chế mạnh bao gồm cả hai mặt: kế thừa giấy phép hạn chế mạnh và kế thừa kích hoạt hạn chế mạnh, nên hệ quả được suy ra từ sự chứng minh Định lý 3.3.1 và định nghĩa của các quan hệ phân cấp này.

4. CÁC LUẬT SUY DIỄN TRONG PHÂN CẤP VAI VỚI RÀNG BUỘC THỜI GIAN

Một phân cấp vai được thiết kế hoàn hảo sẽ cho phép đặc tả và quản lý hiệu quả các cấu trúc kiểm soát truy nhập của một hệ thống. Khi hai vai liên hệ với nhau về mặt phân cấp thì một vai được gọi là vai cấp trên và vai kia được gọi là vai cấp dưới. Vai cấp trên kế thừa

tất cả các giấy phép được gán cho các vai cấp dưới. Việc một vai cấp trên kế thừa các giấy phép được gán cho các vai cấp dưới làm giảm đáng kể chi phí cho các phép gán, vì các giấy phép chỉ cần được gán rõ cho các vai cấp dưới. Chúng ta xem xét các vấn đề có được giấy phép và kích hoạt vai khi nhiều kiểu phân cấp cùng tồn tại bên trong một phân cấp vai, đặc biệt là phân tích các quan hệ phân cấp giữa một cặp vai mà không liên hệ nhau trực tiếp thì có thể được suy diễn như thế nào từ tập các vai liên hệ nhau về mặt phân cấp đã được xác định rõ. Để giải quyết sự tồn tại của tất cả các kiểu phân cấp trong một phân cấp vai, sau đây chúng ta đưa vào khái niệm quan hệ phân cấp suy dẫn cho phép có được nhiều tính chất kế thừa và kích hoạt phức tạp của một sự phân cấp vai. Đồng thời chúng ta đưa vào một tập các luật suy diễn được dùng để xác định tất cả các quan hệ suy dẫn có thể có giữa các vai trong một sự phân cấp. Trong một phân cấp mà cả ba kiểu phân cấp có thể cùng tồn tại, thì một quan hệ phân cấp giữa một cặp vai liên hệ nhau gián tiếp có thể được sản sinh. Thực tế phần lớn các quan hệ được suy diễn như thế rơi vào ba kiểu phân cấp được xác định ở trên, nhưng vẫn tồn tại một kiểu phân cấp suy dẫn đặc biệt mà ta sẽ định nghĩa dưới đây, được gọi là quan hệ suy dẫn có điều kiện, được viết là $(x[\mathrm{S}]\langle f\rangle y)$, trong đó [S] là một tập vai (để phân biệt với tập các phiên và cũng hàm ý là trong [S] có quan hệ phân cấp). Ta dùng kí hiệu $R(H)$ để chỉ tập vai được chứa trong một phân cấp H. Khi đó ta định nghĩa quan hệ suy dẫn có điều kiện như sau.

Định nghĩa 4.1. (Quan hệ suy dẫn có điều kiện) Cho $H\tau$ là một phân cấp vai trong khoảng thời gian $\tau \subseteq T$, xét $\langle f\rangle \in \{\geqslant_\tau, >_\tau, \geqslant_\tau\}$. Cho $x, z \in R(H\tau), [Y] = \{y_1, y_2, ..., y_n\} \subseteq R(H\tau)$, thì $x[Y]\langle f\rangle z$ được gọi là quan hệ suy dẫn có điều kiện của x trên z với các điều kiện trên các vai của $[Y]$ trong khoảng thời gian τ, nếu thoả mãn: $\forall y \in \{y_1, y_2, ..., y_n\}, n > 0$ thì $(x >_\tau y) \wedge (y\langle f\rangle z)$.

Trong [4], Joshi và cộng sự đưa ra một tập luật suy diễn trong phân cấp vai với ràng buộc thời gian. Trong mục này chúng tôi củng cố thêm các lập luận của Joshi bằng việc chứng minh tính đúng đắn của tập luật này thông qua Định lý 4.1, Định lý 4.2 và Định lý 4.3. Mục đích của các luật suy diễn là để có được tất cả các quan hệ suy dẫn trong một tập hợp vai. Ta xét các quan hệ phân cấp kế thừa giấy phép, kế thừa kích hoạt và kế thừa tổng quát trong khoảng thời gian τ.

Định lý 4.1. *(Phân cấp với các quan hệ phi điều kiện) Cho $H\tau$ là một phân cấp vai trong khoảng thời gian $\tau \subseteq T$ và $x, y, z \in R(H\tau)$. Thế thì các luật suy diễn sau đây là đúng:*

1) $\forall\langle f\rangle \in \{\geqslant_\tau, >_\tau, \geqslant_\tau\} : (x\langle f\rangle y) \wedge (y\langle f\rangle z) \to (x\langle f\rangle z)$
2) $\forall\langle f_1\rangle, \langle f_2\rangle \in \{\geqslant_\tau, \geqslant_\tau\}$ mà $\langle f_1\rangle \neq \langle f_2\rangle$ thì $: (x\langle f_1\rangle y) \wedge (y\langle f_2\rangle z) \to (x \geqslant_\tau z)$
3) $\forall\langle f_1\rangle, \langle f_2\rangle \in \{>_\tau, \geqslant_\tau\}$ mà $\langle f_1\rangle \neq \langle f_2\rangle$ thì $: (x\langle f_1\rangle y) \wedge (y\langle f_2\rangle z) \to (x >_\tau z)$
4) $\forall\langle f\rangle \in \{\geqslant_\tau, >_\tau, \geqslant_\tau\}$ thì $: (x >_\tau y) \wedge (y\langle f\rangle z) \to (x\{y\}\langle f\rangle z)$.

Chứng minh:

1) Do tính bắc cầu của các quan hệ kế thừa giấy phép, kế thừa kích hoạt và kế thừa tổng quát nên với mọi $\langle f\rangle \in \{\geqslant_\tau, >_\tau, \geqslant_\tau\}$, luật suy diễn sau là đúng: $(x\langle f\rangle y) \wedge (y\langle f\rangle z) \to (x\langle f\rangle z)$.

2) Xét $\forall\langle f_1\rangle, \langle f_2\rangle \in \{\geqslant_\tau, \geqslant_{\cdot\tau}\}$ mà $\langle f_1\rangle \neq \langle f_2\rangle$. Nếu $\langle f_1\rangle$ là quan hệ kế thừa tổng quát thì $\langle f_2\rangle$ là quan hệ kế thừa giấy phép, nghĩa là ta có $(x \geqslant_{\cdot\tau} y) \wedge (y \geqslant_\tau z)$. Nhưng: $(x \geqslant_{\cdot\tau} y) \to (x \geqslant_\tau y) \wedge (x >_\tau y)$, thế thì $(x \geqslant_\tau y) \to (x \geqslant_\tau y)$. Nên $(x \geqslant_\tau y) \wedge (y \geqslant_\tau z) \to (x \geqslant_\tau$

$y) \wedge (y \geqslant_\tau z)$. Do tính bắc cầu của quan hệ $\geqslant_\tau$ nên: $(x \geqslant_\tau y) \wedge (y \geqslant_\tau z) \to (x \geqslant_\tau z)$. Vậy $(x \geqslant_{\cdot\tau} y) \wedge (y \geqslant_\tau z) \to (x \geqslant_\tau z)$ tức $(x\langle f_1\rangle y) \wedge (y\langle f_2\rangle z) \to (x \geqslant_\tau z)$. Tương tự nếu $\langle f_1\rangle$ là quan hệ $\geqslant_\tau$ thì $\langle f_2\rangle$ là quan hệ $\geqslant_\tau$ và luật suy diễn đã cho vẫn đúng.

3) $\forall\langle f_1\rangle, \langle f_2\rangle \in \{\succ_\tau, \geqslant_{\cdot\tau}\}$ mà $\langle f_1\rangle \neq \langle f_2\rangle$ ta xét trường hợp: Nếu $\langle f_1\rangle$ là quan hệ $\geqslant_{\cdot\tau}$ thì $\langle f_2\rangle$ là quan hệ $\succ_\tau$, nghĩa là ta có $(x \geqslant_{\cdot\tau} y) \wedge (y \succ_\tau z)$. Nhưng $(x \geqslant_{\cdot\tau} y) \to (x \succ_{\cdot\tau} y)$. Nên $(x \geqslant_{\cdot\tau} y) \wedge (y \succ_\tau z) \to (x \succ_{\cdot\tau} y) \wedge (y \succ_{\cdot\tau} z)$. Do tính bắc cầu của quan hệ $\succ_{\cdot\tau}$ nên: $(x \succ_\tau y) \wedge (y \succ_\tau z) \to (x \succ_\tau z)$. Vậy: $(x \geqslant_\tau y) \wedge (y \succ_\tau z) \to (x \succ_\tau z)$. Tương tự nếu $\langle f_1\rangle$ là quan hệ $\succ_\tau$ thì $\langle f_2\rangle$ là quan hệ $\geqslant_\tau$ và luật suy diễn đã cho vẫn đúng.

4) Xét mọi $\langle f\rangle \in \{\geqslant_\tau, \succ_\tau, \geqslant_\tau\}$. Vì với $\forall y \in \{y\}$ ta có $(x \succ_\tau y) \wedge (y\langle f\rangle z)$ nên theo định nghĩa của quan hệ suy dẫn có điều kiện thì $(x\{y\}\langle f\rangle z)$. Vậy $(x \succ_\tau y) \wedge (y\langle f\rangle z) \to (x\{y\}\langle f\rangle z)$.

■

Định lý 4.2. *(Phân cấp với một quan hệ suy dẫn có điều kiện): Cho $H\tau$ là một phân cấp vai trong khoảng thời gian $\tau \subseteq T, x, y, z \in R(H\tau)$ và $[\mathrm{S}] \subseteq R(H\tau)$. Thế thì các luật suy diễn sau đây là đúng:*

1) $\forall\langle f\rangle \in \{\geqslant_\tau, \geqslant_\tau\}$ ta có : $(x[\mathrm{S}] \geqslant_\tau y) \wedge (y\langle f\rangle z) \to (x[\mathrm{S}] \geqslant_\tau z)$

2) $\forall\langle f\rangle \in \{\geqslant_\tau, \geqslant_\tau\}$ ta có : $(x[\mathrm{S}] \geqslant_{\cdot\tau} y) \wedge (y\langle f\rangle z) \to (x[\mathrm{S}]\langle f\rangle z)$

3) $(x[\mathrm{S}] \geqslant_{\cdot\tau} y) \wedge (y \succ_\tau z) \to (x \succ_\tau z)$.

Chứng minh:

1) Xét $\forall\langle f\rangle \in \{\geqslant_\tau, \geqslant_{\cdot\tau}\}$. Nếu $\langle f\rangle$ là quan hệ kế thừa tổng quát thì $(y \geqslant_{\cdot\tau} z)$ kéo theo $(y \geqslant_\tau z)$, nên ta chỉ cần xét trường hợp $\langle f\rangle$ là quan hệ kế thừa giấy phép $\geqslant_\tau$. Nghĩa là ta xét $(x[\mathrm{S}] \geqslant_\tau y) \wedge (y \geqslant_\tau z)$. Vì $(x[\mathrm{S}] \geqslant_\tau y)$ nên $\forall r \in [\mathrm{S}]$ thì $(x \succ_\tau r) \wedge (r \geqslant_\tau y)$. Mà có $(y \geqslant_\tau z)$ nên theo tính chất bắc cầu của quan hệ $\geqslant_\tau$ ta được: $\forall r \in [\mathrm{S}]$ thì $(x \succ_\tau r) \wedge (r \geqslant_\tau y) \wedge (y \geqslant_\tau z) \to (x \succ_\tau r) \wedge (r \geqslant_\tau z)$. Vậy $\forall r \in [\mathrm{S}]$ thì $(x \succ_\tau r) \wedge (r \geqslant_\tau z)$ hay $(x[\mathrm{S}] \geqslant_\tau z)$. Do đó luật suy diễn đã cho là đúng.

2) Xét $\forall\langle f\rangle \in \{\geqslant_\tau, \geqslant_\tau\}$. Với $(x[\mathrm{S}] \geqslant_{\cdot\tau} y)$ ta có $\forall r \in [\mathrm{S}], (x \succ_\tau r) \wedge (r \geqslant_{\cdot\tau} y)$. Theo định nghĩa của quan hệ $\geqslant_\tau$ ta có $(r \geqslant_{\cdot\tau} y) \to (r \geqslant_\tau y)$ nên $\forall r \in [\mathrm{S}], (x \succ_\tau r) \wedge (r \geqslant_\tau y)$. Nếu $\langle f\rangle$ là quan hệ kế thừa tổng quát thì từ $(x[\mathrm{S}] \geqslant_{\cdot\tau} y) \wedge (y \geqslant_{\cdot\tau} z)$ ta có $\forall r \in [\mathrm{S}], (x \succ_\tau r) \wedge (r \geqslant_{\cdot\tau} y) \wedge (y \geqslant_{\cdot\tau} z)$. Theo tính chất bắc cầu của quan hệ $\geqslant_\tau$ ta được: $\forall r \in [\mathrm{S}], (x \succ_\tau r) \wedge (r \geqslant_{\cdot\tau} z)$ hay $(x[\mathrm{S}] \geqslant_{\cdot\tau} z)$. Nếu $\langle f\rangle$ là quan hệ kế thừa giấy phép thì với $(x[\mathrm{S}] \geqslant_{\cdot\tau} y)$ ta có $\forall r \in [\mathrm{S}], (x \succ_\tau r) \wedge (r \geqslant_\tau y)$. Thế thì từ $(x[\mathrm{S}] \geqslant_{\cdot\tau} y) \wedge (y\langle f\rangle z)$ ta được: $\forall r \in [\mathrm{S}], (x \succ_\tau r) \wedge (r \geqslant_\tau y) \wedge (y \geqslant_\tau z)$. Do tính chất bắc cầu của quan hệ $\geqslant_\tau$ ta được: $\forall r \in [\mathrm{S}], (x \succ_{\cdot\tau} r) \wedge (r \geqslant_\tau z)$ hay $(x[\mathrm{S}] \geqslant_\tau z)$, tức $(x[\mathrm{S}]\langle f\rangle z)$. Vậy luật suy diễn là đúng.

3) Với $(x[\mathrm{S}] \geqslant_{\cdot\tau} y)$ ta có $\forall r \in [\mathrm{S}], (x \succ_\tau r) \wedge (r \geqslant_{\cdot\tau} y)$. Theo định nghĩa của quan hệ kế thừa tổng quát thì $(r \geqslant_{\cdot\tau} y)$ kéo theo $(r \succ_{\cdot\tau} y)$, nên ta được: $\forall r \in [\mathrm{S}], (x \succ_{\cdot\tau} r) \wedge (r \succ_{\cdot\tau} y)$. Theo tính chất bắc cầu của quan hệ $\succ_\tau$ ta được $(x \succ_{\cdot\tau} y)$. Do đó từ $(x[\mathrm{S}] \geqslant_{\cdot\tau} y) \wedge (y \succ_\tau z)$ ta có $(x \succ_\tau y) \wedge (y \succ_\tau z)$. Suy ra: $(x \succ_\tau z)$. Vậy $(x[\mathrm{S}] \geqslant_{\cdot\tau} y) \wedge (y \succ_\tau z) \to (x \succ_\tau z)$.

Định lý 4.3. *(Phân cấp với nhiều đường dẫn giữa hai vai) Cho $H\tau$ là một phân cấp vai trong khoảng thời gian $\tau \subseteq T$ và $[\mathrm{S}], [\mathrm{S}_1], [\mathrm{S}_2] \subseteq R(H\tau)$. Kí hiệu $(x\langle f\rangle y)_i$ là quan hệ phân cấp $x\langle f\rangle y$ theo đường dẫn $i (i = 1, 2, ...)$, ta có $[S_1 \cup S_2] = [\mathrm{S}_1] \cup [\mathrm{S}_2]$. Thế thì các luật suy diễn sau đây là đúng:*

1) *Với mọi* $\langle f\rangle \in \{\geqslant_\tau, >_\tau, \geqslant_\tau\}$ *ta có:* $(x\langle f\rangle y)_1 \wedge (y\langle f\rangle z)_2 \to (x\langle f\rangle z)$

2) *Với mọi* $\langle f_1\rangle, \langle f_2\rangle \in \{\geqslant_\tau, >_\tau, \geqslant_\tau\}$ *mà* $\langle f_1\rangle \neq \langle f_2\rangle$ *thì*
$$(y\langle f\rangle z)_2 \wedge (x\langle f_2\rangle y)_2 \to (x \geqslant_\tau y)$$

3) *Ta có:*

a. Với mọi $\langle f\rangle \in \{\geqslant_\tau, >_\tau, \geqslant_\tau\}$ *thì* $(x[\mathrm{S}]\langle f\rangle y)_1 \wedge (y\langle f\rangle z)_2 \to (x[\mathrm{S}]\langle f\rangle z)$

b. Với mọi $\langle f\rangle \in \{>_\tau, \geqslant_\tau\}$ *thì* $(x[\mathrm{S}]\langle f\rangle y)_1 \wedge (y >_\tau z)_2 \to (x[\mathrm{S}] >_\tau z)$

c. Với mọi $\langle f_1\rangle, \langle f_2\rangle \in \{\geqslant_\tau, \geqslant_\tau\}$ *mà* $\langle f_1\rangle \neq \langle f_2\rangle$ *thì*
$$(x[\mathrm{S}]\langle f_1\rangle y)_1 \wedge (x\langle f_2\rangle y)_2 \to (x \geqslant_\tau y).$$

4) *Với mọi* $\langle f\rangle \in \{>_\tau, \geqslant_\tau, \geqslant_\tau\}$, *ta có:*
$$(x[\mathrm{S}_1]\langle f\rangle y)_1 \wedge (x[\mathrm{S}_2]\langle f\rangle y)_2 \to (x[S_1 \cup S_2]\langle f\rangle y)$$

5) *Với mọi* $\langle f_1\rangle, \langle f_2\rangle \in \{\geqslant_\tau, \geqslant_\tau\}$ *mà* $\langle f_1\rangle \neq \langle f_2\rangle$, *ta có:*
$$(x[\mathrm{S}_1]\langle f_1\rangle y)_1 \wedge (x[\mathrm{S}_2]\langle f_2\rangle y)_2 \to (x[S_1 \cup S_2] \geqslant_\tau y).$$

Chứng minh:

1) Với mọi $\langle f\rangle \in \{\geqslant_\tau, >_\tau, \geqslant_\tau\}$ ta có $(x\langle f\rangle y) \wedge (y\langle f\rangle z)$. Do tính chất bắc cầu của các quan hệ $\geqslant_\tau, >_\tau, \geqslant_\tau$ nên ta được $(x\langle f\rangle z)$. Vậy luật suy diễn là đúng.

2) Xét $\forall\langle f_1\rangle, \langle f_2\rangle \in \{\geqslant_\tau, >_\tau, \geqslant_\tau\}$ sao cho $\langle f_1\rangle \neq \langle f_2\rangle$

- Nếu $\langle f_1\rangle$ là quan hệ kế thừa tổng quát thì từ $(x\langle f_1\rangle y)_1$ ta được $(x \geqslant_\tau y)$. Nếu $\langle f_2\rangle$ là quan hệ kế thừa tổng quát thì từ $(x\langle f_2\rangle y)_2$ ta được $(x \geqslant_\tau y)$. Do đó : $(x\langle f_1\rangle y)_1 \wedge (x\langle f_2\rangle y)_2 \to (x \geqslant_\tau y)$.

- Nếu $\langle f_1\rangle$ và $\langle f_2\rangle$ không phải là quan hệ kế thừa tổng quát, tức $\langle f_1\rangle, \langle f_2\rangle \in \{\geqslant_\tau, >_\tau\}$ và $\langle f_1\rangle \neq \langle f_2\rangle$ thì $(x\langle f_1\rangle y)_1 \wedge (x\langle f_2\rangle y)_2$ có dạng $(x \geqslant_\tau y)_1 \wedge (x >_\tau y)_2$ hoặc dạng $(x >_\tau y)_1 \wedge (x \geqslant_\tau y)_2$ nên nếu xảy ra $(x\langle f_1\rangle y)_1 \wedge (x\langle f_2\rangle y)_2$ thì sẽ xảy ra $(x >_\tau y)$ và $(x \geqslant_\tau y)$. Theo định nghĩa của quan hệ $\geqslant_\tau$ thì xảy ra $(x \geqslant_\tau y)$. Vậy $(x\langle f_1\rangle y)_1 \wedge (x\langle f_2\rangle y)_2 \to (x \geqslant_\tau y)$.

3) Xét $\forall\langle f\rangle, \langle f_1\rangle, \langle f_2\rangle \in \{\geqslant_\tau, \geqslant_\tau\}$ sao cho $< f_1 >\neq \langle f_2\rangle$.

a. Với $(x[\mathrm{S}]\langle f\rangle y)_1$ ta có $\forall r \in [\mathrm{S}], (x >_\tau r) \wedge (r\langle f\rangle y)$ nên từ $(x[\mathrm{S}]\langle f\rangle y)_1 \wedge (y\langle f\rangle z)_2$ ta được $\forall r \in [\mathrm{S}], (x >_\tau r) \wedge (r\langle f\rangle y) \wedge (y\langle f\rangle z)$. Do tính chất bắc cầu của các quan hệ $\langle f\rangle$ ta có $\forall r \in [\mathrm{S}], (x >_\tau r) \wedge (r\langle f\rangle z)$, hay $(x[\mathrm{S}]\langle f\rangle z)$.

b. Với $\forall\langle f\rangle \in \{>_\tau, \geqslant_\tau\}$, ta chứng minh: $(x[\mathrm{S}]\langle f\rangle y)_1 \wedge (y >_\tau z)_2 \to (x[\mathrm{S}] >_\tau z)$. Từ $(x[\mathrm{S}]\langle f\rangle y)_1 \wedge (y >_\tau z)_2$ ta có $\forall r \in [\mathrm{S}], (x >_\tau r) \wedge (r\langle f\rangle y) \wedge (y >_\tau z)$. Nếu $\langle f\rangle$ là quan hệ kế thừa kích hoạt thì $\forall r \in [\mathrm{S}], (x >_\tau r) \wedge (r >_\tau y) \wedge (y >_\tau z)$. Do quan hệ $>_\tau$ có tính bắc cầu nên $\forall r \in [\mathrm{S}], (x >_\tau r) \wedge (r >_\tau z)$, hay $(x[\mathrm{S}] >_\tau z)$. Nếu $\langle f\rangle$ là quan hệ kế thừa tổng quát thì từ $(x[\mathrm{S}] \geqslant_\tau y)_1 \wedge (y >_\tau z)_2$ ta có $\forall r \in [\mathrm{S}], (x >_\tau r) \wedge (r \geqslant_\tau y) \wedge (y >_\tau z)$. Do $(r \geqslant_\tau y) \to (r >_\tau y)$ nên có $\forall r \in [\mathrm{S}], (x >_\tau r) \wedge (r >_\tau y) \wedge (y >_\tau z)$. Do tính chất bắc cầu của các quan hệ $>_\tau$ ta được $\forall r \in [\mathrm{S}], (x >_\tau r) \wedge (r >_\tau z)$, hay$(x[\mathrm{S}] >_\tau z)$. Vậy luật suy diễn là đúng.

c. Ta chứng minh: $(x[\mathrm{S}]\langle f_1\rangle y)_1 \wedge (x\langle f_2\rangle y)_2 \to (x \geqslant_\tau y)$.

Nếu $\langle f_1\rangle$ là quan hệ $\geqslant_\tau$ thì $\langle f_2\rangle$ là quan hệ $\geqslant_\tau$ và ta có $(x[\mathrm{S}] \geqslant_\tau y)_1 \wedge (x \geqslant_\tau y)_2$ nên $(x \geqslant_\tau y)$. Nếu $\langle f_1\rangle$ là quan hệ $\geqslant_\tau$ thì $\langle f_2\rangle$ là quan hệ $\geqslant_\tau$ và ta có $(x[\mathrm{S}] \geqslant_\tau y)_1 \wedge (x \geqslant_\tau y)_2$

nên $\forall r \in [S], (x >_{\cdot\tau} r) \wedge (r \geqslant_{\cdot\tau} y) \wedge (x \geqslant_\tau y)$. Vì $(r \geqslant_{\cdot\tau} y)$ kéo theo $(r >_{\cdot\tau} y)$ nên $\forall r \in [S]$, $(x >_\tau r) \wedge (r >_\tau y) \wedge (x \geqslant_\tau y)$. Do tính chất bắc cầu của quan hệ $>_\tau$ ta được $(x >_\tau y) \wedge (x \geqslant_\tau y)$. Suy ra $(x \geqslant_\tau y)$.

4) Xét $\forall \langle f \rangle \in \{>_\tau, \geqslant_\tau, \geqslant_\tau\}$. Ta chứng minh

$$(x[\mathrm{S}_1]\langle f \rangle y)_1 \wedge (x[\mathrm{S}_2]\langle f \rangle y)_2 \to (x[S_1 \cup S_2]\langle f \rangle y).$$

Từ $(x[\mathrm{S}_1]\langle f \rangle y)_1$ ta có $\forall r \in [\mathrm{S}_1], (x >_{\cdot\tau} r) \wedge (r \langle f \rangle y)$. Từ $(x[\mathrm{S}_2]\langle f \rangle y)_2$ ta có $\forall r \in [\mathrm{S}_2]$, $(x >_\tau r) \wedge (r \langle f \rangle y)$. Nên từ $(x[\mathrm{S}_1]\langle f \rangle y)_1 \wedge (x[\mathrm{S}_2]\langle f \rangle y)_2$ ta có $\forall r \in [\mathrm{S}_1] \cup [\mathrm{S}_2], (x >_\tau r) \wedge (r \langle f \rangle y)$, hay $\forall r \in [S_1 \cup S_2], (x >_\tau r) \wedge (r \langle f \rangle y)$. Thế thì ta có $(x[S_1 \cup S_2]\langle f \rangle y)$.

5) Với $\forall \langle f_1 \rangle, \langle f_2 \rangle \in \{\geqslant_\tau, \geqslant_\tau\}$ sao cho $\langle f_1 \rangle \neq \langle f_2 \rangle$, ta xét trường hợp : Nếu $\langle f_1 \rangle$ là quan hệ $\geqslant_\tau$ thì $\langle f_2 \rangle$ là quan hệ $\geqslant_{\cdot\tau}$ do đó ta có $(x[\mathrm{S}_1] \geqslant_\tau y)_1 \wedge (x[\mathrm{S}_2] \geqslant_{\cdot\tau} y)_2$ nên $\forall r \in [\mathrm{S}_1]$, $(x >_\tau r) \wedge (r \geqslant_\tau y)$ và $\forall r \in [\mathrm{S}_2], (x >_\tau r) \wedge (r \geqslant_\tau y)$ nên $\forall r \in [\mathrm{S}_2], (x >_\tau r) \wedge (r \geqslant_\tau y)$, do đó $\forall r \in [S_1 \cup S_2], (x >_\tau r) \wedge (r \geqslant_\tau y)$, nghĩa là $(x[S_1 \cup S_2] \geqslant_\tau y)$. Do vai trò tương đương của $\langle f_1 \rangle$ và $\langle f_2 \rangle$ trong luật suy diễn nên nếu $\langle f_1 \rangle$ là quan hệ $\geqslant_\tau$, $\langle f_2 \rangle$ là quan hệ $\geqslant_\tau$ thì luật suy diễn này vẫn đúng.

Để chứng minh tính đúng đắn của các luật suy diễn trong Định lý 4.1, Định lý 4.2, Định lý 4.3, chúng ta đã sử dụng tính chất bắc cầu của các quan hệ phân cấp không hạn chế và các định nghĩa của các quan hệ này. Ngoài ra có sử dụng định nghĩa quan hệ suy dẫn có điều kiện. Vì các quan hệ phân cấp hạn chế mạnh và hạn chế yếu là một trường hợp riêng của các quan hệ phân cấp không hạn chế tương ứng (kế thừa giấy phép, kế thừa kích hoạt, kế thừa tổng quát) khi xét đến thời gian có khả năng của các vai cấp trên, vai cấp dưới, nên chúng ta cũng có các luật suy diễn tương ứng với các luật suy diễn ở trên áp dụng cho các quan hệ phân cấp hạn chế với một định nghĩa quan hệ suy dẫn có điều kiện thích hợp. Do khuôn khổ của bài báo, chúng tôi không nêu chi tiết các luật này ở đây và cũng không đưa ra chứng minh về tính đầy đủ của tập luật này.

5. KẾT LUẬN

Trong bài báo này chúng tôi đã trình bày và củng cố thêm lập luận của Joshi trong [2] và [4] về các loại phân cấp vai của mô hình kiểm soát truy nhập dựa trên vai với ràng buộc thời gian: phân cấp kế thừa giấy phép, phân cấp kế thừa kích hoạt và phân cấp kế thừa tổng quát và chứng minh tính bắc cầu của chúng. Từ đó xây dựng và chứng minh tính đúng đắn của một tập luật suy diễn trong các quan hệ phân cấp vai theo thời gian dạng không hạn chế (được mở rộng cho dạng hạn chế mạnh và hạn chế yếu) của ba kiểu phân cấp trên. Trong một phân cấp mà cả ba kiểu phân cấp có thể cùng tồn tại, thì một quan hệ phân cấp giữa một cặp vai liên hệ nhau gián tiếp có thể được sản sinh (gọi là quan hệ suy dẫn). Tập luật suy diễn cũng bao hàm các quan hệ suy dẫn có thể được suy diễn từ một tập hợp các quan hệ phân cấp đã được xác định trước. Để hoàn thiện các thành phần và các chức năng của kiểm soát truy nhập dựa trên vai trong quản lí tài nguyên của một tổ chức, chúng tôi sẽ đi sâu vào nghiên cứu tập các ràng buộc theo thời gian cần cho kiểm soát truy nhập dựa trên vai.

TÀI LIỆU THAM KHẢO

[1] E. Bertino, P. A. Bonatti, E. Ferrari, TRBAC: A temporal role-based access control model, *ACM Transactions on Information and System Security* **4** (4) (2001).

[2] James B. D. Joshi, Elisa Bertino, Arif Ghafoor, Temporal hierarchies and inheritance semantics for GTRBAC, *Seventh ACM symposium on access control models and technologies* (June 2002) 74–83.

[3] James B. D. Joshi, Elisa Bertino, U. Latif, Arif Ghafoor, "Generalized temporal role based access control model (GTRBAC) (Part I)- Specification and Modeling", *CERIAS TR 2001-47, Purdue University, USA* 2001.

[4] James B. D. Joshi, Elisa Bertino, Arif Ghafoor, Hybrid role hierarchy for generalized temporal role based access control model. *Proceedings of the 26th annual international computer software and applications conference (COMPSAC' 02), 2002 IEEE.*

[5] Lê Thanh, Nguyễn Thúc Hải, Phát triển giao thức xác thực kiểu Kerberos kết hợp kiểm soát truy nhập dựa trên vai cho hệ thống quản lí tài nguyên, *Tạp chí Tin học và Điều khiển học* **20** (4) (2004) 305–318.

[6] R. Sandhu, E. J. Coyne, H. L. Feinstein, C. E. Youman, Role-based access control models, *IEEE Computer* **29** (2) (1996) 38–47.

[7] Sylvia Osborn, Ravi Sandhu, Qamar Munawer, Configuring role-based access control to enforce mandatory and discretionary access control policies, *ACM Transactions on Information and System Security* **3** (2) (May 2000) 85–106.

Nhận bài ngày 10 - 8 - 2005
Nhận lại sau sửa ngày 07 - 11 -2005