한국산학기술학회논문지
Vol. 8, No. 2, pp. 250-256, 2007

분산환경에서의 권한필터링을 위한 접근제어 모델

심완보[1*], 민병석[1], 조태경[2]

An Access Control Model For The Authority Filtering in the Distributed Environment

Won-Bo Shim[1*], Byong-Seok Min[2] and Tae-Kyung Cho[3]

요 약 역할기반접근제어(RBAC)는 사용자나 네트워크상의 자원을 관리하는데 있어 오류를 최소화하기위해 가장 적합한 접근제어 모델로 인정되고 있다. 본 논문에서는 역할기반 접근제어기법을 응용하여 기존의 RBAC에 Role의 상위 개념인 워크(Work)개념을 도입한다. 워크개념을 이용하면 사용자는 자신의 업무를 수행시 역할(Role)이 아닌 좀더 추상적이고 포괄적 개념인 워크를 선택할 수 있게 된다. 워크는 사용자가 선택된 업무에 따라 정해지지만 정해진 워크에 따라 자신에게 부여되어 있는 권한이라 할지라도 현재 처리하고 있는 업무에 관련성이 없는 권한은 시스템적으로 차단되도록 하고자하는 방법을 제안한다.

Abstract Role-based Access Control (RBAC) model appears to be the most appropriate technique for access control to minimize the errors likely to occur in managing users and network resources. In this paper, we introduced the Work-concept RBAC model that is the result of the Work concept imported to the role based access control model. Using our extended access control model a user could select a work which is more abstract and more inclusive concept than role to do his work.
Additionally even if the user has an authority through selecting a work, if a user has no relation to his assigned job, it will be automatically prohibited.

Key Words : RBAC, access control model, work, security

1. 서론

Role 개념[2]은 사용자와 자원을 사용할 수 있는 권한 사이에 존재하는 매개적인 개념으로 정보시스템 내에서의 접근제어에 유용하게 사용될 수 있다. 그러나 이 Role 개념은 상위 Role이 하위 Role의 권한을 모두 상속받는다는 개념으로 인해 관리에 편리함도 주지만 많은 제약도 주는 것이 사실이다. 실제 정보시스템의 자원에 대한 접근제어를 구현함에 있어 이러한 Role의 수직적 개념도 필요하지만 수평적 개념[1][3][6]을 사용하여 문제를 해결할 수 있는 상황도 많이 발생하게 된다.

이 논문은 2006년 충청대학 산학협력진흥연구비의 지원에 의하여 연구되었음
[1]충청대학 디지털전자통신과
[2]상명대학교 정보통신공학과
*교신저자: 심완보(cool96@ok.ac.kr)

예를 들면 회사의 구조조정이라는 Task Force팀에 소속된 사용자가 회사의 구조조정이라는 업무를 수행한다고 하자. 이 업무는 회사의 여러 자료들을 사용해야만 수행될 수 있을 것이다. 하지만 회사의 자료들이 업무별로 분리되어 정보시스템상의 별도의 서버들에 의해 각각 분산되어 관리되고 있고 각각의 서버들의 정보자원은 RBAC에 의해 접근제어 되고 있다고 가정해 볼 수 있다.

이러한 상황에서 사용자는 자신의 업무를 수행하기 위해서는 기존의 각 서버가 갖는 수직적 구조에 대한 Integrity를 침해하지 않으면서 각 서버의 여러 복합적인 Role들의 권한을 가질 필요가 있게 된다. 이러한 개념을 본 논문에서는 워크(Work)[5]이라 부를 것이다. 이 논문에서는 이 워크개념을 이용해 분산 웹 환경에서 사용자가 여러 서버에 있는 Role의 권한을 수평적으로 가질 수 있게 하여 수직적 Role구조만을 갖는 RBAC운영에 융통성을 갖게 하고 이를 통해 사용자가 각각의 서버 내에 부여된 Role의 권한을 이용해 웹서버들에 대한 접근제어

를 받을 수 있도록 하고자 한다. 그렇게 되면 다른 서버에서 업무를 처리하기 위해 또 다시 각각의 서버에서 인증을 받아야 하는 부담 없이 복수개의 웹서버를 사용하는데 있어 사용자는 마치 하나의 웹서버에서 자원을 접근하고 있는 듯한 투명성을 제공할 받을 수 있게 될 것이다.

권한 필터링을 위한 접근제어 모델관점에서 기존의 관련 연구들을 살펴보면 다음과 같다.

Sandhu RBAC 모델[2]에서는 업무의 개념으로 역할을 사용할 수 있겠으나 역할은 바로 퍼미션으로 연결되기 때문에 업무의 개념으로 이용하기는 한계가 있다. TRBAC 모델[4]에서는 역할과 퍼미션 사이에 태스크의 개념을 사용하여 역할과 퍼미션 사이에 하나의 계층을 더 두어 역할을 제한적으로 업무의 개념으로 사용할 수도 있으나 권한을 필터링하는 기능은 없다. TMAC 모델[1]에서는 팀역할 개념을 업무의 개념으로 사용할 수 있겠으나 팀 내에는 다양한 업무가 존재하는데 이를 반영하기는 역부족이다. C-TMAC 모델[3]에서는 팀 역할 개념이외에 시간, 장소 등의 컨텍스트 정보를 추가하였으나 다양한 업무의 개념을 반영하기는 역시 역부족이다. 이상과 같이 기존의 RBAC 모델에서는 본 논문에서 제안하는 권한 필터링의 기능을 제공하는데 한계점을 보인다. 그러나 본 논문에서 제안하는 모델에서는 워크와 역할간의 관계를 적절히 설정해 줌으로 해서 서브워크로 구성되는 워크 개념을 도입해 팀내의 다양한 업무의 개념으로 사용할 수 있게 하고 이를 통해 최소권한의 원칙도 더욱 강화 되도록 하였다.

2. 워크개념을 이용한 권한 필터링

가. 워크개념의 개요

[그림1]은 워크개념을 이용한 필터링 모델을 보여준다.

워크에는 I-RWA에 의해 해당 워크를 수행 중에 활성가능한 역할들이 정해져 있어 사용자가 가진 역할 중에서 현재 수행하고 있는 워크에 관련된 역할 권한만을 활성화 할 수 있도록 역할 필터링(role filtering) 기능을 해준다.

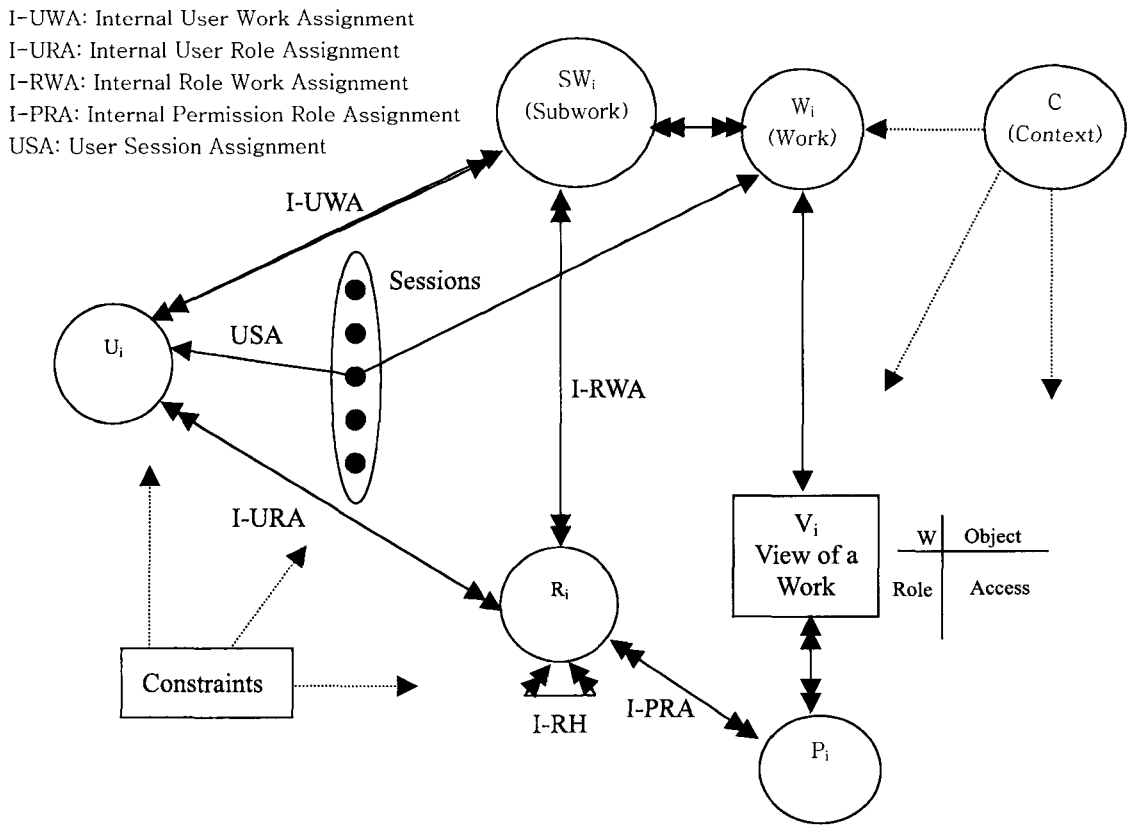


그림 1. 워크개념을 이용한 필터링 모델

여기서 워크를 통한 역할 필터링은 의무분리와는 다른 개념이다. 의무분리는 서로 이해관계에 있는 두 개의 역할을 한 사용자가 동시에 갖지 못하게 해 부정을 미연에 방지하고자 하는 목적인 반면에 여기서 워크 개념은 사용자가 여러 역할을 갖고 있다 하더라도 이를 현재 수행하는 업무에 관련된 역할만을 활성화가 시킬 수 있게 하는 Need-To-Know를 실현하기 위한 것이라고 할 수 있다.

이 개념을 이용하면 비록 의무분리 관계에 있지 않은 역할이라 하더라도 업무에 관계없이 필요 이상의 역할권한을 사용할 수 없게 해 최소권한의 원칙을 더욱 충실히 지원할 수 있다. 또한 업무를 선택하는 것만으로도 업무를 처리하기 위해 필요한 역할들을 모두 활성화시킬 수 있어 사용자 측면에서의 편이성을 제공받을 수 있다. 각 역할은 I-PRA에 의해 자원에 대한 퍼미션을 갖지만 여기서도 해당 워크에 따라 역할이 객체에 대해 갖는 접근권한을 매트릭스 형태의 뷰 기능을 제공해 보다 세밀한 접근관리가 가능하도록 한다.

여기서 제안하는 역할 모델은 역할기반 접근제어 모델을 기반으로 했기 때문에 일반적인 요구사항들은 모델에 반영되었다고 할 수 있다.

다음은 내부역할 모델에서 사용하는 워크와 역할의 관계를 나타낸 명제이다.

명제 1. 사용자는 자신에게 할당된 역할만을 활성화할 수 있다.

$$\forall u : users, r : roles$$
$$r \in active-roles(u) \Rightarrow u \in role-members(r)$$

명제 2. 사용자는 역할을 활성화해야만 역할에 할당된 Operation을 수행할 수 있다.

$$\forall u : user, op : operation :$$
$$exed(u, op) \Rightarrow active-roles(u) \neq \varnothing$$

명제 3. 사용자의 역할에 어떤 객체를 접근하기 위한 권한이 주어져 있고 그 역할이 사용자에 의해 활성화되어있을 때만 사용자가 그 객체에 접근하는 것이 가능하다.

$$\forall u : user, o : object :$$
$$access(u, o) \Rightarrow \exists r : roles, op : operation :$$
$$r \in active-roles(u) \wedge op \in role-operations(r, o)$$

명제 4. 역할에 대한 사용자 지정 수는 역할의 cardinality를 초과할 수 없다.

$$\forall r : roles :$$
$$number-of-members(r) \leq membership-\lim it(r)$$

명제 5. 어떤 사용자가 어느 한 역할에 할당을 받으면 그 사용자는 할당 받은 역할의 하위역할도 할당 받은 것으로 본다.

$$\forall u : user, r_{i,j} : roles$$
$$r_j \in authorized-roles(u) \wedge r_j \phi\ r_i \Rightarrow$$
$$r_i \in authorized-roles(u)$$

명제 6. 사용자는 자신에게 할당된 워크에 관계된 역할만을 활성화할 수 있다.

$$\forall u : users, r : roles, w : works$$
$$r \in active-roles(u) \Rightarrow u \in work-members(w) \wedge$$
$$r \in authorized-work-roles(w) \wedge u \in role-members(r)$$

나. 분산 환경에서의 워크개념

워크개념을 분산환경으로 확장하면 [그림2]와 같다.

SiteA, SiteB에는 각각 서로 다른 구조의 RBAC이 구축되어 있다. 워크는 다시 여러개의 서브워크로 나누어져 있으며, 각각의 서브워크들은 SiteA와 SiteB의 역할들에 연결되어 있다.

즉 Subwork1은 SiteA에서는 PE1의 역할을 갖고 있고 SiteB에서는 PL2'의 역할을 갖고 있게 된다. 반면 Subwork2는 SiteA에서는 QE1의 역할을 갖고 SiteB에서는 QE2'의 역할을 가질 수 있게 구성되어 있다. 이러한 서브워크들이 Work1에 속해 있게 된다.

이때 만일 사용자가 이러한 Work1의 권한을 부여 받는다면 사용자는 SiteA에서는 PE1의 권한을 갖고 자신의 업무를 수행해 나갈 수 있고, SiteB에서는 PL2'의 권한을 갖고 업무를 수행해 나갈 수 있을 것이다.

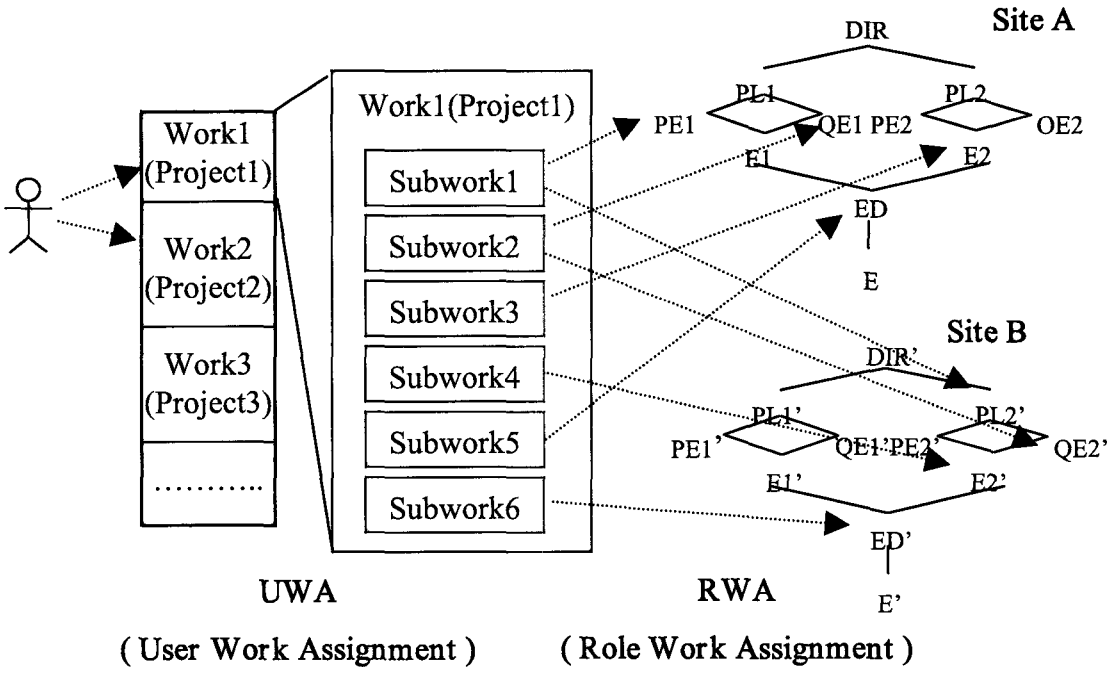


그림 2. 분산환경에서의 워크개념

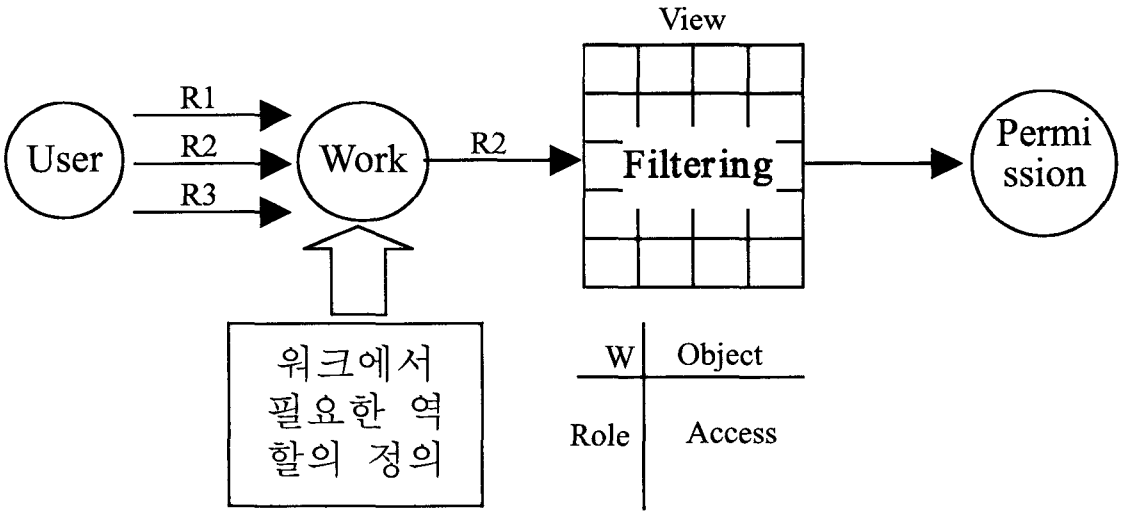
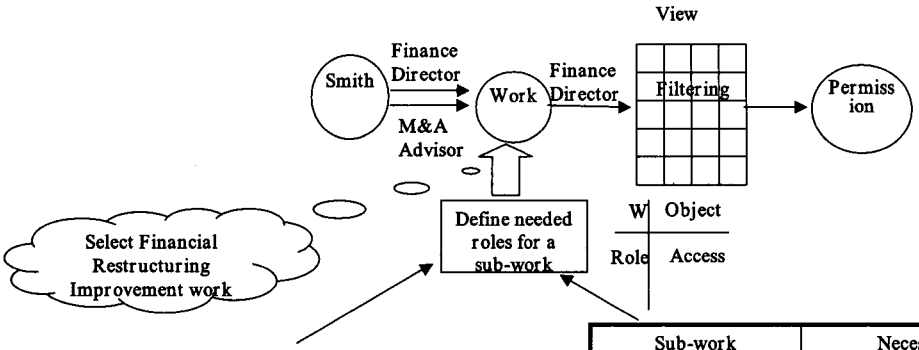


그림 3. 워크개념을 이용한 필터링

다. 워크개념을 이용한 권한 필터링

본 논문에서는 역할의 상위 개념인 워크개념을 도입해 사용자가 자신의 업무를 수행시 역할이 아닌 좀더 추상적이고 포괄적 개념인 워크를 선택할 수 있게 함으로 해서 선택된 워크에 따라 자신에게 부여되는 권한을 이용해 원활하게 업무를 수행할 수 있도록 하며 또한 이를 이용해 최소권한의 원칙이 더욱 충실히 지켜지도록 하는 방법을 제안한다. 다음은 이러한 워크 개념을 접근제어에 있어 역할 권한을 필터링하는 방법에 사용하는 예를 보인다.

[그림3]에서 사용자가 다수의 역할을 갖고 있다고 할 때 이 사용자의 역할을 통한 권한이 업무에 관련되어서



Sub-work	Necessary Roles
Accounting	Finance Director role
Debt	Debt Manager role, Finance Director role
Asset Management	Assets Manager role
Stock Management	Stock Advisor role, Assets Manager role

Sub-works of the Financial Restructuring Improvement work

Sub-work	Necessary Roles
Acquisition	Purchase Manager role, M&A Advisor role
Sale	Sale Manager role, Finance Director role
Public Relations	Relations Manger role
Law Suits	Law Advisor role, Assets Manager role

Sub-works of the Sale of Businesses work

그림 4. 워크개념을 이용한 필터링 예제

만 활성화될 수 있도록 할 필요가 있다. 사용자가 역할 R1, R2, R3를 갖고 어떠한 워크를 수행한다고 할 때 이 워크를 수행하는데 필요한 역할은 R2뿐이라면 사용자가 비록 R1, R2, R3 역할을 갖고 있다 할지라도 이 워크를 수행 중에는 R2만이 활성화될 수 있다. 또한 활성화된 R2도 R2에 부여된 모든 권한이 가능한 것이 아니라 주어진 워크에서 역할에 따른 객체들의 접근 허용 매트릭스에 정의된 접근만이 가능해 좀더 정밀한 객체접근을 하게 할 수 있다.

라. 워크개념을 이용한 권한 필터링 예

[그림 4] 워크개념을 이용한 필터링 예제를 보이고 있다. Smith는 팀내에서 역할 Finance Director, M&A Advisor를 할당받고 있고, 재무구조 개선 업무, 기업매각 업무를 수행하고 있다고 가정하자.

재무구조 개선 업무는 다음과 같은 서브워크로 나뉘어져 있고 각각의 서브워크에는 업무수행에 필요한 역할이 다음과 같이 할당되어 있다.

1) 회계업무 : Finance Director
2) 부채관련업무 : Debt Manager, Finance Director
3) 자산관리업무 : Assets Manager
4) 증권업무 : Stock Advisor, Assets Manager

기업 매각 업무는 다음과 같은 서브워크로 나뉘어져 있고 각각의 서브워크에는 업무수행에 필요한 역할이 다음과 같이 할당되어 있다.

1) 매수업무 : Purchase Manager, M&A Advisor
2) 매각업무 : Sale Manager, Finance Director
3) 섭외업무 : Relation Manager
4) 소송업무 : Law Advisor, Assets Manage

사용자는 I-UWA에 의해 서브워크에 할당된다. 그림 19에서와 같이 Smith가 I-UWA에 의해 재무구조 개선업무(Financial Restructuring Improvement work)의 서브워크인 회계업무(Accounting)와 기업매각 업무(Sale of Business work)의 서브워크인 매수업무(Acquisition)에 할당되어 있다고 가정하자.

시스템은 업무리스트에 서브워크 단위가 아닌 워크 단위로 보여줄 것이다. 이때 업무리스트에는 여러 개의 워크가 보이게 된다. 그러나 Smith는 회계업무 서브워크를 포함하는 재무구조 개선업무와 매수업무 서브워크를 포함하는 기업매각 업무만이 선택 가능하다.

두 가지 업무 중에서 Smith는 재무구조 개선업무를 선택했다고 하자. Smith가 재무구조 개선업무를 선택하면 Smith가 팀내에서 부여 받은 내부역할 Finance Director, M&A Advisor 역할 중에서 재무구조 개선업무에 필요한

Finance Director 역할만이 자동으로 활성화되고 M&A Advisor 역할은 재무구조 개선업무에는 관계가 없는 역할이므로 활성화되지 않는다. 이를 통해 Smith가 할당 받은 역할의 권한을 업무에 관련되어서만 사용할 수 있게 해준다.

3. 구현 및 평가

다음은 내부역할 모델에서 사용한 워크 개념을 도입한 RBAC 모델이 사용자가 자신의 업무를 처리하기 위해 동일 도메인 내에서의 복수개의 웹서버 접근제어를 위해 어떻게 사용될 수 있는지 프로토타입 시스템 구현을 통해 보이고자 한다. [그림 5]에 나타난 것처럼 multi 서버에 있는 웹문서를 접근할 때 사용자는 인증을 요구 받게 되고 인증에 성공을 하게 되면 사용자에게 부여된 워크들을 보여주게 된다.

이때 사용자는 자신에게 부여된 워크들 중에서 수행하고자 하는 워크를 선택하게 된다. 여기서는 사용자가 Project1이라는 워크를 선택한 것으로 가정한다. 워크가 선택되면 다음 화면에서는 해당 워크인 Project1의 서브워크들을 볼 수 있게 된다. 이 서브워크들은 궁극적으로는 각 서버에 있는 역할에 매핑되어 있기 때문에 이를 통해 사용자는 자신이 업무를 처리하는데 각 서버 내에서 필요한 역할권한을 확보하게 되는 것이다. 이때 사용자는 multi 서버내에서 최상위 권한을 갖기 때문에 Top Secret 영역을 포함하는 모든 웹 문서의 내용을 볼 수 있게 된다. 구현 내용을 분석해 보면, 분산 웹 환경에서는 대규모의 사용자와 웹 서버가 존재하게 되고 이때 이들에 대한 효율적인 접근제어가 필요하게 된다. 이에 현재 사용자와 네트워크상의 자원에 대한 관리상의 오류를 줄여 주고 관리비용을 감소시켜 줄 수 있도록 할 수 있는 접근제어의 가장 적합한 개념인 역할기반 접근제어기법에 워크개념을 도입한 RBAC 모델을 이용하여 동일 도메인 내에서 다수의 웹 서버들이 존재할 때 사용자가 이들 웹 서버를 사용하여 업무를 처리함에 있어 매번 각 서버의 웹 문서를 접근할 때마다 인증을 받아야 하는 불편을 없애 사용자가 불필요한 추가적인 인증 절차 없이 자신의 업무를 수행해 나갈 수 있는 방법을 제시했다. 또한 간단한 구현을 통해 타당성을 확인해 봄으로 해서 제안한 워크 개념을 도입한 모델이 웹 환경 하에서 시스템의 투명성을 제고 시켜 사용자의 효율적인 업무 수행을 가능하도록 할 수 있다는 것을 보였다.

4. 결론

본 논문에서는 현재 사용자와 네트워크상의 자원에 대한 관리상의 오류를 줄여 주고 관리비용을 감소시켜 줄 수 있도록 할 수 있는 접근제어의 가장 적합한 개념인 역

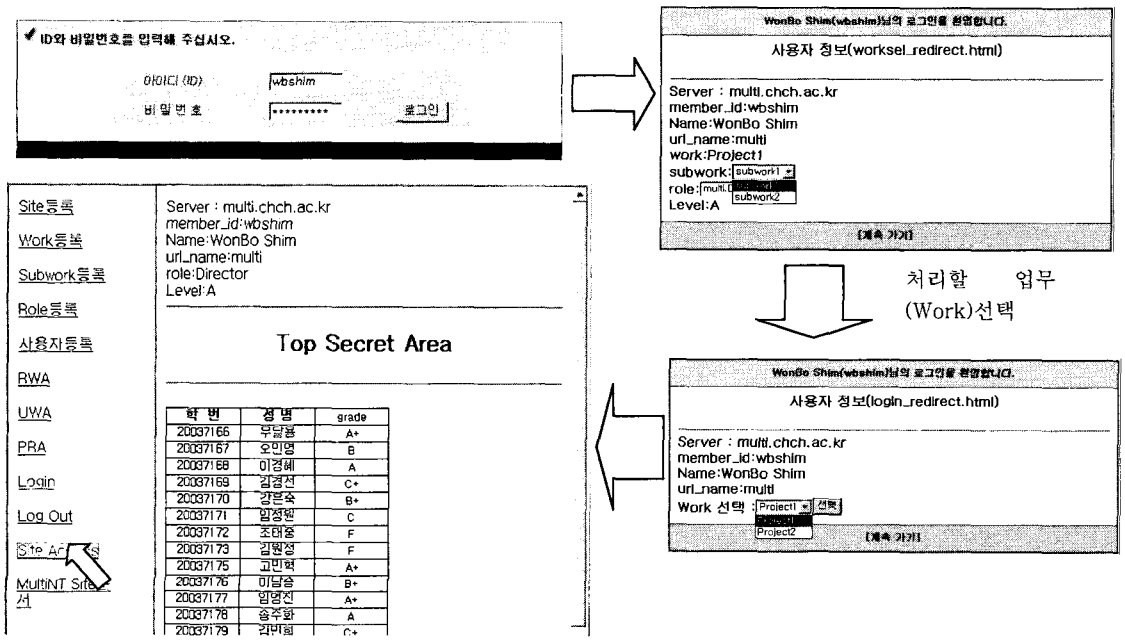


그림 5. 워크개념을 이용한 필터링 모델 구현

할기반 접근제어기법에 워크개념을 도입한 확장된 RBAC 모델을 제시하고 정의하였다. 이를 통해 사용자가 가지고 있는 역할을 통한 권한의 사용이 현재 수행중인 업무에 국한되어 사용할 수 있도록 권한 필터링을 할 수 있는 모델을 제안하였다. 워크개념을 이용해 팀 조직과 같이 팀원간의 관계가 상하간의 수직적인 구조보다는 상호 긴밀한 협력이 요구되는 수평적 조직에서 적절하게 사용될 수 있는 접근제어 모델을 제안해 보고 예제를 통해 모델의 타당성을 확인해 봄으로 해서 본 논문에서 제시한 워크개념을 도입한 RBAC확장 모델이 시스템의 투명성을 제고 시켜 사용자의 효율적인 업무 수행을 돕고 최소권한의 원칙을 충실히 하여 보안기능을 강화할 수 있다는 것을 보였다.

참고문헌

[1] Rosan K. Thomas, "Team-based Access Control (TMAC): A Primitive for Applying Role-based Access Controls in Collaborative Environments", ACM RBAC'97, pp. 13-19, 1997

[2] R. Sandhu, E. Coyne, H. Feinstein, and C. Younman, "Role-Based Access Control Models", IEEE Computer Magazine Vol. 29, pp. 38-47, 1996

[3] Christos K. Georgiadis, Ioannis Mavridis, G. Pangalos, Rosan K. Thomas, "Flexible Team-Based Access Control Using Contexts", Proc. of the 6th SACMAT, pp. 21-27, 2001

[4] Rosan K. Thomas, RaviSandhu "Task-based Authorization Controls (TBAC): A Family of Models for Active and Enterprise-oriented Authorization Management".11th IFIP Working Conference on Database Security, pp. 166-181, 1997

[5] Won Bo Shim, Seog Park, "The Work Concept RBAC Model for the Access Control of the Distributed Web Server Environment", LNAI (Lecture Notes in Artificial Intelligence) Vol. 2198, pp.262-266, 2001.10

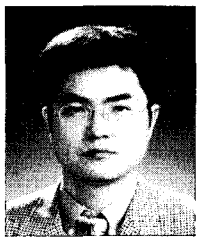
[6] 심완보, 박석, "애드호크러시 조직의 특성을 고려한 역할기반 모델", 한국정보보호학회논문지 12권4호, pp. 41-53, 2002.8

[7] Ravi Sandhu and Joon S. Park,"Secure Cookies on the Web", IEEE Internet Computing, pp. 36-44, 2000.7

[8] NIST SP 800-53, "Recommended Security Controls for Federal Information Systems", Public Draft, Revision 1, 2006. 3

[9] NIST SP 800-53A, "Guide for Assessing the Security Controls in Federal Information Systems", Second Public Draft, 2006. 4

심 완 보(Won-Bo Shim) **[정회원]**



- 1985년 2월 : 한양대학교 전자공학과 (공학사)
- 1986년 5월 : 스티븐스공과대학 전산과학과 (이학석사)
- 2003년 2월 : 서강대학교 컴퓨터학과 (공학박사)
- 1995년 9월 ~ 현재 : 충청대학 디지털전자통신과 부교수

<관심분야>
인터넷보안, 유비쿼터스시스템, 임베디드시스템

민 병 석(Byong-Seok Min) **[정회원]**

- 1990년 2월 : 한양대학교 전자통신공학과 (공학사)
- 1992년 8월 : 한양대학교 전자통신공학과 (공학석사)
- 2002년 8월 : 한양대학교 전자통신공학과 (공학박사)
- 2003년 7월 ~ 2004년 7월 : 캐나다 앨버타대학교 전자 및 컴퓨터공학과 박사후 연수
- 1995년 3월 ~ 현재 : 충청대학 디지털전자통신과 부교수

<관심분야>
영상처리, 영상통신, 멀티미디어통신

조 태 경(Tae-Kyung Cho) **[종신회원]**

- 1984년 : 한양대학교 전자통신공학과 (공학사)
- 1986년 : 한양대학교 대학원 전자통신공학과 (공학석사)
- 2001년 : 한양대학교 대학원 전자통신공학과 (공학박사)
- 현재 : 상명대학교 정보통신공학과 교수

<관심분야>
초고속통신망, e-Learning