제 18 회 한국정보처리학회 추계학술발표대회 논문집 제 9 권 제 2 호 (2002.11)

웹 기반 협업 시스템의 문서 보안

김양석, 강주미, 원용관
전남대학교 컴퓨터공학과
e-mail : horangin@grace.chonnam.ac.kr

Document Security for Web-Based Collaboration System

Yang-Suk Kim, Ju-mi Kang, Yong-gwan Won
Dept. of Computer Engineering, Chonnam national University

요 약

인터넷 이용의 확산과 컴퓨팅 환경이 급속히 변화되면서 특수 소수 그룹의 구성원들 간의 정보 공유와 재사용을 지원하는 웹 기반 협업 시스템 개발이 고조되고 있다. 하지만 이러한 웹 기반 협업 시스템들은 시스템 사용자 인증만의 절차에 의한 특수 소수 그룹간에 정보를 공유하고 있어 인가된 사용자를 가장한 악의의 사용자에 의한 정보의 삭제, 수정, 파괴 등의 불법적인 행동을 막을 수 없을 뿐만 아니라 민감한 정보의 공유는 더욱더 어렵게 했다. 따라서 본 논문에서는 이러한 문제점을 해결 하기 위해 웹 기반 협업 시스템의 성격을 고려한 유연성 있는 보안정책과 보안모델을 바탕으로 소 그룹단위로 을 제어할 수 있는 접근제어와 민감한 정보의 불법적인 접근을 제어 할 수 있는 접근제어 시스템을 제안한다.

1. 서론

인터넷과 하드웨어의 발전에 힘입어 현재의 컴퓨팅 환경은 과거의 컴퓨팅 환경 보다 복잡해지고 다양한 환경에서 실행 되는 분산 환경으로 발전 되고 있다. 따라서 사용자 들은 더욱더 가상 공간에서 서로 정보를 공유하고 협력할 수 있는 시스템 개발을 요구하게 되고, 그 결과 많은 협업 시스템(Collaboration System)들이 개발 되었다. 지금까지 개발된 협업 시스템들로는 BSCW(Basic Support Cooperative Work), DOMINO (IBM), NETFINDER (APPLE), Wiki 등이 있다[1]. 이러한 협업 시스템들은 여러 사용자들이 쉽게 정보를 공유하고 재사용할 수 있으나 인가된 사용자임을 가장한 악의의 사용자들에 의한 정보(Sensitive Information)의 삭제, 수정, 파괴 등의 불법적인 행동을 막을 수 없다. 따라서 정보보호 측면의 중요한 요소인 기밀성(Confidentiality), 무결성(Integrity), 가용성(Availibility)의 위배를 가져온다. 따라서 본 논문에서는 웹 기반 협업 시스템들 상에서 공통작업문서를 보호하기 위한 효율적인 보안정책을 세우고, 보안모델을 설계하여 유연성(Flexibility) 있는 접근제어(Access Control)시스템을 제안한다. 본 논문의 구성으로 2 장에서 접근통제 시스템을 설계하기 위한 보안모델 과 기존에 연구되었던 접근제어 방법, 3 장에서 제안된 접근제어 시스템의 설계 , 4 장에서 제안된 접근제어시스템 구현 및 결과를 알아보고 5 장에서 결론을 맺는다.

2. 관련연구

접근제어(Access Control)란 인가된 사용자의 정보를 확인한 후에 그 사용자의 접근권한(Access Right)을 확인하고, 사용자가 어떤 기능을 사용할 수 있는지 그 여부를 판단하여 권한을 할당한다[2]. 보안 모델의 기본적인 구성으로 주체(Subject), 객체(Object), 접근권한(Access Right)으로 구성된다. 주체(Subject)는 일반적으로 사용자나 프로세스(Process)와 같이 능동적인 개체(Entity)를 말하며, 객체(Object)는 파일과 같이 수동적인 개체를 말한다. 접근권한(Access Right)은 하나의 주체(Subject)에 의해서 액세스(Access)는 방법이다[3].

2.1 Access Control Matrix 모델

Access Control Matrix(ACM) 보안 모델은 주체(Subject)와 객체(Object) 간에 허가된 접근권한에서 주체를 행(row)으로 객체를 열(Column)로 하여 테이블로 나타낸 보안 모델이다. [그림 1]은 접근권한 관계를 하나의 테이블로 나타낸 것 이다. [그림 1]에서 하나의 예를 들어서 접근제어의 흐름을 살펴보면 User1 은 File_1 에 대해서 아무런 권한이 없으나 File_2 에 대해서는 execute(실행) 권한을 그리고, File_3 에 대해서는 execute(실행), read(읽기) 권한을 갖고 제어 됨을 알 수 있다[4][5].

	File_1	File_2	File_3
User1	-	{execute}	{execute,read}
User2	{read,write}	{execute}	-

[그림 1] ACM 테이블

2.2 임의적 접근제어 (Discretionary Access Control)

임의적 접근 제어는 주체(Subject)의 신분(Identify)에 근거하여 객체(Object)에 대한 접근을 제어한다. 지금까지 연구된 일반적인 특징은 다음과 같이 요약된다 [6][7].

- 허가된 주체에 의해 변경 가능한 하나의 주체와 객체간의 접근권한 관계를 정의한다.
- 한 주체(Subject)가 한 객체를 읽고 그 내용을 다른 한 객체로 복사하는 경우 처음 객체에 내포된 접근권한이 복사된 객체로 전파(Propagate)되지 않는다.
- 모든 주체와 객체들간에 일정하지 않고 하나의 주체/객체 단위로 접근권한을 설정한다

2.3 강제적 접근제어 (Mandatory Access Control)

강제적 접근제어(MAC)는 주체에 허용된 접근수준과 객체에 부여된 허용 등급에 따른 접근제어를 한다. MAC 의 일반적인 속성은 다음과 같이 요약 된다[4].

- 객체의 소유자에 의해서 변경할 수 없는 한 주체와 한 객체간의 접근제어 관계를 정의한다.
- 최초의 객체에 내포된 접근권한이 복사된 객체로 전파 (Propagate)되지 않는다
- 모든 주체 및 객체에 대해서 일정하고, 하나의 주체 및 객체단위로 접근권한 설정이 불가피 하다.

3. 접근제어 시스템 (Access Control system) 설계

본 장에서는 웹 기반 협업 시스템에서 악의의 사용자의 불법적인 정보의 삭제, 수정, 파괴를 막을 수 있는 제안된 보안정책, 보안모델을 적용한 접근제어 시스템을 설명한다. 3.1 절은 웹 기반 협업 시스템상에서 사용자의 민감한 정보의 보호를 위해 요구되는 접근제어 시스템이 갖추어야 할 사항들을 기술하고, 3.2 절에서 요구사항에 맞는 보안 정책을 제안하며, 3.3 절에서 보안정책을 적용 하기 위한 보안모델을 설계한다. 그리고 3.4 절에서 보안모델을 적용한 전체 시스템 구조, 마지막으로 3.5 절에서는 전체시스템 중요한 모듈별 기능을 알아본다. 본 논문에서 사용되는 정보, 공통작업 문서, Page 는 같은 의미를 갖는다.

3.1 접근제어 요구사항

웹 기반 협업 시스템들이 갖는 문제점을 해결하기 위해서 제안하고자 하는 접근제어 시스템이 갖추어야 할 요구사항 들은 다음과 같다.

- 보안정책의 모든 것을 관리 할 수 있는 사용자와 각각의 사용자를 그룹으로 관리 할 수 있는 사용자과 그리고 일반 사용자가 있어야 한다.
- 접근제어 시스템을 총 관리하는 사용자와 그룹을 관리 할 수 있는 사용자는 인원이 제한 되어야 한다.
- 접근제어 시스템을 총관리 할 수 있는 사용자는 는 모든 사용자의 정보에 대해서 읽기, 쓰기, 삭제가 가능하여야 한다.
- 그룹을 관리 할 수 있는 사용자는 자기가 속한 그룹의 정보에 대해서만 읽기(Read), 쓰기(Write), 삭제(Delete)가 가능하여야 한다.
- 사용자가 직접 생성한 정보는 그 사용자만이 정보를 읽기, 쓰기, 삭제가 가능하여야 하여야 한다.
- 모든 사용자들의 정보 보호를 위해서 악의의 사용자들의 불법적인 행동을 접근제어 시스템을 통해서 제어 할 수 있어야 한다.

3.2 접근 제어 보안정책

요구사항에 맞는 보안정책을 수립하기 위해서는 접근제어의 기본적인 구성요소 인 주체(Subject), 객체(Object) , 접근권한(Access Right)이 명시 되어야 한다. [그림 2]는 이러한 접근 제어 구성요소를 명시한 테이블이다.

주체(subject)	객체(Object)	접근권한(Access Right)
사용자(User) 그룹(Group)	웹 기반 협업 시스템상에서 공유 하고자 하는 모든 공용 작업문서	읽기(Read), 쓰기(Write), 삭제(Delete)

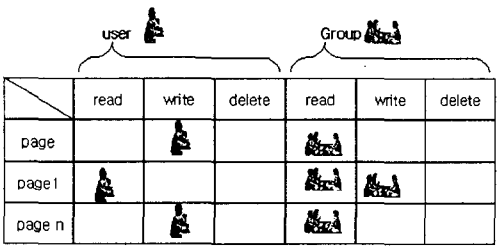
[그림 2]접근 제어 구성 테이블

그리고, 접근제어 구성 테이블을 바탕으로 효과 적인 보안정책을 세워야 한다. 접근제어 시스템의 보안 정책은 다음과 같다.

- 주체(Subject)의 구성요소의 모든 사용자는 접근제어 시스템의 총관리자에 의해 임의의 그룹에 속해야 한다.
- 주체(Subject)의 구성 요소인 그룹의 구성은 총관리할 수 있는 총관리자 그룹, 그룹을 관리할 수 있는 그룹관리자그룹, 일반 사용자들의 그룹인 일반그룹으로 구성되어야 한다.
- 만일 특정한 그룹에 속한 사용자가 다른 그룹과의 정보의 공유를 원한다면 총관리자에 의해 특수(Special)그룹에 할당되어야 한다.

3.3 접근제어 모델

본 절에서는 사용자 및 그룹 목록 기반의 접근제어 모델을 소개한다. 2.1 절의 기존의 Access Control Model 은 사용자가 증가 하였을 경우 복잡한 보안메커니즘이 필요로 한다. 보안메커니즘이 복잡하다는 것은 오히려 보안에 악영향을 미칠 수 있다. 따라서 정보보호 측면의 기밀성(Confidentiality), 무결성(Integrity), 가용성(Availibility)을 보장 하기 어렵다. 본 논문에서는 제안된 모델은 3.2 절에서 명시한 보안 정책(Security Policy)을 바탕으로 사용자의 증가에 대비하고 그룹으로 관리 할 수 있다. [그림 3]은 정보(공통작업문서 또는 Page)를 행(Column)에 그리고 사용자와 그룹의 접근권한(읽기, 쓰기, 삭제)을 열(Row)에 둔 보안 모델이다. 즉, 각각의 중요한 정보에 사용자와 그룹을 할당하여 접근을 통제하는 모델이다. 따라서 웹 기반 협업 시스템의 특성에 따라 사용자와 그룹으로 관리할 수는 유연성(Flexibility)을 가지게 된다. 또한 보안 메커니즘면에서 단순한 접근제어 시스템을 구축할 수 있게 된다.



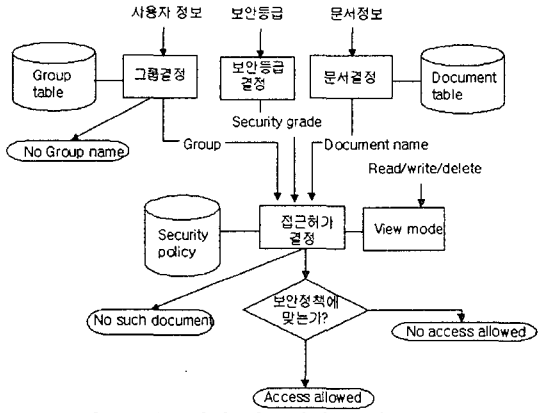
[그림 3] 사용자와 그룹 목록기반의 테이블

3.4 접근제어 시스템 전체 구조도

사용자와 그룹목록 기반의 Access Control Model 을 적용한 제안된 접근제어 시스템의 시나리오는 다음과 같다.

- 인가된 사용자가 웹 기반 협업 시스템에 정보의 접근을 요청한다.
- 요청된 사용자가 어느 그룹에 할당 되었는지 검색한다. 만일 그룹이 없으면 거부한다.
- 해당하는 그룹이 있으면 보안 정책 테이블에서 그룹에 할당된 접근권한(Access Right)을 참조하여 공통작업 문서의 접근 여부를 결정한다.

[그림 4]는 위의 시나리오 흐름을 가지고 웹 기반 협업 시스템상에서 접근제어(Access Control)를 할 수 있는 접근제어시스템(Access Control System)전체 구조도를 나타낸다. [그림 4]의 전체 구조를 보면, 사용자를 그룹(Group)화하는 그룹결정 모듈과 모든 공통작업문서에서 접근제어를 적용할 문서를 선택 할 수 있는 문서결정 모듈, 그리고 그룹 안에서도 권한이 다른 등급을 주기위한 보안등급 결정모듈로 구성된다. 또한, 이러한 각 모듈들은 입출력 정보를 필요로 한다. [그림 5]는 그룹의 정보를 가지고 있는 Group Table 과, 공통작업문서의 정보를 담고 있는 Document Table, 접근권한(Access Right)을 가지고 있는 Security Table 의 간단한 설명을 나타낸 표이다.



[그림 4] 접근제어 시스템의 전체 구조도

Group table

Object	Type	Description
Group Name	Varchar	그 룹 이 름
User_InGroup	varchar	그룹에 배정된 사용자
Group_Manager	varchar	그룹 관리자

Document table

Object	Type	Description
PageName	Varchar	공통작업문서이름
PageContent	text	공통작업 문서내용
Author	varchar	공통 작업문서 생성자

Security table

Object	Type	Description
PageName	Varchar	공통작업 문서
Read	varchar	사용자의 읽기 권한
Wrtie	Varchar	사용자의 쓰기 권한
Delete	Varchar	사용자의 삭제 권한
Group_read	Varchar	그룹의 읽기 권한
Group_write	Varchar	그룹의 삭제 권한
Group_delete	Varchar	그룹의 삭제 권한

[그림 5] Group , Document ,Security table 정보

3.5 주요 기능 모듈

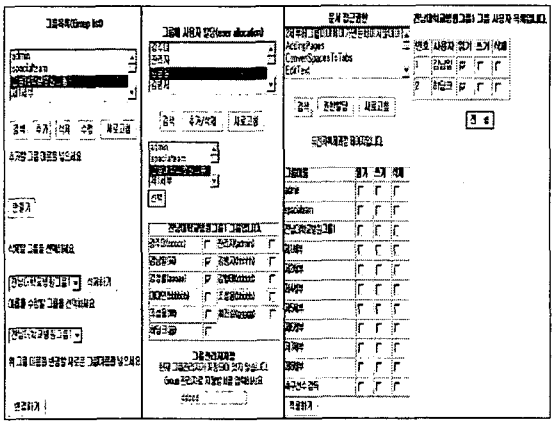
3.4 의 접근제어 시스템(Access Control System)의 전체 구조에서 본 바와 같이 중요한 모듈은 그룹 결정 모듈과 보안등급 결정 모듈 그리고, 문서결정 모듈이다. 각각의 중요 모듈들은 다음과 같은 기능들을 수행한다.

- 그룹결정모듈은 새로운 그룹을 생성하거나 그룹의 이름을 변경할 수 있고, 추가 할 수 있다.
- 보안등급결정 모듈은 접근제어 시스템의 각 그룹의 관리자를 결정한다.
- 문서결정모듈은 공통작업 문서정보에서 어떤 사용자의 정보(즉,공통 작업문서)를 보호할 것인지 선택한다.
- View 모듈은 각 그룹에 또는 그룹의 특정한 사용자에게 접근권한(Access Right) 즉, 읽기,쓰기,삭제 권

한을 할당 한다.

4. 구현 및 결과

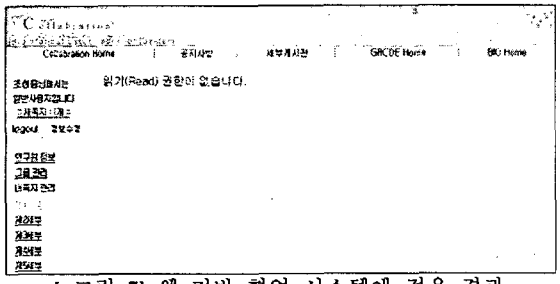
지금까지 요구사항과 보안정책 그리고, 보안모델을 적용하기 위한 사용자와 그룹 목록 기반의 접근제어 시스템(Access Control System)에 대해서 살펴보았다. 본 장에서는 접근제어시스템의 구현 및 웹 기반 협업 시스템에 적용된 결과를 보인다. [그림 6]은 실제 그룹을 생성,추가,삭제 할 수 있는 그룹 결정 모듈 과 그룹의 보안등급을 줄 수 있는 보안등급 결정 모듈 부분,사용자의 정보(즉, 공통작업 문서)에 대해서 접근권한(Access Right)을 주는 문서결정 모듈 부분을 각각 (a),(b),(c)에 보인 그림이다.



(a) (b) (c)

[그림 6] 접근제어시스템의 인터페이스

[그림 7]은 웹 기반 협업 시스템에서 본 논문에서 제안한 접근통제시스템을 적용하여 어떤 사용자가 '읽기' 권한이 없는 정보(웹 페이지)에 접근하려 한 경우 접근이 금지된 결과를 보여주고 있다.



[그림 7] 웹 기반 협업 시스템에 적용 결과

제안된 접근제어 시스템을 웹 기반 협업 시스템에 적용한 결과, 기존의 Access Control Matrix 모델의 접근제어 메커니즘 보다 간단하고, 그룹 개념을 도입하여 더 효율적이고 유연성(Flexibility) 있는 접근제어를 수행할 수 있다. 또한 본 논문에서 제안한 접근제어시스템은 협업 환경에서 소 그룹 단위의 접근제어 및 민감한 정보(Sensitive Information)의 보안에도 적용이 가능하다.

5.결론 및 향후 연구 방향

기존 웹 기반 협업 시스템(Web Based Collaboration System)에서는 시스템 사용자 인증만의 절차로 악의의 사용자에 의한 정보의 삭제, 수정, 파괴 등의 불법적인 행동을 가져왔다. 따라서 웹 기반 협업 시스템상에서 민감한 정보의 공유 및 소 그룹단위의 정보 공유가 어려웠다. 이러한 문제점을 해결하기 위해서 본 논문에서는 사용자와 그룹목록 기반의 접근제어시스템(Access Control System)을 제안하고 웹 기반 협업 시스템에 적용한 결과 더 효과적이고 유연(Flexibility)하게 접근 통제(Access Control)를 할 수 있었다. 앞으로 연구되어야 할 것은 하나의 정보 (즉, 공통작업 문서) 안에서 각 사용자 또는 사용자 그룹별로 문서의 부분적 접근제어를 제공하는 기법을 개발 하는 것이다.

참고문헌

[1]R.Bentley, "Basic Support for Cooperative Work on the Word Wide Web", International Journal of Human Computer Studies, 1997.

[2]Ravi S.Sandhu* and Pierangela Samarati, "Access Control: Principles and Practice", IEEE Communications, Volume 32, Number 9/September 1994.

[3]최용락, 소우영, "통신망 정보보호" 1997.

[4]홍승필, 고제욱, " 정보보안 기술과 구현", 1998.

[5]C.Eckert, "On Security Models", International Conference on Information Security, 1996.

[6]S.Osborn, "Mandatory Access Control and Role-based Acces Control Revisited", In Proceedings of the second ACM workshop on Role Based Access Control ACM, 1997.

[7]D.D Downs, "Issues in Discretionary Access Control", Proceedings of IEEE Symposium on Security and Privacy, pp 208-218, 1985.