원격의료 서비스를 위한 상황 및 프라이버시를 고려한 역할기반 접근제어 위임모델

황유동*, 박동규**
*순천향대학교 정보보호학과
**순천향대학교 정보통신공학과
e-mail:hwangyudong@gmail.com

The Delegation Model of the Role-based Access Control considering Context and Privacy for the Telemedicine service

Yu-Dong Hwang*, Dong-Gue Park**
*Dept of Information Security Engineering, SoonChunHyang University
**Dept of Infomation and communication Engineering, SoonChunHyang University

요 약

본 논문에서는 유비쿼터스 환경에서의 원격 의료 서비스를 위한 상황 및 프라이버시를 고려한 역할기반 접근제어 모델에서의 위임 모델을 제안한다. 제안 모델은 원격 의료 서비스에서 반드시 필요하고 빈번히 발생할 수 있는 사용자 대 사용자 위임, 역할 대 역할 위임, 다단계 위임, 다중 위임 등의 기능을 제공한다. 따라서 본 논문에서 제안하는 모델을 이용하여 원격의료 서비스를 위한 사용자의 프라이버시 보호와 세밀한 접근제어가 가능하다.

1. 서론

유비쿼터스 환경에서의 원격 의료 서비스는 모바일 의료 서비스가 진화된 형태로 공간적, 시간적 제약을 없애고 환자가 생활공간 속에서 다양한 의료 센서 및 기기를 통하여 수집된 생체 정보와 환경 정보를 기반으로 중앙의 원격 의료 시스템을 통하여 언제 어디서나 의료 피드백을 받을 수 있는 서비스를 총칭한다.

원격 의료 시스템이 제대로 갖춰지게 되면 언제 어디서라도 응급 처치를 위한 치료가 가능하다. 그러나 사용자가 언제 어디서나 의료 데이터에 접근 할 수 있다는 것은 의료 데이터가 보안에 취약하다는 것을 의미한다. 유비쿼터스 환경에서의 원격 의료 서비스는 환자의 의무기록 뿐 아니라 각종 검사 자료 등 환자에 대한 대부분의 정보를 데이터화 하게 되므로 인증되지 않은 사용자가 의료 데이터를 원래의 목적과 다른 목적으로 사용하게 된다면 환자의 생명과 관련된 중요한 정보에 큰 위협을 가져올 수 있다. 따라서 이러한 문제 해결을 위하여 유비쿼터스 환경에서의 원격 의료 서비스에 적합한 접근제어 모델이 필요하다. 또한 원격의료 서비스를 위한 접근제어는 진료 시 환자의 증상과 병력에 따라 환자, 보호자, 의사와 간호사 들 간에 환자의 의료 정보를 액세스하기 위해 빈번한 역할과 권한의 위임이 발생하게 된다.

본 논문에서는 유비쿼터스 환경을 고려하여 시간, 객체, 공간과 같은 상황(context), 부정적인 허가(negative permission), 프라이버시, 의무(obligation)의 개념을 포함하는 원격의료 서비스를 위한 접근제어 모델에서의 사용자 대 사용자 위임, 역할 대 역할 위임, 다단계 위임, 다중 위임 등의 기능을 제공하는 위임 모델을 제안한다.

본 논문의 구성은 다음과 같다. 2장에서 원격 의료 서비스를 위한 접근제어 모델을 제시하고 3장에서 기존 모델과의 비교를 하며 4장에서 결론을 내린다.

2. 원격의료 서비스를 위한 접근제어 모델

2.1 유비쿼터스 환경에서의 원격의료 서비스를 위한 접근제어 모델

다음 그림 1에서 유비쿼터스 환경에서의 원격 의료 서비스를 위한 접근제어 모델을 보여준다.

이 모델의 특징은 다음과 같다.

첫째, 허가는 각 역할의 멤버들을 위해 개인화된다. 하나의 역할은 개인적인 역할 멤버들의 상황 정보와 목적, 의무사항, 조건들을 기반으로 하는 다른 객체의 오퍼레이션에 의해서 실행된다.

둘째, 역할은 의료 상황에 따라서 역할 위임시 동적이고 부분적인 위임을 위하여 하나의 역할은 4개의 부역할로 나누어진다.

셋째, 허가-역할 할당시 긍정적인 허가와 부정적인 허가를 제약 조건으로 주어 환자가 공개하길 원치 않는 정보에 대한 접근은 부인되어야 한다.

넷째, 상황 정보가 객체 및 역할의 할당과 활성화 조건으로 사용된다.

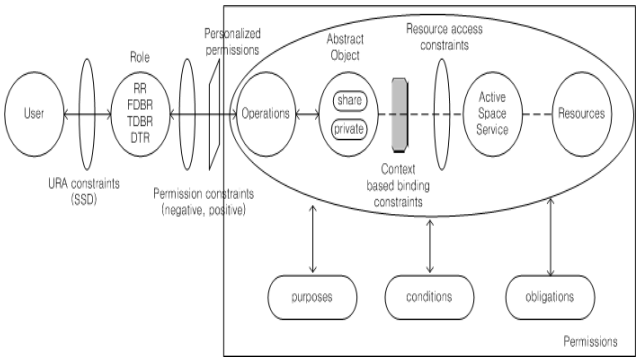

그림 1 원격의료 서비스를 위한 접근제어 모델

2.2 유비쿼터스 환경에서의 원격의료 서비스를 위한 접근제어 위임 모델

제안 모델에서는 위임모델의 그래프적인 표현, 다단계 위임, 다단계 취소, 관리 역할, 상/하향 위임, 혼성계층에서의 위임정책을 표현할 수 있도록 하였다.

1. 상향 위임

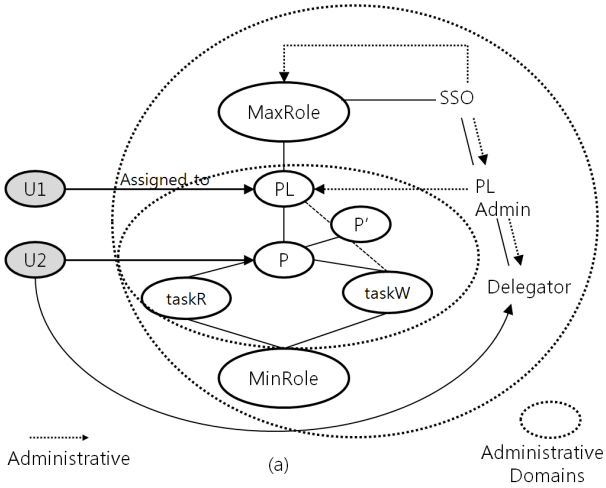

그림 2 제안 모델의 상향 위임

그림 2에서 관리 역할이나 MinRole, MaxRole를 갖는 것은 Role Graph Delegation 모델[12]과 동일하고 차이점은 역할 계층의 표현이다. 위의 그림에서 역할 PL과 P 사이, 역할 P와 taskR 사이는 I-역할 계층으로 형성되어 있으며, 역할 P와 taskW는 A-역할 계층으로 형성되어 있다. 기존의 Role Graph Delegation 모델과는 달리 I, A, IA 계층으로 계층을 구성할 수 있다는 점이 가장 큰 차이점이다. 위 그림 2는 역할 계층에서 상위 역할로 권한을 위임하는 상향 위임을 표현한다. 제안 모델의(에서) 위임 모델 생성은 위임하려고 하는 주체가 Delegator 역할에 할당되면서 시작된다.

Delegator 역할은 관리 역할의 하위 역할이며, 위임 역할의 생성, 사용자-역할 할당 취소, 권한 취소 등의 관리를 맡게 된다. 위임하려고 하는 하위 역할이 Delegator 역할에 할당되면서 P역할의 위임 역할인 P′를 만들고 P와 I-계층(이)으로 형성된다. taskW 역할도 P 역할과 같은 방법으로 위임 역할을 만들고 생성되어진 빈 역할 P′와 taskW′는 I-계층에 의해서 하위 역할인 P와 taskW의 권한을 상속한다. 그리고 위임역할들은 처음 할당된 역할의 관계와 같이 A-계층으로 형성되고 이를 PL 역할과 다시 A-계층을 형성하여 권한을 위임한다.

2. 제안 모델의 IA-계층 하향 위임

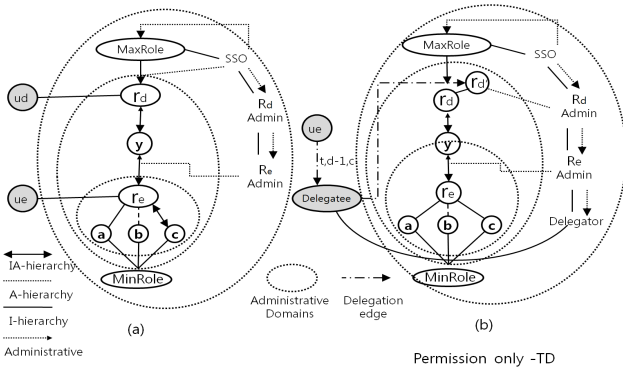

그림 3 제안 모델의 IA-계층 하향위임(권한)

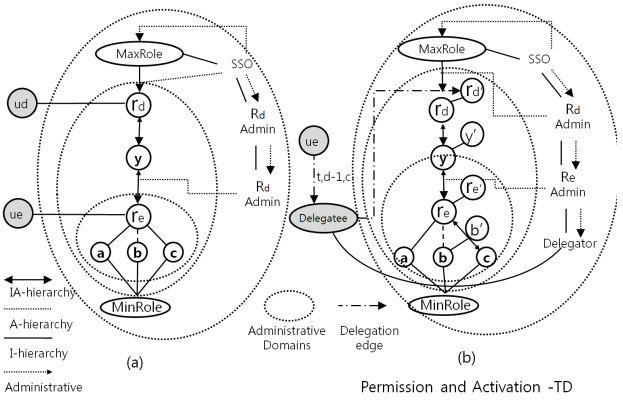

그림 4 제안 모델의 IA-계층 하향위임(활성화)

그림 3은 제안 모델의 IA-계층에서의 하향 위임을 보여준다. IA-계층에서의 위임은 두 가지 경우로 나눌 수 있는데, 첫 번째로 권한(활성화)위임이고(그림 3), 두 번째로 권한-활성화 위임이다. (그림 5) IA-계층의 경우 위임에

서 속성에 맞추어 IA-계층 자체 속성에 의한 위임과 I 또는 A 계층에 의한 속성에 따라 위임을 진행할 수 있다.

3. 제안 모델의 혼성계층 상향 위임

그림 5는 제안모델의 혼성계층 상향 위임이다. 그림 2의 상향 위임과 같은 방법으로 위임이 되지만 차이점은 다양한 계층을 지원한다는 점이다. 또한 Block assign을 통해 위임 기간 동안 전체 권한이 위임되는 것을 방지할 수 있으며, 혼성계층으로 역할계층의 유연성을 높일 수 있다.

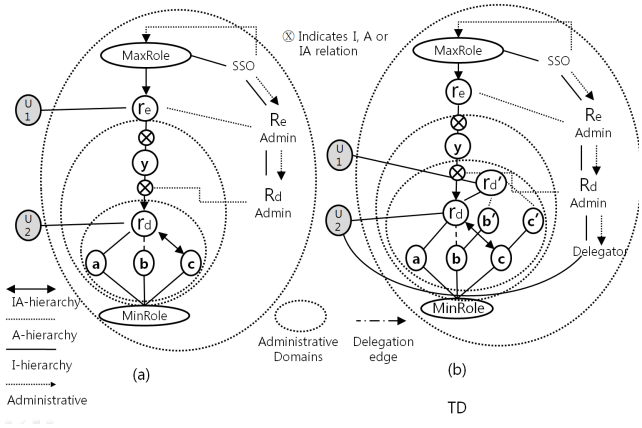

그림 5 제안 모델의 혼성계층 상향 위임

4. 제안 모델의 위임 취소

제안 모델에서 위임 취소의 기본동작은 위임 에지를 지우는 것이다. 위임 에지가 삭제되면 위임은 더 이상 존재하지 않게 된다. 위임 취소 스키마는 다음과 같은 동작으로 이루어진다. 먼저 취소를 요청한 사용자나 역할로부터 시작하여 위임 에지를 획득한다. 다음 위임 에지에 명시된 위임 깊이(d : depth)로부터 위임의 깊이를 획득하고 취소하고 싶은 만큼의 깊이를 삭제한다.

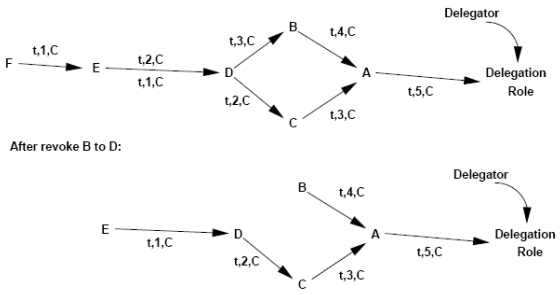

그림 6 제안 모델의 제한 깊이 위임 취소

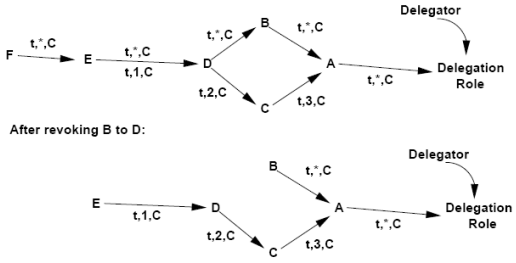

그림 7 제안 모델의 무한 깊이 위임 취소

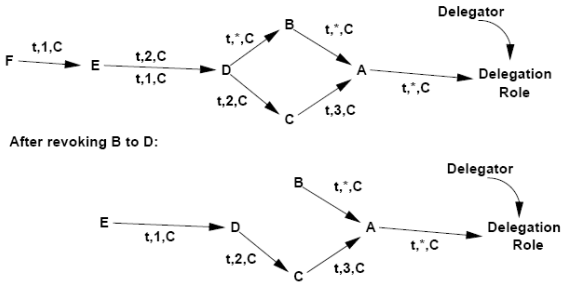

그림 8 제안 모델의 깊이 변화 위임 취소

그림 6은 정해진 깊이를 갖는 위임의 취소이다. 사용자 A는 B와 C에게 A의 권한을 위임하였다. 하지만 B로부터 시작된 권한 만 취소할 경우 B로부터 위임받은 D, E, F는 에지가 삭제되고 위임은 취소된다. 만약 깊이가 없다면 위임자로부터 시작된 에지를 삭제한다. 그림 7은 무한 깊이를 갖는 위임 취소를 보여준다. A는 그림 6과 마찬가지로 두 개의 위임 에지를 가지고 있지만, 마찬가지로 D 또한 두 개의 에지를 가지고 있다. 하지만 D 위임의 시작위치는 다르고 *(무한)위임을 갖는 속성과 제한 위임 속성을 갖는 에지를 갖기 때문에 무한 속성의 위임 쪽을 취소할 수 있게 된다. 그림 8은 무한 위임과 제한 위임의 두 가지 속성을 갖게 되는 경우의 취소이다. B는 무한 위임을 줄 수 있어도 문제가 생기지 않는 반면 D가 무한 위임을 하게 되면 문제가 발생하는 것을 고려해 D가 제한 위임을 갖게 되었을 경우, 에지 또한 다른 속성의 에지를 가져야 한다. D가 무한 위임을 하지 못하는 경우라면 당연히 제한 위임속성을 가지고 있어야 하고 에지에는 위임 깊이를 표시해야 하기 때문이다. 중요한 점은 E 또한 두 개의 에지를 가지고 있고 같은 제한 위임의 속성이지만, 위임이 시작된 위치가 다르고 위임이 시작된 곳으로부터의 깊이를 가지고 있기 때문에, B->D->E에 이르는 위임에지를 삭제할 수 있다.

3. 기존 모델과의 비교

본 논문에서 제안한 유비쿼터스 환경에서의 원격 의료 서비스 제공을 위한 접근제어 모델이 기존의 접근제어 모델과 다른 특징은 다음 표 1과 같다.

표 1. 기존 모델과의 비교표

Model	negative permission	user-to-user delegation	context based	partial delegation	role-to-role delegation	temporal delegation	Privacy
CA-RBAC [6]	x	o	o	x	x	x	x
A flexible Delegation Model in RBAC[7]	x	o	x	o	o	o	x
P-RBAC[8]	x	x	x	x	x	x	o
An Obligation Model[9]	x	x	x	x	x	x	o
proposed model	o	o	o	o	o	o	o

4. 결론

본 논문에서는 유비쿼터스 환경에서의 원격 의료 서비스를 위한 접근제어 모델에서의 위임을 위하여 사용자 대 사용자 위임, 역할 대 역할 위임, 다단계 위임, 다중 위임 등의 기능을 제공하는 위임 모델을 제안하였다. 따라서 본 논문에서 제안한 위임 모델을 원격의료 서비스를 위한 접근제어 모델에 적용하면 유비쿼터스 환경에서의 원격 의료 시스템을 사용하는 사용자의 프라이버시 보호 및 유동성 있고 세밀한 접근제어가 가능하게 된다.

참고문헌

[1] Ravi Sandhu., "Role-based access control." In Advances in Computers, Vol.46. Academic Press, pp. 237-286, 1998.

[2] R.S.Sandhu, E.J.Coyne, H.L.Feinstein, C.E.Youman., "Role-Based Access control Models", IEEE Computer, vol.29, 1996.

[3] David F. Ferraiolo, Janet A. Cugini, D. Richard Kuhn., "Role- based Access Control(RBAC) : Features and motivations", Proc. of 11th Annual Computer Security Application Conference, 1995.

[4] Matthew J. Moyer, Mustaque Ahamad., "Generalized Role-based Access Control", In IEEE International Conference on Distributed Computing Systems(ICDCS2001), pp.391-398, Mesa, Arizona, USA, April, 2001.

[5] Gustaf Neumann, Mark Strembeck., "An Approach to Engineer and Enforce Context Constraints in an RBAC Environment", Symposium on Access Control Models and Technologies(SACMAT 2003), pp. 65-79, June, 2003.

[6] Devdatta Kulkarni, Anand Tripathi, "Context-aware Role Based Access Control in Pervasive Computing Systems", Proc. 13th ACM Symposium on Access Control Models and Technologies (SACMAT 2008), pp.113-122, June, 2008.

[7] Dong Gue Park, You ri Lee, "A Flexible Role Based Delegation Model Using Characteristics of Permissions", Proc. 16th International Conference, DEXA 2005, pp.310-323, August, 2005.

[8] Qun Ni, Alberti Trombetta, "Privacy-aware Role Based Access Control", Symposium on Access Control Models and Technologies(SACMAT 2007), pp. 41-50, June, 2007.

[9] Qun Ni, Elisa Bertino, Jorge Lobo, "An Obligation Model Bridging Access Control Policies and Privacy Policies", Symposium on Access Control Models and Technologies(SACMAT 2008), pp. 133-142, June, 2008.

[10] Dong Gue Park, You ri Lee, Yu-dong Hwang, Seung-yeop Yoo, "The role-based access control model considering context and privacy," Korea Information and Communications Society, vol. 34, pp. 179-187, 2009.

[11] Dong-wook Shin, Yu-Dong Hwang, Dong-Gue Park, "Context awareness Access Control for Ubiquitous Environment," Korea Information and Communications Society, vol. 34, pp. 179-187, 2008.

[12] He Wang, Sylvia L. Osborn, "Delegation in the Role Graph Model", SACMAT, 2006.

[13] J. B. D. Joshi and E. Bertino "Fine-grained Role-based Delegation in Presence of the Hybrid Hierarchy", SACMAT, 2006.