그리드 환경에서의 사이트 자율성 보장을 위한 접근 제어 시스템 개발

김법균°, 황호전, 두길수*, 곽의종, 안동언, 정성종, 장행진**
전북대학교, *서남대학교, **한국과학기술정보연구원
{kyun°, mainclass, hjhwang, dgs}@duan.chonbuk.ac.kr.kr
{kej, duan, sjchung}@moak.chonbuk.ac.kr, hjjang@hpcnet.ne.kr**

Implementation of Access Control System for Site Autonomy in Grid Environment

Beobkyun Kim, Kyoungik Jang, Hojeon Hwang, Gilsu Doo*, Eujong Kwak, Dongun Ahn,
Seungjong Chung, Haengjin Jang**
Dept. of Computer Engineering, Chonbuk National University
Dept. of Electric & Electronic Engineering, Seonam University*
Korea Institute of Science and Technology Information**

요 약

지리적으로 분산된 이 기종의 유휴 자원들을 서로 연결하여 가상의 고성능 컴퓨팅 자원으로 사용하는 그리드에서 자원에 대한 접근 제어 시스템의 구축은 필수적이다. 본 논문에서는 자원에 대한 접근 제어 시스템을 설계 및 구현한다. 특히, 그리드 환경 구축 시 가장 많이 사용되는 Globus Toolkit을 기반으로 하고 각 자원을 제공하는 사이트의 자율성을 보장하는 자원 접근 제어 시스템을 설계 및 구현하였다.

1. 서 론

인터넷이 보편화되고 컴퓨터 및 네트워크 성능이 향상됨에 따라 분산 자원 기반의 고성능 어플리케이션들은 더 큰 컴퓨팅 파워를 요구하고 있다. 그리드는 지리적으로 분산된 고성능, 대용량의 자원들과 첨단 장비들을 원격에서 동시적으로 사용하여 단일 시스템처럼 사용하는 환경이다. 이런 그리드 환경에서 어플리케이션을 수행하기 위해서는 각 자원에 대한 접근 권한을 가지거나 비슷한 수준의 제어권을 가지고 있어야 한다. 따라서, 그리드 환경의 적용과 보급을 위해서는 자원 접근 제어 시스템이 반드시 구현되어야만 한다.

그리고 그리드 환경에 대한 자원의 제공을 위해 자원의 고유한 운영 정책을 수정해서는 안된다. 즉, 각 사이트의 자율성을 보장해 주어야 한다. 각 자원 소유자의 그리드 환경에 대한 자원 제공 의욕 고취를 위해서도 각 자원 소유자의 고유한 운영 정책을 그리드 환경에서도 그대로 적용할 수 있어야 한다.

본 논문에서는 그리드 환경에서의 자원 접근 제어 시스템을 설계 및 구현한다. 특히, 그리드 환경 구축시 가장 많이 사용되는 Globus Toolkit을 기반으로 하며, 각 자원의 소유자의 자율성을 최대한 보장할 수 있는 구조로 설계 및 구현하였다.

2. 접근 제어 시스템 설계 및 구현

2.1 Globus Toolkit에서의 접근 제어

Globus Toolkit은 현재 진행되고 있는 그리드 환경 구축 프로젝트에서 가장 많이 사용되는 미들웨어이다. Globus Toolkit에서는 사용자의 해당 자원에 대한 접근 권한을 " grid-mapfile" 에 사용자의 DN과 로컬 자원의 계정을 함께 기입함으로써 부여한다. 기본적으로 다수의 DN과 하나의 로컬 계정이 결합 가능하며 각 DN은 신뢰가능한 CA (Certificate Authority)에서 부여받은 인증서로 확인된다.

```
"/O=Grid/OU=hi.ac.kr/CN=hdg" gw1
"/O=Grid/OU=hi.ac.kr/CN=how" gw2
"/O=Grid/OU=bye.com/CN=say" gw3
```

그림 1. grid-mapfile

이러한 방식은 다수의 DN과 하나의 로컬 계정이 결합됨으로써 로컬 시스템 내에서 발생하는 기록이 어느 외부 그리드 사용자가 발생시킨 것인지 추적하기 힘들다. 이를

추적하기 위해서는 작업을 제출할 때부터 사용자의 행위를 추적하는 별도의 모니터링 모듈이 필요하며 로컬 시스템에 상당한 부하를 줄 수도 있다.

또한, 자원에 대한 접근 권한 요청이 수시로 일어나므로 관리자가 일일이 대응한다는 것은 상상할 수 없으므로 별도의 어느 정도 자동화된 시스템이 필요하다.

그리고 외부 사용자와 로컬 계정은 일시적으로 1:1 결합되는 것이 보안 및 시스템 유지 관점에서 가장 적절한 형태라는 것이 일반적인 의견이므로 이러한 처리를 위한 모듈은 필수적이라 할 수 있다.

2.2 접근 제어 시스템의 설계

따라서, 본 논문에서는 이러한 문제점을 해결하고 그리드 환경에서의 부가 서비스를 위해 다음과 같은 접근 제어 시스템을 설계하였다.

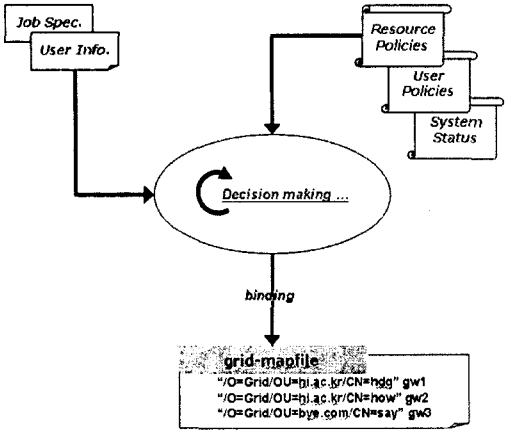

그림 2. 접근 제어 시스템

그리드 사용자는 각 로컬 자원을 사용하기 이전에 각 로컬 자원에 위치한 접근 제어 시스템에 로컬 자원 사용을 위한 바인딩 요청을 해야 한다. 이 때, 사용자는 자신의 신상 정보와 함께 자신이 원하는 자원의 명세를 보내야 한다.

접근 제어 시스템은 사이트 관리자가 수립한 그리드 사용자 관리정책, 그룹 관리 정책, 호스트 관리 정책 등을 참조하여 사용자가 제공한 신상 정보가 등록 가능한 사용자인지를 판별하며, 사이트 자원 관리 정책과 로컬 자원의 상태 등을 참조하여 제공 가능한 수준의 자원 요구인지를 판별하게 된다. 만약, 등록 가능한 사용자이고 제공 가능한 수준의 자원 요구라면, 사용자에게 발급할 로컬 계정을 선택하여 사용자에게 그 정보를 제공한다.

사용자는 이 정보를 바탕으로 스케줄링을 마치고 작업을 수행한다.

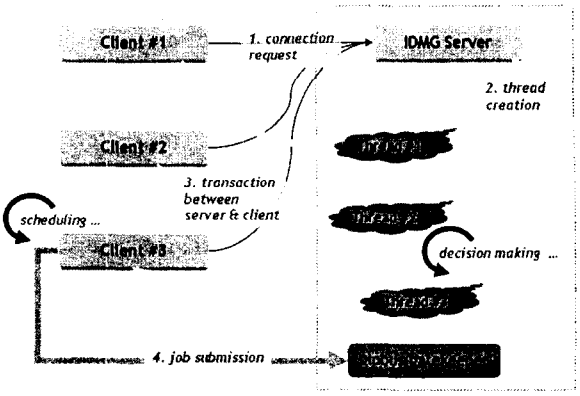

그림 3. 사용자의 접근 권한 요청 처리 과정

Globus Toolkit의 경우, 사용자가 접근 권한 획득 후 작업을 제출하면, gatekeeper가 이를 받아 처리하면서 globus-gatekeeper.log 라는 이름으로 기록을 남긴다. 대부분의 어카운팅 프로젝트의 경우 이 파일을 이용하여 로컬 자원내의 각 프로세스를 실행시킨 실제 외부 그리드 사용자를 구분하고 있으나, 이 파일 자체의 결함 때문에 실제 상황에 적용할 경우 심각한 장애가 발생할 수 있다. 그래서, 본 논문에서는 각 클라이언트와의 연결을 담당하는 별도의 쓰레드를 두고 기록을 남기며, 연결이 종료되면 기록을 전담하는 프로세스에게 전달하여 처리함으로써 기록의 무결성을 보장받을 수 있도록 하였다.

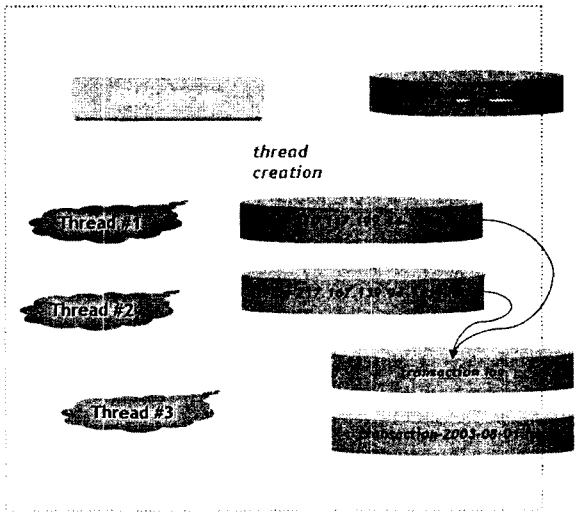

그림 4. 접근 제어 시스템의 로그 관리

또한, 본 과제에서 설계한 시스템은 각 자원의 고유한 운영정책을 그대로 반영시켜 사이트의 자율성을 보장한다.

예를 들면, limits.conf와 같이 기존의 시스템에서 활용하던 사용자 관련 설정 파일들을 이용하여 결합 여부를 결정하며 그 이외의 어카운팅 관련 정책 등도 새로운 설정 파일을 이용하여 사이트의 자율에 맡기도록 설계하였다.

```
acceptable-user-DN
{
        /what a wonderful grid..
}
# give priority to all user-DN which starts with ...
acceptable-user-VO
{
        /grid_team
}
acceptable-user-status
{
        worker,
        director
}
deniable-user-DN
{
        /sleeper
}
# deny all user-DN which starts with ...
deniable-user-VO
{
        /sleep
}
deniable-user-status
{
        student
}
```

그림 5. policy-user.conf

2.3 접근 제어 시스템의 구현

본 논문에서 구현한 시스템은 각 플랫폼에서 동일하게 동작하고 적용 가능하도록 파이썬을 사용하였다.

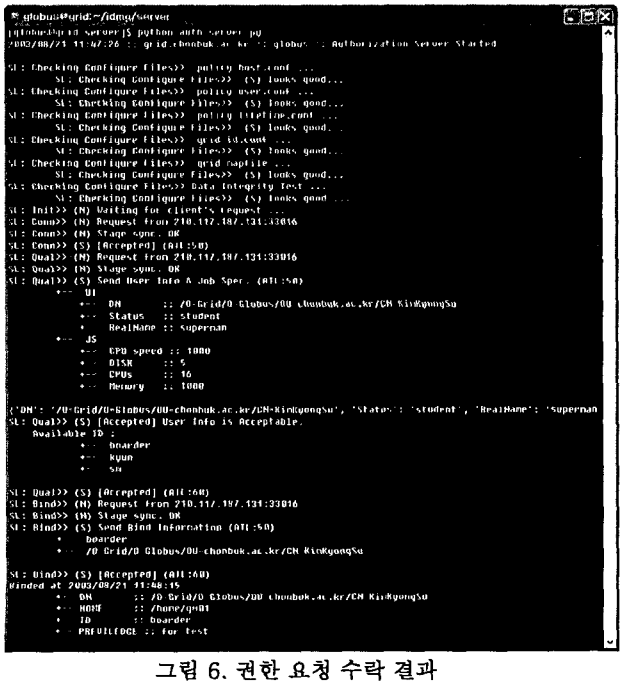

그림 6. 권한 요청 수락 결과

3. 결론 및 향후 연구 과제

본 논문에서는 그리드 환경의 구축에 있어서 필수적이라 할 수 있는 접근 제어 시스템을 Globus Toolkit을 기반으로 Globus Toolkit에서의 문제점을 해결하고 기존에 사용하던 각종 사용자 및 자원 관련 설정 파일들과 그리드 환경에 필요한 새로운 설정파일을 도입하여 자원 제공자의 관리 정책을 그대로 반영할 수 있도록 설계 구현하였다.
앞으로, 좀더 세밀한 제어를 위한 추가적인 연구와 함께 이를 이용한 어카운팅 및 과금 서비스와 같은 부가 서비스에 대한 연구가 필요하다.

참고문헌

[1] Foster, C. Kesselman(eds), "The Grid : Blueprint for a New Computing Infrastructure" Mogan Kaufmann Publishers, 1998.

[2] Foster, C. Kesselman(eds), S. Tuecke "The Anatomy of the Grid: Enabling Scable Virtual Organizations", Intl. J. Supercomputer Applications, 2001.

[3] S. Mullen et al, " Grid Authentication, Authorization and Accounting Requirements Research Document" , (draft), GGF8, 2003

[4] Sebastian Ho, " GridX System Design Documentation" , (draft), Bioinformatics Institute, 2002

[5] A. Beardsmore et al, " GSAX (Grid Service Accounting Extensions)" , (draft), GGF6, 2002

[6] R. Baker et al, " Conceptual Grid Authorization Framework and Classification" , (draft), GGF8, 2003

[7] K. Czajkowski, I. Foster, et al, "A Resource Managment Architecture for Metacomputing Systems", Proc. of the 4th Workchop on Job Scheduling Strategies for Parallel Processing, 1998

[8] Thomas J. Haker, Brian D. Athey, "Account Allocations on the Grid", Center for Parallel Computing University of Michigan. 2000.

[9] http://www.girdforum.org

[10] http://www.globus.org

[11] http://www.gridforumkorea.org