

WebDAV 기반 협업시스템 접근 제어 설계

변상희⁰, 박희중, 박양수, 이명준
울산대학교 컴퓨터정보통신공학부
(heeya⁰, heejong34, yspk56, mjlee)@ulsan.ac.kr

Design of an Access Control for WebDAV-based Collaborative System

Sang-Hee Byun⁰, Hee-Jong Park, Yang-Su Park, Myung-Joon Lee
School of Computer Engineering & Information Technology, University of Ulsan

요 약

WebDAV(Web-based Distributed Authoring and Versioning)는 웹 통신 프로토콜로서 인터넷을 통하여 다양한 콘텐츠의 비동기적인 협업 저작을 지원한다. 따라서 WebDAV를 지원하는 다양한 종류의 서버들은 상호간의 협업 작업이 가능하다. 특히 WebDAV의 접근 제어 프로토콜은 특정 자원에 대한 접근 제어 권한을 정의하기 위하여 표준 Privilege들을 정의하고 있다.

본 논문에서는 웹기반 협업시스템의 핵심 기능인 팀 작업장과 공개 작업장의 자원에 접근할 때, 사용자의 권한과 작업장의 특성 그리고 자원의 특성에 따라 접근 제어 관리를 할 수 있도록 접근 제어 기법을 설계하였다. 특히 공개 작업장은 파일 올리기만 가능한 작업장, 내려받기만 가능한 작업장, 올리기/내려받기 가능한 작업장과 같이 성격이 다양하다. 이를 지원하기 위하여 작업장내 파일에 대한 접근 권한을 구체적으로 설계함으로써 협업작업을 체계적이고 안정적으로 지원할 수 있다.

1. 서 론

최근 인터넷 사용이 기하급수적으로 증가하면서 웹에 관련된 신기술과 소프트웨어의 개발속도가 급격히 빨라졌다. 이러한 발전 추세는 통신망의 역할을 새롭게 변화시키고 있으며, 또한 웹을 이용한 응용분야도 급속도로 확대되고 있다. 웹이 가 는 다양한 장점은 기업 및 공공기관과 같은 조직 내의 정보를 효율적으로 활용하기 위한 협업시스템을 구축하는 다양한 기술들이 개발되었다.

초기 협업시스템은 HTTP(가)yperText Transfer Protocol) 프로토콜을 활용하거나 또는 각자의 고유 프로토콜들을 HTTP 프로토콜에 추가 정의하는 형태로 구현하였다. 이러한 방법은 공급업체들 간의 상호 운용성이 결여되는 문제를 발생시켰다. 협업시스템들 간의 상호 운용성을 보장하기 위한 웹 기반의 분산 저작과 버전관리 표준의 필요성이 증가되었고, 이러한 요구를 충족시키기 위하여 W3C(가)World Wide Web Consortium)의 IETF 산하의 작업 그룹에 의해서 WebDAV 명세가 1999년 2월에 발표되었다[1].

WebDAV는 HTTP를 확장한 웹 통신 프로토콜로서 인터넷을 통하여 다양한 콘텐츠의 비동기적인 협업 제작을 원하기 위한 표준 하부구조를 제공한다. WebDAV 명세를 원하는 다양한 종류의 서버들은 상호간의 협업 작업이 가능하게 되었다[2,3].

본 논문에서는 효율적인 공동작업을 위하여 시스템 관리자(가)Administrator), 팀 생성자(가)Team Author), 팀 관리자(가)Team Manager), 사용자(가)User), 시스템에 소속된 많은 사용자(가)Guest)의 역할을 정의하고 각각의 역할에 대한 권한 및 WebDAV에서 원하는 접근 제어 프로토

콜(가)Access Control Protocol)을 이용하여 자원 공유, 협업그룹(가)팀)의 생성과 관리 등의 접근 제어 기법을 설계하였다.

본 논문의 구성은 다음과 같다. 서론에 이어 2장에서 관련 연구를 통하여 WebDAV와 웹 기반 협업시스템인 iPlace[4,5]에 대하여 살펴보고 3장에서는 실제로 설계한 WebDAV 기반의 협업시스템 접근 제어 방법에 대하여 설명한다. 끝으로 4장에서는 결론 및 향후 연구과제에 대하여 기술한다.

2. 관련연구

2.1 WebDAV

WebDAV는 인터넷을 통하여 광범위하고 다양한 콘텐츠의 비동기적인 협업 저작을 원하기 위한 프로토콜이다. WebDAV는 HTTP 프로토콜의 확장을 통하여 사용자들에게 원격 서버들의 파일들을 수정하고 관리할 수 있도록 한다. 특히 WebDAV의 접근 제어 프로토콜은 WebDAV 서버에 의해 관리되고 있는 자원의 특징에 따라 접근 제어 관리를 할 수 있도록 기능이 확장되었다.

WebDAV 접근 제어 프로토콜 및 WebDAV 메서드를 수행하기 위해 설정되어야하는 권한들에 대해서 살펴본다.

2.1.1 WebDAV 접근 제어 프로토콜 용어

WebDAV 접근 제어 프로토콜의 이해를 돕기 위하여 주요 용어들은 다음과 같다.

- **Principal** : 사용자가 누구(가)UserID)이며 어떤 그룹

† 본 연구는 한국과학재단 목적 기초연구(가)05-2004-000-10662-0)의 원으로 수행되었음.

그룹)에 속하여 있는 그룹을 정의한다.

- **Group** : 공통된 권한을 갖는 사용자들을 대표할 수 있는 Principal을 의미한다.
- **Privilege** : 서버에서 관리되는 자원을 관리하기 위한 접근 제어 권한을 정의한다.
- **ACE (Access Control Element)** : 특정 자원에 대한 Privilege들의 권한을 부여(grant) 또는 거부(deny) 여부를 정의한다.
- **ACL (Access Control List)** : 특정 자원에 대한 접근 제어를 정의한 ACE의 리스트를 의미한다.

2.1.2 표준 Privilege

특정 자원에 대한 접근 제어 권한을 정의하기 위하여 WebDAV에서는 표준 Privilege를 정의하고 있다. [표 1]은 WebDAV에서 제공하는 10개의 표준 Privilege를 보여 준다. 사용자는 이러한 기본 Privilege들을 이용하여 사용자가 필요로 하는 새로운 Privilege를 정의할 수 있다.

[표 1] 표준 Privilege

PRIVILEGE	설 명
read	파일 또는 디렉토리의 내용을 읽을 수 있는 권한
read-acl	ACL 속성을 읽을 수 있는 권한
read-current-user-privilege-set	현재 사용자에게 주어진 privilege들을 읽을 수 있는 권한
write	파일의 속성과 내용을 쓰거나 수정할 수 있는 권한(lock설정 가능)
write-properties	파일의 속성을 변경할 수 있는 권한
write-content	파일의 내용을 수정할 수 있는 권한
write-acl	ACL 속성을 수정할 수 있는 권한
bind	디렉토리를 생성하거나 디렉토리의 내용을 추가, 수정할 수 있는 권한
unbind	디렉토리를 이동, 삭제할 수 있는 권한
unlock	lock설정이 되어있는 파일 또는 디렉토리를 unlock 시킬 수 있는 권한

2.1.3 WebDAV 메서드와 Privilege의 관계

WebDAV는 서버에 존재하는 자원의 특징에 따라 접근 제어 관리를 위하여 WebDAV 메서드들의 사용여부를 정의한다. WebDAV 메서드 사용 여부를 결정하기 위해서는 메서드와 관련된 특정 Privilege들이 요구된다. 파일을 저장하기 위하여 WebDAV의 GET 메서드를 호출하고자 한다면 사용자에게 read 권한이 주어져 있어야 한다. [표 2]는 이와 같은 WebDAV 메서드를 수행하기 위하여 사용자에게 주어질 수 있는 Privilege들을 보여주고 있다.

2.2. iPlace 협업시스템

iPlace 시스템은 공동작업을 수행하는데 필요로 하는

[표 2] WebDAV 메서드와 관련된 Privilege

METHOD		PRIVILEGE
GET		read
PUT	파일	write-content
	디렉토리	bind
PROPPATCH		write-properties
ACL		write-acl
PROPFIND		read-acl + read-current-user-privilege-set)
COPY	파일	read, write-content, write-properties
	디렉토리	read, bind
MOVE		unbind, bind
DELETE	팀 작업장/디렉토리	unbind
LOCK	파일	write-content
	디렉토리	bind
MKCOL	팀 작업장/디렉토리	bind
UNLOCK		unlock
CHECKIN		write-properties
CHECKOUT		write-properties
REPORT		read
VERSION-CONTROL		write-properties

그룹간의 공유 작업공간을 원함으로써 여러 작업그룹의 구성원이 이러한 환경에서 효과적으로 서로의 정보를 교환하고 공유할 수 있도록 원해 주는 웹 기반 협업원 시스템이다. iPlace는 개인의 자료 공유를 위한 개인 작업장, 자신이 속한 팀의 자료 관리를 위한 팀 작업장 등을 원한다. 특히 팀작업에 대해서 사용자들이 웹이라는 가상공간에서 역적인 제약 없이 정보의 공유를 통해 편리하게 공동작업을 할 수 있다는 장점이 있다. 그러나 이런 작업들은 iPlace 사용자들 간에 로그인(lock-in)을 통해서 사용할 수 있다는 제약이 있다. 이를 보완하기 위하여 iPlace 사용자들은 다수의 익명사용자들을 위하여 공개된 개념의 공동 작업공간인 공개 작업장을 추가로 원한다[5].

3. WebDAV 기반의 협업시스템 접근 제어 설계

본 논문에서는 기본적으로 시스템 관리자, 팀 생성자, 팀 관리자, 사용자, 시스템에 소속된 많은 사용자와 같이 5개의 역할을 기준으로 팀 작업장과 공개 작업장 단 위에서 자원을 추가, 수정 등의 관리를 할 수 있도록 설계하였다. 협업시스템에서 사용자는 누구나 공동과제를 수행하기 위하여 팀 작업장을 필요에 따라 동적으로 생성할 수 있다. 팀 작업장을 생성한 사용자는 작업그룹의 생성자가 되며, 다른 사용자를 작업그룹의 구성원으로 초청하는 과정을 통하여 동적으로 작업그룹의 구성원을 조직할 수 있다. 또한 그룹의 관리 권한을 위임받아 팀 관리자가 될 수도 있다.

3.1 팀 작업장에 대한 접근 제어 설계

팀 작업장은 사용자들이 공동작업을 목적으로 자원(폴더, 파일, URL, 메모 등)을 공유하거나 교환하기 위한 공간이다. 팀 작업장에 참여하고 있는 구성원은 공동으로 관리되는 자원을 작업장내에서 직접 생성, 삭제, 변경 등을 할 수 있다. 그림 1)은 팀 작업공간의 명령어들을 보여주고 있으며, 공개 작업장에서도 또한 이들 대부분의 명령어가 적용된다.

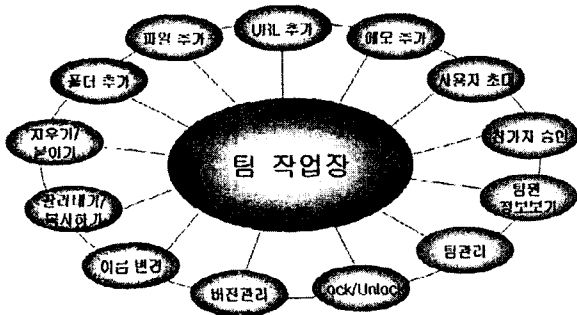


그림 1) 팀 작업장에서 사용 가능한 명령어

팀 작업장에서는 여러 작업을 수행하기 위한 접근 제어 방법을 WebDAV 메서드와 팀 관리자, 사용자의 역할을 기준으로 기본 권한이 설계되었다. 시스템 관리자, 팀 생성자, 팀 관리자는 팀 작업장 내에서 팀 관리자와 동일한 기능을 갖는다. 그리고 시스템에 속하 않은 사용자는 팀 작업장 내에서 작업이 불가능하다. 팀 관리자는 WebDAV 메서드를 모두 사용할 수 있 만, 사용자는 경우에 따라 ACL을 사용하는 권한 설정을 제외한 다른 메서드들만 사용이 가능하다.

사용자는 기본적으로 파일의 이름을 변경할 수 있다 (PROPPATCH). 이때 write-properties 권한이 설정이 되어 있어야 한다(메서드관련 권한은 [표 2] 참조). 또한 사용자는 파일추가(PUT) 및 내용수정을 위해 파일을 내려 받을 수 있고(GET), 파일과 디렉토리를 복사(COPY), 이동(MOVE), 삭제(DELETE) 그리고 잠금(LOCK) 및 잠금해 (UNLOCK)가 가능하다. 사용자는 한 파일에 대한 공동 작업을 가능하게 하기위하여 버전 컨트롤 관련 기능들(CHECKIN, CHECKOUT, VERSION-CONTROL, REPORT)을 원한다. 하 만 권한 설정의 변경(ACL)은 불가능하다.

3.2 공개 작업장에 대한 접근 제어 설계

공개 작업장은 시스템에 소속된 많은 사용자들이 협업작업을 수행할 수 있는 공간으로 이용된다. 공개 작업장에서 사용자 및 시스템에 소속된 많은 사용자는 동일한 접근 제어 권한가 며, 시스템 관리자, 팀 생성자 그리고 팀 관리자는 동일한 권한을 가진다. 사용자에게는 파일에 대한 읽기와 쓰기 기능만이 제공되며 수정은 허용되지 않는다.

공개 작업장은 그 성격에 따라서 올리기 기능(upload

Only), 내려받기 기능(download Only), 올리기/내려받기 기능(upload/download)의 3가 기능설정이 가능하다. 이와 같은 작업장을 기준으로 사용자와 팀 관리자의 접근 제어 기법을 설계하였다. [표 3]에서는 공개 작업장에 대한 접근 제어 방법을 보여준다.

[표 3] 공개 작업장에서 접근 제어를 위한 역할 설계

METHOD		Role	
		팀 관리자	사용자
Upload만	GET	O	X
	PUT	O	O
Download만	GET	O	O
	PUT	O	X
Up/Download	GET	O	O
	PUT	O	O

※ O : 사용 가능, X : 사용 불가능

4. 결론 및 향후 연구과제

본 논문에서는 협업시스템의 중심 기능인 팀 작업장 및 공개 작업장의 자원에 접근할 때, 사용자의 권한과 작업장의 특성 그리고 자원의 특징에 따라 접근 제어 관리를 할 수 있도록 접근 제어 기법을 설계하였다. 특히 공개 작업장은 작업장별 기능(올리기만 가능한 작업장, 내려받기만 가능한 작업장, 올리기/내려받기가 가능한 작업장)이 다르다. 이를 원하기 위하여 사용자와 시스템에 속하 않은 사용자의 작업장내 파일에 대한 접근 권한을 구체적으로 설계함으로써 협업시스템을 체계적이고 안정적으로 원할 수 있다.

향후 연구과제로 본 논문에서 설계한 작업장별 접근 제어 기법을 적용하여 사용자 및 시스템 관리 도구를 개발할 계획이다.

5. 참고 문헌

- [1] Y. Goland, E. Whitehead, A. Faizi, S. Carter, D. Jensen, "HTTP Extensions for Distributed Authoring - WEBDAV," RFC 2518, Standards Track, February, 1999
- [2] 황의운, 안건태, 정혜영, 김진홍, 이명준, "리눅스 기반의 WebDAV 클라이언트의 설계", 한국정보과학회 봄 학술발표논문집, Vol.31, No 1, pp. 814-816, 2004
- [3] G. Clemm, J.F. Reschke, E. Sedlar, J Whitehead, "Web Distributed Authoring and Versioning (WebDAV) Access Control Protocol," RFC 3744, Standards Track, May, 2004
- [4] 안건태, 정명희, 이근용, 문남두, 이명준, "iPlace: EJB 기술을 이용한 웹 기반 협업시스템", 한국정보처리학회 논문 D, 제8-D권, pp. 735-746, 2001년 12월
- [5] 박희중, 김진홍, 신원준, 박양수, 이명준, "iPlace 시스템에서의 공개 작업공간 원", 한국정보과학회 봄 학술 발표논문집, Vol.31, No 1, pp. 478-480, 2004