VỀ MỘT PHƯƠNG PHÁP ĐẢM BẢO AN TOÀN TRUY CẬP TÀI NGUYÊN ĐÁM MÂY

Nguyễn Đào Trường*, Đoàn Thị Bích Ngọc

Tóm tắt: *Điện toán đám mây ngày nay không chỉ phổ biến với khách hàng thương mại mà còn cả với những khách hàng giáo dục. Khi mà toàn bộ dữ liệu của chủ sở hữu được đưa lên đám mây thì bài toán an toàn truy cập lại càng trở lên cấp thiết hơn bao giờ hết. Bài báo này đề xuất một mô hình kiểm soát truy cập dựa trên vai trò được lượng hóa cho đám mây, cung cấp giải pháp ủy quyền hiệu quả và điều chỉnh quyền linh hoạt khi có những truy cập trái phép. Giải pháp đề xuất chống lại các tấn công leo thang đặc quyền dựa trên cơ chế xác thực với mỗi vai trò trong từng phiên liên lại của mỗi đối tượng khác nhau. Kết quả phân tích được triển khai thực nghiệm trên ứng dụng trong đám mây IaaS.*

Từ khóa: Đám mây; Quyền; Đặc quyền; Vai trò.

1. GIỚI THIỆU

Điện toán đám mây là sự kết hợp của các tài nguyên điện toán có thể cấu hình khác nhau như mạng, máy chủ, kho lưu trữ, dịch vụ, ứng dụng giúp cung cấp truy cập thuận tiện và theo yêu cầu cho người dùng đám mây [1]. Điện toán đám mây được nhiều nhà nghiên cứu đề cập đến và hiện đang được sử dụng trong nhiều lĩnh vực thương mại, trong đó, đám mây IaaS là một trong những lựa chọn khá nhiều. Các nhà cung cấp dịch vụ đám mây chịu trách nhiệm quản lý trong môi trường đám mây. Tuy nhiên, một số lượng lớn sự cố rò rỉ dữ liệu và bảo mật thông tin là do các lỗ hổng trong hệ thống [2-4].

Trong mô hình kiểm soát truy cập bắt buộc, mỗi đối tượng hệ thống tệp có một nhãn phân loại chẳng hạn như, bí mật, mức tối mật hoặc mức tuyệt mật. Hệ điều hành hoặc trung tâm bảo mật kiểm tra thông tin đăng nhập của từng người hoặc hệ thống trong khi truy cập một tài nguyên cụ thể để xác định quyền truy cập của người hoặc thiết bị cụ thể đó [5]. Kiểm soát truy cập dựa trên vai trò (RBAC) là một cơ chế kiểm soát truy cập được sử dụng rộng rãi và ủy quyền dựa trên vai trò là cách phổ biến nhất để chủ sở hữu dữ liệu cấp đặc quyền cho người dùng trong môi trường đám mây [6]. Trong bài báo này, chúng tôi đề xuất việc tạo vai trò, quyền, và phân quyền được giao cho người quản trị đám mây của bên thuê.

Chúng tôi tiến hành gán giá trị cho mỗi quyền trong từng vai trò để thuận lợi trong việc kiểm soát truy cập vào dữ liệu đám mây. Với giá trị định lượng được gán cho các bộ (vai trò, quyền), có thể mô tả chính xác bất kỳ đặc quyền nào của một vai trò được định lượng [7], chi tiết sẽ được trình bày trong các phần tiếp theo của bài báo.

2. MỘT SỐ CÔNG TRÌNH NGHIÊN CỨU TRƯỚC ĐÓ VÀ MỘT SỐ ĐỊNH NGHĨA, KÝ HIỆU TOÁN HỌC

2.1. Một số nghiên cứu liên quan

Trong [8], Gartner đã đưa ra một số rủi ro bảo mật mà các hệ thống đám mây phải đối mặt. Trong [9], chính sách kiểm soát truy cập được xác định dựa trên các thuộc tính dữ liệu. Trong [10], mô hình kiểm soát truy cập dựa trên vai trò có giới hạn thời gian (GTRBAC) được áp dụng cho các tài nguyên đám mây. Các vấn đề về truy vấn đặc quyền kết hợp với phân cấp vai trò trình bày trong [11]. Dựa trên mô hình RBAC, trong [13] trình bày một mô hình bảo mật thích ứng để mô tả việc chuyển đổi vai trò trong môi trường đám mây. Cho đến nay, các mô tả về đặc quyền trong các mô hình này là khá chi tiết. Như chúng ta đã biết, các hệ thống đám mây có rất nhiều tài nguyên và người dùng, để đáp ứng các yêu cầu về quyền của những người dùng khác nhau, một số lượng lớn các vai trò sẽ được tạo và duy trì nếu sử dụng các mô hình RBAC truyền thống. Do đó, nó sẽ tiêu tốn rất nhiều tài nguyên hệ thống. Trong bài báo này sử dụng một số

định nghĩa về quyền, giá trị quyền, vai trò được định lượng và giá trị hành vi để đề xuất một mô hình kiểm soát truy cập mới.

2.2. Một số định nghĩa và ký hiệu toán học

2.2.1. Định nghĩa mô hình RBAC

Định nghĩa 1: Mô hình RBAC được định nghĩa gồm các tập hợp, quan hệ và ràng buộc sau:

a. Tập người dùng đám mây $U=\{u_1,u_2,\ldots u_n\}$, tập vai trò $R=\{r_1,r_2,\ldots,r_k\}$, tập quyền $P=\{p_1,p_2,\ldots,p_m\}$; tập phiên làm việc $S=\{s_1,s_2,\ldots,s_m\}$;

b. Gán vai trò cho người dùng, ký hiệu $URA=\{ur_1,ur_2,...,ur_m\}, m\in N$, $URA\in U\times R$ là một ánh xạ từ $U\to R$ và ký hiệu $ur_i=(u,r), i=1...m,$ là người dùng *u* được gán vai trò *r*.

c. Gán vai trò với phiên làm việc, ký hiệu $SRA=\{sr_1,sr_2,...,sr_m\}, m\in N$, $SRA\in S\times R$ là một ánh xạ từ $S\to R$ và ký hiệu là $sr_i=(s,r), i=1...m,$ là phiên *s* được gán vai trò *r*.

d. Gán quyền với vai trò, ký hiệu $RPA=\{rp_1,rp_2,...,rp_m\}, m\in N,$, $RPA\in R\times P$ là một ánh xạ từ $R\to P$ và ký hiệu $rp_i=(r,p), i=1,...,m,$ là đặc quyền *p* được gán cho vai trò *r*. Với một vai trò *r* có thể có nhiều hơn một quyền, ngược lại một quyền *p* có thể được gán cho nhiều hơn một vai trò, tùy thuộc vào ngữ cảnh cụ thể, do người quản trị bên thuê đám mây sẽ quyết định.

2.2.2. Lượng hóa vai trò với quyền

Cần có một cơ chế ủy quyền và điều chỉnh quyền linh hoạt hơn trong đám mây. Một số vai trò và phân quyền chính của hệ thống được thống kê trong bảng 1. Trong mô hình RBAC, một vai trò *r* liên kết với một tập các bộ dưới dạng (r,p) tạo thành quyền của *r*. Trong đó, hàm quyền được thể hiện trong định nghĩa 2 [14].

Định nghĩa 2. Hàm xác định quyền của vai trò *rP* được định nghĩa là một ánh xạ $rP: R\to 2^{PRA}$ từ *R* vào *PRA* được viết thành $rP(r)=\{\overline{(r,p)}\,|\,(r,p)\in RPA\}$.

Để xác định bộ quyền của vai trò *r*, như đã định nghĩa trong định nghĩa 1.d), tuy nhiên để có thể thực hiện được trong quá trình thử nghiệm thì cần phải xác định dưới dạng định lượng, như vậy trong bài báo này sẽ sử dụng dạng chuỗi nhị phân, và được đại diện bởi một số duy nhất $2^i\,(i\in N\cup\{0\})$ được gán cho mỗi bộ tương ứng, trong đó *N* là tập số tự nhiên. Với quy định từng giá trị cụa thể cho một bộ (*r, p*) là $2^0,2^1,\ldots,2^{|r|-1}$, từng giá trị rời nhau với mỗi quyền. Giá trị quyền của các bộ (*r, p*) trong *bảng 1* được thể hiện trong *bảng 2*. Trong hai bảng 1 và 2 với dữ liệu cụ thể ở đây là bảng dữ liệu điểm của sinh viên.

Việc định nghĩa các quyền với các vai trò này được thực hiện bởi người quản trị của bên thuê đám mây. Trong bài báo này chúng tôi sử dụng mô hình quản trị đám mây IaaS trên nền OpenStack (Chi tiết sẽ được trình bày trong phần 3 và 4 của bài báo).

Định nghĩa 3 [14]. Hàm giá trị quyền $\overline{tQ}$ được định nghĩa là một ánh xạ $\overline{tQ}: PRA\to N$ được viết như sau $\overline{tQ}(\tilde{t})=\{n\,|\,n\in N\}$, *N* là tập số tự nhiên.

Định nghĩa 4 [14]. Tổng các giá trị quyền của *r* được định nghĩa là tổng của toàn bộ các giá trị quyền của các bộ (*r, p*); hàm giá trị tổng quyền $\overline{rQ}$ được định nghĩa là một ánh xạ $\overline{rQ}: R\to N$, được viết như sau: $\overline{rQ}(r)=\sum_{\tilde{t}\in rP(r)}\overline{tQ}(\tilde{t})$ .Thêm giá trị *k* vào *r*, nhận được một tổ hợp

nhị phân (*r, k*), với $r \in R, k \in N \wedge 0 < k \le \overline{rQ}(r)$ và tổ hợp (*r, k*) được định nghĩa là vai trò được định lượng, nó thể hiện các đặc quyền của *r*, phạm vi quyền được điều khiển bằng tham số *k*. Từ bảng 2 cho thấy giá trị quyền vai trò của các bộ gồm một dãy tăng về số mũ khác nhau. Với $\forall(r,k), k = \sum_{0 \le i < |r|} a_i 2^i$ có duy nhất một giải pháp {0, 1} [7]. Phương pháp để đánh giá xem một bộ quyền phụ thuộc vào (*r, k*) cho trước như sau: Nếu các giá trị $a_{i_1}, a_{i_2}, \ldots, a_{i_m}$ ($0 < m \le |r|$) tương ứng đều bằng 1, thì tập $\left\{2^{i_1}, 2^{i_2}, \ldots, 2^{i_m}\right\}$ chính là tập giá trị quyền của (*r, k*). Nếu 2^i nằm trong tập giá trị quyền của (*r, k*), bộ quyền tương ứng có giá trị 2^i chính là của (*r, k*).

Ví dụ, vai trò được định lượng (*GU*, 17) bao gồm hai bộ quyền của (*GU*, *pRd*) và (*GU*, *pQry*), trong khi vai trò được định lượng (*SV*, 2) chỉ chứa bộ (*SV*, *pGet*).

Bảng 1. *Gán quyền cho các vai trò* (*PRA*).

Ký hiệu vai trò	Ký hiệu quyền có thể, không đồng thời	Ý nghĩa quyền
Giáo vụ (GU)	pRd pUp pMng pDel pQry	Quyền đọc dữ liệu Quyền đẩy dữ liệu lên Quyền quản lý dữ liệu Quyền xóa dữ liệu Quyền truy vấn dữ liệu
Chủ nhiệm Bộ môn (BM)	pCk pCr	Quyền kiểm tra dữ liệu Quyền tạo dữ liệu
Sinh viên (SV)	pView pGet	Quyền xem dữ liệu Quyền lấy dữ liệu
Giảng viên (GV)	pEd pDn	Quyền nhập dữ liệu Quyền tải dữ liệu về

Bảng 2. *Bảng giá trị quyền của bộ cho các vai trò.*

$\tilde{t}(r,p)$	*Giá trị*	$\tilde{t}(r,p)$	*Giá trị*	$\tilde{t}(r,p)$	*Giá trị*	$\tilde{t}(r,p)$	*Giá trị*
(GU, pRd)	2^0	(BM, pCk)	2^0	(SV, pView)	2^0	(GV, pEd)	2^0
(GU, pUp)	2^1	(BM, pCr)	2^1	(SV, pGet)	2^1	(GV,pDn)	2^1
(GU, pMng)	2^2						
(GU, pDel)	2^3						
(GU, pQry)	2^4						

Định nghĩa 5 [14]. Tập vai trò được định lượng $\overline{R}$, hàm giá trị quyền $\overline{ks}$, và hàm nguồn quyền $\overline{rP}$ của các vai trò được định lượng được định nghĩa như sau: $\overline{R} = \left\{(r,k) \mid r \in R \wedge 0 < k \le \overline{rQ}(r)\right\}$.

Hàm $\overline{ks}$ được định nghĩa là ánh xạ $\overline{ks}: \overline{R} \to 2^{N \cup \{0\}}$, được viết thành $\overline{ks}\left((r,k)\right) = \left\{2^{i-1}\right\}$ giá trị bít thứ *i* trong bảng 1.

Hàm $\overline{rP}$ được định nghĩa là ánh xạ $\overline{rP}: \overline{R} \to 2^{PRA}$ từ tập các vai trò được định lượng vào *PRA*, được viết như sau: $\overline{rP}\left((r,k)\right) = \left\{(r,p) \mid (r,p) \in PRA \wedge \overline{tQ}\left((r,p)\right) \in \overline{ks}\left((r,k)\right)\right\}$.

3. ĐỀ XUẤT MÔ HÌNH KIỂM SOÁT TRUY CẬP ĐÁM MÂY

3.1. Cấu trúc của mô hình đề xuất

Trong bài báo này, xin đề xuất một mô hình kiểm soát truy cập dựa trên vai trò được định

lượng có cấu trúc như trong hình 1. Đầu tiên người dùng sẽ đăng nhập bằng tài khoản của mình vào đám mây, tại Keystone sẽ tiến hành xác thực, nếu xác thực thành công sẽ tạo một phiên làm việc chuyển sang máy Nova. Nova tiến hành gán vai trò, gán quyền cho vai trò, gán vai trò cho phiên. Nếu vai trò không khớp với phiên làm việc thì quyền sẽ không được cấp. Nếu vai trò phù hợp với phiên thì sẽ đượcc cấp quyền tương ứng truy cập vào dữ liệu. Sau đây là một số thuật toán (hàm, thủ tục) được sử dụng trong các module điều khiển quyền quy cập đám mây IaaS:

Thuật toán 1. Init ( ) //(Khởi tạo)

Đầu vào: $U = \{\ \}; P = \{\ \}; R = \{\ \};$

Đầu ra: $U, P, R;$

CreateUser(*u*: NAME), $U = U \cup \{u\};$

CreatePermission(*p*: NAME), $P = P \cup \{p\};$

CreateRole(*r*:NAME), $R = R \cup \{r\};$

Thuật toán 2. URAssign (*u, r*) //Gán vai trò cho người dùng

Đầu vào: *u*, *r*
Đầu ra: update(URA)

ur = UserRoleAssign (u, r);
$URA = URA \cup \{ur\};$

Thuật toán 3. RPAssign (*r, P'*) //Gán quyền cho vai trò

Đầu vào: *r*, *p*
Đầu ra: update(RPA)

While (*p in P'*) do
    rp = RolePermissionAssign (*r, p*);
    $RPA = RPA \cup \{rp\};$

Thuật toán 4. Login (*u*) //Đăng nhập

Đầu vào: u
Đầu ra: Success or UnSuccess

If (u in U) then return Success
else return UnSuccess;

Thuật toán 5. CreateSession (u) // Tại một phiên làm việc cho người dùng

Đầu vào: *u*,
Đầu ra: s(*u*)

If Login(u) then
    $s = newSession(u);$
    $S = S \cup \{s\};$
    Return S;

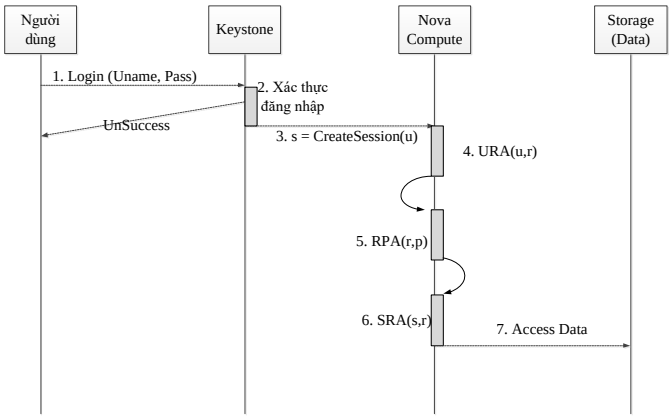
Thuật toán 6. SRA (s, r) // Gán vai trò cho một phiên cụ thể

Đầu vào: s, r
Đầu ra: update(SRA)

sr = SessionRoleAssign (s, r);
$SRA = SRA \cup \{sr\};$
Return SRA;

3.2. Kiểm soát và điều chỉnh hành vi bất thường

Việc điều chỉnh bất thường được thực hiện ngay trong bước chuyển từ 5 sang 6 tại hình 1. Tại bước này cần kiểm tra quyền được cấp ở bước 5 và nhu cầu quyền ở bước 6. Nếu hàm tính tổng quyền với vai trò *r* tại phiên làm việc *s*, $\overline{rQ}(r) > \sum_{\tilde{t} \in PRA} \overline{tQ}(\tilde{t})$ thì quyền của người dùng *u* với vai trò *r* này sẽ bị điều chỉnh xuống đến mức an toàn theo một ngưỡng cho trước. Vì tại thời điểm này người dùng *u*, với vai trò *r* đã xác thực xong hệ thống, do đó người dùng *u* sẽ có được những quyền được gán với vai trò tương ứng nhưng rất có thể người dùng u này sẽ tiến hành tấn công leo thang đặc quyền. Việc leo thang đặc quyền sẽ rất nguy hiểm, sau khi leo thang đặc quyền người dùng này có thể sẽ được nhiều hơn những quyền được phép thực sự. Do đó cần có hàm cấp quyền với phiên làm việc cụ thể với vai trò cụ thể SRA (*s*, *r*) để đảm bảo điều chỉnh lại quyền của người dùng *u* trước khi người này tiến hành truy cập vào cơ sở dữ liệu thực sự.



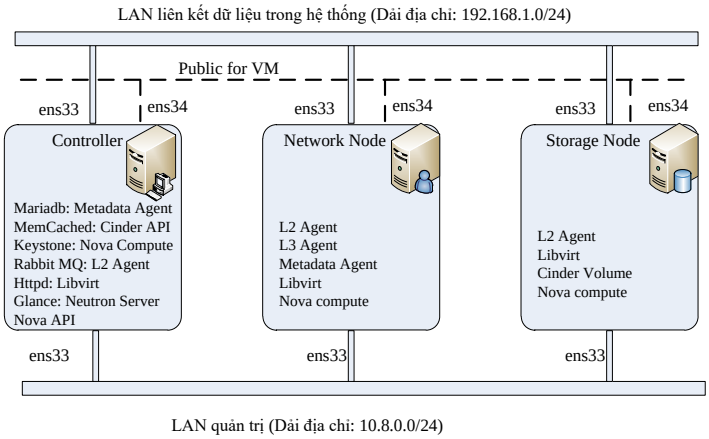
Hình 1. *Quá trình xử lý của mô đề xuất.*

4. THỰC NGHIỆM VÀ PHÂN TÍCH KẾT QUẢ

Để đánh giá được khả năng thực thi của giải pháp đề xuất, chúng tôi đã tiến hành cài đặt thử nghiệm trên đám mây IaaS rút gọn của OpenStack như đã trình bày ở phần 3. Mô hình thực nghiệm để cài đặt như sau:

4.1. Mô hình thực nghiệm

Trong phần này, chúng tôi triển khai trong đám mây IaaS trên nền OpenStack [15] với các thành phần cơ bản gồm: Nova, Swift, Glance, Cinder, Keystone,... Để thực nghiệm, chúng tôi tiến hành cài đặt một kiến trúc IaaS rút gọn như thể hiện trong hình 2.

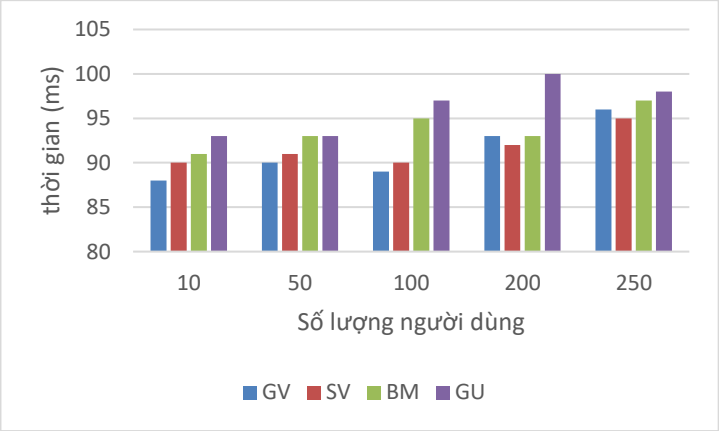


Hình 2. *Mô hình thực nghiệm rút gọn.*

4.2. Thực hiện ủy quyền

Kết quả thực hiện ủy quyền để cấp quyền truy cập cho những cán bộ làm những nhiệm vụ chuyên môn gồm: (1) Giáo vụ (GU) có giáo vụ của các Khoa, Trung tâm đào tạo, giáo vụ của Phòng đào tạo; (2) Chủ nhiệm bộ môn (BM) có chủ nhiệm bộ môn của các Khoa và Trung tâm đào tạo; (3) Sinh viên (SV) là các sinh viên của 04 khoa chuyên ngành; (4) Giảng viên là các giảng viên của 04 khoa chuyên ngành.

Trong số liệu phân tích chúng tôi chỉ xem 04 vai trò ứng với 04 đối tượng thường xuyên phải truy cập vào cơ sở dữ liệu điểm để tạo, cập nhật, xem, chỉnh sửa, thống kê, tổng hợp; Riêng đối tượng là sinh viên (SV) thường là số lượng lớn hàng nghìn sinh viên vào truy vấn, xem điểm cùng một lúc trong những thời điểm vào giai đoạn giữa, cuối mỗi học kỳ và kết thúc năm học. Nhưng trong số liệu thử nghiệm chúng tôi chưa thử được hết số lượng lớn này. Thời gian ủy quyền cho mỗi đối tượng với những số lượng nhỏ được thể hiện trong hình 3.



Hình 3. *Thời gian ủy quyền truy cập cho người dùng với các vai trò khác nhau.*

Qua thử nghiệm số liệu thì thấy, giai đoạn đầu với những giao dịch nhỏ thì thời gian có thể lớn hơn khi số lượng giao dịch lớn hơn, cụ thể với 10 hoặc 50 người dùng thì thời gian ủy quyền có thể lớn hơn do độ trễ của đường truyền và tính ổn định của hệ thống, tuy nhiên, khi số lượng ổn định tăng từ 100 lên 250 thì thời gian ổn định hơn nhưng xu hướng tăng thời gian là không đáng kể khi tăng gấp đôi số giao dịch từ 100 lên 200 hoặc cao hơn là 250. Thời gian ủy quyền truy cập của vai trò giáo vụ luôn luôn cao hơn do số lượng quyền cần được ủy quyền cho vai trò này luôn lớn hơn các đối tượng khác.

5. KẾT LUẬN

Mô hình đề xuất cho thấy những ưu điểm của nó đó là: thời gian để thực hiện ủy quyền rất ngắn, việc hoạch định các vai trò được rõ ràng, quá trình gán quyền với vai trò được lượng hóa rất nhanh. Mô hình có thể kiểm soát tốt các hành động của người dùng khi truy cập vào dữ liệu đám mây nhờ vào việc ủy quyền, cấp quyền cho từng người dùng với từng vai trò khác nhau. Mô hình đề xuất được áp dụng thử nghiệm trong hệ thống quản lý hệ thống điểm của một đơn vị đào tạo. Việc khi bị tấn công leo thang đặc quyền cũng được hạn chế nhờ vào cơ chế kiểm soát tự động, do người quản trị đã cấp cho từng phiên giao dịch với những vai trò riêng của người dùng. Khi người dùng sử dụng quá tổng quyền mà mình có được sẽ được giám sát bằng việc cấp quyền cho vai trò theo phiên. Bên cạnh đó, mô hình đề xuất cũng chống lại một số tấn công phổ biến được liệt kê trong [12].

TÀI LIỆU THAM KHẢO

[1]. CSA (2009), *"Security Guidance Critical Areas of Focus for Critical Areas of Focus in Cloud Computing V2.1"*, Cloud Security Alliance, No. 1, pp. 1–76.

[2]. S. Eludiora (2011), *"A user identity management protocol for cloud computing paradigm"*, Int. J. Commun. Netw. Syst. Sci. 4 (2011), pp.152–163,
[3]. Almulla S A, Chan Y Y (2010). *"Cloud computing security management [A]"*. Proceedings of the International Conference on Engineering Systems Management and Its Applications [C]. Sharjah, UAE, 2010, pp.1-7.
[4]. Mell P, Grance T. (2009), *"The NIST definition of cloud computing [J]"*. National Institute of Standards and Technology, 2009, 53(6): pp.50-57.
[5]. R. Jiang, X. Wu, B. Bhargava (2016), *"SDSS-MAC: secure data sharing scheme in multiauthority cloud storage systems"*, Comput. Secur. 62 (2016) pp.193–212.
[6]. Yang Liu, Tang Zhuo, Li Renfa, et al (2011), *"Roles query algorithm in cloud computing environment based on user require [J]"*. Journal on Communications, 2011, 32(7): pp.169-175.
[7]. Zhai Zhengde (2006), *"Quantified-role based controllable delegation model [J]"*. Chinese Journal of Computers, 2006, 29(8): pp.1401-1407.
[8]. Brodkin (2008), Gartner: seven cloud-computing security risks. http://www.networkworl.com/news/2008/070208-cloud.html.
[9]. Yu S, Wang C, Ren K, et al (2010), *"Achieving secure, scalable, and finegrained data access control in cloud computing [C]"*. In Proceedings of IEEE INFOCOM, 2010: pp.534-542.
[10]. Joshi J B D, Bertino E, Latif U, et al. *"A generalized temporal role-based access control model [J]"*. IEEE Transaction on Knowledge and Data Engineering, 2005, 17(1): pp.4-23.
[11]. Chandran S M, Joshi J B D. *"Towards administration of a hybrid role hierarchy [A]"*. Proceedings of the IEEE International Conference on Information Reuse and Integration [C]. Las Vegas, USA, 2005, pp.500-505.
[12]. I. Indu, P.M. Rubesh Anand, Vidhyacharan Bhaskar (2018), *"Identity and access management in cloud environment: Mechanisms and challenges, Engineering Science and Technology"*, an International Journal, 2018.
[13]. Jung Y, Chung M (2010), *"Adaptive security management model in the cloud computing environment [A]"*. Proceedings of the International Conference on Advanced Communication Technology [C]. Washington DC, USA, 2010, pp.1664-1669.
[14]. Chunlei Wu, Zhongwei Li, and Xuerong Cui (2012), *"An Access Control Method of Cloud Computing Resources Based on Quantified-Role"*, Natural Science Foundation of Shandong Province of China, pp. 919-923.
[15]. Openstack. http://www.openstack.org/.

ABSTRACT

A SECURE METHOD OF ACCESSING CLOUD RESOURCES

Cloud computing today is not only popular with business customers but also with educational customers. When all the owner's data is put on the cloud, the problem of secure access becomes more urgent than ever. This paper proposes a quantified role-based access control model for the cloud, providing an effective authorization solution and flexible permission adjustment when there are unauthorized accesses. The proposed solution againsts privilege escalation attacks based on the authorization mechanism for each role in each session of each different object. The analysis results are tested by the application in the IaaS cloud.

Keywords: Cloud; Behavior; Permissions; Privilege permission; Role.

Nhận bài ngày 31 tháng 7 năm 2021
Hoàn thiện ngày 08 tháng 9 năm 2021
Chấp nhận đăng ngày 10 tháng 10 năm 2021

Địa chỉ: Học viện Kỹ thuật Mật mã – Ban Cơ yếu Chính phủ - Bộ Quốc phòng.
*Email: truongnguyendao@gmail.com.